ИНСТИТУТ ИССЛЕДОВАНИЙ ИНТЕРНЕТА

АНАЛИЗ

возможных последствий и влияния Регламента General Data Protection Regulation (GDPR) Европейского Союза на бизнес российских операторов персональных данных (телекоммуникационные компании, интернет-компании) предоставляющих услуги через интернет для лиц в странах ЕС в контексте действующего и вступающего с силу регулирования в Российской Федерации

Москва, 2017

Содержание

Введение

В настоящее время на развитие отрасли связи, в том числе ниши интернет-провайдеров в Российской Федерации оказывает существенное влияние разработка и применение законодательства в области сбора и хранения данных пользователей услуг связи, прежде всего – телекоммуникационных услуг, в том числе передачи данных в сети Интернет.

Принятый 6 июля 2016 г. «Пакет Яровой» (ФЗ №374, ФЗ №375) обязывает операторов связи и организаторов распространения информации хранить не только метаданные, но и (до 6 месяцев) непосредственно данные, передаваемые пользователями в рамках телекоммуникационных услуг, - существенная часть таких данных является персональными данными.

В рамках выполненной Институтом исследований интернета НИР по теме «Зарубежный опыт нормативно-правового регулирования деятельности операторов связи в области сбора и хранения данных пользователей телекоммуникационных услуг (Telecommunications Data Retention Legislation) в контексте деятельности государственных правоохранительных органов» эксперты Института исследований интернета отметили, что принятый Регламент GDPR является одним из весомых оснований для отмены или корректировки странами Евросоюза нормативно-правового регулирования деятельности операторов связи и интернет-компаний в области сбора и хранения данных пользователей телекоммуникационных услуг (Telecommunications Data Retention Legislation).

При этом, в результате проведённого анализа было установлено, что регулирование деятельности операторов связи и интернет-компаний в области сбора и хранения данных пользователей телекоммуникационных услуг и интернет-сервисов в Российской Федерации является наиболее непроработанным и потенциально нарушает нормы международного права, в

частности принятый Регламент General Data Protection Regulation (GDPR) Европейского Союза.

Настоящая работа направлена на анализ и моделирование возможных последствий вступления в силу в мае 2018 года Регламента General Data Protection Regulation (GDPR) Европейского Союза для российских операторов персональных данных (телекоммуникационных компаний, интернет-компаний) предоставляющих услуги через интернет для лиц в странах ЕС, в контексте действующего и вступающего с силу регулирования в Российской Федерации.

1. Общие положения

Правовое регулирование защиты персональных данных в Европейском Союзе фактически насчитывает более 20 лет и правомерно связывается с соответствующей «европейской моделью», формирование и использование которой стало возможным в рамках европейского регионального интеграционного объединения, обладающего «наднациональными» характеристиками. Система «европейской модели» основана на нормативно-правовом и организационном (институциональном) механизмах порядка и процедур защиты персональных данных.

Нормативно-правовой механизм, с одной стороны, охватывает документы руководящих органов Европейского Союза (директивы, регламенты), набор базовых принципов основных прав субъектов данных и т.д., с другой стороны, имплементирована в национальное право стран-членов Европейского Союза. Основу нормативно-правового механизма порядка и процедур защиты персональных данных составляют документы, принимаемые Европейским Парламентом и Европейским Советом – директивы (*Directive*) и регламенты (*Regulation*). Правовая природа и формально-юридический порядок применения директив и регламентов Европейского Парламента и Совета, различны. Так, нормативные документы Европейского Союза, принятые в форме регламента, в отличие от директив, *непосредственно* применяются в государствах-членах Европейского Союза и не требуют имплементации в национальное право государств-членов.

Сказанное делает понятным, что правовое регулирование защиты персональных данных в Европейском Союзе, начиная с 2016 г. получило новый импульс развития. Это связано с принятием в апреле 2016 г. Регламента (ЕС) 2016/679 Европейского Парламента и Совета «О защите физических лиц в отношении обработки персональных данных и о

свободном перемещении таких данных и отмене Директивы 95/46/ ЕС (Общие положения о защите данных)»[1].

Регламент (ЕС) 2016/679 (далее – «Регламент GDPR»), *de facto* и *de facto jure* является документом прямого действия, что означает в практическом плане следующее.

Во-первых, Регламент GDPR выступает не только как регулирующий механизм для государств-членов Евросоюза, непосредственно влияющий и на уровень правотворчества и на уровень правоприменения. В связи с тем, что Регламент GDPR направлен на гармонизацию защиты основных прав и свобод физических лиц в отношении обработки данных и обеспечения свободного перемещения персональных данных между государствами-членами Евросоюза, Регламент GDPR обязывает государства-членов гармонизировать и уровень правотворчества, и уровень правоприменения.

На уровне правотворчества государства-члены Евросоюза обязаны гармонизировать с Регламентом GDPR свое национальное право посредством принятия, изменения, дополнения своего национального права.

На уровне правоприменения в рамках юрисдикции государств-членов Евросоюза Регламент GDPR непосредственно применяется национальными судами государств-членов. Более того, Регламент GDPR закрепляет номы о том, что государства-члены обязаны гармонизировать воздействие административных наказаний за нарушения Регламента GDPR.

Во-вторых, Регламент GDPR непосредственно применяется Судом справедливости Евросоюза (*European Court of Justic*), решения которого обладают прецедентным характером.

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

2. Территориальная применимость Регламента (General Data Protection Regulation, GDPR), начало действия Регламента GDPR, основные требования Регламента GDPR к защите персональных данных

В соответствии со Статьей 99 Регламента GDPR, он вступил в силу в мае 2016 г., а его применение начнется с 25 мая 2018 г., как обязательный нормативно-правовой документ, подлежащий прямому применению в государствах-членах Евросоюза. Основные положения и требования Регламента GDPR закреплены в преамбуле, содержащей 173 пункта, и в 99 статьях.

Регламент GDPR устанавливает цели, принципы, общие правила защиты физических лиц в отношении обработки персональных данных, их свободного перемещения в рамках Евросоюза, включая трансграничную передачу данных. Регламент GDPR закрепляет в том числе следующие принципы обработки персональных данных. Персональные данные должны:

– быть обработаны правомерно, справедливо и прозрачно в отношении субъекта данных («принцип законности, справедливости и прозрачности»);

– быть собраны для определенных, четких и законных целей и в дальнейшем не обрабатываться способом, несовместимым с этими целями; дальнейшая обработка данных для архивных целей, в интересах общества, научных и исторических исследований или статистических целей, не рассматривается как несовместимая с первоначальным целям («принцип целевого сбора данных»);

– быть обработаны адекватно и ограничиваться целями, для которых они обрабатываются (принцип «минимизации данных»);

– быть обработаны точно и там, где это необходимо, а также должны обновляться; должны приниматься все разумные меры для гарантии того, что персональные данные, которые являются неточными, с учетом целей, для которых они обрабатываются, будут удалены или исправлены без задержки (принцип «точности»);

– храниться в форме, позволяющей идентифицировать субъекта данных, не дольше, чем это необходимо для целей, для которых персональные данные обрабатываются; персональные данные могут храниться в течение более длительных периодов, т.к. персональные данные могут обрабатываться только для архивных целей в интересах общества, научных или исторических исследовательских целей или для целей статистики, с учетом осуществления соответствующих технических и организационных мер («принцип ограничения хранения данных»);

– быть обработаны таким образом, чтобы обеспечить надлежащую сохранность персональных данных, включая защиту от несанкционированной или незаконной обработки и случайной потери, уничтожения или повреждения, с использованием соответствующих технических или организационных мер («принцип целостности и конфиденциальности»).

Правомерность обработки данных оценивается исходя из следующих требований и условий:

– субъект данных дал согласие на обработку его персональных данных для одного или более конкретных целей;

– обработка необходима для исполнения договора, стороной которого субъект данных является стороной или для принятия мер по просьбе субъекта данных до заключения контракта;

– обработка необходима для соблюдения соответствующих обязательств контроллера;

– обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица;

– обработка необходима для выполнения определенных задач и осуществляется в общественных интересах или для исполнении функций контроллера;

– обработка необходима для законных целей и интересов регулятора третьих лиц.

Регламент GDPR отменяет действующую в настоящее время Директиву 95/46/ЕС Европейского Парламента и Совета от 24 октября 1995 об обеспечении отдельных лиц в отношении обработки их персональных данных и свободном перемещении таких данных[2] и заменяет ее.

Согласно Статье 29 названной Директивы 95/46/ ЕС была учреждена Рабочая группа по защите физических лиц при обработке персональных данных (*Data Protection Working Party, WP29*)[3]. Рабочая группа по защите физических лиц при обработке персональных данных (далее – «Рабочая группа *WP29*») действует в настоящее время, разрабатывая разъяснения и рекомендации по различным аспектам будущего применения Регламента GDPR[4].

Деятельность Рабочей группы *WP29* прекратится 25 мая 2018 г., в связи с отменой Директивы 95/46/ ЕС. При этом с этой даты, т.е. с 25 мая 2018 г., начинает функционировать вновь созданный орган Евросоюза – Европейский совет по защите данных (*European Data Protection Board, EDPB*), который учрежден в соответствии с Регламентом GDPR. В организационном плане этот орган будет включать руководителя Европейской службы по защите данных и старших представителей Национальных органов по защите данных (*Data Protection Authorities*) стран-участниц Евросоюза (Статья 94 Регламента GDPR).

Компетенция Европейского совета по защите данных будут связаны с:

– подготовкой заключений и руководящих положений относительно единообразного применения Регламента GDPR;

– подготовкой заключений и отчетов в сфере защиты данных для Европейской Комиссии;

---

[2] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[3] См. например, URL:https://www.iabeurope.eu/policy/data-protection/the-wp29-will-become-the-edpb-but-what-does-that-mean/

[4] В числе первых подобных разъяснений можно назвать документы, принятые в апреле 2017 г., который касались, в частности, Европейского инспектора по защите данных (*European Data Protection Supervisor*), механизма «единого окна» (*one-stop-shop mechanism*). О последующих документах см., например, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

– осуществлением ключевой роли в реализации «механизма единого окна» (*находится в стадии уточнения регулирования*).

В контексте содержания Регламента GDPR к субъектам, осуществляющим «обработку» «персональных данных», относятся «контролер» и «обработчик».

«Персональные данные» (*personal data*) – означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо является лицом, которое может быть идентифицировано прямо или косвенно, в частности, на основе идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификатор в интернете (онлайн-идентификатор) или посредством одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица;

«Обработка» (*processing*) означает любую операцию или набор операций, которые совершаются с персональными данными или набором персональных данных, с использованием автоматизированных средств и без таковых, в числе которых сбор, запись, организация, структурирование, хранение, переработка или изменение, поиск и выборка, экспертиза, использование, раскрытие посредством передачи, рассылка или иной способ предоставления для доступа, группировка или комбинирование, отбор, стирание или уничтожение (Статья 4 Регламента GDPR).

«Контролер» (*controller*) – это физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими, определяет цели и средства обработки персональных данных (Статья 4 Регламента GDPR).

Регламент GDPR закрепляет, что контролёр обязан: в определенных случаях сотрудничать с обработчиками данных; вести учетную

документацию; осуществлять оценку воздействия обработки персональных данных на права субъектов данных для некоторых видов обработки данных; внедрять механизмы защиты данных; в момент сбора персональных данных предоставлять субъектам данных полную информацию о целях сбора персональных данных, о правах субъектов данных и т.д.; обязаны, по возможности, в течение 72 часов уведомлять национальные органы по защите данных (*Data Protection Authorities*) об обнаружении утечек персональных данных, и соответствующих субъектов персональных данных[5].

«Обработчик» (*processor*) – это физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени и по поручению контролёра. Обработчик обязан: вести письменный реестр операций по обработке персональных данных, выполненных от имени и по поручению каждого контролёра; если у обработчика нет представителя в Евросоюзе, он обязан назначить такое лицо в определенных случаях; без задержек уведомлять контролёра об утечках персональных данных; участвовать в деятельности по трансграничной передаче данных.

Кроме того, контролёры и обработчики, в рамках своих программ отчетности обязаны назначить инспектора по защите данных (*Data Protection Officer*). Согласно Регламенту GDPR, инспектор по защите данных в обязательном порядке назначается в следующих случаях:

– обработка данных осуществляется государственным органом;

– основная деятельность контролёра или обработчика связана с такой обработкой данных, которая по своему охвату, целям и сути, требует крупномасштабного, регулярного и систематического мониторинга субъектов данных; при обработке специальной категории данных.

Территориальная сфера применения непосредственно закреплена в Статье 3 Регламента GDPR. Территориальная сфера применения

[5] В настоящее время находится в стадии уточнения регулирования Рабочей группы WP29.

ограничивается переделами Европейского Союза, однако юрисдикционно действие Регламента GDPR распространяется на субъектов за пределами Европейского Союза.

В целях обеспечения того, чтобы физические лица не были лишены защиты, на которую они имеют право в соответствии с Регламентом GDPR, обработка персональных данных субъектов данных в Евросоюзе контролёром или обработчиком, которые не учреждены в Евросоюзе, подпадает под действие Регламента GDPR в случаях, когда:

а) обработка персональных данных субъектов данных в Евросоюзе связана с предложением товаров или услуг субъектам данных в Евросоюзе, независимо от того, связано это с их с оплатой или нет. При этом Регламент GDPR устанавливает, что признаками, которые с очевидностью свидетельствуют о намерении предлагать товары или услуги субъектам данных в Евросоюзе, являются:

– использование языка или валюты, обычно используемой в одном или нескольких государствах-членах, с возможностью заказывать товары и услуги на этом языке;

– упоминание потребителей или пользователей, которые находятся в Евросоюзе (пункт (23) Преамбулы Регламента GDPR);

б) обработка персональных данных субъектов данных, находящихся в Евросоюзе также является предметом регулирования Регламента GDPR, когда это связано с мониторингом действий/поведения субъектов данных в Евросоюзе, постольку, поскольку их действия совершаются на территории Евросоюза. Для того, чтобы определить, подпадает ли деятельность по обработке данных для целей мониторинга действий субъекта данных, устанавливается факт того, осуществляют ли физические лица деятельность в интернете, в том числе потенциальную возможность последовательного использования технологии обработки персональных данных и т.д. (пункт (24) Преамбулы Регламента GDPR).

3. Соотношение норм Регламента GDPR и Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (ETS-108), иных международных соглашений в области защиты ПД

Соотношение норм Регламента GDPR, Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (ETS-108) и иных международных соглашений в области защиты персональных данных.

Регламент GDPR согласован с положениями целого ряда международно-правовых актов и документов как универсального, так и регионального и билатерального характера, речь в том числе идет о:

– Хартии Европейского Евросоюза об основных правах;

– Конвенции Совета Европы от 28 января 1981 г. о защите физических лиц при автоматизированной обработке персональных данных и Дополнительного протокола к Конвенции;

– Европейской Конвенции о защите прав человека и основных свобод;

– Женевских Конвенциях, связанные с соблюдением международного гуманитарного права, применяемого в период вооружённых конфликтов

– действующих договорах государств-членов Европейского Союза о взаимной правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам.

Регламент GDPR исходит из того, что в отношении защиты персональных данных, трансграничной передачи данных в третью страну, международную организацию, Европейская Комиссия должна принимать во внимание, не только, к примеру, участие, присоединение третьей страны к Конвенции Совета Европы от 28 января 1981 г. о защите физических лиц при автоматизированной обработке персональных данных и к Дополнительному протокол, а также участие третьей страны или международной организации в многосторонних или региональных системах в отношении защиты

персональных данных, а также исполнение таких международных обязательств. Международные обязательства третьих стран или международных организаций принимаются во внимание Европейской Комиссией, в том числе для приятия решения о трансграничной передаче персональных данных в третью страну (пункт (105) Преамбулы Регламента GDPR).

4. Нормы Регламента GDPR, распространяющиеся на российских операторов персональных данных (телекоммуникационные компании, интернет-компании) предоставляющих услуги через интернет для лиц в странах ЕС

Регламент GDPR распространяется на российских операторов персональных данных (телекоммуникационные компании, интернет-компании) как на компании, не учреждённые в Евросоюзе, но обрабатывающие персональные данные находящихся в Евросоюзе субъектов данных, если их деятельность по обработке данных связана с предложением товаров и услуг таким субъектам данных в Евросоюзе, вне зависимости от того, требуется ли оплата от субъекта данных, либо связана с мониторингом деятельности субъектов данных постольку, поскольку она осуществляется в Евросоюзе.

В практическом плане сказанное означает, во-первых, что на российские компании, «ориентированные» на субъектов в Евросоюзе (потребители Евросоюза), после 26 мая 2018 г. окажутся в сфере действия Регламента GDPR. В этой связи, согласно требованиям Регламента GDPR, во-вторых, такие компании должны назначить своего представителя в Евросоюзе (пункт (80) Преамбулы Регламента GDPR).

Представитель (*representative*) – это физическое или юридическое лицо, созданное в Евросоюзе, которое специально уполномочено в письменной форме контролёром или обработчиком и представляет контролёра или обработчика, в отношении их соответствующих обязательств, предусмотренных Регламентом (Статья 4 Регламента GDPR). Порядок и основные функции представителя регулируются Статьей 27 Регламента GDPR.

Представитель может не назначаться, в частности, когда обработка носит случайный характер, не включает в себя масштабную обработку конкретных категорий персональных данных, либо обработка персональных

данных, связана с уголовными приговорами и правонарушениями, или если контролёр является органом или учреждением государственной власти.

Представитель должен действовать от имени контролёра или обработчика, может взаимодействовать с любыми компетентными органами Евросоюза, государства-члена, включая надзорные органы. Представитель должен быть специально уполномочен, посредством письменного предписания контролёра или обработчика, действовать от их имени в отношении их обязательств, вытекающих из Регламента GDPR. Назначение такого представителя не влияет на ответственность или обязанности контролёра или обработчика вытекающие из Регламента GDPR.

Представитель должен выполнять свои задачи согласно предписанию, полученному от контролёра или обработчика, и осуществлять любые действия в целях обеспечения соблюдения Регламента GDPR. Представитель подпадает под действие исполнительного производства в случае несоблюдения требований Регламента GDPR контролёром или обработчиком.

Если у российских операторов персональных данных (телекоммуникационных компаний, интернет-компаний), к примеру, предоставляющие услуги через интернет для лиц в странах Евросоюза, есть представительства и филиалы в странах Евросоюза, то функции представителя могут быть возложены на них.

Регламент GDPR при регулировании отношений, связанных со сбором и хранением персональных данных субъектов данных исходит из обязательного требования получения «согласия» (*consent*) субъекта на обработку персональных данных. Согласие должно быть настолько же легко отозвать, как и предоставить, а для специальных категорий данных согласие должно быть явно выраженным. В Преамбуле Регламента GDPR разъясняется, что согласие не считается добровольным, если субъект данных не имеет подлинного и свободного выбора либо возможности отказать в предоставлении согласия или отозвать согласие без ущерба для себя.

Контролёр данных обязан быть в состоянии предоставить доказательства получения согласия.

5. Нормативные требования действующего российского законодательства, в контексте возможных коллизий с нормами Регламента GDPR

Представляется, что настоящее время преждевременно анализировать возможные коллизии между нормативными требованиями действующего российского законодательства, и нормами Регламента GDPR. Это связано, прежде всего, с отмеченными ранее факторами.

Во-первых, предполагается принятие целого ряда разъяснительных и директивных документов применения Регламента GDPR Рабочей группой *WP29*. Во-вторых, несмотря на непосредственное действие Регламента GDPR в государствах-членах Евросоюза, на государства-члены возложена обязанность «трансформировать» национальное право к требованиям Регламента GDPR, включая «переходные положения»[6].

Во-вторых, после мая 2018 г. начнет формироваться национальная правоприменительная (судебная, административная) практика. Кроме того, т.к. Регламент GDPR непосредственно будет применяться Судом справедливости Евросоюза (*European Court of Justic*), после мая 2018 г. также начнет формироваться практика Суда справедливости.

В действующем российском законодательстве в регулировании отношений в сфере персональных данных системообразующим актом является Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, с поправками Федерального закон № 242-ФЗ 2015 г. (далее – «ФЗ РФ о персональных данных»). В этой связи целесообразно обратить внимание на то, что Регламент GDPR и ФЗ РФ о персональных данных имеют различное действие в пространстве, по кругу лиц, и во времени.

[6] Первые законодательные акты приняты в таких странах-членах Евросоюза как Германия, Польша, Нидерланды. См., например, URL: https://www.datastax.com/resources/whitepapers/eu-gdpr-a-pocket-guide-a-clear-concise-primer-on-the-eu-gdpr-German?utm_campaign=GDPR_DACH_connectcom&utm_medium=cpc&utm_source=Google&utm_content=gdpr&gclid=CjwKEAjwruPNBRCKkbL9zqKcrHwSJABGDVyI_LtgAW9GE6IC4rXYELZE_fUqetX-fSp_0ijMK1Z9vBoCWUbw_wcB; URL: http://www.eversheds-sutherland.com/global/en/where/europe/ireland/services/data_protection/gdpr.page

ФЗ РФ о персональных данных не обладает экстерриториальным действием, не распространяется на нерезидентов, собирающих персональные данные российских граждан за границей, в случае, если они не осуществляют деятельность в интернете, направленную на Российскую Федерацию.

В контексте содержания Регламента GDPR субъектами, осуществляющим обработку персональных данных являются «контролер» и «обработчик», а в терминологии ФЗ РФ о персональных данных – «оператор». «Оператор» – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (пункт 2 Статьи 3 ФЗ № 152-ФЗ «О персональных данных»).

«Европейская модель» защищает персональные данные как основное право человека, является нейтральной к «национальному признаку». Право на защиту персональных данных, согласно Регламенту GDPR, осуществляется на территории Евросоюза и в государствах-членах независимо от гражданства или проживания, тем самым не ограничивается сфера действия права о персональных данных по «национальному принципу»[7].

ФЗ РФ о персональных данных распространяется на граждан Российской Федерации, что в том числе следует из нормативных положений Федерального закона от 21.07.2014 № 242-ФЗ (в редакции от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

[7] См., к примеру, см. материалы Рабочей группы *WP29* о приемлемости защиты лиц, проживающих в ЕС. https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiQoarl_qjWAhUsCZoKHRiDCIUQFggxMAE&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D43823&usg=AFQjCNEmByOWl_41poQ-zIX4TWGpzxqhMA

1) ФЗ №149-ФЗ (в редакции от 31.12.2014) «Об информации, информационных технологиях и о защите информации» дополнено нормой части 4 Статьи 16: «нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение *персональных данных граждан Российской Федерации*».

2) ФЗ № 152-ФЗ «О персональных данных» дополнено, в частности:

– частью 5 Статьи 18: «При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных *данных граждан Российской Федерации* с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона»;

– частью 3 Статьи 22: «сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации» (пункт 10.1).

Таким образом, сбор персональных данных и их защита связана с гражданами России, т.е. сфера применения законов о персональных данных в российском праве ограничена «по национальному принципу». При этом на практике сложно, а порой невозможно, российскому оператору данных, в частности при обработке персональных, полученных через интернет, определить гражданство субъекта данных. Как правило, интернет-услуги не предоставляются «по национальному признаку», даже если регистрационные формы могут содержать графу о гражданстве пользователя, проверить достоверность предоставленной информации по общему правилу не представляется возможным.

Роскомнадзор *de facto* «переложил» бремя идентификации гражданства субъекта данных на обработчиков данных. Поскольку

определение способов идентификации гражданства субъекта данных может быть различным, скорее всего российские операторы данных будут собирать все персональные данные субъектов данных на территории России с тем, чтобы выполнить требования российского права.

ФЗ № 242-ФЗ 2015 г. (в редакции от 29.07.2017 г.) предусматривает новые требования защиты персональных данных, связанные с локализацией данных[8]. Требования к регулированию сферы защиты персональных данных, связанные с локализацией данных относятся к следующему кругу лиц:

– российские юридические лица;

– иностранные компании, у которых есть филиалы/представительства в Российской Федерации;

– иностранные компании, осуществляющие деятельность в интернете, направленную на Российскую Федерацию, если они, к примеру, используют доменные имена в зоне .ru, .рф; имеют русскоязычный сайт; используют рекламу на русском языке и т.д.).

Временн***о***е требование ФЗ о персональных данных о локализации персональных данных распространяется на персональные данные, собранные или обрабатываемые после 1 сентября 2015 г. При этом, исходя из нормативных требований российского законодательства о персональных данных, связывающие защиту с принципом гражданства, достаточно сложно однозначно ответить на вопрос: распространяются ли требования к локализации данных к персональным данным российских граждан, собранных за пределами Российской Федерации. Представляется, что ответ на этот вопрос будет зависеть от вида обработки персональных данных.

По смыслу нормативных положений части 5 Статьи 18, объем обязательств по локализации данных «ограничен» тем, что при сборе персональных данных, в том числе посредством информационно-

[8] В общем плане требования локализации персональных данных согласуются с нормативными положениями Конвенции Совета Европы (№108) о защите частных лиц в отношении автоматической обработки персональных данных 1981 г. участником которой является Российская Федерация. См. также информацию URL:http://www.minsvyaz.ru/ru/personaldata

телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации…». Соответственно, в объем обязательств по локализации данных не подпадают, к примеру, такие виды обработки, как удаление, использование, распространение, псевдонимизация. Таким образом, формально-юридически обозначенные операции обработки могут осуществляться и быть локализованы вне пределов Российской Федерации.

Кроме того, в интересах оператора по обработке персональных данных могут действовать на договорно-правовой основе обработчики, которые не являются российскими лицами. В этих случаях лишь российский оператор обязан соблюдать требования о локализации, и требования локализации не распространяются на обработчиков данных, именно оператор данных, вне зависимости от области его деятельности, несет ответственность за локализацию[9].

Требования локализации данных, закрепленные ФЗ РФ о персональных данных, непосредственно связываются с таким важным аспектом как трансграничная передача персональных данных российских граждан. В контексте сопоставления ФЗ РФ о персональных данных и Регламента GDPR следует отметить следующее.

Регламент GDPR закрепляет понятие трансграничная обработка» (*cross-border processing*), которое означает: а) обработку персональных данных, которая имеет место в контексте деятельности учреждений в более чем одном государстве-члене контролёра или обработчика в Евросоюзе, в случае, если этот контролёр или обработчик учреждены в более чем одном государстве-члене; или б) обработку персональных данных, которая имеет

[9] Министерство связи и массовых коммуникаций Российской Федерации разъясняет вопросы, связанные с регулированием персональных данных и их локализацией, подготовленные на основании информации, полученной от представителей бизнеса, научного сообщества и органов государственной власти РФ (Совет Федерации РФ, Минкомсвязи РФ, Роскомнадзор). URL: http://minsvyaz.ru/ru/personaldata/

место в контексте деятельности единственного учреждения контролёра или обработчика в Евросоюзе, но которая существенно влияет или может существенно повлиять на субъектов данных в более чем одном государстве-члене.

Регламент GDPR регулирует порядок трансграничного перемещения персональных данных за пределы Евросоюза в Главе V «Передача персональных данных третьим странам или международным организациям».

В связи с тем, что о, что это может передача персональных данных может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в том числе, защитить себя от неправомерного использования или разглашения информации, Регламент GDPR предусматривает, что в соответствии с ним, а также на основе взаимности применяются, в частности:

– механизм согласования;

– механизм сотрудничества между надзорными органами государств-членов и надзорными органами третьих государств;

– механизм взаимной помощи и совместные операции между соответствующими контролирующими органами на двусторонней или многосторонней основе.

С учетом того, что надзорные органы могут быть не в состоянии рассмотреть жалобу субъекта данных или провести расследование в отношении деятельности, осуществляемой за пределами границ своего государства-члена, их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или полномочиями, связанными с исправлением ситуации, противоречивым режимом правового регулирования, а также препятствиями практического характера, например, ограничением источников сведений.

Передача персональных данных третьей стране или международной организации может иметь место, когда Европейская Комиссия приняла решение, что третья страна, территория, или один или несколько особых

секторов третьей страны, либо соответствующая международная организация обеспечивают надлежащий уровень гарантий. При этом Регламент GDPR закрепляет критерии оценки надлежащего уровня защиты, из которых должна исходить Европейская Комиссия при принятии решения (Статья 45 Регламента GDPR).

Если Европейская Комиссия будет обладать соответствующей информацией, что третья страна (территория, или один или несколько особых секторов третьей страны) либо международная организация не обеспечивают надлежащий уровень защиты, она вправе отменить, изменить или приостановить решение о передаче данных. Европейская Комиссия должна опубликовать в Официальном Журнале Европейского Союза[10], а также на своем веб-сайте список третьих стран (территорий и особых секторов третьей страны), а также международных организаций, в отношении которых она приняла решение о том, что надлежащий уровень защиты существует, либо не обеспечивается (пункт 8 Статьи 45 Регламента GDPR).

Согласно ФЗ РФ о персональных данных, в частности Статьи 12 ФЗ № 152, трансграничная передача персональных данных осуществляется в иностранные государства, которые являются сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также в иные иностранные государства, обеспечивающие адекватную защиту прав субъектов персональных данных. При том трансграничная передача персональных данных в иностранные государства может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

[10] *Official Journal of the European Union*

Роскомнадзор (уполномоченный орган РФ по защите прав субъектов персональных данных) утверждает перечень[11] иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных[12].

Один из наиболее важных аспектов требований российского законодательства локализации данных, в контексте трансграничной передачи персональных данных в иностранные государства связано с тем, что хранение данных (граждан РФ) должно быть локализовано на территории РФ, а при трансграничной передаче данные так или иначе будут храниться на сервере, расположенном за границей. При трансграничной передаче персональных данных он «не могут не подвергаться обработке», однако, с позиции официальных российских регуляторов, российские нормы локализации данных предназначены для предотвращения злоупотребления

[11] Приказ Роскомнадзора от 15.03.2013 № 274 (в редакции от 15.06.2017) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

[12] В соответствии с Приказом Роскомнадзора № 274 от 15 марта 2013 года (в редакции 15.06.2017) среди таких стран: Австралия (Австралийский союз), Аргентинская Республика, Габонская Республика, Государство Израиль, Государство Катар, Канада, Королевство Марокко, Малайзия, Мексиканские Соединенные Штаты, Монголия, Новая Зеландия, Республика Ангола, Республика Бенин, Республика Кабо-Верде, Республика Казахстан, Республика Коста-Рика, Республика Корея, Республика Мали, Республика Перу, Республика Сингапур, Тунисская Республика, Республика Чили, Южно-Африканская Республика. Критерии, которые Роскомнадзор использует для оценки, формально-юридически не закреплены, к примеру, А. Савельев указывает на следующие: 1) наличие законодательства, основанного на тех же принципах, которые отражены в Конвенции СЕ № 108; 2) наличие специальной государственной администрации, ответственной за обеспечение безопасности, которая сотрудничает с Роскомнадзором, и 3) наличие ответственности за нарушение законодательства о персональных данных. См. Savelyev A. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf

персональными данными российских граждан иностранными операторами данных и защиты российских граждан от надзора в иностранных государствах»[13].

Как отмечали некоторые российские эксперты, Роскомнадзору удалось найти решение, позволяющее осуществлять локализацию данных и трансграничную передачу персональных данных. Суть решения состоит в том, чтобы разделить все базы данных, которые могут содержать персональные данные, на две группы: первичные базы данных и другие базы данных»[14]. Так, персональные данные должны быть первоначально записаны, а также сохранены и обновлены на более позднем этапе, должны быть расположены в России («первичная база данных»); после этого информация из таких «первичных баз данных» может быть перенесена в базы данных, расположенные за пределами России («вторичные базы данных»), при условии соблюдения российского законодательства о персональных данных, связанных с трансграничной передачей. «Другими словами, главная копия личных данных российских граждан, собранных в России, должна быть расположена в России, а также как последующие обновления и дополнения к этим личным данным. Технические решения, в которых первичная база данных находится за рубежом, и создается только русская копия («копия» или «зеркало») такой зарубежной базы данных, не соответствуют закону»[15].

За несоблюдение российского законодательства о персональных данных, включая требования о локализации данных, предусматривается административная ответственность, которая с 1 июля 2017 г. существенно

[13] См. например, URL:http://tass.ru/obschestvo/2223739

[14] См., например, Savelyev A. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf

[15] Savelyev A. Указ. Работа. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf

изменена[16]. Статья 13.11. «Нарушение законодательства Российской Федерации в области персональных данных» Кодекса об административных правонарушениях предусматривает следующее:

1. Обработка персональных данных в случаях, не предусмотренных законодательством РФ в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, влечет предупреждение или наложение административного штрафа на граждан в размере от 1 до 3 рублей; на должностных лиц – от 5 до 10 000 рублей; на юридических лиц – 30 000 до 50 000 рублей.

2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, влечет наложение административного штрафа на граждан в размере от 3000 до 5000 рублей; на должностных лиц – 10000 до 20 000 рублей; на юридических лиц – 15 000 до 75 000 рублей.

3. Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных, влечет предупреждение или наложение административного штрафа

[16] Федеральный закон от 07.02.2017 № 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

на граждан в размере от 700 до 1 000 пятисот рублей; на должностных лиц – от 3000 до 6 000 рублей; на индивидуальных предпринимателей – 5000 до 10 000 рублей; на юридических лиц – 15 000 до 30 000 рублей.

4. Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, влечет предупреждение или наложение административного штрафа на граждан в размере от 1 000 до 2 000 рублей; на должностных лиц – 4 000 до 6 000 рублей; на индивидуальных предпринимателей – 10 000 до 15 000 рублей; на юридических лиц – 20 000 до 40 000 рублей.

5. Невыполнение оператором в сроки, установленные законодательством РФ в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, влечет предупреждение или наложение административного штрафа на граждан в размере от 1000 до 2 000 рублей; на должностных лиц – от 4 000 до 10 000 рублей; на индивидуальных предпринимателей – 10 000 до 20 000 рублей; на юридических лиц – 25 000 до 45 000 рублей.

6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные

неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа на граждан в размере от 700 до 2 000 рублей; на должностных лиц – 4 000 до 10 000 рублей; на индивидуальных предпринимателей – 10 000 до 20 000 рублей; на юридических лиц – 25 000 до 50 000 рублей.

Таким образом, в российском законодательстве расширены и изменены виды правонарушений. Правонарушением является «незаконная обработка данных» (т.е. обработка не предусмотрена законом или не соответствующая целям сбора информации). В качестве подобного правонарушения может стать передача данных о сотрудниках третьим организациям в рекламных целях. Правонарушением считается «обработка данных без письменного согласия сотрудника». Самостоятельным видом правонарушения является «доступ к информации о политике компании в области обработки персональных данных». Правонарушением считается «сокрытие данных» (физическое лицо вправе запросить и получить информацию, связанную с обработкой его персональных данных, а если запрос лица не удовлетворен, это может квалифицироваться как правонарушение). Правонарушением является несоблюдение своевременной «корректировки данных», которая коррелирует нормативным положениям статьи 21 ФЗ о персональных данных. Обработчик данных обязан уточнять, уничтожать и т.д. данные о физических лицах. Неполная или устаревшей информация должна быть скорректирована в определенный срок. Обработчик данных обязан обеспечить «сохранность персональных данных», а в случае нарушения (получение несанкционированного доступа, уничтожение информации и т.д.) – это считается правонарушением

С 1 июля 2017 г. изменилась подведомственность дел при нарушении ФЗ о персональных данных: ранее дело, связанное с персональными данными, мог возбудить только прокурор, теперь дела об административных

правонарушениях могут быть инициированы в том числе должностными лицами Роскомнадзора.

Регламент GDPR закрепляет нормативные положения, предусматривающие принятие мер юридического характера компетентными надзорными органами Евросоюза и государств-членов, включая наложение административных штрафов. Административные штрафы и потенциальные санкции государств-членов (соответствующее законодательство в ряде государств ЕС формируется) за нарушение Регламента GDPR, выше, чем санкции за нарушения российского законодательства о персональных данных. Меры юридического характера принимаются компетентными надзорными органами Евросоюза и государств-членов в том числе на основании жалобы/заявления субъекта персональных данных (Преамбула (130) Регламент GDPR).

Для того, чтобы усилить обязательность соблюдения норм Регламент GDPR, санкции, в том числе административные штрафы, должны налагаться за любое его нарушение, в дополнение или вместо соответствующих мер, налагаемых надзорным органом государства-члена. В случае если нарушение незначительное или если вероятное наложение штраф может повлечь несоразмерную нагрузку для физического лица, вместо штрафа может быть объявлен выговор. При это принимается во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения нанесенного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролёра или обработчика, соблюдение кодексов поведения, а также любые иные отягчающие или смягчающие вину обстоятельства. Для назначения наказаний, в том числе для наложения административных штрафов, необходимо наличие соответствующих процессуальных гарантий в соответствии с общими принципами права Евросоюза и Хартии Европейского Евросоюза об основных правах, включая эффективную

судебную защиту и надлежащую правовую процедуру. Государства-члены Евросоюза могут предусматривать уголовную ответственность за нарушение настоящего Регламента GDPR, включая нарушения национальных норм, принятых согласно и в соответствии Регламентом GDPR Регламента. (Преамбула (148)-(151), Статьи 58, 70, 83 Регламента GDPR).

Изложенное выше обобщенно свидетельствует о том, что Регламент GDPR и российское законодательство, регулирующее сферу персональных данных, имеют самостоятельную территориальную и «юрисдикционную» сферу применения; при этом некоторая общность подходов регулирования не дает основания сделать вывод относительно их «гармонизации». В практическом плане для российских компаний, деятельность которых связана со сферой персональных данных, ориентированных на пользователей в Евросоюзе, имеющих договорно-правовые обязательства с контрагентами Евросоюза, – это означает «двойное обременение».

5.1. Возможные риски и последствия нарушения норм Регламента GDPR для российских операторов персональных данных (интернет-компании и телекоммуникационные компании), предоставляющих услуги через интернет для лиц в странах ЕС

Возможные риски и последствия нарушения норм Регламента GDPR для российских операторов персональных данных (интернет-компании и телекоммуникационные компании), предоставляющих услуги через интернет для лиц в странах Евросоюза непосредственно связаны с тем, что Регламент GDPR закрепляет обязанности обработчиков данных. К числу прямых обязанностей относятся, к примеру:

– ведение письменного реестра операций по обработке персональных данных, осуществляемых от имени и по поручению каждого контролера;

– назначение своего представителя в Европейском Союзе (о котором было сказано ранее);

– представление уведомления об утечках персональных данных, по возможности 72 часов после обнаружения утечки[17];

– соблюдение целого ряда закрепленных механизмов, включая механизм сертификации[18];

– предоставление субъектам данных в момент сбора персональных данных транспарентную (прозрачную) информацию об обработке и о целях такой обработки;

– соблюдение норм, предусмотренных Статьей 83, которые подпадают под административные штрафы; при этом при наложении штрафов в порядке Статьи 83, всегда берется та сумма, которая больше (из двух сумм);

[17] В последней декаде 2017 г. ожидается принятие Рабочей группой по защите физических лиц при обработке персональных данных (*Data Protection Working Party, WP29*) Руководящих положений *WP29* по уведомлению об утечках данных.

[18] См. например, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*
URL:https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf

– представление доказательств о правомерности деятельности, связанной по обработке (т.е. бремя доказывания возлагается, по смыслу Регламента GDPR, на лиц, обрабатывающих персональные данные субъектов данных).

Избежать возможных рисков и последствий нарушения норм Регламента GDPR компания может посредством своевременного принятия мер, которые способны продемонстрировать соблюдение требований Регламента GDPR.

В их числе могут быть следующие:

1. Необходимо проанализировать операции по обработке данных на предмет добросовестности их осуществления, а также пересмотреть существующие формы уведомления субъекта данных. Это связано с тем, что Регламент GDPR обязывает предоставлять субъекту данных детализированную информацию: об обработке данных в момент ее сбора; целях обработки; о правах субъекта данных (необходимо, к примеру, указать право на отзыв согласия на обработку); о сроке хранения данных и др.

2. Разработать внутренние регламенты, определяющие политику компании в сфере обработки персональных данных, включая назначение инспектора по защите данных.

3. Осуществить «аудит», в случае наличия, действующих договоров с компаниями из Европейского Союза, на предмет правовых оснований обработки, использования, хранения и т.д. персональных данных. Это связано с тем, что Регламент GDPR предусматривает, наряду с согласием субъекта персональных данных на обработку, и иные правовые основания обработки. Правомерность обработки, к примеру, может вытекать из контрактных обязательств. Контрагенты из Европейского Союза могут потребовать внести изменения в существующие договоры для соблюдения требований Регламента GDPR. В этой связи следует, в том числе, решить вопрос: когда и как изменить (дополнить, отменить) условия действующих

договоров, кто будет нести бремя расходов, связанных с такими изменениями и проч.

4. Регламент GDPR предусматривает и регулирует порядок осуществления трансграничной (международной) передачи данных, включая условия и порядок перемещения персональных данных в третьи государства, в международные организации, а также в рамках группы компаний, осуществляющих совместную экономическую деятельность. При этом такая трансграничная передача данных не исключает портативности данных, «права на забвение» и иных прав субъектов данных. Соответственно, целесообразно проанализировать правомерность хранения персональных данных для обоснования того, что интересы компании (обрабатывающих персональные данные) обладают правомерной преимущественной силой по сравнению с правами субъектов данных, поскольку нередко субъекты данных обладают «завышенным пониманием» своих прав.

5. Регламент GDPR признает обязательный характер (в правовом значении) корпоративных кодексов поведения (*Binding corporate rules*), как регулирующий нормативный механизм «законной/правомерной» трансграничной передачи данных в рамках группы компаний/предприятий, осуществляющих совместную экономическую деятельность. Целесообразно проанализировать существующие (и утвержденные в будущем корпоративные кодексы поведения). Нередко корпоративные кодексы поведения (*Binding corporate rules*) рассматривают как «золотой стандарт» регулирования передачи данных в рамках трансграничной передачи данных в рамках группы компаний/предприятий.

5.2 Возможные риски последствия реализации Пакета Яровой (№374-ФЗ) для российских операторов персональных данных

Российское законодательство о персональных данных, в том числе, Федеральный закон от 06.07.2016 № 374-ФЗ и Федеральный закона от 06.07.2016 № 375-ФЗ, – имеют разную предметную сферу регулирования, самостоятельное действие в пространстве, по кругу лиц и во времени. При этом Федеральный закон от 06.07.2016 № 374-ФЗ и Федеральный закона от 06.07.2016 № 375-ФЗ (далее – «Пакет Яровой») относится к публично-правовой сфере; Регламент GDPR, преимущественно – к частноправовой сфере.

Российские операторы связи и организаторы распространения информации оказываются в условиях «двойного обременения»: исполнение требований российского права, с одной стороны, и исполнение норм тех юрисдикций, в рамках которых, в том числе, осуществляется их коммерческая деятельность – с другой.

Российские операторы связи и организаторы распространения информации обязаны выполнять требования законодательства, вытекающие из Федерального закона от 06.07.2016 N 374-ФЗ "О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" (*Далее – «Пакет Яровой» (общеупотребимое*), которое вступит в силу с 1 июля 2018 г., постольку, поскольку его предметная сфера связана исключительно публично-правовой сферой, и касается реализации мер противодействия терроризму и обеспечения общественной безопасности в Российской Федерации. Нормы Пакета Яровой являются императивными, и их несоблюдение может повлечь применение соответствующих санкций.

Напомним, согласно Пакету Яровой, ФЗ «О связи» изменен и дополнен следующими нормами:

1) оператор связи обязан прекратить при поступлении соответствующего запроса

от органа, осуществляющего оперативно-розыскную деятельность, оказание услуг связи в случае неподтверждения в течение пятнадцати суток соответствия персональных данных фактических пользователей сведениям, заявленным в абонентских договорах. (Статья 46 пункт 1);

2) операторы связи обязаны хранить на территории Российской Федерации:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет с момента окончания осуществления таких действий;

– текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи - до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации (пункт 1 Статьи 64);

– операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами (пункт 1.1. Статьи 64).

Пакет Яровой внес изменения и дополнения в ФЗ №149-ФЗ «Об информации, информационных технологиях и о защите информации», а именно в Статью 10.1 следующего содержания:

1) организатор распространения информации в сети «Интернет» обязан хранить на территории Российской Федерации:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

– текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации (пункт 3);

2) организатор распространения информации в сети «Интернет» обязан предоставлять указанную в пункте 3 настоящей статьи информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами (пункт 3.1);

3) организатор распространения информации в сети «Интернет» обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети «Интернет» возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений (пункт 4.1).

В той редакции Пакета Яровой, в которой приняты изменения и дополнения, связанные с деятельностью операторов связи и организаторов распространения информации, не ограничивается круг лиц, на который распространяются обозначенные выше нормы. В практическом плане это означает, что Пакет Яровой «по умолчанию» распространяется и на иностранные физические лица (иностранные граждане; граждане, проживающие на территории иностранных государств, иные лица, проживающие на территории иностранных государств).

В контексте императивного действия норм Пакета Яровой, российские операторы связи и организаторы распространения информации должны, в том числе, обеспечить сбор, обработку сообщений, хранение и т.д. на территории Российской Федерации соответствующей информации («локализация»), а также обязаны предоставить соответствующую информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечивающим безопасность Российской Федерации по их запросу.

При этом деятельность российских операторов связи и организаторов распространения информации, нередко связана с обработкой и хранением персональных данных физических лиц Европейского Союза. Поскольку Регламент GDPR не регулирует отношения, и не применяется к отношениям, связанным с защитой физических лиц при обработке персональных данных компетентными органами в целях «…предотвращения угроз общественной безопасности». (Преамбула (19) Регламента GDPR). В этой связи одновременно с Регламентом GDPR, в целях предупреждения, расследования, выявления или судебного рассмотрения уголовных преступлений, либо приведения в исполнение уголовных наказаний, включая обеспечение защиты и предотвращения угроз общественной безопасности, в Европейском Союзе принят специальный нормативно-правовой акт, а именно: Директива (ЕС) 2016/680 Европейского парламента и Совета от 27

апреля 2016 г. «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных наказаний и о свободном перемещении таких данных и отмене Рамочного Решения Совета ЕС 2008/977/ JHA»[19] (далее – «Директива (ЕС) 2016/680»).

Как было отмечено ранее, правовая природа директивы (*Directive*) предполагает принятие государствами-членами соответствующих имплементирующих национальных актов. При этом, в значении Директивы (ЕС) 2016/680, такие национальные акты должны быть приняты к 25 мая 2018 г. Какие акты примут государства-члены в настоящее время сказать определенно достаточно сложно, но именно Директива (ЕС) 2016/680 предметно в большей степени связана с предметной сферой «пакета Яровой».

Вместе с тем, Регламент GDPR закрепляет достаточно определенные параметры критериев обработки персональных данных, в случае если они в том числе, связаны с мерами безопасности.

Во-первых, Регламент GDPR содержит нормы, предусматривающие, что обработка персональных данных связанных «…с мерами безопасности», осуществляется только под контролем официального органа, либо когда обработка разрешена правом Евросоюза или государства-члена, предусматривающим соответствующие гарантии для прав и свобод субъектов данных (Статья 10 Регламента GDPR).

Во-вторых, Регламент GDPR исходит из того, что когда обработка персональных данных частными организациями попадает под его действие, должна существовать возможность для государств-членов ЕС ограничивать по закону осуществление отдельных обязанностей и прав, если такое ограничение представляет собой необходимую и соразмерную меру в демократическом обществе для защиты конкретных жизненных интересов,

[19] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA*

включая общественную безопасность, … в том числе защиту и предотвращение угроз общественной безопасности, к примеру, в рамках борьбы с отмыванием доходов. (Преамбула (19) Регламента GDPR).

В-третьих, Регламент GDPR также предусматривает, что обработка персональных данных органами государственной власти, центрами реагирования на компьютерные чрезвычайные происшествия (*CERTs*), центрами реагирования на инциденты, связанные с компьютерной безопасностью (*CSIRTs*), поставщиками сетей электронных коммуникаций и услуг, а также поставщиками технологий и услуг по обеспечению безопасности является законным интересом соответствующего контролёра данных в той мере, в какой она необходима и соразмерна целям обеспечения сетевой и информационной безопасности, то есть способности сети или информационной системы противостоять, на заданном уровне достоверности, случайным событиям, незаконным или преднамеренным действиям, которые компрометируют доступность, подлинность, целостность и конфиденциальность сохранённых или переданных персональных данных, а также безопасность соответствующих услуг, переданных через указанные сети или системы. Такой законный интерес может включать в себя, к примеру, предотвращение несанкционированного доступа к сетям электронных коммуникаций и распространение вредоносного кода, а также пресечение сетевых атак и угроз для компьютерных и электронных систем связи. (Преамбула (49) Регламента GDPR).

Вышеизложенное дает основание сделать вывод о том, что государства-члены ЕС, при принятии ими соответствующих национальных актов, имплементирующих Директиву (ЕС) 2016/680, будут как минимум, исходить из тех норм, которые предусмотрены Регламентом GDPR, т.е. не «пойдут по пути» установления требований, аналогичных установленным «Пакетом Яровой», предусматривающего избыточное ужесточение регулирования порядка хранения данных с декларируемой целью обеспечения безопасности.

Минимизация рисков в «правовом поле», как коммерческих, так и некоммерческих (политических) российских операторов связи и организаторов распространения информации в контексте Пакета Яровой ФЗ практически невозможна[20], однако, потенциально в «правовом поле» влияние окажут:

– то, каким образом Правительство РФ определит порядок, сроки и объем хранения информации в подзаконных актах, которые еще не приняты, т.к. реализация Пакета Яровой увязана с рядом поручений Правительству в «целях минимизации возможных негативных последствий и рисков»;

– оспаривание в Конституционном Суде Пакета Яровой, с учетом того, каким образом будет формироваться правоприменительная практика, которая в настоящее время отсутствует.

Пакет Яровой, как отмечено ранее, изменяет и дополняет ФЗ № 149-Ф «*Об информации, информационных технологиях и о защите информации»*, соответственно, требования по хранению данных распространяется на <u>всех</u> организаторов распространения информации, потенциально включая и иностранных операторов. С одной стороны, иностранные операторы (участвующие, к примеру, в обеспечении приема, передачи, доставки и/или обработки данных), будут обязаны соблюдать императивные требования Пакета Яровой, а это может привести к нарушению ими соответствующих норм иностранного права, прежде всего касающихся конфиденциальности персональных данных, получения согласия субъекта данных на обработку, целевую обработку данных и т.д. Такая ситуация, в свою очередь, может повлиять на сокращение присутствия иностранных компаний на российском рынке телекоммуникационных услуг (если не к полному их уходу).

С другой стороны, сети ряда российских операторов расположены за рубежом и российские компании находятся в договорно-правовых

[20] Реализация Пакета Яровой потребует от российских операторов связи и организаторов распространения информации сокращения прямых затрат, запуск новых сетей и сервисов, модернизацию существующих оборудования и т.д. В свою очередь, принятие мер экономического характера, могут оказаться непосильными для целого ряда компаний, что приведет, если не к «самоубийству» отрасли, то, несомненно, к сокращению интернет-компаний, увеличению тарифов.

отношениях с европейскими компаниями. Соблюдение российскими операторами требований Пакета Яровой о хранении данных (данные переписки, данные разговора между пользователями и т.д.) может привести к нарушению российским оператором не только условий заключенных договоров, но и законодательных норм, действующих в иностранном государстве, к примеру, тех же требований о конфиденциальности, которые значительно расширены в Регламенте GDPR. Как следствие, на российских операторов в юрисдикции государств-членов Евросоюза могут быть наложены значительные штрафные санкции, согласно Регламенту GDPR; иные меры юридического характера в соответствии с правом государств-членов, не говоря уже об ответственности, вытекающей из условий заключенных договоров. В итоге, это может привести к прекращению договорно-правовых отношений российских операторов с их иностранными контрагентами, сокращению их коммерческих возможностей и присутствия российских операторов в юрисдикции государств-членов Евросоюза[21].

В этой связи российским операторам связи и организаторам распространения информации для минимизации возможных рисков потребуется:

1. Осуществить аудит заключенных договоров (если таковые есть) с компаниями из государств-членов Евросоюза для приведения в соответствие условий договоров с требованиями Регламента GDPR, а также с учетом императивных требований норм Пакета Яровой;

[21] Помимо Пакета Яровой Российская Федерация может оказаться первой страной, которая избыточно ужесточает регулирование порядка «обмена сообщениями», т.к. инициировано внесение соответствующих изменений и поправок в ФЗ № 149-Ф «Об информации, информационных технологиях и о защите информации». При прохождении всех законодательных процедур, согласно изменениям и поправкам ФЗ № 149-Ф, с 1 января 2018 г. приложения обмена сообщениями, которые пока позволяют пользователям регистрироваться анонимно, будут, в том числе связаны с идентификацией пользователей См. подробнее, например, URL:http://www.globalprivacyblog.com/legislative-regulatory-developments/messaging-apps-may-face-new-obligations-in-russia/

2. Внести соответствующие изменения в действующие договоры с компаниями-контрагентами из стран Европейского Союза и распределить возможные финансовые затраты;
3. Назначить в рамках компании компетентное лицо (группу лиц), ответственных за мониторинг разъясняющих норм применения Регламента GDPR, включая подзаконные и имплементирующие акты, принятые в соответствии с настоящим Регламентом и с правом государств-членов Евросоюза для уточнения положений Регламента GDPR, которые в перспективе могут быть приняты государствами-членами Евросоюза и Комиссией Европейского Союза;
4. Назначить своего представителя в соответствующем государстве-члене Евросоюза для взаимодействия с национальными надзорными органами.

Отметим, что Регламент GDPR предусматривает, что в соответствии с правом государства-члена ответственность за его нарушения может быть соразмерно распределена в отношении ущерба, причинённого обработкой, контролёр или обработчик, которые заплатили полную компенсацию, может обратиться в суд с регрессным требованием относительно других контролёров или обработчиков, участвовавших в одной и той же обработке. (Преамбула (146) Регламента GDPR).

Как отмечалось ранее, Регламент GDPR юрисдикционно расширен и может применяться к российским операторам связи и организаторам распространения информации, которые не учреждены в Евросоюзе, но обрабатывают персональные данные находящихся в Евросоюзе субъектов данных, если их деятельность по обработке данных связана с предложением товаров и услуг таким субъектам данных в Евросоюзе, вне зависимости от того, требуется ли оплата от субъекта данных, либо связана с мониторингом деятельности субъектов данных постольку, поскольку она осуществляется в Евросоюзе.

Можно смоделировать следующую ситуацию. Субъект персональных данных из стран-членов Евросоюза, в соответствии с Регламентом GDPR хочет обжаловать действия российской компании-обработчика, связанные с обработкой его персональных данных, т.к. они обработаны без его согласия и такая обработка нанесла ему ущерб. Субъект данных вправе обратиться в соответствующий компетентный орган. Но даже если такой компетентный орган вынесет решений, оно не будет исполнимо на территории Российской Федерации, поскольку отсутствуют адекватных правовых механизмов, в том числе из-за отсутствия правовых договоров о правовой помощи.

Важным аспектом является то, что Регламент GDPR регулирует трансграничную передачу данных за пределы Евросоюза, что может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в том числе, защитить себя от неправомерного использования или нарушение конфиденциальности. Надзорные органы Евросоюза могут быть не в состоянии рассмотреть жалобу или провести расследование в отношении деятельности, осуществляемой за пределами границ своего государства-члена. Их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или полномочиями, связанными с исправлением ситуации, противоречивым режимом правового регулирования, а также препятствиями практического характера, например, ограничением источников сведений. Вследствие этого Регламент GDPR исходит из необходимости содействовать тесному сотрудничеству между надзорными органами по защите персональных данных для того, чтобы они могли обмениваться информацией и проводить расследования с надзорными органами других стран. В целях разработки механизмов международного сотрудничества для содействия и обеспечения международной взаимной помощи при исполнении законодательства о защите персональных данных, Европейская Комиссия и надзорные органы обмениваются информацией и сотрудничают в рамках

своей компетенции с компетентными органами в третьих странах на основе взаимности и в соответствии с Регламентом GDPR.

Европейская Комиссия, согласно Регламенту GDPR, вправе оценивать уровень защиты персональных данных в третьих странах, учитывать то, каким образом третья страна соблюдает принципы правового государства, обеспечивает доступность правосудия, так же, как и соблюдает нормы и стандарты международного права прав человека. Европейская Комиссия, согласно Регламенту GDPR, может принять решение о недостаточности мер защиты персональных данных в отношении третьей страны, если третья страна не предоставляет гарантии, обеспечивающие соответствующий уровень защиты, соразмерный уровню, гарантированному в Евросоюзе, эффективный независимый мониторинг защиты данных, не предусматривает механизмы сотрудничества с органами защиты данных государств-членов Евросоюза по защите данных, а субъектам данных должны не предоставляет административные и судебные средства защиты. В этом случае трансграничная передача данных такой третьей стране может быть запрещена. Статья 70 (s) Регламента GDPR возлагает определенные полномочия по этим вопросам на новый орган – Европейский совет по защите данных (*European Data Protection Board, EDPB*).

Пакет Яровой, а также предлагаемые изменения и дополнения действующего российского законодательства в сфере персональных данных могут потенциально привести к принятию решения о недостаточности мер защиты персональных данных в России. Если подобное решение будет принято в отношении России, минимизировать подобные риски российским операторам связи и организаторам распространения информации не удастся.

Приложение: Перевод Регламента General Data Protection Regulation (GDPR) Европейского Союза

Перевод выполнен Д.Ю.Н., Профессором Дипломатической Академии МИД РФ, Заведующей кафедрой международного частного права Касеновой Мадиной Балташевной

О защите физических лиц относительно обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС

(Общий Регламент по защите персональных данных)[22]

Европейский Парламент и Совет Европейского Союза,

Принимая во внимание Договор о функционировании Европейского Евросоюза, и в частности Статью 16,

Руководствуясь предложением Европейской Комиссии,

После передачи проекта законодательного акта национальным Парламентам,

Принимая во внимание позицию Европейского экономического и социального Комитета ([1])[23],

Принимая во внимание позицию Комитета регионов ([2])[24],

Действуя в соответствии с обычной законодательной процедурой ([3])[25],

Принимая во внимание, что:
(1) Защита физических лиц в отношении обработки персональных данных является основным правом. Статья 8 (1) Хартии Европейского Евросоюза об основных правах (далее – «Хартия»)[26] и статья 16 (1) Договора о функционировании Европейского Евросоюза (далее – «Договор TFEU»)[27]

---

[22] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) – OJ L 119, 04.05.2016, C. 1 - 88.*

[23] (1) Опубликовано в Официальном Журнале Европейского Союза № C 229, 31.07.2012, С. 90.(*OJ C 229, 31.7.2012, p. 90*.).

[24] (2) Опубликовано в Официальном Журнале Европейского Союза № C 391, 18.12.2012, С. 127. (*OJ C 391, 18.12.2012, p. 127*.)

[25] (3) Позиция Европейского Парламента от 12 марта 2014 г. (еще не опубликована в Официальном Журнале Европейского Союза) и позиция Совета по первому чтению от 8 апреля 2016 г.– *Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.*

[26] *Примечание переводчика: «Хартия Европейского Союза об основных правах» – Charter of Fundamental Rights of the European Union 2000.*

[27] Примечание переводчика: «Договор о функционировании Европейского Союза» – *Treaty on the Functioning of the European Union.*

предусматривают, что каждый имеет право на защиту персональных данных, касающихся его/ее.

(2) Принципы и правила защиты физических лиц в отношении обработки их персональных данных должны, независимо от гражданства или места жительства лиц, уважать их основные права и свободы, в частности их право на защиту персональных данных. Настоящий Регламент призван содействовать формированию пространства свободы, безопасности и справедливости, а также общего экономического пространства, экономическому и социальному прогрессу, укреплению и сближению экономик на внутреннем рынке, содействовать благосостоянию физических лиц.

(3) Директива 95/46/ЕС Европейского Парламента и Совета ([4])[28] направлена на гармонизацию защиты основных прав и свобод физических лиц в отношении обработки данных и обеспечить свободное перемещение персональных данных между государствами-членами.

(4) Обработка персональных данных должна служить человечеству. Право на защиту персональных данных не является абсолютным правом; его следует рассматривать в соответствии с его предназначением для общества, и оно должно быть уравновешено с иными основными правами и в соответствии с принципом пропорциональности. Настоящий Регламент исходит из соблюдения всех основных прав, свобод и принципов, закреплённых в Хартии, предусмотренные в договорах, в том числе, уважение частной и семейной жизни, жилища и переписки, защиты персональных данных, свободы мысли, совести и вероисповедания, свободы выражения мнений и информации, свободы предпринимательской деятельности, право на эффективные средства правовой защиты и справедливое судебное разбирательство, а также на культурное, религиозное и языковое разнообразие.

(5) Экономическая и социальная интеграция, обусловленная функционированием внутреннего рынка, привела к существенному росту трансграничных потоков персональных данных. Увеличился обмен персональными данными между государственными и частными структурами, включая физических лиц, организации и предприятия в рамках Евросоюза. Национальные органы государств-членов призваны сотрудничать и обмениваться персональными данными с тем, чтобы иметь возможность осуществлять свои обязательства, либо решать задачи от имени уполномоченного органа в другом государстве-члене.

(6) Стремительные технологические изменения и глобализация вызвали

[28] (5) Директива 95/46/ЕС Европейского Парламента и Совета от 24 октября 1995 об обеспечении отдельных лиц в отношении обработки их персональных данных и свободном перемещении таких данных. (Официальный Журнал Европейского Союза № L 281, 23.11.1995, p. 31). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).*

новые проблемы в защите персональных данных. Значительно увеличился масштаб сбора и обмена персональными данными. Технология позволяет и частным компаниям, и государственным органам, использовать персональные данные в беспрецедентных масштабах для осуществления своей деятельности. Физические лица все в возрастающем объёме предоставляют персональную информацию публично и в глобальном масштабе. Технологии изменили как экономику, так и общественную жизнь, при этом технологии должны способствовать свободному распространению персональных данных в рамках Евросоюза, а также передаваться в третьи страны, международным организациям, с условием обеспечения высокого уровня защиты персональных данных.

(7) Такие обстоятельства требуют решительных и более согласованных основ организации защиты данных в рамках Евросоюза, которые обеспечиваются строгими правоприменительными мерами, с учётом важности создания атмосферы доверия позволяющей цифровой экономике развиваться на внутреннем рынке. Физические лица должны контролировать свои личные данные. Необходимо укрепить юридическую однозначность и практическую достоверность для физических лиц, хозяйствующих субъектов и органов государственной власти.

(8) Если настоящий Регламент содержит требования или ограничения действия его норм в соответствии с правом государства-члена, государства-члены могут инкорпорировать основы настоящего Регламента в своё национальное право, насколько это необходимо для обеспечения согласованности, а также обеспечения того, чтобы нормы национального права были понятными для лиц, в отношении которых они применимы.

(9) Цели и принципы Директивы 95/46/ЕС сохраняют свою силу, но они не предотвращают фрагментацию при осуществлении защиты данных в рамках Евросоюза, правовую неопределённость или широко распространённое общественное мнения о том, что существуют значительные риски для защиты физических лиц, особенно в отношении их деятельности в интернете. Различия в уровне защиты прав и свобод физических лиц, в частности права на защиту персональных данных, в отношении обработки персональных данных в государствах-членах, могут препятствовать свободному перемещению персональных данных в масштабах всего Евросоюза. Такие различия могут, следовательно, препятствовать ведению экономической деятельности в рамках Евросоюза, нарушать свободу конкуренции и затруднять органам власти исполнять их обязанности в соответствии с правом Евросоюза. Такая разница в уровнях защиты обусловлена существованием различий в имплементации Директивы 95/46 / ЕС и ее применении.

(10) Для обеспечения согласованного и высокого уровня защиты физических лиц и устранения препятствий для движения потоков персональных данных в рамках Евросоюза, уровень защиты прав и

свобод физических лиц в отношении обработки таких данных должен быть одинаковым во всех государствах-членах. В масштабах всего Евросоюза должно обеспечиваться последовательное и гармонизированное применение норм о защите фундаментальных прав и свобод физических лиц в отношении обработки персональных данных. В отношении обработки персональных данных на предмет соответствия соблюдению обязанностей, предусмотренных законом, для выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролёра, государствам-членам необходимо разрешить утверждать или принимать национальные нормы для применения положений настоящего Регламента. В комплексе нормативно-правовых актов общих норм и норм, действующих на одном уровне, в сфере защиты данных, которые имплементируют Директиву 95/46/ЕС, в государствах-членах существует отдельное отраслевое законодательство в сферах, которые нуждаются в более конкретных нормах. Настоящий Регламент, в свою очередь, предоставляет возможность свободы действий государствам-членам принимать собственные правила, в том числе, и для обработки особых категорий персональных данных («Специальные категории персональных данных» – «*sensitive data*»). При этом настоящий Регламент не исключает право государства-члена, которое определяет обстоятельства для особых ситуаций обработки данных, включая определение более чётких условий, при которых такая обработка персональных данных будет правомерной.

(11) Эффективная защита персональных данных в масштабах Евросоюза требует укрепления и детального изложения прав субъектов данных, и обязанности тех лиц, кто осуществляет обработку и определяет порядок обработки персональных данных, а также аналогичные полномочия по мониторингу и обеспечению соблюдения норм защиты персональных данных, и соответствующие санкции за нарушения в государствах-членах.

(12) Статья 16 (2) Договора TFEU уполномочивает Европейский Парламент и Европейский Совет устанавливать правила, касающиеся защиты физических лиц в отношении обработки персональных данных и правила, касающиеся свободного перемещения персональных данных.

(13) В целях обеспечения соответствующего уровня защиты физических лиц на территории Евросоюза и предотвращения расхождений, затрудняющих свободное перемещение персональных данных в пределах внутреннего рынка, Регламент необходим для обеспечения правовой определённости и прозрачности для хозяйствующих субъектов, в том числе микро, малых и средних предприятий, для предоставления физическим лицам во всех государствах-членах одинакового уровня юридически закреплённых прав и обязанностей, а также функциональных обязанностей контролёров и обработчиков; обеспечения соответствующего мониторинга обработки персональных данных и равнозначных санкций во всех государствах-членах, равно как и для обеспечения эффективного сотрудничества между надзорными органами различных государств-членов. Надлежащее функционирование внутреннего рынка требует, чтобы свободное перемещение персональных данных в пределах Евросоюза не ограничивалось или запрещалось по причинам, связанным с защитой физических лиц при обработке персональных данных. Для учёта конкретной ситуации на микро, малых и средних предприятиях, настоящий Регламент предусматривает изъятия в отношении ведения учёта для организаций с менее чем 250 сотрудников. Кроме того, учреждениям и органам Евросоюза, а также государствам-членам и их надзорным органам, рекомендуется учитывать конкретные потребности микро, малых и средних предприятий по применению настоящего Регламента. Понятие микро, малых и средних предприятий должно пониматься исходя из статьи 2 Приложения Рекомендации Комиссии 2003/361/ЕС (5)[29].

(14) Защита, предусмотренная настоящим Регламентом, должна применяться к физическим лицам, независимо от их национальной принадлежности или места жительства, в связи с обработкой их персональных данных. Настоящий Регламент не распространяется на обработку персональных данных юридических лиц и, в частности, на предприятия, созданные как юридические лица, включая наименование и организационно-правовую форму юридического лица, а также и реквизиты юридического лица.

(15) Для предотвращения риска обхода норм, защита физических лиц должна быть технологически нейтральной и не должна зависеть от используемых технологий. Защита физических лиц должна применяться для обработки персональных данных автоматическими средствами, а также для обработки вручную, если персональные данные содержатся или предназначены для содержания в системе

[29] (5) Рекомендация Комиссии от 6 мая 2003 г. относительно микро, малых и средних предприятий (Официальный Журнал Европейского Союза № L 124, 20.5.2003, С. 36). *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36). –*

учёта. Файлы или наборы файлов, а также их титульные страницы, которые не структурированы в соответствии со специальными критериями, не должны подпадать под действие настоящего Регламента.

(16) Настоящий Регламент не применяется к вопросам защиты основных прав и свобод человека или свободному перемещению персональных данных, в отношении деятельности, которая выходит за рамки права Евросоюза, к примеру, деятельности, связанной со сферой национальной безопасности. Настоящий Регламент не распространяется на обработку персональных данных государствами-членами при осуществлении деятельности, связанной с общей внешней политикой и политикой безопасности Евросоюза.

(17) Регламент (ЕС) № 45/2001 Европейского Парламента и Совета ([6])[30] применяется к обработке персональных данных учреждениями, органами, организациями и агентствами Евросоюза. Регламент (ЕС) № 45/2001, а иные нормативно-правовые акты Евросоюза, применимые к такой обработке персональных данных, должны быть адаптированы к принципам и нормам, предусмотренным настоящим Регламентом и применяться в соответствии с настоящим Регламентом. Для обеспечения чёткой и согласованной защиты данных в рамках Евросоюза, после принятия настоящего Регламента, необходимо внести изменения в Регламент (ЕС) № 45/2001, для того чтобы обеспечить возможность его применение наряду с настоящим Регламентом.

(18) Настоящий Регламент не применяется к обработке персональных данных физическим лицом при осуществлении сугубо личной или бытовой деятельности и, соответственно, не связанной с профессиональной или коммерческой деятельностью. Личная или бытовая деятельности может охватывать переписку и хранение адресов, или взаимодействие в социальных сетях и онлайн операции, осуществляемые в контексте такой деятельности. Однако настоящий Регламент распространяется на контролёров и обработчиков, которые предоставляют средства для обработки персональных данных для такой личной или бытовой деятельности.

(19) Защита физических лиц при обработке персональных данных компетентными органами в целях предупреждения, расследования,

[30] (6) Регламент (ЕС) № 45/2001 Европейского Парламента и Совета от 18 декабря 2000 о защите лиц в отношении обработки персональных данных учреждениями и организациями Сообщества и о свободном перемещении таких данных. (Официальный Журнал Европейского Союза № L 8, 12.1.2001, С. 1.).
Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

выявления или судебного рассмотрения уголовных преступлений, либо приведения в исполнение уголовных наказаний, включая обеспечение защиты и предотвращения угроз общественной безопасности, а также свободное перемещение таких данных, является предметом регулирования специального правового акта Евросоюза. Соответственно, настоящий Регламент не применяется к обработке (данных) для таких целей. При этом, персональные данные, обрабатываемые государственными органами в соответствии с настоящим Регламентом, при их использовании в обозначенных целях, должны регулироваться более конкретным нормативно-правовым актом Евросоюза, а именно Директивой (ЕС) 2016/680 Европейского Парламента и Совета (7)[31]. Государства-члены могут поручить компетентным органам, в значении Директивы (ЕС) 2016/680, осуществление задач, которые не обязательно выполняются для целей предотвращения, расследования, выявления преступлений привлечения к ответственности или приведения в исполнение уголовных наказаний, включая обеспечение защиты общественной безопасности и предотвращение угроз общественной безопасности, так, чтобы обработка персональных данных для таких других целей попадала под действие настоящего Регламента, в той мере в какой она находится в рамках права Евросоюза.

В отношении обработки персональных данных такими компетентными органами в целях, попадающих под действие настоящего Регламента, государства-члены должны обладать возможностью сохранять или принимать более конкретные нормы для применения положений настоящего Регламента. Такие нормы могут более точно определять конкретные требования к обработке персональных данных этими компетентными органами для таких других целей, принимая во внимание конституционное, организационное и административное устройство соответствующего государства-члена. Когда обработка персональных данных частными организациями попадает под действие настоящего Регламента, данный Регламент должен обеспечивать возможность для государств-членов, при наличии конкретных условий, ограничивать по закону осуществление отдельных обязанностей и прав, если такое ограничение представляет собой необходимую и соразмерную меру в демократическом обществе для защиты конкретных жизненных интересов, включая общественную безопасность, а также предупреждение, расследование, выявление уголовных преступлений, либо привлечение к ответственности или приведение в исполнение

[31] (7) Директива (ЕС) 2016/680 Европейского парламента и Совета о 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных наказаний и о свободном перемещении таких данных и отмене Рамочного Решения Совета ЕС 2008/977/ JHA. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA*

уголовных наказаний, в том числе защиту и предотвращение угроз общественной безопасности. Это имеет значение, к примеру, в рамках борьбы с отмыванием доходов или деятельности лабораторий судебной экспертизы.

(20) Исходя из того, что настоящий Регламент применяется, помимо всего прочего, к деятельности судов и других судебных органов, право Евросоюза или право государства-члена может определять порядок и процедуру применительно к обработке персональных данных судами и иными судебными органами. Компетенция надзорных органов не должна охватывать обработку персональных данных, для того, чтобы суды действовали в рамках своей судебной дееспособности, с тем, чтобы обеспечить независимость судебной власти при выполнении ею судебных задач, включая принятие решений. Должна быть предусмотрена возможность поручить надзор за такими операциями по обработке данных специально уполномоченным органам судебной системы государства-члена, которые должны, в частности, обеспечить соблюдение норм настоящего Регламента, повысить осведомлённость представителей судебных органов относительно их обязанностей в соответствии с настоящим Регламентом, а также рассматривать жалобы в отношении таких операций по обработке данных.

(21) Настоящий Регламент действует без ущерба для применения Директивы 2000/31/ЕС Европейского Парламента и Совета ([8])[32], в частности, правил об ответственности поставщиков посреднически услуг предусмотренных статьями 12-15 этой Директивы. Данная Директива направлена на содействие надлежащему функционированию внутреннего рынка путём обеспечения свободного обращения услуг информационного общества среди государств-членов.

(22) Любая обработка персональных данных в контексте деятельности по учреждению контролёра или обработчика в Евросоюзе должна осуществляться в соответствии с настоящим Регламентом, независимо от того, осуществляется ли собственно сама обработка не территории Евросоюза. Учреждение подразумевает эффективное и реальное осуществление деятельности постоянных структур. Организационно-правовые формы таких структур, будь то отделение, дочернее предприятие, обладающее правосубъектностью, не является определяющим фактором в таких случаях.

[32] (8) Директива 2000/31/ЕС Европейского Парламента и Совета ЕС от 8 июня 2000 г. о некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности, об электронной коммерции. «Директива об электронной коммерции». (Официальный Журнал Европейского Союза. № L 178, 17.7.2000, С. 1).
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market («Directive on electronic commerce») (OJ L 178, 17.7.2000, p. 1)

(23) В целях обеспечения того, чтобы физические лица не были лишены защиты, на которую они имеют право в соответствии с настоящим Регламентом, обработка персональных данных субъектов данных в Евросоюзе контролёром или обработчиком, которые не учреждены в Евросоюзе, подпадает под действие настоящего Регламента в случаях, когда обработка связана с предложением товаров или услуг таким субъектам данных, независимо от того, связано это с их с оплатой или нет. Чтобы определить, предлагает ли такой контролёр или обработчик товары или услуги субъектам данных, находящихся в Евросоюзе, следует установить очевидность того, что контролёр или обработчик намеревается предлагать услуги субъектам данных в одном или нескольких государствах-членах Евросоюза. Исходя из того, что сама по себе доступность веб-сайта контролёра, обработчика или посредника в Евросоюзе, адреса электронной почты или иных контактных данных, либо использование языка, обычно используемого в третьей стране, в которой учреждён контролёр, являются недостаточными для установления подобных намерений, признаки, среди которых использование языка или валюты, обычно используемой в одном или нескольких государствах-членах, с возможностью заказывать товары и услуги на этом языке, либо упоминание потребителей или пользователей, которые находятся в Евросоюзе, могут делать очевидным то, что контролёр намерен предлагать товары или услуги субъектам данных в Евросоюзе.

(24) Обработка персональных данных субъектов данных, находящихся в Евросоюзе, контролёром или обработчиком, которые не учреждены в Евросоюзе, также является предметом регулирования настоящего Регламента, когда это связано с мониторингом действий таких субъектов данных, постольку, поскольку их действия совершаются на территории Евросоюза. Чтобы определить, подпадает ли деятельность по обработке данных для целей мониторинга действий субъекта данных, следует установить осуществляют ли физические лица деятельность в интернете, в том числе потенциальную возможность последовательного использования технологии обработки персональных данных, посредством которых осуществляется составление профиля физического лица, в частности, для принятия решений относительно анализа либо прогнозирования ее/его личных предпочтений, особенностей поведения, а также личностных характеристик.

(25) В случае, если применяется право государства-члена в силу международного публичного права, настоящий Регламент должен также применяться в отношении контролёра, не учреждённого в Евросоюзе, и, в частности, в дипломатическом представительстве или консульском учреждении государства-члена.

(26) Принципы защиты данных должны применяться к любой информации, касающейся идентифицированного или идентифицируемого физического

лица. Личные данные, подвергнутые псевдонимации[33], которые могут быть соотнесены с физическим лицом посредством использования дополнительной информации, следует рассматривать как информацию об идентифицируемом физическом лице. Для того, чтобы определить, идентифицируемо ли физическое лицо, следует учитывать все средства, которые могут быть достоверно с большей вероятностью быть использованы, к примеру – выявление, либо контролёром, либо иным лицом, для того, чтобы идентифицировать физическое лицо прямо или косвенно. Чтобы установить используются ли средства с достаточной степенью вероятности для идентификации физического лица, учитывать следует все объективные факторы, в том числе расходы и количество времени, необходимое для идентификации, принимая во внимание имеющиеся технологические возможности на момент обработки, а также развитие технологий. В силу этого принципы защиты данных не применяются к анонимной информации, т.е. к информации, не относящейся к идентификации физического лица или с помощью которой идентифицируется физическое лицо, или не относится к персональным данным, предоставленных анонимно (обезличено) таким способом, что субъект данных не идентифицируется или не поддаётся идентификации. Настоящий Регламент не распространяется по этой причине на обработку такой анонимной информации, в том числе для статистических или исследовательских целей.

(27) Настоящий Регламент не применяется к персональным данным умерших лиц. Государства-члены могут принять нормы, касающиеся обработки персональных данных умерших лиц.

(28) Применение псевдонимации к персональным данным может снизить риски для соответствующих субъектов данных и помочь контролёрам и обработчикам данных выполнить свои обязанности по защите данных. Формальное использование «псевдонимации» в настоящем Регламенте не подразумевает отказ от каких-либо иных мер защиты данных.

(29) Ради создания стимулов применения псевдонимизации при обработке персональных данных, меры псевдонимизации, допускающие общий анализ, должны быть доступны у одного и того же контролёра, в тех случаях, когда этот контролёр принял технические и организационные меры, необходимые для того, чтобы обеспечить соответствующую обработку, исполнение настоящего Регламента, а также чтобы дополнительная информация, для соотнесения персональных данных с определённым субъектом данных хранилась отдельно. Контролёр, обрабатывающий персональные данные, должен назначить уполномоченных лиц в составе того же контролёра.

(30) Физические лица могут быть определены интернет-идентификаторами,

[33] Псевдонимация – замена имени, фамилии, использование псевдонима (прим. переводчика)

посредством их устройств, приложений, инструментов и протоколов, такими как IP-адреса, идентификационные файлы, сохраняемые в клиентской системе (*cookie identifiers*), либо иными устройствами опознавания, например, тегами радиочастотной идентификации. Они могут оставлять следы, которые, именно в сочетании с уникальными идентификаторами и иной, полученной серверами информацией, могут быть использованы для профилирования физических лиц и их идентификации.

(31) Государственные органы, которым раскрываются персональные данные, в соответствии с правовыми обязанностями по осуществлению их официальной деятельности, такие как налоговые и таможенные органы, органы финансовых расследований, самостоятельные административные органы или службы по делам финансового рынка, ответственные за регулирование и надзор на рынке ценных бумаг, не должны рассматриваться в качестве получателей данных, если они получают персональные данные, которые в соответствии с правом Евросоюза или государства-члена, необходимы для проведения конкретного расследования в общих интересах. Запросы на раскрытие данных, направляемые государственными органами, всегда должны быть в письменной форме, обоснованными и носить нерегулярный характер обоснованными, а также они не должны касаться всей системы учёта, либо приводить к объединению систем учёта. Обработка персональных данных такими государственными органами должна соответствовать применимым нормам по защите данных в соответствии с целями обработки.

(32) Согласие должно даваться посредством ясного утвердительного действия, устанавливающего свободно предоставленное, конкретное, обоснованное и однозначное указание на согласие субъекта данных относительно обработки персональных данных, касающихся его/ее, среди которых письменное заявление, поданное, в том числе, в электронной форме, либо устное заявление. Такое согласие может охватывать и проставление галочки при посещении сайта в интернете, выбор технических настроек услуг информационного общества, либо иное документальное подтверждение или способы действий, которые ясно указывают, в данном контексте, принятие субъектом данных предлагаемой обработки ее/его персональных данных. Молчание, ранее проставленная галочка при посещении сайта или бездействие не должны, в свою очередь, рассматриваться как согласие. Согласие должно охватывать всю обработку данных, осуществляемую для той же самой цели, либо в таких целях. В том случае, когда обработка данных имеет несколько целей, согласие необходимо для каждой из них. Если согласие субъекта данных даётся в соответствии с запросом, с помощью электронных средств, этот запрос должен быть ясным, чётким и не должен неоправданно нарушать использование услуги, для которой он

предназначен.

(33) Часто невозможно в полной мере определить цель обработки персональных данных, предназначенных для научных исследований на момент сбора данных. Соответственно, субъектам данных должно быть разрешено давать своё согласие в отношении отдельных сфер научных исследований, исходя из соответствия целей признанным этическим стандартам научных исследований. Субъекты данных должны иметь возможность давать своё согласие только в отношении отдельных сфер исследований или части научно-исследовательских проектов в соответствии с поставленной целью.

(34) Генетические данные следует рассматривать как персональные данные, в отношении унаследованных или приобретённых генетических характеристик физического лица, которые являются результатом анализа биологического образца физического лица, в частности, исследования хромосомной, дезоксирибонуклеиновой кислоты (ДНК) или рибонуклеиновой кислоты (РНК) или анализа иного элемента, позволяющего получить адекватную информацию.

(35) Персональные данные, касающиеся здоровья, должны охватывать все данные, относящиеся к состоянию здоровья субъекта данных, которые раскрывают информацию, касающуюся о прошлом, текущем или будущем физическом или психическом состоянии субъекта данных. Это охватывает информацию о физическом лице, собранную в ходе регистрации или при предоставлении медицинских услуг такому физическому лицу, в соответствии с Директивой 2011/24/ЕС Европейского Парламента и Совета ([9])[34]; номер, код или деталь, присвоенные физическому лицу однозначно идентифицируют физическое лицо для целей здравоохранения; информация, полученная в результате тестирования или изучения части тела или тканей, включая генетические данные и биологические образцы; а также любую информацию, касающуюся, например, заболевания, инвалидности, риска заболевания, истории болезни, клинического лечения или физиологического или биомедицинского состояния субъекта данных, независимо от его источника, например, информацию, полученную от врача или иного медицинского работника, из больницы, по медицинским приборам или тест-системам диагностики в лабораторных условиях.

(36) Главное учреждение контролёра в Евросоюзе, должно являться местом его центральной администрации в Евросоюзе, кроме тех случаев, когда решения о целях и средствах обработки персональных данных не принимаются иной организацией контролёра в Евросоюзе, в таком

[34] (9) Директива 2011/24/ЕС Европейского Парламента и Совета ЕС от 9 марта 2011 г. о правах пациентов при трансграничном медицинском обслуживании. (Официальный Журнал Европейского Союза. № L 88, 4.4.2011, С. 45). *Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).*

случае, такая иная организация должна рассматриваться как основное учреждение контролёра. Главное учреждение контролёра в Евросоюзе, должно быть определено в соответствии с объективным критерием, что подразумевает эффективное и реальное осуществление управленческой деятельности, принятие основных решений относительно целей и средств обработки посредством стабильных механизмов. Такой критерий не должен зависеть от того, осуществляется ли обработка персональных данных в указанном месте. Наличие и использование технических средств и технологий для обработки персональных данных или деятельности по обработке, не создают сами по себе главного учреждения и, следовательно, не являются определяющим критерием о главного учреждения. Главное учреждение обработчика должно быть местом его центральной администрации в Евросоюзе либо, если он не имеет центральной администрации в Евросоюзе, место, где осуществляется основная деятельность по обработке данных в Евросоюзе. В случае участия и контролёра, обработчика, компетентным руководящим надзорным органом должен рассматриваться надзорный орган государства-члена, в котором находится главное учреждение контролёра, но надзорный орган обработчика должен рассматриваться как заинтересованный надзорный орган и этот надзорный орган должен участвовать в совместных действиях, предусмотренных настоящим Регламентом. В любом случае надзорные органы государства-члена или государств-членов, в которых обработчик имеет одно или несколько организаций, не должны рассматриваться в качестве заинтересованных надзорных органов если проект решения касается только контролёра. Когда обработка осуществляется группой компаний, основное учреждение контролирующей компании должно рассматриваться как основное учреждение группы компаний, за исключением случаев, когда цели и средства обработки определяются иной компанией.

(37) Группа хозяйствующих субъектов должна охватывать контролирующую компанию и ее подконтрольные компании, т.е. контролирующая компания может оказывать доминирующее влияние на другие компании в силу, например, права владения, финансового участия или правил, которые регулируют его возможность применять правила защиты персональных данных. Компания, которая контролирует обработку персональных данных в связанных с нею компаниях, должна рассматриваться вместе с такими компаниями как группа хозяйствующих субъектов.

(38) Дети нуждаются в особой защите в отношении их персональных данных, поскольку они в меньшей степени осведомлены о рисках, последствиях и соответствующих средствах защиты, а также их правах в отношении обработки персональных данных. Такие особые меры защиты должны, в частности, применяться к использованию персональных данных детей в

целях маркетинга или создания персонального или пользовательского профилей и сбора персональных данных, связанных с детьми при использовании услуг, предлагаемых непосредственно ребёнку. Согласие лиц, обладающих родительской ответственностью, не является необходимым в контексте превентивных мероприятий или консультационных услуг, предоставляемых непосредственно ребёнку.

(39) Любая обработка персональных данных должна быть правомерной и справедливой. Для физических лиц должно быть очевидно, что персональные данные, связанные с ними, собираются, используются, учитываются или иным образом обрабатываются, а также должно быть очевидно в каком объёме персональные данные обрабатываются или будут обрабатываться. Принцип прозрачности (траспарентости) требует, чтобы любые сведения и сообщения, относящиеся к обработке таких персональных данных, были легко доступны и ясны для понимания, а также, чтобы использовался чёткий и простой язык. Этот принцип касается, в частности, извещения субъектов данных о личности контролёра и о целях обработки данных, а также дополнительной информации для обеспечения справедливой и прозрачной (транспарентной) обработки отношении соответствующих физических лиц и их права на получение подтверждения и сообщения относительно того, какие относящиеся к ним персональные данные обрабатываются. Физические лица должны быть осведомлены о рисках, правилах, средствах защиты и правах в отношении обработки персональных данных и о том, как реализовать свои права в связи с такой обработкой. В частности, конкретные цели, для которых обрабатываются персональные данные, должны быть ясными и законными и определяться на момент сбора персональных данных. Персональные данные должны быть достоверными, адекватными и ограничиваться тем, что необходимо для целей, для которых они обрабатываются. Это требует, в частности, обеспечения того, чтобы период, в течение которого персональные данные хранятся, ограничивался строгим минимумом. Персональные данные должны обрабатываться только в том случае, если цель обработки не может быть разумно достигнута иными средствами. Чтобы гарантировать, что персональные данные не будут храниться дольше, чем это необходимо, ограничение сроков хранения должны быть установлены контролёром для удаления или для периодического пересмотра. Все обоснованные меры должны быть приняты для того, чтобы обеспечить исправление или удаление персональных данных, которые являются неточными. Персональные данные должны обрабатываться таким образом, чтобы обеспечить надлежащую безопасность и конфиденциальность этих персональных данных, в том числе для предотвращения несанкционированного доступа к персональным данным или использования персональных данных, а также оборудования, используемого для обработки.

(40) Для того, чтобы обработка была правомерной, персональные данные должны обрабатываться на основании согласия заинтересованного субъекта данных или на ином законном основании, установленном законом, либо настоящим Регламентом, либо правом Евросоюза, либо правом государства-члена, указанном в настоящем Регламенте, в том числе необходимость соблюдения правовых обязательств, под действие которых подпадает контролёр, или необходимость исполнения договора, стороной которого является субъект данных, или для принятия мер по запросу субъекта данных до заключения договора.

(41) В тех случаях, когда настоящий Регламент ссылается на правовые основания или законодательные меры, это необязательно требует принятие законодательного акта Парламентом, без ущерба для требований, связанных с конституционным устройством заинтересованного государства-члена. Однако такие правовые основания или законодательные меры должны быть ясными и предсказуемыми для лиц, к которым они относятся, в соответствии с прецедентным правом Европейского Суда Справедливости («Суд Справедливости») и Европейского суда по правам человека.

(42) В случаях, когда обработка основана на согласии субъекта данных, контролёр должен быть способен подтвердить, что субъект данных дал согласие на процедуру обработки данных. В частности, в этом контексте письменное заявление по другому вопросу, средства защиты должны гарантировать, что субъект данных осведомлён о том, что он дал своё согласие, а также о том, в каком объёме такое согласие дано. В соответствии с Директивой Совета 93/13/ЕЭС (10)[35], согласие предварительно сформулированное контролёром, предоставляется в понятной и доступной форме, с использованием ясного и понятного языка, и оно не должно содержать несправедливые условия. Для того чтобы сообщить о согласии, субъект данных должен знать, как минимум, идентификационные данные контролёра, а также цели обработки персональных данных для которых персональные данные предназначены. Согласие не рассматриваться как данное добровольно, если у субъекта персональных данных нет действительного или свободного выбора или не в состоянии без ущерба отказаться или отозвать своё согласие.

(43) Для обеспечения того, что согласие предоставлено свободно, согласие не должно предоставлять допустимое юридическое основание для обработки персональных данных в специфическом случае, при котором существует явное расхождение между субъектом данных и контролёром, в частности, в случае, когда контролёр является государственным органом, и поэтому

[35]Директива 93/13/ЕЭС Совета ЕС от 5 апреля 1993 г. о несправедливых условиях в договорах с потребителями. (Официальный Журнал Европейского Союза. № L L 95, 21.4.1993, p. 29). Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

маловероятно, что согласие предоставлено свободно о во всех обстоятельствах в такой специфической ситуации. Предполагается, что согласие не предоставлено свободно, если не дано отдельное согласие на различные операции обработки персональных данных, несмотря на то, что оно подходит для отдельного случая, либо если исполнение контракта, включая предоставление услуги, зависит от согласия, несмотря на то, что такое согласие не является необходимым для подобного исполнения.

(44) Обработка должна быть дозволена, когда это необходимо в контексте контракта, либо намерения заключить контракт.

(45) В случае если обработка осуществляется согласно правовым обязательствам, которым подчиняется контролёр или если обработка необходима для выполнения задачи осуществляемой в общественных интересах либо должностных полномочий, обработка должна основываться на праве Евросоюза или государства-члена. Настоящий Регламент не требует специального законодательства в отношении каждого отдельного вида обработки. Право, в качестве основания для нескольких видов обработки, когда обработка данных основана на правовых обязательствах, которым подчиняется контролёр, когда обработка необходима для выполнения задачи, осуществляемой общественных интересах либо должностных полномочий, может быть достаточно. Также необходимо, чтобы право Евросоюза или право государства-члена определяло цель обработки. Более того, такое право может уточнять общие условия настоящего Регламента, определяя правомерность обработки персональных данных, может устанавливать функциональные требования для определения контролёра, типы подлежащих обработке персональных данных, соответствующих субъектов данных, организации, которым персональные данные могут раскрываться, целевые ограничения, срок хранения и другие меры, обеспечения правомерности и справедливости обработки. Необходимо также, чтобы право Евросоюза или право государства-члена определяло, должен ли контролёр, выполняющий задачи осуществляемые в общественных интересах или должностные полномочия, быть органом власти, или быть иным физическим или юридическим лицом, которое руководствуется публичным правом, или, если это в интересах общества, действует для этих целей, включая основы жизнедеятельности, например, здравоохранение, социальная защита и управление медицинскими услугами, либо подчиняется частному праву, например, в качестве объединения лиц свободных профессий.

(46) Обработка персональных данных также должна считаться правомерной, когда необходимо защищать интерес, который критически важен для субъекта данных или иного физического лица. Обработка персональных данных, основанная на жизненно важном интересе другого физического лица, должна в принципе иметь место только, если она не может быть осуществлена на ином правовом основании. Некоторые виды обработки могут служить как важными причинами общественного интереса, так и жизненно важными интересами субъекта данных, например, когда обработка

необходима для гуманитарных целей, в том числе для мониторинга эпидемий и их распространения или в ситуациях чрезвычайных гуманитарных ситуаций, в частности, в ситуациях природных и техногенных катастроф.

(47) Законные интересы контролёра, включая контролёра, которому могут быть раскрыты персональные данные, или третьей стороны могут создать правовые основания для обработки, при условии, что они не имеют преимущественной силы над интересами или основными правами и свободами субъекта данных, с учётом разумных ожиданий субъектов данных, основанных на взаимоотношении с Контролёром. Такой законный интерес может иметь место, например, если между субъектом данных и контролёром существуют соответствующие отношения в ситуациях, когда субъект данных является клиентом или состоит на службе контролёра. В любом случае наличие законного интереса нуждается в тщательной оценке, в том числе относительно того, может ли субъект данных при сборе персональных данных разумно ожидать, что обработка будет осуществляться для указанной цели. Интересы и основные права субъекта данных могут, в частности, иметь преобладающую силу над интересом контролёра данных, если персональные данные обрабатываются в условиях, когда субъекты данных обоснованно не ожидают проведения последующей обработки. Так как законодатель обязан на уровне правового акта предусмотреть правовые основания для обработки персональных данных органами государственной власти, такое правовое основание не должно применяться в отношении обработки органами государственной власти при выполнении ими своих задач. Обработка персональных данных, необходимая в целях предотвращения мошенничества, также является законным интересом соответствующего контролёра данных. Обработка персональных данных в целях адресного маркетинга может рассматриваться в качестве обработки, служащей законному интересу.

(48) Контролёры, являющиеся частью группы компаний или учреждений, относящихся к центральному органу, могут иметь законный интерес, связанный с передачей персональных данных в рамках группы компаний для внутренних административных целей, включая обработку персональных данных клиентов и работников. Общие принципы передачи персональных данных в рамках группы компаний расположенному в третьей стране предприятию сохраняют свою силу.

(49) Обработка персональных данных органами государственной власти, центрами реагирования на компьютерные чрезвычайные происшествия (*CERTs*), центрами реагирования на инциденты, связанные с компьютерной безопасностью (*CSIRTs*), поставщиками сетей электронных коммуникаций и услуг, а также поставщиками технологий и услуг по обеспечению безопасности является законным интересом соответствующего контролёра данных в той мере, в какой она необходима и соразмерна а целям обеспечения сетевой и информационной безопасности, то есть способности сети или информационной системы противостоять, на заданном уровне

достоверности, случайным событиям, незаконным или преднамеренным действиям, которые компрометируют доступность, подлинность, целостность и конфиденциальность сохранённых или переданных персональных данных, а также безопасность соответствующих услуг, переданных через указанные сети или системы. Такой законный интерес может включать в себя, к примеру, предотвращение несанкционированного доступа к сетям электронных коммуникаций и распространение вредоносного кода, а также пресечение сетевых атак и угроз для компьютерных и электронных систем связи.

(50) Обработка персональных данных в целях, отличных от тех, для которых персональные данные первоначально собирались, должна быть разрешена только, если она соответствует целям, для которых персональные данные были изначально получены. В этом случае не требуется иное правовое основание, отдельное от того, посредством которого был разрешено осуществлять сбор персональных данных. Если обработка необходима для выполнения задачи в общественных интересах при осуществлении публичных полномочий, возложенных на контролёра, право Евросоюза или право государства-члена может предусмотреть и установить задачи и цели, в которых последующая обработка считается надлежащей и правомерной. Дальнейшая обработка для архивных целей в общественных интересах, в целях научного или исторического исследования или в статистических целях рассматривается в качестве надлежащей правомерной обработки. Правовое основание, предусмотренное правом Евросоюза или правом государства-члена для обработки персональных данных, может также предусматривать правовое основание для последующей обработки. Для того чтобы убедиться в том, соответствует ли цель дальнейшей обработки цели, для которой персональные данные были первоначально получены, Контролёр, после выполнения всех требований относительно законности первоначальной обработки, должен принять во внимание, в числе прочего, следующее: любую связь между указанными целями и целями запланированной дальнейшей обработки; контекст, в котором были получены персональные данные, в частности, разумные ожидания субъектов данных, основанные на отношении с контролёром, касающиеся их дальнейшего использования; характер персональных данных; последствия предполагаемой дальнейшей обработки для субъектов данных, и наличие соответствующих гарантий первоначальной и предполагаемой обработки.

В случае если субъект данных дал своё согласие или если обработка основана на праве Евросоюза или праве государства-члена, которое в демократическом обществе является необходимой и надлежащей мерой для защиты, в том числе, веских целей общественного интереса, необходимо разрешить контролёру дальнейшую обработку персональных данных независимо от согласования целей. В любом случае необходимо обеспечить применение принципов, предусмотренных настоящим Регламентом и, в частности, информирование субъекта данных об указанных других целях, а

также о его правах, в том числе о праве на возражение. Указания контролёра на возможные уголовно-наказуемые деяния или угрозы общественной безопасности и передача конкретных персональных данных в отдельных случаях или в нескольких случаях, связанных с одним и тем же уголовно-наказуемым деянием или угрозами общественной безопасности, компетентному органу, должны рассматриваться в качестве законного интереса контролёра. Однако такая передача в рамках законного интереса контролёра или последующая обработка персональных данных должны быть запрещены, если обработка не соответствует законным, профессиональным или иным обязательствам соблюдения конфиденциальности.

Персональные данные, которые по своей природе особенно чувствительны к основным правам и свободам, заслуживают особой защиты, в связи с тем, что контекст их обработки может создать значительные риски для основных прав и свобод

(51) Персональные данные, которые по своей природе особенно чувствительны к основным правам и свободам, заслуживают особой защиты, поскольку контекст их обработки может создать значительные риски для основных прав и свобод. Такие персональные данные должны включать в себя персональные данные, раскрывающие расовое и этническое происхождение, при этом использование термина «расовое происхождение» в настоящем Регламенте не означает, что Евросоюз поддерживает подходы, которые пытаются установить существование отдельных человеческих рас. Обработка фотографий не должна систематически считаться обработкой особых категорий персональных данных, так как они охвачены определением понятия «биометрические данные» только, когда они обрабатываются посредством специальных технических средств, позволяющих осуществить уникальную идентификацию или аутентичность физического лица. Такие персональные данные не должны обрабатываться за исключением случаев, когда обработка разрешена в конкретных случаях, предусмотренных настоящим Регламентом, принимая во внимание, что право государств-членов может установить конкретные положения о защите данных, чтобы адаптировать применение норм Регламента в отношении соблюдения правовых обязательств или выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролёра. В дополнение к конкретным требованиям для указанной обработки должны применяться общие принципы и иные положения настоящего Регламента, в том числе, относительно условий правомерности обработки. Изъятия из общего запрета на обработку таких особых категорий персональных данных должны быть чётко предусмотрены, в том числе когда субъект данных даёт своё явное согласие или в отношении конкретных потребностей, в частности, когда обработка осуществляется в ходе правомерной деятельность конкретных ассоциаций или фондов, целью которых является обеспечение осуществления основных свобод.

(52) Изъятия из запрета на обработку особых категорий персональных данных также должны быть разрешены, если они предусмотрены в праве Евросоюза или праве государства-члена и обладают надлежащим гарантиями защиты персональных данных и других основных прав, если это оправдано с точки зрения общественного интереса, в частности, в отношении обработки персональных данных в области трудового права, права социальной защиты, включая пенсии, и в целях обеспечения безопасности, мониторинга здоровья и предупреждения заболеваний, профилактики или борьбы с инфекционными заболеваниями и других серьёзных угроз здоровью. Такое изъятие может быть сделано для целей здравоохранения, включая здравоохранение и управление медицинскими услугами, особенно в целях гарантии качества и экономической эффективности методов, используемых для урегулирования претензий в системе медицинского страхования, или для архивных целей в интересах общества, для научных или исторических исследований или для статистических целей. Изъятие также может быть сделано для обработки персональных данных, необходимой для обоснования, исполнения или оспаривания исковых требований, в рамках судебной процедуры или в рамках административных или внесудебной процедур.

(53) Особые категории персональных данных, которые требуют более высокой степени защиты, должны обрабатываться в целях, связанных со здоровьем, только если это необходимо для достижения целей в интересах физических лиц или общества в целом, в том числе, в контексте управления медицинскими или социальными услугами и системами, включая обработку таких данных центральными национальными органами здравоохранения в целях контроля качества, информации управления и общего национального и местного надзора за системой медицинского и социального обслуживания и в целях обеспечения непрерывности медицинского обслуживания или социального обеспечения, а также трансграничного медицинского обслуживания, или в целях обеспечения безопасности, мониторинга здоровья и профилактики заболеваний, или в архивных целях в общественных интересах, в целях научного или исторического исследования, или в статистических целях, на основании права Евросоюза или права государства-члена, которое должно соответствовать цели общественного интереса, равно и в отношении исследований, проводимых в области общественного здравоохранения в общественных интересах. Вследствие этого, настоящий Регламент должен предусмотреть гармонизированные условия для обработки особых категорий персональных данных, связанных со здоровьем, в отношении особых потребностей, в частности, если обработка данных осуществляется в конкретных, связанных со здоровьем, целях лицами, которые несут юридические обязательства о соблюдении профессиональной тайны. Право Евросоюза или право государства-члена должно предусматривать конкретные и приемлемые меры для защиты основных прав и персональных данных физических лиц. Государства-члены могут сохранять или утверждать дополнительные условия, в том числе

ограничения, в отношении обработки генетических данных, биометрических данных или данных, касающихся здоровья. Однако это не должно препятствовать свободному перемещению персональных данных в Евросоюзе, если указанные условия применяются в отношении трансграничной обработки этих данных.

(54) По причинам общественного интереса в областях общественного здравоохранения может быть необходимо проведение обработки особых категорий персональных данных без согласия субъекта данных. Указанная обработка должна осуществляться в соответствии с приемлемыми и конкретными мерами по защите прав и свобод физических лиц. В указанном контексте понятие «общественное здравоохранение» должно пониматься в значении Регламента (ЕС) 1338/2008 Европейского Парламента и Совета ЕС[36] и включать в себя все элементы, связанные со здоровьем, а именно: состояние здоровья, в том числе заболеваемость и нетрудоспособность, факторы, влияющие на состояние здоровья, потребности в медицинском обслуживании, ресурсы, отнесённые к медицинскому обслуживанию, предоставление и универсальный доступ к медицинскому обслуживанию, а также соответствующие расходы и финансирование и причины смертности. Указанная обработка данных, касающихся здоровья, по причинам общественного интереса не должна приводить к тому, что персональные данные будут обрабатываться в других целях третьей стороной, например работодателями или страховыми и банковскими компаниями.

(55) Вместе с тем, обработка персональных данных официальными органами для достижения целей, предусмотренных конституционным правом или международным публичным правом цели официально признанных религиозных организаций осуществляется по основаниям общественного интереса.

(56) В случае если в ходе предвыборной деятельности функционирование демократической системы в государстве-члене требует того, чтобы политические партии собирали персональные данные о политических взглядах лиц, обработка указанных данных может быть разрешена по основаниям общественного интереса, при условии наличия соответствующих гарантий.

(57) Если персональные данные, обрабатываемые контролёром, не позволяют ему идентифицировать физическое лицо, контролёр данных не обязан стремиться получить дополнительную информацию для идентификации субъекта данных с единственной целью соблюдения любого положения настоящего Регламента. Однако контролёр не должен отказываться принять дополнительную информацию, предоставляемую субъектом данных в целях содействия осуществлению своих прав.

[36] Регламент (ЕС) 1338/2008 Европейского Парламента и Совета от 16 декабря 2008 г. о статистике Сообщества в отношении общественного здравоохранения и безопасности на рабочих местах (Официальный Журнал Европейского Союза № L 354, 31.12.2008, С. 70). *Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70)*

Идентификация должна включать в себя цифровую идентификацию субъекта данных, например, посредством механизма аутентификации, такой как те же учётные данные, которые используются субъектом данных для входа под своим логином в онлайновую службу, предоставляемую контролёром данных.

(58) Принцип прозрачности требует, чтобы любая информация, адресованная общественности или субъекту данных, была краткой, легко доступной и понятной, а также чтобы использовался ясный и простой язык и дополнительно, в случаях необходимости, использовались визуальные элементы. Эта информация может предоставляться в электронной форме, например, если она адресована общественности, на интернет-сайте. Это имеет существенное значение в ситуациях, когда вследствие большого количества участников и сложности необходимой техники субъекты данных не могут узнать и понять, кем и для каких целей относящиеся к ним персональные данные собираются, например, в случае рекламы в интернете. Учитывая, что дети требуют особой защиты, любая информация и сообщения, если обработка адресована ребёнку, должны быть составлены на ясном, простом и понятном ребёнку языке.

(59) Должны быть предусмотрены условия для содействия осуществления прав субъекта данных на основании настоящего Регламента, включая механизмы для запроса и, когда это применимо, бесплатно получать, в частности, доступ и исправление или удаление персональных данных и осуществление права на возражение. Контролёр также должен предусмотреть средства для электронного запроса, особенно, если персональные данные обрабатываются электронным способом. На контролёра должна быть возложена обязанность без неоправданных задержек и как минимум в течение одного месяца ответить на запросы субъекта данных и, указать причины, если контролёр не намерен удовлетворить любой такой запрос.

(60) Принципы справедливой и прозрачной обработки требуют, чтобы субъект данных был проинформирован о наличии процесса обработки и его целях. Контролёр должен предоставить субъекту данных всю дополнительную информацию, необходимую для обеспечения справедливой и прозрачной обработки, принимая во внимание конкретные обстоятельства и условия при которых обрабатываются данные. Кроме того, субъект данных должен быть проинформирован о составлении профиля и последствиях такого составления профиля. Если персональные данные получены от субъекта данных, он также должен быть проинформирован о том, обязан ли он предоставлять персональные данные, а также о последствиях их непредставления. Указанная информация может предоставляться совместно со стандартизированными графическими обозначениями, для того чтобы в ясно видимой, понятной и чёткой форме дать общее представление о предполагаемой обработке. Если графические обозначения представлены в электронной форме, они должны быть машиночитаемы.

(61) Информация относительно обработки персональных данных, относящихся к субъекту данных, должна быть предоставлена ему/ей момент сбора у субъекта данных или, если персональные данные получены из других источников, в разумный срок, в зависимости от обстоятельств дела. Если персональные данные могут быть на законных основаниях раскрыты другому получателю, субъект данных должен быть проинформирован, если персональные данные впервые раскрываются получателю. Если контролёр намерен обрабатывать персональные данные в целях, отличных от целей, для которых они собирались, он до начала обработки должен представить субъекту данных информацию относительно такой другой цели, а также иную необходимую информацию. Если информация о происхождении персональных данных не может быть предоставлена субъекту данных вследствие использования разнообразных ресурсов, должна быть предоставлена общая информация.

(62) Однако, нет необходимости налагать обязанность предоставлять информацию, если субъект данных уже обладает информацией, в которой регистрация или раскрытие персональных данных прямо закреплена правом или когда предоставление информации субъекту данных оказывается невозможно или будет сопряжено с несоразмерными усилиями. Последнее, в частности, может иметь место, когда обработка осуществляется для архивных целей в общественных и интересах, для целей научных или исторических исследований или для статистических целей. В этой связи следует учитывать количество субъектов данных, возраст данных и любые соответствующие принятые гарантии.

(63) Субъект данных должен иметь право доступа к относящимся к нему/к ней собранным персональным данным, это право должно осуществляться беспрепятственно и с определённой периодичностью в целях получения информации об обработке и проверки правомерности обработки. Это охватывает право субъектов данных на доступ к данным, касающихся их здоровья, например, данным в их медицинских документах, содержащих следующую информацию: диагнозы, результаты обследований, наблюдения лечащих врачей и сведения о любом лечении или вмешательствах. Каждый субъект данных должен, поэтому иметь право знать и получать сведения в отношении целей, для которых обрабатываются персональные данные, по возможности, в отношении срока, в течение которого обрабатываются данные, получателей персональных данных, алгоритма схемы любой автоматизированной обработки персональных данных и последствий такой обработки, если она как минимум основана на составлении профиля. При наличии соответствующей возможности контролёр должен обеспечить удалённый доступ к защищённой системе, которая даст субъекту данных прямой доступ к его/ее персональным данным. Указанное право не должно отрицательно влиять на права или свободы иных лиц, включая коммерческую тайну или результаты интеллектуальной деятельности и, в частности, авторское право на программное обеспечение. При этом такие

ограничения не должны вести к отказу на предоставление всей информации субъекту данных. В том случае, когда контролёр обрабатывает большое количество информации, касающейся субъекта данных, он должен иметь возможность до передачи информации запросить субъекта данных уточнить информацию или вид обработки, к которому относится запрос.

(64) Контролёр должен использовать все приемлемые способы для того, чтобы проверить и подтвердить личность субъекта данных, который запрашивает доступ, в частности, в рамках онлайновых служб и в случае онлайновых идентификаторов. Контролёр не должен сохранять персональные данные только для реагирования на потенциальный запрос.

(65) Субъект данных должен иметь право на исправление относящихся к нему/ к ней персональных данных, а также «право на забвение», если сохранение указанных данных нарушает положения настоящего Регламента или право Евросоюза или право государства-члена, применимого к контролёру. В частности, субъект данных должен иметь право на удаление его/ее персональных данных и на то, чтобы его данные больше не обрабатывались, если в персональных данных относительно целей, для которых они собирались или иным образом обрабатывались, больше нет необходимости, если субъект данных отозвал его/ее согласие или возражает против обработки относящихся к нему/к ней персональных данных или если обработка персональных данных не соответствует настоящему Регламенту. Это право имеет существенное значение в случае, когда субъект данных давал его/ее согласие, будучи ребёнком, и полностью не мог осознавать риски, связанные с обработкой, а позже он хочет удалить персональные данные, особенно, в сети интернет. Субъект данных должен иметь возможность осуществлять такое право, невзирая на тот факт, что он больше не является ребёнком. Однако дальнейшее хранение персональных данных правомерно, если оно является необходимым для осуществления права на свободу выражения мнения и распространения информации, для соблюдения юридических обязательств, для выполнения задачи в общественных интересах или при осуществлении должностных полномочий предоставленных контролёру, по причинам общественного интереса в области социального здравоохранения, в архивных целях в общественных интересах, в целях научного или исторического исследования или в статистических целях, или для обоснования, исполнения или оспаривания исковых требований.

(66) Для того чтобы укрепить право на забвение в онлайн-среде, право на удаление данных также должно быть расширено таким образом, чтобы контролёр, который опубликовал персональные данные, был обязан проинформировать контролёров, которые обрабатывают указанные персональные данные, и удалить все ссылки, копии или дубликаты таких персональных данных. При этом этот контролёр должен принять соответствующие меры принимая во внимание имеющиеся технологические возможности и доступных средств, включая технические средства, чтобы

проинформировать о запросе субъекта данных контролёров, которые обрабатывают персональные данные.

(67) Методы, с помощью которых ограничивается обработка персональных данных, могут включать, среди прочего, временную передачу отдельных данных другой системе обработки, обеспечение недоступности отдельных персональных данных для пользователей или временное удаление опубликованных данных с интернет-сайта. В автоматизированных системах учёта ограничение обработки в принципе должно обеспечиваться техническими средствами таким образом, чтобы персональные данные не подвергались дальнейшей обработке и не могли быть изменены. Тот факт, что обработка персональных данных ограничена, должен быть ясно указан в системе (учёта).

(68) Для усиления контроля над его/ее в случае, когда обработка персональных данных осуществляется при помощи автоматизированных средств, субъект данных может также получить персональные данные, относящиеся к нему/к ней, которые он/она предоставил контролёру, в структурированном, широко используемом, машиночитаемом и функционально совместимом формате, и передать их другому контролёру. Контролёры данных должны усовершенствовать функционально совместимые форматы, чтобы способствовать переносимости данных. Такое право должно применяться, если субъект данных предоставил персональные данные на основании своего согласия или если обработка необходима для исполнения договора. Оно не применяется, если обработка осуществляется на правовом основании, не связанном с согласием или договором. По своему характеру такое право не должно осуществляться в отношении контролёров, обрабатывающих персональные данные при исполнении своих публичных обязанностей. Вследствие этого, оно не должно применяться, если обработка персональных данных необходима для соблюдения правового обязательства, применимого к контролёру, или для выполнения задачи в общественных интересах или при осуществлении должностных обязанностей контролёра. Право субъекта данных на передачу или получение относящихся к нему/к ней персональных данных не должно порождать обязательство для контролёров принимать или сохранять технически совместимые системы обработки. Когда, в рамках конкретного персональных данных, затронут более чем один субъект данных, право на получение персональных данных должно действовать без ущерба правам и свободам остальных субъектов данных в соответствии с настоящим Регламентом Кроме того, это право не должно наносить ущерб праву субъекта данных на удаление персональных данных и ограничений этого права, согласно настоящему Регламенту и, в частности, не должно означать удаление персональных данных, касающихся субъекта данных, которые были предоставлены им для выполнения договора в той степени, в какой и до тех пор, пока персональные данные необходимы для выполнения этого договора. контракта. В тех случаях, когда это

технически возможно, субъект данных должен иметь право передавать персональные данные напрямую от одного контролёра другому.

(69) В случае, когда персональные данные могут обрабатываться на законном основании поскольку обработка является необходимой для выполнения задачи в общественных интересах или при осуществлении должностных полномочий, возложенных на контролёра, или на основании законных интересов контролёра или третьей стороны, тем не менее, субъект данных должен иметь право на возражение против обработки любых персональных данных, относящихся к нему/к ней в конкретной ситуации. Контролёр должен доказать, что его законный интерес имеет преимущественную силу над интересами или основными правами и свободами субъекта данных.

(70) Когда персональные данные обрабатываются в целях прямого маркетинга, субъект данных должен иметь право на возражение против такой обработки, включая составление профиля, в той мере, в какой это связано с этим прямым маркетингом, будь то в отношении первоначальной или дальнейшей обработки, в любое время и на безвозмездной основе. Это право должно быть прямо доведено до сведения субъекта данных и представлено в чёткой форме и отдельно от любой иной информации.

(71) Субъект данных должен иметь право не подчиняться действию решения, которое может включать в себя меры по оценке личных аспектов, относящихся к нему/к ней, которая основана исключительно на автоматизированной обработке и которая порождает правовые последствия для него/неё или аналогичным образом существенно влияет на него/неё, например, автоматический отказ от онлайн-заявки на получение кредита или практики электронного найма персонала без какого-либо вмешательства человека. Такая обработка включает в себя составление профиля, состоящее из любой формы автоматизированной обработки персональных данных при оценке относящихся к физическому лицу персональных аспектов, в том числе, для анализа или прогнозирования аспектов, касающихся производственных показателей указанного лица, экономической ситуации, здоровья, индивидуальных предпочтений, интересов, надёжности, поведения, месторасположения или передвижения, если это порождает правовые последствия в отношении него/неё или аналогичным образом влияет на него/неё. Тем не менее, принятие решений, основанных на такой обработке, включая профилирование, должно быть разрешено там, где это прямо допустимо правом Евросоюза или правом государства-члена, которое применимо к контролёру, в том числе для целей мониторинга и предотвращения мошенничества и уклонения от уплаты налогов, проводимых в соответствии с правилами, стандартами и рекомендациями учреждений Евросоюза или национальных надзорных органов, а также обеспечения безопасности и надёжности услуг, предоставляемой контролёром, или если это необходимо для заключения или исполнения договора между субъектом данных и контролёром, или когда субъект данных

дал его/ее прямое согласие. В любом случае такая обработка должна осуществляться в соответствии с надлежащими гарантиями, включающими конкретное информирование субъекта данных и право на вмешательства человека, чтобы выразить свою точку зрения, получить объяснение решения, принятого после такой оценки, а также оспорить это решение. Такая мера не должна касаться ребёнка.

Для того чтобы обеспечить справедливую и прозрачную обработку в отношении субъекта данных, принимая во внимание конкретные обстоятельства и контекст, при которых обрабатываются персональные данные, контролёр должен использовать соответствующие математические и статистические методы для составления профиля, применять технические и организационные меры в целях обеспечения того, чтобы факторы, которые приводят к неточностям персональных данных, были исправлены, а риски возникновения ошибок минимизированы, защитить персональные данные таким образом, чтобы учесть потенциальные риски для интересов и прав субъекта данных и не допустить дискриминационного воздействия на физических лиц на основе расового или этнического происхождения, политических убеждений, религии и воззрений, членства в профессиональном союзе, генетических предрасположенностей, состояния здоровья или сексуальной ориентации, или не допустить принятия мер, которые могут иметь такое влияние. Автоматизированное принятие решений и составление профиля на основе конкретных категорий персональных данных допускается только в определённых условиях.

(72) Составление профиля должно соответствовать нормам настоящего Регламента, регулирующим обработку персональных данных, в том числе правовым снованиям обработки или принципам защиты данных. Европейский совет по защите данных (далее – «Совет»), учреждённый в соответствии с настоящим Регламентом, должен обладать возможностью издавать директивные указания в этом контексте.

(73) Ограничения в отношении конкретных принципов и прав на получение информации, доступа к данным и исправления персональных данных, права на переносимость данных, право на возражение, решения, основанные на составленном профиле, также как и сообщения о нарушении персональных данных субъекту данных и некоторые связанные с ними обязанности контролёров могут налагаться правом Евросоюза или государства-члена, насколько это необходимо и соразмерно в демократическом обществе для защиты общественной безопасности, включая защиту человеческой жизни, особенно в качестве ответной меры на стихийные бедствия и техногенный катастрофы, для обеспечения предотвращения и расследования преступлений и уголовного преследования или исполнения наказаний, включая предотвращение угроз общественной безопасности или нарушений этики для регулируемых профессий, для обеспечения других важных целей общественного интереса Евросоюза или

государства-члена, в частности важных экономических или финансовых интересов Евросоюза или государства-члена, ведение публичных реестров, хранящихся по соображениям общественного интереса, последующая обработка архивных персональных данных для предоставления конкретной информации, касающейся политического поведения в бывших тоталитарных государственных режимах или защиты субъекта данных или прав и свобод других лиц, включая социальную защиту, здравоохранение и гуманитарные цели. Указанные ограничения должны соответствовать требованиям, закреплённым в Хартии и в Европейской Конвенции о защите прав человека и основных свобод.

(74) Должна быть установлена ответственность и обязательства контролёра за любую обработку персональных данных, осуществляемую контролёром или от имени контролёра. В частности, контролёр должен быть обязан выполнять соответствующие и действенные меры и быть в состоянии продемонстрировать соответствие обработки данных настоящему Регламенту, включая эффективность этих мер. Такие меры должны учитывать характер, сферу применения, контекст и цели обработки и риск для прав и свобод физических лиц.

(75) Риск для прав и свобод физических лиц, разной степени вероятности и серьёзности, может быть результатом обработки персональных данных, которые могут привести к физическому, материальному или нематериальному ущербу, в том числе: когда обработка может привести к дискриминации, краже персональных данных или мошенничеству с персональными данными, финансовым потерям, ущербу для репутации, нарушению конфиденциальности персональных данных, находящихся под защитой профессиональной тайны, несанкционированной отмене псевдонимизации, или к иным неблагоприятным экономическим или социальным потерям; в случае, когда субъекты данных могут быть лишены своих прав и свобод или возможности осуществлять контроль над своими персональными данными; если обрабатываются персональные данные, которые раскрывают расовое или этническое происхождение, политические убеждения, религиозные и философские воззрения, членство в профессиональном союзе, а также генетические данные, данные, касающиеся здоровья или данные о половой жизни или уголовных судимостях и правонарушениях или соответствующих мерах безопасности; если оцениваются персональные аспекты, в частности, для анализа или прогнозирования аспектов, касающихся эффективности трудовой деятельности, экономической ситуации, здоровья, личных предпочтений, интересов, надёжности, поведения, местонахождения или передвижения, в целях создания или использования персональных профилей; когда обрабатываются персональные данные социально незащищённых физических лиц, в частности, детей; или когда обработка охватывает большое количество персональных данных и влияет на большое количество субъектов данных.

(76) Вероятность и серьёзность риска для прав и свобод субъекта данных должны определяться с учётом характера, сферы применения, контекста и целей обработки. Риск должен оцениваться на основе объективной оценки, с помощью которой устанавливается, связаны ли операции обработки данных с риском либо высоким риском.

(77) Руководства по имплементации соответствующих мер и по подтверждению соблюдения требований контролёром или обработчиком, особенно в отношении идентификации риска, связанного с обработкой, их оценки с точки зрения происхождения, характера, вероятности и серьёзности и определения передовой практики для смягчения риска, могут быть предоставлены, в частности, с помощью могут быть предоставлены, в том числе, в форме утверждённых кодексов поведения, утверждённых сертификатов, директивных указаний Совета или указаний инспектора по защите персональных данных. Совет может также издавать директивные указания по операциям обработки, которые вероятнее всего не ли могут привести к высокому риску прав и свобод физических лиц, а также и указать, какие меры могут быть достаточными в этих случаях для устранения такого риска.

(78) Защита прав и свобод физических лиц в отношении обработки персональных данных требует принятия надлежащих технических и организационных мер для того, чтобы требования настоящего Регламента были выполнены. В целях доказательства соблюдения настоящего Регламента, контролёр должен принять локальные нормативные акты и внутренние правила и осуществить меры, которые, в том числе, соответствуют принципам защиты данных для определённых целей/случаев (*by design*) и защиты данных по умолчанию (*by default*)[37]. Такие меры могут включать, среди прочего, своевременно минимизацию обработки персональных данных, псевдонимизацию персональных данных при появлении возможности, прозрачность применительно к методам и обработке персональных данных, позволяющим субъекту данных осуществлять мониторинг обработки данных, позволяющих контролёру создавать и совершенствовать средства защиты. При разработке, проектировании, подборе и использовании приложений, услуг и товаров, которые основаны на обработке персональных данных, либо которые обрабатывают персональные данные для того, чтобы выполнить свои задачи, производители товаров, услуг и приложений должны учитывать право на защиту данных при разработке и проектировании таких товаров, услуг и приложений, а также, с учётом современного технологического развития, сделать все необходимое для того, чтобы контролёры и обработчики были в состоянии исполнять свои обязанности по защите данных. Принципы защиты данных для определённых целей/случаев и защиты данных по умолчанию, также должны учитываться применительно к публичным торгам.

[37] Прим. Переводчика: защита данных для определённых целей/случаев – *by design*; защита данных по умолчанию – *by default*.

(79) Защита прав и свобод субъектов данных, а равно ответственность и обязательства контролёров и обработчиков, также по мониторингу и мероприятиям надзорных органов, требует чёткого распределения обязанностей в соответствии с настоящим Регламентом, включая случаи, когда контролёр определяет цели и средства обработки совместно с другими контролёрами, либо когда обработка осуществляется от имени контролёра.

(80) Если контролёр или обработчик, не учреждённые в Евросоюзе, обрабатывают персональные данные находящихся в Евросоюзе субъектов данных и если их деятельность по обработке связана с предложением товаров и услуг этим субъектам данных в Евросоюзе, вне зависимости от того, требуется ли оплата от субъекта данных, либо связана с мониторингом их деятельности постольку, поскольку она осуществляется в Евросоюзе, контролёр или обработчик должны назначить представителя, за исключением случаев, когда обработка носит случайный характер, не включает в себя масштабную обработку конкретных категорий персональных данных, либо обработка персональных данных, связанных с уголовными приговорами и правонарушениями, едва ли обернётся рисками для прав и свобод физических лиц, с учётом характера, обстоятельств, сферы применения и целей обработки, или если контролёр является органом или учреждением государственной власти. Представитель должен действовать от имени контролёра или обработчика, и может рассматриваться любым надзорным органом. Представитель должен быть специально уполномочен, посредством письменного предписания контролёра или обработчика, действовать от их имени в отношении их обязательств, вытекающих из настоящего Регламента. Назначение такого представителя не влияет на ответственность или обязанности контролёра или обработчика вытекающие из настоящего Регламента. Такой представитель должен выполнять свои задачи согласно предписанию, полученному от контролёра или обработчика, в том числе путём сотрудничества с компетентными надзорными органами в отношении любых действий, предпринятых в целях обеспечения соблюдения настоящего Регламента. Назначенный представитель подпадает под действие исполнительного производства в случае несоблюдения требований контролёром или обработчиком.

(81) Для обеспечения соблюдения требований настоящего Регламента в отношении обработки, осуществляемой обработчиком от имени контролёра, в случаях, когда на обработчика возложена деятельность по обработке, контролёр должен использовать обработчика, предоставляющего соответствующие гарантии, в частности, в отношении экспертной осведомлённости, добросовестности и источников информации, для того чтобы применять технические и организационные меры, которые будут отвечать требованиям настоящего Регламента, в том числе в отношении безопасности обработки. Следование обработчика утверждённым кодексам поведения или утверждённым механизмам сертификации, может быть использовано в качестве показателя для подтверждения соблюдения

обязанностей контролёра. Осуществление обработки обработчиком должно регулироваться договором, либо иным правовым актом вытекающим из права Евросоюза или государства-члена, которые возлагают обязательства на обработчика по отношению к контролёру, определяют содержание предмет и продолжительность обработки, характер и цели обработки, тип персональных данных и категории субъектов данных, принимая во внимание специфику задач и обязанностей обработчика в контексте осуществления обработки, а также риска для прав и свобод субъекта данных. Контролёр и обработчик могут выбрать использование самостоятельного договора или стандартных договорных условий, которые приняты либо Европейской Комиссией, или надзорным органом в соответствии с механизмом согласования, а затем утверждённые Европейской Комиссией. После завершения обработки от имени контролёра, обработчик должен, по выбору контролёра, возвратить или удалить персональные данные, за исключением случаев, когда существует требование о хранении персональных данных вытекающее из права Евросоюза или государства-члена, под действие которого подпадает обработчик.

(82) Для того чтобы подтвердить соблюдение настоящего Регламента, контролёр или обработчик должны вести **учёт деятельности по обработке,** осуществляемой под их ответственностью. Каждый Контролёр и обработчик обязаны сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение такие учётные сведения в целях мониторинга процесса обработки.

(83) Для того чтобы обеспечить безопасность и предотвратить обработку в нарушение настоящего Регламента, контролёр или обработчик должны оценить риски, связанные с обработкой, и использовать меры по снижению этих рисков, такие как криптографическая защита. Такие меры должны обеспечить соответствующий уровень защиты, в том числе конфиденциальности, принимая во внимание уровень развития техники и расходов на применение в отношении рисков, а также характер подлежащих защите персональных данных. При оценке риска для защиты данных необходимо уделить внимание рискам, имеющим место при обработке персональных данных, например, случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или несанкционированному доступу к переданным, сохранённым или иным образом обрабатываемым данным, которые могут привести к физическому, материальным или нематериальным потерям.

(84) В целях улучшения соблюдения положений настоящего Регламента, в случаях, когда возможными последствиями обработки данных являются риски высокой степени для прав и свобод физических лиц, контролёр должен нести ответственность за проведение оценки воздействия на защиту данных для того, чтобы определить, в частности, происхождение, характер, специфику и степень опасности такого риска. Результаты оценки должны приниматься во внимание при определении соответствующих мер, которые

необходимо принять для подтверждения того, что обработка персональных данных соответствует настоящему Регламенту. В тех случаях, когда оценка воздействия на защиты данных указывает на то, что обработка данных связана с высоким риском, который контролёр не может смягчить с помощью соответствующих мер с точки зрения имеющихся технологий и затрат на реализацию, перед обработкой следует проконсультироваться с надзорным органом.

(85) Утечка персональных данных, если она надлежащим образом и своевременно не была устранена, может привести к физическому, материальному или нематериальному ущербу для физических лиц, таким как утрата контроля над персональными данными или ограничение их прав, дискриминация, кража идентификационных данных или мошенничество с персональными данными, финансовые потери, несанкционированный отказ от псевдонимизации, ущерб репутации, нарушение конфиденциальности персональных данных, защищённых профессиональной тайной, или любые иные существенные экономические или социальные потери для соответствующих физических лиц. Поэтому, как только контролёру станет известно об утечке персональных данных, контролёр должен незамедлительно уведомить об утечке персональных данных надзорный орган, без неоправданной задержки и, когда это возможно, не позднее чем через 72 часа после того, как ему стало известно об этом, за исключением случаев, когда контролёр может доказать в соответствии с принципом подотчётности, что утечка персональных данных едва ли обернётся рисками для прав и свобод физических лиц. Если такое уведомление не может быть сделано в течение 72 часов, причины задержки должны быть указаны в уведомлении, а информация может предоставляться поэтапно без неоправданной дальнейшей задержки.

(86) Контролёр должен сообщить субъекту данных об утечке персональных данных без неоправданной задержки, когда когда возможными последствиями такой утечки персональных данных данных является риск высокой степени для прав и свобод физических лиц, с тем чтобы позволить ему/ей принять необходимые меры предосторожности. Это сообщение должно представить характер утечки персональных данных, а также рекомендации физическому лицу по снижению возможного негативного воздействия. Такой обмен сообщениями с субъектами данных должен быть осуществлён как можно разумнее оправданно и в тесном сотрудничестве с надзорным органом, с соблюдением директивных указаний, данных им, либо иными заинтересованными органами, среди которых правоохранительные органы. В частности, необходимость смягчить непосредственный риск ущерба потребует безотлагательной связи с субъектами данных, тогда как необходимость принятия соответствующих мер против продолжающейся или такой же утечки персональных данных может потребовать большего времени для взаимодействия.

(87) Следует выяснить, была ли использована вся соответствующая технологическая защита и организационные меры, чтобы незамедлительно установить утечку персональных данных, а также оперативно проинформировать надзорный орган и субъекта данных. Тот факт, что уведомление сделано без неоправданной задержки, должен быть установлен с учётом, в частности, характера и серьёзности утечки персональных данных, ее последствий, а также неблагоприятного воздействия на субъекта данных. Такое уведомление может привести к вмешательству надзорного органа в соответствии с его задачами и полномочиями, предусмотренными настоящим Регламентом.

(88) При установлении подробных правил, касающихся формата и процедур, применимых к уведомлению об утечке персональных данных, следует уделить должное внимание обстоятельствам такой утечки, в том числе независимо от того, были ли персональные данные защищены соответствующими мерами технической защиты, что фактически ограничивало вероятность мошенничества с персональными данными или иных форм злоупотреблений использования данных. Более того, такие правила и процедуры должны учитывать законные интересы правоохранительных органов, когда раннее раскрытие информации может воспрепятствовать расследованию обстоятельств утечки персональных данных.

(89) Директива 95/46/ЕС предусматривает общую обязанность по уведомлению надзорных органов об обработке персональных данных. Поскольку указанная обязанность связана с административной и финансовой нагрузкой, она не всегда содействовала улучшению защиты персональных данных. Поэтому такие неизбирательные общие обязательства по уведомлению должны быть отменены и заменены эффективными процедурами и механизмами, в которых основное внимание уделяется тем видам операций по переработке, которые могут привести к высокому риску прав и свобод физических лиц в силу их характера, сферы охвата, контекстом и целями. Такими видами операций обработки могут быть те, которые, в частности, связаны с использованием новых технологий или или которые сами являются новыми, и когда оценка воздействия защиты данных не проводилась ранее контролёром или если они необходимы с учётом времени, которое прошло с момента первоначальной обработки.

(90) В таких случаях оценка воздействия на защиту данных должна осуществляться контролёром до обработки данных с тем, чтобы оценить конкретную вероятность и серьёзность риска высокой степени, с учётом характера, сферы применения, контекста и целей обработки, а также источников риска. Эта оценка воздействия должна включать, в том числе, меры, гарантии и механизмы, предусмотренные для смягчения этого риска, обеспечивая защиту персональных данных и подтверждая соблюдение настоящего Регламента.

(91) Это должно, в частности, применяться при масштабной обработке данных, которая направлена на обработку значительного числа персональных данных на региональном, национальном или наднациональном уровне, и которая может повлиять на большое число субъектов данных, а также привести к высокой степени риска, к примеру, вследствие их уязвимости когда в соответствии с достигнутым уровнем технологических знаний используется новая технология в широких масштабах, и иная обработка данных приводит к высокому риску прав и свобод субъектов данных особенно в тех случаях, когда эта обработка затрудняет для субъектов данных осуществление своих прав. Оценка воздействия на защиту данных также должна проводиться там, где персональные данные обрабатываются для принятия решений относительно конкретных физических лиц после любой систематической и обширной оценки личных характеристик, связанных с физическим лицам на основе составленного профиля этих данных или после обработки отдельных категорий персональных данных, биометрических данных, либо данных об уголовных приговорах и преступлениях или о соответствующих мерах безопасности. Оценка воздействия на защиты данных в равной степени требуется для мониторинга широкомасштабных общедоступных сфер, особенно при применении оптико-электронных устройства, либо для любой иной деятельности, когда компетентный надзорный орган полагает, что обработка, вероятно, приведёт к высокой степени риска для прав и свобод субъектов данных, в частности потому, что они препятствуют субъектам данных использовать права, или услугу, или договор, либо потому, что обработка осуществляется систематически в широком масштабе. Обработка персональных данных не должна рассматриваться как масштабная, если обработка относится к персональным данным пациентов или клиентов и осуществляется лечащим врачом, иным медицинским работником или юристом. В этих случаях оценка воздействия на защиту данных не должна быть обязательной.

(92) Существуют обстоятельства, при которых может быть приемлемо и целесообразно с экономической точки зрения не относить оценку воздействия на защиту данных к конкретному проекту, например, когда органы государственной власти или учреждения намерены создать общую платформу приложений или обработки информации или если несколько контролёров планируют ввести общее применение или условие обработки для промышленном сектора, или сегмента, или для широкого использования в деятельности равноправных участников.

(93) В контексте применения права государства-члена, на основе которого орган государственной власти или частная организация осуществляют свои задачи и которое регулирует конкретный вид обработки или ряд соответствующих обработок, государства-члены могут счесть необходимым провести указанную оценку до осуществления обработки.

(94) В тех случаях, когда оценка воздействия на защиту данных указывает на то, что обработка при отсутствии гарантий, мер безопасности и механизмов для снижения риска приведёт к высокой степени риска для прав и свобод физических лиц, и контролёр считает, что риск не может быть смягчён разумными средствами с точки зрения доступных технологий и затрат по реализации, с надзорным органом следует проконсультироваться до начала действий по обработке. Такой высокий риск, вероятно, может быть связан с конкретными видами обработки, а также степенью и частотой обработки, что может также привести к возникновению ущерба или вмешательства в права и свободы физического лица. Надзорный орган должен ответить на запрос о проведении консультаций в течение установленного срока. Однако отсутствие ответа надзорного органа в течение установленного срока не должно наносить ущерба любому вмешательству надзорного органа в соответствии с его задачами и полномочиями, предусмотренными настоящим Регламентом, включая полномочия запретить обработку данных. В рамках этого процесса консультаций, результаты оценки воздействия на защиту данных, проводимые в отношении обрабатываемой информации, могут быть представлены надзорному органу, в частности меры, предусмотренные для смягчения риска для прав и свобод физических лиц.

(95) Обработчик должен оказывать содействие контролёру, когда это необходимо, а также по запросу, для обеспечения соблюдения обязательств, вытекающих из проведения оценки воздействия на защиту данных, и для соблюдения предварительной консультации надзорного органа.

(96) Консультация надзорного органа должна также иметь место в ходе подготовки законодательных или нормативно-правовых мер, которые предусматривают обработку персональных данных, чтобы обеспечить соответствие предполагаемой обработки настоящему Регламенту и, в частности, смягчить риск для субъекта данных.

(97) В случае, когда обработка осуществляется органом государственной власти, за исключением судов или независимых судебных органов, действующих в рамках своей судейской дееспособности, если в частном секторе, обработка осуществляется контролёром, целевая деятельность которого состоит в обработке, требующей регулярного и систематического мониторинга субъектов данных, или если целевая деятельность контролёра или обработчика состоит в масштабной обработке специальных категорий персональных данных и данных, связанных с уголовными приговорами и правонарушениями, лицо, обладающее экспертными знаниями в области права защиты персональных данных и практики, должно содействовать контролёру или обработчику в осуществлении внутреннего мониторинга для соблюдения настоящего Регламента. В частном секторе целевая деятельность контролёра относится к его основной деятельности и не относится к обработке персональных данных в качестве вспомогательного вида деятельности. Необходимый уровень экспертных знаний должен

определяться, в том числе, в соответствии с проведённой обработкой данных и требуемой защитой для персональных данных, обработанных контролёром или обработчиком. Инспекторы по защите персональных данных, вне зависимости от того, являются ли они работниками контролёра, должны быть в состоянии исполнять свои обязанности и задачи независимым образом.

(98) Ассоциации или иные органы, представляющие конкретные категории контролёров или обработчиков, могут в рамках настоящего Регламента разработать кодексы поведения для того, чтобы способствовать эффективному применению настоящего Регламента, учитывая при этом характеристики обработки, осуществляемой в конкретных секторах, и специфические потребности микро, малых и средних предприятий. В частности, такие кодексы поведения могут точно определять обязательства контролёров и обработчиков, принимая во внимание риск для прав и свобод физических лиц в результате обработки.

(99) При разработке кодексов поведения, при изменении или расширении таких кодексов, ассоциации и иные органы, представляющие конкретные категории контролёров или обработчиков, должны проконсультироваться с соответствующими стейкхолдерами, включая субъектов данных, при наличии возможности, и принять во внимание полученные при этом заключения и мнения.

(100) Для того чтобы повысить прозрачность и улучшить соблюдение настоящего Регламента, необходимо содействовать установлению сертификационных механизмов, а также печатей и маркировочных знаков о защите данных, которые позволят субъектам данных быстро оценить уровень защиты данных соответствующих товаров и услуг.

(101) Потоки персональных данных в страны за пределами Евросоюза и международные организации необходимы для расширения международной торговли и международного сотрудничества. Увеличение таких потоков вызвало новые проблемы и проблемы в отношении защиты персональных данных. Увеличение объёмов указанных потоков привело к новым вызовам и требованиям, связанным с защитой персональных данных. Однако, когда персональные данные передаются из Евросоюза контролёрам, обработчикам или иным получателям в третьих странах или в международные организации, уровень защиты физических лиц, гарантированный Евросоюзе настоящим Регламентом, не должен ослабляться, в том числе в случаях последующей передачи персональных данных из третьей страны или международной организации контролёрам, обработчикам в той же или другой третьей стране или международной организации. В любом случае передача данных третьим странам и международным организациям могут осуществляться только при полном соблюдении положения настоящего Регламента. Передача может иметь место только, если в соответствии с другими положениями настоящего Регламента, контролёр или обработчик соблюдает условия, предусмотренные положениями настоящего Регламента относительно передачи персональных данных третьим странам или международным организациям.

(102) Настоящий Регламент действует без ущерба международным соглашениям между Евросоюзом и третьими странами в отношении передачи персональных данных, в том числе соответствующие гарантии для субъектов данных. Государства-члены могут заключать международные соглашения, касающиеся передачи персональных данных третьим странам и международным организациям, в той части, в какой такие соглашения не влияют на настоящий Регламент либо на иные положения права Евросоюза, а также включают соответствующий уровень защиты основных прав субъектов данных.

(103) Комиссия может принять решение в отношении всего Союза о том, что третья страна, территория или особый сектор в третьей стране или международная организация предлагает адекватный уровень защиты данных, обеспечивая тем самым правовую определённость и единообразие на территории Евросоюзе в отношении третьей стране или международной организации, которая, как считается, обеспечивает такой уровень защиты. В таких случаях передача персональных данных в эту третью страну или международную организацию может осуществляться без необходимости получения какого-либо дополнительного разрешения. Европейская Комиссия может также отозвать такое решение, предоставив уведомление и полную информацию о причинах отмены, третьей стране или международной организации.

(104) В соответствии с основополагающими ценностями Евросоюза, к которым, в том числе, относится защита прав человека, Европейская Комиссия при оценке третьей страны или территории или особого сектора в третьей стране должна учитывать то, каким образом третья страна соблюдает принципы правового государства, обеспечивает доступность правосудия, так же как и соблюдает нормы и стандарты международного права прав человека, равно как и его общего и отраслевого законодательства, включая законодательство, касающегося общественной безопасности, обороны и национальной безопасности, наряду с публичным порядком и уголовным правом. При принятии решения о достаточности мер в отношении территории или особого сектора в третьей стране следует учитывать чёткие и объективные критерии, например, конкретный вид обработки и область применения правовых стандартов и действующего в третьей стране законодательства. Третья страна должна предоставить гарантии, обеспечивающие соответствующий уровень защиты, соразмерный уровню, гарантированному в Евросоюзе, в особенности, если персональные данные обрабатываются в одном или нескольких особых секторах. В частности, третья страна должна обеспечить эффективный независимый мониторинг защиты данных и должна предусматривать механизмы сотрудничества с органами защиты данных государств-членов Евросоюза по защите данных, а субъектам данных должны быть предоставлены действительные и подлежащие исполнению права, а также эффективные административные и судебные средства защиты.

(105) Наряду с международными обязательствами, которые приняла на себя третья страна или международная организация, Европейская Комиссия должна принять во внимание обязательства, возникающие вследствие участия третьей страны или международной организации в многосторонних или региональных системах, в частности, в отношении защиты персональных данных, а также исполнение таких обязательств. В частности, необходимо учесть присоединение третьей страны к Конвенции Совета Европы от 28 января 1981 г. о защите физических лиц при автоматизированной обработке персональных данных и к ее дополнительному протоколу. Европейская Комиссия должна проконсультироваться с Советом при оценке уровня защиты в третьих странах или международных организациях.

(106) Европейская Комиссия должна осуществлять мониторинг исполнения решений относительно уровня защиты в третьей стране, территории или особом секторе в третьей стране или в международной организации, а также осуществлять мониторинг исполнения решений, принятых в порядке Статьи 25 (6) или Статьи 26 (4) Директивы 95/46/ЕС. В своих решениях о достаточности мер Европейская Комиссия должна предусмотреть механизм периодической проверки их исполнения. Периодическая проверка должна проводиться по согласованию с третьей страной или международной организацией и учитывать все соответствующие изменения в третьей стране или международной организации. В целях мониторинга и осуществления периодических проверок Европейская Комиссия должна учитывать мнения и замечания Европейского Парламента и Европейского Совета, а также всех других соответствующих органов и источников. Европейская Комиссия в приемлемый срок должна оценить исполнение таких решений и направить отчёт со всеми соответствующими выводами Комитету, предусмотренному положениями Регламента (ЕС) 182/2011 Европейского Парламента и Европейского Совета ЕС[38] порядке, предусмотренным настоящим Регламентом, а также Европейскому Парламенту и Европейскому Совету.

(107) Европейская Комиссия может признать, что третья страна, территория или особый сектор в третьей стране или международная организация больше не гарантируют соответствующий уровень защиты данных. Следовательно, передача данных указанной третьей стране или международной организации должна быть запрещена кроме случаев, когда соблюдаются требования настоящего Регламента в отношении передачи данных в соответствии с надлежащими гарантиями, включая обязательные корпоративные правила, и изъятия в конкретных ситуациях. В этом случае следует предусмотреть консультации между Европейской Комиссией и

[38] Регламент (ЕС) 182/2011 Европейского Парламента и Совета от 16 февраля 2011 г., устанавливающий правила и общие принципы механизмов контроля со стороны государств-членов за осуществлением Европейской Комиссией имплементирующих полномочий (Официальный Журнал Европейского Союза № L 55, 28.02.2011, С. 13). *Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).*

такими третьими странами или международными организациями. Европейская Комиссия своевременно должна проинформировать третью страну или международную организацию о причинах и начать консультации для устранения возникших затруднений.

(108) При отсутствии решения о достаточности мер, контролёр или обработчик должны принять меры для уравновешивания недостаточности защиты данных в третьей стране посредством надлежащих гарантий для субъекта данных. Такие надлежащие гарантии могут включать в себя использование обязательных корпоративных правил, принятые Европейской Комиссией, стандартных условий по защите данных, принятые надзорным органом, стандартных условий по защите данных или договорных условий, утверждённые надзорным органом. Эти гарантии должны обеспечивать соблюдение требований защиты данных и прав субъектов данных, соответствующих обработке в рамках Евросоюза, включая наличие подлежащих исполнению прав субъекта данных и эффективных средств правовой защиты, в том числе права получения эффективного административного или судебного возмещения вреда, а также требования компенсации, в Евросоюзе или в третьей стране. Они должны относиться, в частности, к соблюдению общих принципов, связанных с обработкой персональных данных для определённых целей/случаев и по умолчанию. Передача данных может также осуществляться органами государственной власти, или учреждениями с органами государственной власти, или учреждениями в третьей стране, или с международными организациями с соответствующими обязанностями или функциями, в том числе на основе положений, которые должны быть включены в административные договорённости, такие как протокол о взаимопонимании, предусматривающий защищённые и эффективные права субъектов данных. Разрешение компетентного надзорного органа должно быть получено, если гарантии предусмотренные в административных договорённостях, не носят юридически обязательный характер.

(109) Возможность контролёра или обработчика использовать стандартные условия защиты данных, утверждённые Европейской Комиссией или надзорным органом, не должна служить препятствием контролёрам или обработчикам ни для включения стандартных условий защиты данных в более широкий договор, к примеру, такого как договор между обработчиком и иным обработчиком, ни для дополнения иными условиями, либо дополнительными гарантиями, при условии, что они прямо или косвенно не противоречат стандартным договорным условиям, утверждённым Европейской Комиссией или надзорным органом, или не противоречат основным правам и свободам субъектов данных. Контролёры или обработчики должны способствовать обеспечению дополнительных мер защиты посредством договорных обязательств, которые дополняют стандартные условия защиты.

(110) Группа компаний или группа предприятий, участвующих в совместной экономической деятельности, должна иметь возможность использовать утверждённые обязательные корпоративные правила для передачи своих данных из Евросоюза за границу организациям в рамках той же группы компаний или группы предприятий, участвующих в совместной экономической деятельности, при условии, что такие корпоративные правила включают в себя все ключевые принципы и права, обеспеченные исполнением для соблюдения соответствующей защиты передачи или категорий передачи персональных данных.

(111) Следует предусмотреть возможность передачи данных в конкретных обстоятельствах, когда субъект данных дал его/ее явное согласие, если передача является случайной и необходимой в отношении договора или судебного иска, независимо от того, происходит ли это в рамках в судебном порядке или в административной или иной внесудебной процедуре, включая процедуры в регулирующих органах. При определённых условиях необходимо предусмотреть возможность передачи данных, если субъект данных дал своё прямое согласие, если передача носит периодический характер и необходима в рамках договора или судебного иска, вне зависимости от того, происходит ли это в рамках судебной процедуры, административной или внесудебной процедуры, включая процедуру рассмотрения регулятивными органами. Следует также предусмотреть возможность для передачи данных, если этого требуют веские основания общественного интереса, предусмотренные правом Евросоюза или правом государства-члена, или когда передача осуществляется из реестра, предусмотренного законом и предназначена для ознакомления общественности или лиц, имеющих законный интерес. В последнем случае такая передача не должна затрагивать все персональные данные или категории данных, содержащиеся в реестре, и, когда реестр предназначен для ознакомления лиц, имеющих законный интерес, передача должна осуществляться только по запросу этих лиц или, если они являются получателями, необходимо полностью учитывать интересы и основные права субъекта данных.

(112) Такие изъятия, в том числе, должны применяться в отношении передачи данных, требуемых или необходимых по веским причинам общественного интереса, например, в случаях международного обмена данными между антимонопольными, налоговыми и таможенными органами, между органами финансового надзора, между службами, отвечающими за социальное обеспечение или социальное здравоохранение, к примеру, в случае отслеживания контактов при инфекционных заболеваниях или в целях сокращения и/или исключения допинга в спорте. Передача персональных данных также считается законной, если она необходима для защиты интереса, который имеет существенное значение для жизненно важных интересов субъекта данных или иного лица, включая физическую неприкосновенность или жизнь, если субъект данных не в состоянии дать

своё согласие. При отсутствии решения о достаточности мер, право Евросоюза или право государства-члена может по веским причинам общественного интереса прямо ограничить передачу особых категорий данных третьей стране или международной организации. Государства-члены должны уведомить об указанных положениях Европейскую Комиссию. Любая передача международной гуманитарной организации персональных данных субъекта данных, который физически или юридически не в состоянии дать своё согласие, в целях выполнения задачи, возложенной Женевскими Конвенциями, или в целях соблюдения международного гуманитарного права, применяемого в период вооружённых конфликтов, может рассматриваться в качестве необходимой для веских причин общественного интереса или вследствие того, что она относится к жизненно важному интересу субъекта данных.

(113) Передача, которая может быть квалифицирована как не носящая повторяющийся характер и которая касается только ограниченного числа субъектов данных, также может быть возможна в целях насущных законных интересов, которые преследует контролёр, если такие интересы не превалируют над интересами или правами, а также свободами субъекта данных, и когда контролёр оценил все обстоятельства, связанные с передачей данных. Контролёр должен уделить особое внимание характеру персональных данных, цели и продолжительности предлагаемой обработки или обработкам данных, в том числе и положение дел в стране происхождения, третьей стране и стране конечного пункта назначения, а также должен обеспечить надлежащие гарантии для защиты основных прав и свобод физических лиц в отношении обработки их персональных данных. Такая передача должна быть возможна только в крайних случаях, когда ни одно из других оснований для передачи не применимо. Для научных или исторических исследований, либо для статистических целей, правомерные ожидания общества относительно расширения знаний должны быть приняты во внимание. контролёр должен проинформировать надзорный орган и субъекта данных о передаче данных.

(114) В любом случае, когда Европейская Комиссия не приняла решения о надлежащем уровне защиты данных в третьей стране, контролёр или обработчик должны использовать решения, посредством которых субъектам данных предоставляются действенные и эффективные права в отношении обработки их персональных данных в Евросоюзе после передачи таких данных с тем, чтобы они продолжали пользоваться основными правами и гарантиями.

(115) Некоторые третьи страны принимают законы, нормативные акты и иные правовые акты, которые направлены на непосредственное регулирование обработки данных физическими и юридическими лицами, находящихся под юрисдикцией государств-членов. Это может включать в себя решения судов или трибуналов или решения административных органов в третьих странах, требующие от контролёра или обработчика передачи или

раскрытия персональных данных и которые не основаны на международном договоре, таком как договор о взаимной правовой помощи, действующий между запрашивающей третьей страной и Евросоюзом или государством-членом. запрашивая третью страну и Союз или государство-член. Экстерриториальное применение таких законов, нормативных актов и иных правовых актов, может нарушать международное право и может препятствовать защите физических лиц, гарантированной в Евросоюзе настоящим Регламентом. Передача данных должна быть разрешена только, при условии соблюдения положений настоящего Регламента, касающихся передачи данных третьим странам. Это может иметь место, в частности, в тех случаях, когда раскрытие информации необходимо по веским основаниям общественного интереса, признанного в праве Евросоюза или праве государства-члена, которое применяется к контролёру.

(116) В случае, когда персональные данные перемещаются за пределы Евросоюза, это может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в том числе, защитить себя от неправомерного использования или разглашения информации. В то же время надзорные органы могут быть не в состоянии рассмотреть жалобу или провести расследование в отношении деятельности, осуществляемой за пределами границ своего государства-члена. Их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или полномочиями, связанными с исправлением ситуации, противоречивым режимом правового регулирования, а также препятствиями практического характера, например, ограничением источников сведений. Вследствие этого существует необходимость содействовать тесному сотрудничеству между надзорными органами по защите персональных данных для того, чтобы они могли обмениваться информацией и проводить расследования с надзорными органами других стран. В целях разработки механизмов международного сотрудничества для содействия и обеспечения международной взаимной помощи при исполнении законодательства о защите персональных данных, Европейская Комиссия и надзорные органы должны обмениваться информацией и сотрудничать в рамках деятельности, которая связана с осуществлением их полномочий, с компетентными органами в третьих странах на основе взаимности и в соответствии с настоящим Регламентом.

(117) Учреждение надзорных органов в государствах-членах, наделённых правом осуществлять свои задачи, а также исполнять своих полномочия на основе полной самостоятельности, является существенным необходимым компонентом защиты физических лиц в отношении обработки их персональных данных. Государства-члены должны иметь возможность учреждать более одного надзорного органа, если это соответствует их конституционному, организационному и административному устройству.

(118) Самостоятельность надзорных органов не означает, что они не подлежат механизмам контроля или мониторинга в отношении их финансовых расходов или судебному надзору.

(119) В случае если государство-член учреждает несколько надзорных органов, оно должно установить правовые механизмы для обеспечения эффективного участия этих надзорных органов в механизме согласования. Это государство-член должно, в частности, назначить надзорный орган, который функционирует как единый контактный пункт для эффективного участия этих органов в механизме, чтобы обеспечить оперативное и бесперебойное сотрудничество с другими надзорными органами, Советом и Европейской Комиссией.

(120) Каждый надзорный орган должен быть обеспечен финансовыми и кадровыми ресурсами, помещениями и инфраструктурой, необходимой для эффективного выполнения своих задач, в том числе тех, которые связаны с взаимной помощью и сотрудничеством с другими надзорными органами в масштабах всего Евросоюза. Каждый надзорный орган должен иметь отдельный, открытый годовой бюджет, который может являться частью общего сводного или национального бюджета.

(121) Общие условия для члена или членов надзорного органа должны быть установлены правом каждого государства-члена и должны, в том числе, предусматривать, чтобы эти члены были назначены посредством прозрачной процедуры либо Парламентом, Правительством, либо главой государства-члена на основе предложения Правительства, члена Правительства, Парламента или Палаты Парламента или независимого органа, на который возложена ответственность в соответствии с правом государства-члена. Для того чтобы обеспечить самостоятельность надзорного органа, член или члены должны действовать добросовестно, воздерживаться от любых действий, несовместимых с их задачами, и не должны в течение срока действия полномочий участвовать в любой несовместимой деятельности на возмездной или безвозмездной основе. Надзорный орган должен обладать своим собственным персоналом, который выбран надзорным органом или самостоятельным органом, учреждённым в соответствии с правом государства-члена, и который должен подчиняться исключительно руководству члена или членов надзорного органа.

(122) обладать компетенцией на территории своего собственного государства-члена для осуществления полномочий и выполнения задач, возложенных на него в соответствии с настоящим Регламентом. Это должно охватывать, в том числе, обработку в контексте деятельности по учреждению контролёра или обработчика на территории его собственного государства-члена, обработку персональных данных, осуществляемых государственными органами или частными органами, действующими в общественных интересах, обработку затрагивающих субъекты данных на его территории или обработку, осуществляемую контроллером или обработку не учреждённых в Евросоюзе, когда целью являются субъекты данных,

проживающие на его территории. Это должно также включать рассмотрение жалоб, поданных субъектом данных, проведение рассмотрений по применению настоящего Регламента, а также содействие информированию общественности о рисках, правилах, гарантиях и правах в отношении обработки персональных данных.

(123) Надзорные органы должны осуществлять мониторинг применения положений настоящего Регламента и вносить свой вклад в его последовательное применение во всем Евросоюзе, для того, чтобы защитить физических лиц при обработке их персональных данных, а также того, чтобы содействовать свободному перемещению персональных данных в пределах внутреннего рынка. С этой целью надзорные органы должны сотрудничать друг с другом и с Европейской Комиссией без необходимости какого-либо соглашения между государствами-членами о предоставлении взаимной помощи или о таком сотрудничестве.

(124) В случае если обработка персональных данных осуществляется в рамках деятельности организаций контролёра или обработчика в Евросоюзе, а контролёр или обработчик учреждены в более чем одном государстве-члене, либо когда обработка, осуществляемая в контексте деятельности единственного учреждения контролёра или обработчика в Евросоюзе, существенно влияет или вероятно может существенно повлиять на субъектов данных в нескольких государствах-членах, надзорный орган для главного учреждения контролёра или обработчика, либо для единственного учреждения контролёра или обработчика, должен действовать как руководящий надзорный орган. Он должен сотрудничать с другими заинтересованными органами, поскольку контролёр или обработчик имеют учреждение на территории своего государства-члена, поскольку существенно затронуты субъекты данных, проживающие на их территории, оказывается существенное воздействие, или поскольку ему была подана жалоба. Кроме того, когда субъект данных, не проживающий в этом государстве-члене, подал жалобу, надзорный орган, в который была подана такая жалоба, должен также значиться как заинтересованный надзорный орган. В рамках своих задач, касающихся издания директивных указаний по любому вопросу, затрагивающих применение настоящего Регламента, Совет должен иметь возможность издавать директивные указания, в том числе, относительно критериев, которые должны быть приняты во внимание, с тем, чтобы выяснить, влияет ли обработка на субъектов данных в более чем одном государстве-члене, а также относительно того, что представляет собой соответствующее и мотивированное возражение.

(125) Руководящий орган должен обладать компетенцией принимать юридически обязательные решения в отношении мер, посредством которых осуществляются полномочия, предоставленные ему в соответствии с настоящим Регламентом. Как руководящий надзорный орган он должен содействовать привлечению заинтересованных надзорных органов к участию в процессе принятия решения, а также их координации. Если принимается

решение относительно полного или частичного отклонения жалобы субъекта данных, такое решение должно быть принято надзорным органом, в который была подана жалоба.

(126) Решение должно быть согласовано совместно руководящим надзорным органом и заинтересованными соответствующими надзорными органами и должно быть прямо адресовано **главному** или единственному учреждению контролёра или обработчика, а также носить обязательный характер для контролёра и обработчика. Контролёр или обработчик должны принять необходимые меры для обеспечения соблюдения настоящего Регламента и для применения решения, о котором руководящий надзорный орган уведомил главное учреждение контролёра или обработчика относительно обработки в Евросоюзе.

(127) Каждый надзорный орган, не действующий в качестве руководящего надзорного органа, должен обладать компетенцией на рассмотрение локальных случаев, когда контролёр или обработчик учреждены в нескольких государствах-членах, но предмет конкретной обработки относится только к обработке, осуществляемой в одном государстве-члене, и только субъектов данных в этом единственном государстве-члене, например, когда предмет касается обработки персональных данных сотрудников в конкретном контексте занятости государства-члена. В таких случаях надзорный орган должен незамедлительно проинформировать руководящий надзорный орган по этому вопросу. После получения соответствующей информации, руководящий надзорный орган должен решить, будет ли он рассматривать этот вопрос в соответствии с положениями о сотрудничестве между руководящим надзорным органом и заинтересованными надзорными органами («механизм единого окна»[39]) или надзорный орган, который его проинформировал, должен рассмотреть дело на локальном уровне. При решении вопроса относительно рассмотрения вопроса руководящий надзорный орган должен принять во внимание, находится ли учреждение контролёра или обработчика в государстве-члене надзорного органа, который его проинформировал, в целях гарантии эффективного исполнения решения в отношении контролёра или обработчика. Если руководящий надзорный орган решает рассматривать вопрос, проинформировавший его надзорный орган должен иметь возможность представить проект решения, который руководящий надзорный орган должен принять во внимание при подготовке своего проекта решения в рамках механизма единого окна.

(128) Положения о руководящем надзорном органе и о механизме единого окна не должны применяться, если обработка осуществляется органами государственной власти или частными организациями в общественных интересах. В указанных случаях единственным надзорным органом, компетентным осуществлять полномочия, предоставленные ему в соответствии с настоящим Регламентом, должен являться надзорный орган

[39] «*one-stop-shop mechanism*»

государства-члена, в котором учрежден орган государственной власти или частная организация.

(129) Для того чтобы обеспечить согласованный мониторинг и исполнение настоящего Регламента в Евросоюзе, надзорный орган в каждом государстве-члене должен иметь одинаковые задачи и осуществлять эффективные полномочия, в том числе полномочия по рассмотрению и полномочиям по устранению недостатков, полномочия наложения санкций, разрешительные и консультативные полномочия, в том числе, в случаях жалоб физических лиц, и без ущерба полномочиям органов уголовного следствия в соответствии с правом государства-члена довести до сведения судебных органов факт нарушения настоящего Регламента, а также участвовать в судебном процессе. Эти полномочия также должны включать в себя полномочие по установлению временного или окончательного ограничения на обработку, в том числе запрета. Государства-члены могут определить иные задачи, связанные с защитой персональных данных в порядке настоящего Регламента. Полномочия надзорных органов должны осуществляться беспристрастно, справедливо и в разумный срок в соответствии с процессуальными гарантиями, установленными в праве Евросоюза или праве государства-члена. В частности, каждая мера должна быть конкретной, необходимой и соразмерной с точки зрения обеспечения соблюдения настоящего Регламента, принимая во внимание обстоятельств каждого отдельного случая, уважать право каждого человека быть услышанным перед любыми индивидуальными мерами, которые могут повлиять на него/нее и не допускать излишних издержек и чрезмерных неудобств для соответствующих лиц. Следственные полномочия в отношении доступа к помещениям должны осуществляться в соответствии с конкретными требованиями процессуального права государства-члена, например, требованием получить предварительное судебное разрешение. Каждая юридически обязывающая мера надзорного органа должна быть составлена в письменной форме, быть чёткой и однозначной, указывать надзорный орган, который принял такую меру, дату принятия меры, иметь подпись руководителя или уполномоченного им члена надзорного органа, указание причин принятия этой меры, а также содержать ссылки на право эффективных средств правовой защиты. Это не должно исключать дополнительных требований в соответствии с процессуальным правом государства-члена. Принятие юридически обязывающего решения подразумевает, что оно может привести к судебному пересмотру в государстве-члене надзорного органа, принявшего решение.

(130) В случае если надзорный орган, в который была подана жалоба, не является руководящим надзорным органом, руководящий надзорный орган должен тесно сотрудничать с надзорным органом, в который была подана жалоба, в соответствии с положениями о сотрудничестве и согласовании, предусмотренными настоящим Регламентом. В этих случаях руководящий надзорный орган при принятии мер, которые должны привести к

юридическим последствиям, включая наложение административных штрафов, должен учесть мнение надзорного органа, которому была подана жалоба и который должен оставаться компетентным при осуществлении рассмотрения на территории его собственного государства-члена совместно с компетентным надзорным органом.

(131) В случае если другой надзорный орган должен выступать в качестве руководящего надзорного органа в отношении обработки контролёра или обработчика, но конкретный предмет жалобы или возможное нарушение касается только обработки контролёра или обработчиков государстве-члене, в котором жалоба была подана или было обнаружено возможное нарушение, а обстоятельство дела существенно не влияет или не должно влиять на субъекты данных в других государствах-членах, надзорный орган, в который подаётся жалоба или который установил или иным образом был проинформирован о ситуациях, которые влекут за собой возможные нарушения настоящего Регламента, должен приложить усилия для мирного разрешения споров с контролёром и, если это окажется безрезультатным, должен использовать все свои полномочия. Это должно включать в себя следующее: конкретную обработку на территории государства-члена надзорного органа или в отношении субъектов данных на территории указанного государства-члена; обработку в контексте предложения товаров или услуг, специально предназначенных для субъектов данных на территории государства-члена надзорного органа; или обработку, которая должна быть оценена с учётом соответствующих правовых обязательств в соответствии с правом государства-члена.

(132) Мероприятия по повышению информированности надзорных органов, адресованные общественности, должны включать конкретные меры, направленные на контролёров и обработчиков, включая микро, малые и средние предприятия, а также физических лиц, в частности в сфере образования.

(133) Надзорные органы должны оказывать друг другу содействие при выполнении своих задач и оказывать взаимную помощь, чтобы обеспечить согласованное применение и исполнение настоящего Регламента на внутреннем рынке. Надзорный орган, запросивший предоставление взаимной помощи, может принять временную меру, если он не получит ответ на свой запрос о взаимной помощи в течение одного месяца после получения указанного запроса другим надзорным органом.

(134) Каждый надзорный орган должен, при необходимости, участвовать в совместной деятельности с другими надзорными органами. Запрашиваемый надзорный орган обязан ответить на запрос в течение установленного периода времени.

(135) В целях обеспечения согласованного применения настоящего Регламента в масштабах Евросоюза должен быть установлен механизм согласования взаимодействия между надзорными органами. Этот механизм должен, в частности, применяться, в тех случаях, когда надзорный орган

намерен принять меру, предназначенную для создания правовых последствий в отношении обработки данных, которая существенно влияет на значительное число субъектов данных в нескольких государствах-членах. Он также должен применяться, в тех случаях, когда любой заинтересованный надзорный орган или Европейская Комиссия запрашивают рассмотрение такого вопроса в рамках механизма согласования. Этот механизм должен действовать без ущерба для любых мер, которые Европейская Комиссия может принять при осуществлении своих полномочий в соответствии с Договорами.

(136) При применении механизма согласования, Совет должен в течение установленного периода времени дать заключение, если большинство его членов примет такое решение, либо если это будет затребовано любым заинтересованным надзорным органом или Европейской Комиссией. Совет должен также обладать полномочием принимать решения, носящих юридически обязательный характер, если существуют разногласия между надзорными органами. Для этой цели он должен, по общему правилу большинством в две трети своих членов, принять решение, носящее юридически обязательный характер, в прямо установленных случаях, если существуют противоречивые точки зрения между надзорными органами, в частности, в рамках механизма сотрудничества между руководящим надзорным органом и заинтересованными надзорными органами по конкретным обстоятельствам дела, в том числе существуют ли нарушения настоящего Регламента.

(137) Может существовать острая необходимость действовать для защиты прав и свобод субъектов данных, в частности, если существует риск того, что принудительное обеспечение права субъекта данных может быть значительно затруднено. Поэтому надзорный орган должен иметь возможность принимать на своей территории надлежащим образом обоснованные временные меры с установленным сроком действия, который не должен превышать трёх месяцев.

(138) Применение такого механизма должно быть условием правомерности меры, предназначенной для осуществления юридических последствий надзорным органом в тех случаях, когда его применение является обязательным. В иных случаях трансграничной востребованности должен применяться механизм сотрудничества между руководящим надзорным органом и заинтересованными надзорными органами, а также взаимная помощь и совместные операции между соответствующими контролирующими органами на двусторонней или многосторонней основе без инициирования механизма согласования.

(139) Для того, чтобы обеспечить согласованное применение настоящего Регламента Совет должен быть учреждён в качестве самостоятельного органа Евросоюза. Для достижения своей цели Совет должен обладать правосубъектностью. Совет должен быть представлен Президиумом. Он заменяет Рабочую группу по защите физических лиц при обработке

персональных данных, учреждённую согласно Директиве 95/46/ЕС. Он должен включать в себя главу надзорного органа каждого государства-члена, а также Европейского инспектора по защите данных или их представителей. Европейская Комиссия должна принимать участие в деятельности Совета без права голоса, а Европейский инспектор по защите данных должен обладать специальным правом голоса. Совет должен способствовать согласованному применению настоящего Регламента в Евросоюзе, в том числе посредством консультирования Европейской Комиссии, в частности, в отношении уровня защиты в третьих странах или международных организациях, а также посредством содействия сотрудничеству надзорных органов в Евросоюзе. Совет должен действовать самостоятельно при осуществлении своих задач.

(140) Совету должен оказывать помощь секретариат, представленный Европейским инспектором по защите данных. Персонал Европейского инспектора по защите данных, который участвует в осуществлении задач, возложенных на Совет настоящим Регламентом, должны выполнять свои задачи исключительно по указанию Президиума Совета и подчиняться ему, а также должен предоставлять ему отчёты.

(141) Каждый субъект данных должен иметь право подать жалобу в один надзорный орган, в частности в государстве-члене его обычного места жительства, а также право на эффективные средства судебной защиты в соответствии со статьёй 47 Хартии, если субъект данных считает, что его/ее права на основании настоящего Регламента нарушены или когда надзорный орган не действует по жалобе, частично или полностью отклоняет жалобу или отказывает в ее удовлетворении, или не действует, когда такая мера необходима для защиты прав субъекта данных. Рассмотрение по жалобе должно проводиться при условии судебного пересмотра в той мере, в какой это уместно в конкретном случае. Надзорный орган в приемлемый срок должен проинформировать субъекта данных о ходе и результатах рассмотрения жалобы. Если дело требует дальнейшего расследования или сотрудничества с другим надзорным органом, субъекту данных должна быть представлена промежуточная информация. В целях содействия рассмотрению жалобы каждый надзорный орган должен принять такие меры, как предоставление формы жалобы, которая может быть заполнена электронным способом, не исключая других средств связи.

(142) В том случае, когда субъект данных считает, что его/ее права по настоящему Регламенту нарушены, он/она вправе передать некоммерческому органу, организации или объединению, которые были образованы в соответствии с правом государства-члена, имеют уставные задачи в сфере общественного интереса, а также осуществляют деятельность в области защиты персональных данных, права подачи в надзорный орган жалобы от его/ее имени, осуществление прав на судебную защиту от имени субъектов данных или в случаях, предусмотренных правом государства-члена, осуществления прав на получение компенсации от имени субъектов данных. Государство-член может предусмотреть, что любой такой орган, организация

или объединение, независимо от поручения субъекта данных, имеет право подавать в указанном государстве-члене жалобу и реализовывать право на эффективное средство судебной защиты, если оно считает, что права субъектов данных были нарушены в результате обработки данных, которая нарушает настоящий Регламент. Такому органу, организации или объединению можно запретить требовать компенсацию от имени субъекта данных, независимо от поручения субъекта данных.

(143) Любое физическое или юридическое лицо имеет право подать иск о расторжении решений Совета в Европейском Суде на условиях, предусмотренных в Статьёй 263 Договора TFEU. В качестве адресатов таких решений соответствующие контролирующие органы, которые хотят оспорить их, должны подать иск в течение двух месяцев после уведомления об этом в соответствии со Статьёй 263 Договора TFEU. Если решения Совета прямо или косвенно относятся к контролёру, обработчику или истцу, последний может подать иск об аннулировании этих решений в течение двух месяцев после их публикации на веб-сайте Совета в соответствии со Статьёй 263 Договора TFEU. Без ущерба для такого права в соответствии со Статьёй 263 Договора TFEU каждое физическое или юридическое лицо должно иметь эффективное судебное средство правовой защиты в компетентном национальном суде против решения надзорного органа, который порождает юридические последствия для этого лица. Такое решение касается, в частности, осуществления полномочий по рассмотрению, полномочий **по** устранению недостатков и разрешительных полномочий надзорного органа или или отклонения жалобы или отказа в ее удовлетворении. Однако право на эффективные судебные средства правовой защиты не охватывает меры, принимаемые надзорными органами, которые не являются юридически обязательными, такие как его заключения или рекомендации. Судебное производство в отношении надзорного органа должно быть возбуждено в судах государства-члена, в котором учреждён надзорный орган, и должно осуществляться в соответствии с процессуальным правом этого государства-члена. Такие суды должны осуществлять юрисдикцию, которая должна включать в себя полномочия на изучение всех вопросов факта и права, относящихся к рассматриваемому ими спору.

(144) В случае если суд, начавший производство против решения надзорного органа, имеет основание полагать, что производство, касающееся той же самой обработки, например, того же самого предмета рассмотрения в отношении обработки одним и тем же контролёром или обработчиком, или тех же оснований для иска, возбуждено в компетентном суде в другом государстве-члене, он должен связаться с этим судом для того, чтобы подтвердить существование такого конкретного производства. Когда конкретного производство осуществляется в суде другого государства-члена, любой суд, рассматривающий дело позднее, может приостановить производство по делу или по заявлению одной из сторон может отказаться от юрисдикции в пользу суда, который первоначально стал рассматривать дело,

если указанный суд уполномочен рассматривать указанные дела и его право разрешает объединение производств дел. Производства считаются смежными, если они настолько тесно взаимосвязаны, что целесообразно рассмотреть их вместе, для того чтобы избежать риска принятия противоречащих друг другу решений в результате раздельных производств.

(145) В случае производства дела в отношении контролёра или обработчика истец может возбудить дело в судах государств-членов, в которых находится учреждение контролёра или обработчика или в которых проживает субъект данных, за исключением случаев, когда контролёр является органом государственной власти государства-члена, осуществляющего свои публичные полномочия.

(146) Контролёр или обработчик должны компенсировать любой ущерб, который лицо может понести в результате обработки, нарушающей настоящий Регламент. Контролёр или обработчик освобождается от ответственности, если он докажет, что он никоим образом не несёт ответственность за ущерб. Понятие ущерба должно широко толковаться в свете прецедентной практики Суд Справедливости[40] таким образом, чтобы полностью соответствовать целям настоящего Регламента. Это положение действует без ущерба любым искам о возмещении ущерба в результате нарушения других норм права Евросоюза или права государства-члена. Обработка, которая нарушает настоящий Регламент, также включает в себя обработку, которая нарушает подзаконные акты и имплементирующие акты, принятые в соответствии с настоящим Регламентом и с правом государства-члена для уточнения положений настоящего Регламента. Субъекты данных должны получить полную и эффективную компенсацию за понесённый ими ущерб. В случае если контролёры или обработчики участвуют в одной и той же обработке данных, каждый контролёр или обработчик должно нести ответственность за ущерб в целом. Однако если они в соответствии с правом государства-члена привлекаются к одному и тому же судебному процессу, компенсация может быть соразмерно распределена согласно ответственности каждого контролёра или обработчика за ущерб, причинённый обработкой, при условии гарантии полной и эффективной компенсации для понесшего ущерб субъекта данных. Любой контролёр или обработчик, которые заплатили полную компенсацию, может впоследствии обратиться в суд с регрессным требованием относительно других контролёров или обработчиков, участвовавших в одной и той же обработке.

(147) В тех случаях, когда в настоящем Регламенте содержатся конкретные правила о юрисдикции, в частности в отношении разбирательств, требующих судебных средств правовой защиты, включая компенсацию, против контролёра или обработчика, общие правила юрисдикции, такие как положения Регламента (ЕС) № 1215/2012 Европейского Парламента и

[40] *EU Court of Justice*

Совета[41] должны действовать без ущерба применению таких конкретных норм.

(148) Для того, чтобы усилить обязательность соблюдения норм настоящего Регламента, санкции, в том числе административные штрафы, должны налагаться за любое нарушение настоящего Регламента, в дополнение или вместо соответствующих мер, налагаемых надзорным органом согласно настоящему Регламенту. В случае если нарушение незначительное или если вероятное наложение штраф может повлечь несоразмерную нагрузку для физического лица, вместо штрафа может быть объявлен выговор. Однако следует принимать во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения нанесенного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролёра или обработчика, соблюдение кодексов поведения, а также любые иные отягчающие или смягчающие вину обстоятельства. Для назначения наказаний, в том числе для наложения административных штрафов, необходимо наличие соответствующих процессуальных гарантий в соответствии с общими принципами права Евросоюза и Хартии, включая эффективную судебную защиту и надлежащую правовую процедуру.

(149) Государства-члены могут устанавливать нормы об уголовном наказании за нарушение настоящего Регламента, включая нарушения национальных норм, принятых согласно и в соответствии настоящего Регламента. Указанные уголовные наказания могут также предусматривать лишение преимуществ, полученных вследствие нарушения настоящего Регламента. Однако наложение уголовных наказаний за нарушения указанных национальных норм и наложение административных штрафов не должны вести к нарушению принципа «не наказывать дважды за одно и то же» (*ne bis in idem*) в толковании Суда Справедливости.

(150) Для того чтобы гармонизировать и усилить воздействие административных наказаний за нарушения настоящего Регламента, каждый надзорный орган должен обладать полномочием налагать административные штрафы. В настоящем Регламенте должны быть указаны нарушения, а также верхние пределы и критерии для установления соответствующих административных штрафов, которые должны определяться компетентным надзорным органом в каждом конкретном случае, принимая во внимание все соответствующие обстоятельства конкретной ситуации, с учётом, в том числе, характера, тяжести и продолжительности нарушения и его последствий, а также мер, принятых для обеспечения соблюдения

[41] Регламент (ЕС) 1215/2012 Европейского Парламента и Совета ЕС от 12 декабря 2012 г. о юрисдикции, признании и исполнении судебных решений по гражданским и коммерческим делам (Официальный Журнал Европейского Парламента № L 351, 20.12.2012, С. 1). *Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).*

обязанностей, согласно настоящему Регламенту, равно как и для предотвращения или смягчения последствий нарушения. В случае, когда административные штрафы налагаются на хозяйствующих субъектов, для таких целей они должны являться компанией в значении Статей 101 и 102 Договора TFEU. Когда административные штрафы налагаются на физических лиц, которые не являются хозяйствующими субъектами, надзорный орган при определении соответствующего размера штрафа должен принять во внимание общий уровень дохода в государстве-члене, а также экономическую ситуацию физического лица. Для содействия согласованному применению административных штрафов также может использоваться механизм согласования. Государства-члены могут установить, подлежат ли надзорные органы административным штрафам и если да, то в какой мере. Наложение административного штрафа или выдача предупреждения не влияет на применение иных полномочий надзорных органов или иных санкций в рамках настоящего Регламента.

(151) Правовая система Дании и Эстонии не предусматривает административных штрафов, установленных настоящим Регламентом. Эти нормы об административных штрафах могут применяться таким образом, что в Дании штраф налагается компетентными национальными судами в качестве уголовной санкции, в Эстонии штраф налагается надзорным органом в рамках процедуры по делам о менее тяжких преступлениях (*мисдиминор*), при условии, что применение норм в указанных государствах-членах имеет воздействие, равноценное применению административных штрафов, налагаемых надзорными органами. Вследствие этого компетентные национальные суды должны учитывать рекомендации надзорного органа, инициировавшего наложение штрафа. В любом случае налагаемые штрафы должны быть эффективными, соразмерными и оказывать сдерживающее воздействие.

(152) В случае, когда настоящий Регламент не гармонизирует административные наказания или если это необходимо в других случаях, например, в случае серьёзных нарушений настоящего Регламента, государства-члены должны внедрить систему, которая предусматривает эффективные, соразмерные и оказывающие сдерживающее воздействие санкции. Характер таких санкций, уголовных или административных, должен определяться в соответствии с правом государства-члена.

(153) В праве государств-членов должно быть гармоничное согласование норм, регулирующие свободу выражения мнений и распространения информации, включая свободу журналистского, научного, художественного и/или литературного самовыражения, с правом на защиту персональных данных в соответствии с настоящим Регламентом. Обработка персональных данных только в публицистических целях или в целях научного, художественного или литературного самовыражения должна быть предметом изъятия или исключению из конкретных положений настоящего Регламента, если это необходимо для того, чтобы сочетать право на защиту

персональных данных со свободой выражения мнений и распространения информации в соответствии со Статьёй 11 Хартии. Это положение должно применяться, в частности, в отношении обработки персональных данных в аудиовизуальной сфере, а также в архивах новостей и в библиотеках прессы. Вследствие этого, государства-члены должны принять законодательные меры, регулирующие изъятия и исключения, необходимые для целей гармоничного сочетания обозначенных основных прав. Государства-члены должны принять такие изъятия и исключения в отношении общих принципов, прав субъектов данных, контролёра и обработчика, передачи персональных данных третьим странам или международным организациям, самостоятельных надзорных органов, сотрудничества и согласования, а также конкретных ситуаций обработки данных. Если эти изъятия или исключения отличаются в одном государстве-члене и в другом государстве-члене, должно применяться право государства-члена, применимого к контролёру. Для того чтобы учесть важность права на свободу выражения мнения в каждом демократическом обществе, необходимо толковать категории, относящиеся к такой свободе, такие как журнализм, в широком смысле.

(154) Настоящий Регламент предусматривает принцип доступа общественности к официальным документам при применении настоящего Регламента. Доступ общественности к официальным документам может рассматриваться в качества общественного интереса. Персональные данные в документах, которые находятся в распоряжении органов государственной власти или учреждений, должны быть опубликованы указанными органами или учреждениями, если раскрытие информации предусмотрено правом Евросоюза или правом государства-члена, применимого к органу государственной власти или учреждению. Такое право должно согласовывать доступ общественности к официальным документам и повторное использование государственной информации с правом на защиту персональных данных и вследствие этого может предусмотреть необходимое согласование с правом на защиту персональных данных согласно настоящему Регламенту. Ссылка на органы государственной власти и учреждения должна включать в себя в этом контексте все органы или иные учреждения, подпадающие под действие права государства-члена о доступе общественности к документам. Директива 2003/98/ЕС Европейского Парламента и Совета[42] не затрагивает и никоим образом не влияет на уровень защиты физических лиц в отношении обработки персональных данных в рамках положений права Евросоюза или права государства-члена, а также, в частности, не изменяет обязанности и права, установленные в настоящем Регламенте. Так, эта Директива не применяется в отношении документов,

[42] Директива 2003/98/ЕС Европейского Парламента и Совета ЕС от 17 ноября 2003 г. о повторном использовании государственной информации (Официальный Журнал Европейского Союза № L 345, 31.12.2003, С. 90). *Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).*

доступ к которым исключён или ограничен в силу действия режимов доступа по причинам защиты персональных данных, или в отношении части документов, которые доступны в силу указанных режимов, если они содержат персональные данные, повторное использование которых предусмотрено правом, несовместимым с правом относительно защиты персональных данных при обработке персональных данных.

(155) В праве государства-члена или коллективных договорах, в том числе в «договорах о производстве работ», могут быть предусмотрены конкретные положения об обработке персональных данных работников при выполнении должностных обязанностей, в том числе условия, согласно которым персональные данные могут обрабатываться на основе согласия работника, в целях приёма на работу, выполнения трудового договора, включая исполнение обязательств, установленных в соответствии с законодательством или коллективным договором, в целях управления, планирования и организации работы, равноправия и многообразия на рабочем месте, охраны труда и производственной безопасности, а также в целях осуществления связанных с занятостью индивидуальных или коллективных прав и гарантий и в целях прекращения трудовых отношений.

(156) Обработка персональных данных для архивных целей в общественных интересах, для целей научного или исторического исследования, а также для статистических целей, должна подлежать соответствующим гарантиям для прав и свобод субъекта данных в соответствии с настоящим Регламентом. Эти гарантии должны обеспечить наличие технических и организационных мер, для того чтобы, в частности, гарантировать принцип минимизации данных. Последующая обработка персональных данных для архивных целей в общественных интересах, для целей научного или исторического исследования, а также для статистических целей, должна осуществляться, если контролёр оценил технические возможности для достижения указанных целей посредством обработки данных, при которой невозможно провести идентификацию субъектов данных, при условии, что имеются соответствующие гарантии (такие как, например, псевдонимизация данных). Государства-члены должны предусмотреть соответствующие гарантии для обработки персональных данных для архивных целей в общественных интересах, для целей научного или исторического исследования, а также для статистических целей. Государствам-членам должно быть разрешено предоставлять на конкретных условиях и при условии надлежащих гарантий для субъектов данных, уточнения и изъятия в отношении требований к информации, а также относительно прав на исправление, уничтожение, на забвение, ограничение обработки, на переносимость данных, на возражение, если персональные данные обрабатываются для архивных целей в общественных интересах, для целей научного или исторического исследования, а также для статистических целей. В рамках соответствующих условий и гарантий могут быть предусмотрены специальные процедуры для осуществления указанных прав

субъектами данных, если это соответствует целям особой обработки, в сочетании с техническими и организационными мерами, направленными на минимизацию обработки персональных данных согласно принципам пропорциональности и необходимости. Обработка персональных данных в научных целях должна также отвечать требованиям другого соответствующего законодательства, например, о клинических испытаниях.
(157) Сопоставляя информацию из реестров, исследователи могут получить новые сведения, имеющие большую ценность в отношении широко распространённых заболеваний, таких как сердечно-сосудистые заболевания, рак и депрессия. На основе реестров могут быть получены улучшенные результаты исследований, так как они основываются на большей части населения. В рамках социальных наук исследования на основе реестров позволяют исследователям получить существенные знания о долгосрочном соотношении ряда социальных условий, таких как безработица и образование с другими условиями жизни. Результаты исследований, полученные посредством реестров, обеспечивают надёжные, достоверные знания, которые могут служить основой для разработки и реализации политики, основанной на знаниях, улучшения качества жизни для ряда людей и повышения эффективности социальных услуг. Для облегчения научных исследований персональные данные могут обрабатываться в научных целях с учётом соответствующих условий и гарантий, установленных правом Евросоюза или правом государства-члена.

(158) Настоящий Регламент также применяется в отношении обработки персональных данных в архивных целях, необходимо учесть, что настоящий Регламент не применяется в отношении умерших лиц. Органы государственной власти, учреждения или частные организации, которые ведут учет общественного интереса, согласно праву Евросоюза или праву государства-члена несут правовую обязанность получать, сохранять, оценивать, классифицировать, описывать, сообщать, содействовать, распространять учетные сведения непреходящей ценности в общественных интересах, а также предоставлять к ним доступ. Государства-члены также вправе предусмотреть дальнейшую обработку персональных данных в архивных целях, например, в отношении представления специальной информации, относящейся к политическим действиям в прежних тоталитарных режимах, геноциду, преступлениям против человечества, в частности, Холокосту, или военным преступлениям.

(159) Настоящий Регламент также применяется в отношении обработки персональных данных в целях научного исследования. В рамках значения настоящего Регламента обработка персональных данных для целей научного исследования должна трактоваться более широко, в том числе, например, технологическое развитие и демонстрация, фундаментальные исследования, прикладные исследования и исследования, финансируемые из частных источников. Кроме того, также должена учитываться цель Евросоюза в

соответствии со Статьей 179 (1) Договора TFEU о создании Европейского исследовательского пространства.

Цели научного исследования также должны включать в себя исследования, проводимые в общественных интересах в сфере социального здравоохранения. Чтобы соответствовать специфике обработки персональных данных для целей научных исследований, должны применяться конкретные условия, в частности, в отношении публикации или иного раскрытия персональных данных в контексте целей научных исследований. Если результат научных исследований, в частности, в контексте здравоохранения, дает основания для осуществления дальнейших мер в интересах субъекта данных, общие положения настоящего Регламента должны применяться с учетом этих мер.

(160) Если личные данные обрабатываются для цели исторических исследований, настоящий Регламент также должен применяться к такой обработке. Это должно также охватывать историческое исследование и исследование в области генеалогии, с учетом того, что настоящий Регламент не применяется в отношении умерших лиц.

(161) В целях согласия на участие в научно-исследовательской деятельности в рамках клинических испытаний должны применяться соответствующие положения Регламента (ЕС) 536/2014 Европейского Парламента и Совета[43].

(162) Настоящий Регламент применяется в отношении обработки персональных данных в статистических целях. Право Евросоюза или право государства-члена в рамках настоящего Регламента должно определить статистический контент, контроль доступа, спецификации для обработки персональных данных в статистических целях и соответствующие меры для гарантии прав и свобод субъекта данных и для обеспечения статистической конфиденциальности. Под понятием «статистические цели» означают любую операцию по сбору и обработке персональных данных, необходимых для статистического изучения или для подготовки статистических результатов. Такие статистические результаты могут быть в дальнейшем использованы виных целях, в том числе в целях научного исследования. Статистическая цель подразумевает, что результатом обработки в статистических целях являются не персональные данные, а сводные данные, и что указанный результат или персональные данные не используются для обеспечения выполнения мер и решений, относящихся к любому конкретному физическому лицу.

(163) Конфиденциальная информация, которую национальные статистические органы и статистические органы Евросоюза собирают для подготовки официальной европейской и официальной национальной

[43] Регламент (ЕС) 536/2014 Европейского Парламента и Совета ЕС от 16 апреля 2014 г. о клинических испытаниях лекарственных средств, предназначенных для использования человеком, и об отмене Директивы 2001/20/ЕС (Официальный Журнал Европейского Союза № L 158, 27.05.2014, С. 1). *Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).*

статистики, должна находиться под защитой. Европейские статистические данные должны разрабатываться, подготавливаться и распространяться в соответствии со статистическими принципами, предусмотренными в Статье Договора TFEU, при этом национальная статистика также должна соответствовать праву государств-членов. Регламент (ЕС) № 223/2009 Европейского парламента и Совета[44] содержит дополнительные разъяснения относительно статистической конфиденциальности для европейской статистики.

(164) Относительно полномочий контролирующих органов по получению от контролёра или обработчика доступа к персональным данным и доступа к их помещениям, государства-члены могут принять на уровне законодательства в рамках настоящего Регламента конкретные правила для того, чтобы защитить обязанности относительно служебной тайны или иные равноценные обязанности о конфиденциальности в случае необходимости, в той мере, в какой это необходимо для согласования права на защиту персональных данных с обязанностью соблюдать служебную тайну. Это положение действует без ущерба существующим обязанностям государства-члена по принятию норм относительно соблюдения служебной тайны, если этого требует право Евросоюза.

(165) Настоящий Регламент соблюдает и не ограничивает статус, регламентированный действующим конституционным правом, церквей и религиозных организаций или общин в государствах-членах, в соответствии со Статьей 17 Договора TFEU.

(166) Для достижения целей настоящего Регламента, а именно защиты основных прав и свобод физических лиц и, в частности, их права на защиту персональных данных и обеспечения свободного перемещения персональных данных в Евросоюзе, полномочие по принятию актов в соответствии со Статей 290 Договора о Европейском Союзе должно быто делегировано Европейской Комиссии. При этом подзаконные акты должны приниматься в отношении критериев и требований для механизмов сертификации, механизмов, информации, представленной посредством стандартизированных графических обозначений, и процедур для предоставления указанных обозначений. Особое значение имеет то, что Европейская Комиссия осуществляет соответствующие консультации в ходе подготовительной работы, в том числе на экспертном уровне. При подготовке и принятии подзаконных актов Европейская Комиссия должна

[44] Регламент (ЕС) 223/2009 Европейского Парламента и Совета от 11 марта 2009 г. о Европейской статистике и об отмене Регламента (ЕС, Евратом) 1101/2008 Европейского Парламента и Совета о передаче данных при условии соблюдения их конфиденциальности Статистическому бюро Европейских Сообществ, Регламента (ЕС) 322/97 Совета о статистике Сообщества, а также Решения 89/382/ЕЭС Совета, Евратома об учреждении комитета по статистическим программам Европейских Сообществ (Официальный Журнал Европейского Союза № L 87, 31.03.2009, С. 164). *Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).*

гарантировать одновременную, своевременную и соответствующую передачу соответствующих документов Европейскому Парламенту и Европейскому Совету.

(167) Для того чтобы гарантировать единообразные условия применения настоящего Регламента, имплементирующие полномочия должны быть предоставлены Европейской Комиссии, если это предусмотрено настоящим Регламентом. Такие полномочия должны осуществляться в соответствии с Регламентом (ЕС) 182/2011. В рамках таких полномочий Европейская Комиссия должна рассмотреть особые меры в отношении микро, малых и средних предприятий.

(168) Процедура проверки должна использоваться для принятия имплементирующих актов относительно стандартных договорных условий между контролёрами и обработчиками, и между обработчиками; кодексов поведения; технических стандартов и механизмов сертификации; надлежащего уровня защиты, который предоставляется третьей страной, территорией или особым сектором в пределах этой третьей страны или международной организацией; стандартных условий о защите; форматов и процедур обмена информацией электронными средствами связи между контролёрами, обработчиками и надзорными органами по обязательным корпоративным правилам; взаимной помощи; а также договоренностей об обмене информацией электронными средствами связи между надзорными органами и между надзорными органами и Советом.

(169) Европейская Комиссия должна незамедлительно принять имплементирующие акты в случае, когда имеющиеся доказательства выявляют, что третья страна, территория или особый сектор в этой третьей стране или международная организация не обеспечивают надлежащий уровень защиты, а также когда этого требуют императивные основания настоятельной необходимости.

(170) Поскольку цель настоящего Регламента, а именно: обеспечение эквивалентного уровня защиты физических лиц и свободного перемещения персональных данных на территории Евросоюза, не может быть в достаточной степени достигнута государствами-членами, и, скорее, в силу масштаба или последствий воздействия, которые будут эффективнее достигнуты на уровне Евросоюза, Евросоюз может принять меры в соответствии с принципом субсидиарности, предусмотренный Статьей 5 Договора о Европейском союзе. Согласно принципу соразмерности, указанному в этой Статье, настоящий Регламент не выходит за пределы того, что необходимо для достижения этой цели.

(171) Директива 95/46/ЕС заменяется настоящим Регламентом. Обработка, уже осуществляемая на момент применения настоящего Регламента, должна быть приведена в соответствии с настоящим Регламентом в течение двух лет после его вступления в силу. Если обработка основана на согласии в соответствии с Директивой 95/46/ЕС, субъекту данных необязательно давать свое согласие снова, если способ, которым

было получено согласие, соответствует условиям настоящего Регламента, чтобы контролёр мог продолжить указанную обработку после даты применения настоящего Регламента. Решения Европейской Комиссии и разрешения надзорных органов, принятые на основе Директивы 95/46/ЕС, сохраняют свою силу до тех пор, пока они не будут изменены, заменены или отменены.

(172) В соответствии со Статьей 28 (2) Регламента (ЕС) 45/2001 была проведена консультация с Европейским инспектором по защите данных, и 7 марта 2012 г. он дал свое заключение[45].

(173) Настоящий Регламент применяется в отношении всех вопросов, связанных с защитой основных прав и свобод при обработке персональных данных, которые не подлежат обязательствам, предусмотренным Директивой 2002/58/ЕС Европейского Парламента и Совета[46] и преследующим одну и ту же цель, включая обязанности контролёра и права физических лиц. Для того чтобы уточнить соотношение между настоящим Регламентом и Директивой 2002/58/ЕС, в указанную Директиву необходимо внести соответствующие изменения. Как только настоящий Регламент будет принят, Директива 2002/58/ЕС должна быть пересмотрена для обеспечения соответствия с настоящим Регламентом,

приняли настоящий Регламент:

ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1

Предмет и цели

1. Настоящий Регламент устанавливает нормы, связанные с защитой физических лиц в отношении обработки персональных данных и нормы, касающиеся свободного перемещения персональных данных.

2. Настоящий Регламент защищает основные права и свободы физических лиц, и, в частности, их право на защиту персональных данных.

3. Свободное перемещение персональных данных в рамках Евросоюза не должно быть ни ограничено, ни запрещено для целей защиты физических лиц в отношении обработки персональных данных.

---

[45] Официальный Журнал Европейского Союза № C 192, 30.06.2012, С. 7. *OJ C 192, 30.6.2012, p. 7.*

[46] Директива 2002/58/ЕС Европейского Парламента и Совета ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) (Официальный Журнал Европейского Союза № L 201, 31.07.2002, С. 37). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).*

Статья 2

Существенная сфера применения

1. Настоящий Регламент применяется к обработке персональных данных обработанных полностью или частично автоматизированными средствами, а также к обработке персональных данных, обработанных иными неавтоматизированными средствами, которые являются частью системы учета либо неотъемлемой частью системы учета.

2. Настоящий Регламент не применяется к обработке персональных данных:

(a) в отношении деятельности, которая выходит за рамки сферы действия права Евросоюза;

(b) при осуществлении деятельности государств-членов, которая подпадает под действие Главы 2 Раздела V Договора о Европейском Союзе;

(c) физическим лицом при осуществлении сугубо личной или бытовой деятельности;

(d) компетентными органами в целях предотвращения, расследования, выявления уголовных преступлений или исполнения уголовных наказаний, включая защиту от угроз общественной безопасности и их предотвращения.

3. Для обработки персональных данных учреждениями, органами, организациями и агентствами Евросоюза применяется Регламент (ЕС) № 45/2001. Регламент (ЕС) № 45/2001, а иные нормативно-правовые акты Евросоюза, применимые к такой обработке персональных данных, в соответствии со Статьей 98 должны быть приведены в соответствие с принципами и нормами настоящего Регламента.

4. Настоящий Регламент действует без ущерба применению Директивы 2000/31/ЕС, в частности, норм об ответственности поставщиков посреднических услуг, предусмотренных Статьями 12-15 этой Директивы.

Статья 3

Территориальная сфера применения

1. Настоящий Регламент применяется к обработке персональных данных в контексте деятельности по учреждению контролёра или обработчика в Евросоюзе, независимо от того, осуществляется ли обработка в Евросоюзе, или нет.

2. Настоящий Регламент применяется к обработке персональных данных субъектов персональных данных, находящихся Евросоюзе, обработанных контролёром или обработчиком, которые не учреждены в Евросоюзе, когда деятельность по обработке связана с:

(a) предложением товаров или услуг, вне зависимости от того, требуется ли оплата от этого субъекта данных в Евросоюзе; или

(b) мониторингом их действий, поскольку их действия совершаются на территории Евросоюза.

3. Настоящий Регламент применяется в отношении обработки персональных данных контролёром, не учрежденном в Евросоюзе, а учрежденном в том месте, в котором применяется право государства-члена в силу международного публичного права.

Статья 4

Понятийно-терминологическая основа

Для целей настоящего Регламента:

(1) «персональные данные» (*personal data*) – означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо является лицом, которое может быть идентифицировано прямо или косвенно, в частности, на основе идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификатор в интернете (онлайн-идентификатор) или посредством одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица;

(2) «обработка» (*processing*) – означает любую операцию или набор операций, которые совершаются с персональными данными или набором персональных данных, с использованием автоматизированных средств и без таковых, в числе которых сбор, запись, организация, структурирование, хранение, переработка или изменение, поиск и выборка, экспертиза, использование, раскрытие посредством передачи, рассылка или иной способ предоставления для доступа, группировка или комбинирование, отбор, стирание или уничтожение;

(3) «ограничение обработки» (*restriction of processing*) – означает маркировку хранимых персональных данных в целях ограничения их обработки в будущем;

(4) «составление профиля» (*profiling*) – означает любую форму автоматизированной обработки персональных данных, включающих использование персональных данных, для оценки определенных персональных характеристик, относящихся к физическому лицу, в частности для анализа или прогнозированию аспектов, связанных с этим физическим, лицом в контексте его действий на рабочем месте, в

экономической ситуации, его состояния здоровья, личных предпочтений, интересов, надежности, поступков, местонахождения или передвижений;

(5) «псевдонимация» (*pseudonymisation*) – означает обработку персональных данных таким образом, что персональные данные не могут быть соотнесены с конкретным субъектом данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно и подпадает под технические и рганизационные меры, обеспечивающие то, что личные данные не могут быть соотнесены с идентифицированным или идентифицируемым физическим лицом;

(6) «система учета» (*filing system*) – означает любой структурированный набор персональных данных, который доступен в соответствии с конкретными критериями, независимо от централизации, децентрализации или распределения на функциональной или географической основе;

(7) «контролёр» (*controller*) – означает физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими, определяет цели и средства обработки персональных данных; в случае, когда цели и средства такой обработки определяются правом Евросоюза или государства-члена, контролёр, либо конкретные критерии для его выдвижения, могут быть предусмотрены правом Евросоюза или государства-члена;

(8) «обработчик» (*processor*) – означает физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени и по поручению контролёра;

(9) «получатель» (*recipient*) – означает физическое или юридическое лицо, государственный орган, агентство или иной орган, которым раскрываются персональные данные, независимо от того являются ли они третьими лицами или нет. Однако, органы государственной власти, которые могут получать персональные данные в рамках конкретного расследования в соответствии с правом Евросоюза или правом государства-члена, не должны рассматриваться в качестве получателей; обработка таких данных такими органами государственной власти должна соответствовать применимым нормам о защите данных в зависимости от целей обработки;

(10) «третье лицо» (*third party*) – означает физическое или юридическое лицо, государственный орган, агентство или иной орган, кроме субъекта данных, контролёра, обработчика, а также лиц, уполномоченных осуществлять обработку персональных данных под непосредственным руководством контролёра или обработчика;

(11) «согласие» (*consent*) – субъекта данных означает любое свободно

данное, конкретное, осознанное и однозначное идентифицируемое желание субъекта данных, посредством которого он/она путем заявления, либо ясным утвердительным действием, выражает согласие на обработку персональных данных, относящихся к нему/к ней;

(12) «утечка персональных данных» (*personal data breach*) – означает нарушение безопасности, приводящее к случайному или противозаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к персональным данным, переданных, хранящихся или обработанных иным образом;

(13) «генетические данные» (*genetic data*) – означают персональные данные, относящиеся к наследственным или приобретенным генетическим характеристикам физического лица, которые дают уникальную информацию о физиологии или здоровье этого физического лица, а также которые являются, в том числе, результатом анализа биологического образца этого физического лица;

(14) «биометрических данные» (*biometric data*) – означают персональные данные, полученные в результате конкретной технической обработки, относящейся к физическим, физиологическим или поведенческим характеристикам физического лица, которые позволяют подтвердить или подтверждают уникальную идентификацию этого физического лица, такие как изображение лица человека или дактилоскопические данные;

(15) «данные о здоровье» (*data concerning health*) – означают персональные данные, относящиеся к физическому или психическому здоровью физического лица, в том числе предоставление медицинских услуг, которые содержат информацию о его/ее состоянии здоровья;

(16) «главное учреждение» (*main establishment*) – означает:

(a) в отношении контролёра, имеющего организации в более чем одном государстве-члене, – месторасположение его центральной администрации в Евросоюзе, кроме тех случаев, когда решения о целях и способах обработки персональных данных принимаются иной организацией контролёра в Евросоюзе, и последняя организация вправе осуществлять такие решения, в этом случае, организацию, принимающую такие решения, следует рассматривать в качестве главного учреждения;

(b) в отношении обработчика, имеющего организации в более чем одном государстве-члене, – месторасположение его центральной администрации в Евросоюзе, либо, если обработчик не имеет

центральной администрации в Евросоюзе, организацию обработчика в Евросоюзе, в которой осуществляется основная деятельность по обработке, в контексте деятельности организации обработчика, в той степени, в какой обработчик подчиняется конкретным обязательствам по настоящему Регламенту;

(17) «представитель» (*representative*) – означает физическое или юридическое лицо, созданное в Евросоюзе, которое специально уполномочено в письменной форме контролёром или обработчиком, в соответствии со Статьей 27, и представляет контролёра или обработчика, в отношении их соответствующих обязательств, вытекающих из настоящего Регламента;

(18) «предприятие» (*enterprise*) – означает физическое или юридическое лицо, осуществляющее хозяйственную деятельность, независимо от его организационно-правовой формы, включая партнерства или ассоциации регулярно занимающиеся экономической деятельностью;

(19) «группа компаний» (*group of undertakings*) – означает контролирующую компанию и подконтрольные ей компании;

(20) «обязательные корпоративные правила» (*binding corporate rules*) – означают принципы и правила защиты персональных данных, обязательные к соблюдению контролёром и обработчиком, которые учреждены на территории государства-члена, связанные с передачей либо системой передачи персональных данных контролёру или обработчику в одной или нескольких третьих странах в рамках группы компаний предприятий или группы предприятий, осуществляющих совместную экономическую деятельность;

(21) «надзорный орган» (*supervisory authority*) – означает самостоятельный полномочный государственный орган, созданный в государстве-члене в соответствии со Статьей 51;

(22) «заинтересованный надзорный орган» (*supervisory authority concerned*) – означает орган власти, имеющий дело с обработкой персональных данных, в связи с тем, что:

(a) контролёр или обработчик учреждены на территории государства-члена данного надзорного органа;

(b) субъекты данных, проживающие в государстве-члене данного надзорного органа, могут быть существенно затронуты или вероятнее всего могут быть существенно затронуты обработкой данных; или

(c) жалоба была подана в данный надзорный орган;

(23) «трансграничная обработка» (*cross-border processing*) – означает либо:

(a) обработку персональных данных, которая имеет место в контексте

деятельности учреждений в более чем одном государстве-члене контролёра или обработчика в Евросоюзе, в случае, если этот контролёр или обработчик учреждены в более чем одном государстве-члене; или

(b) обработку персональных данных, которая имеет место в контексте деятельности единственного учреждения контролёра или обработчика в Евросоюзе, но которая существенно влияет или может существенно повлиять на субъектов данных в более чем одном государстве-члене;

(24) «соответствующее и мотивированное возражение»(*relevant and reasoned objection*) – означает возражение против проекта решения относительно того, существует ли нарушение настоящего Регламента, либо предусмотрено ли установленное настоящим Регламентом действие в отношении контролёра или обработчика, что наглядно демонстрирует значимость рисков, связанных с проектом решения в части основных прав и свобод субъектов данных и, где это применимо, свободного движения персональных данных в рамках Евросоюза;

(25) «услуга информационного общество» (*information society service*) – означает услугу, которая определена пунктом (b) статьи (1) of Директивы (ЕС) 2015/1535 Европейского Парламента и Совета ([19])[47];

(26) «международная организация» (*international organisation*) – означает организацию и ее вспомогательные органы, деятельность которых регулируется международным публичным правом, либо любой иной орган, созданный в соответствии или на основании соглашения между двумя или более странами.

ГЛАВА II.
ПРИНЦИПЫ

Статья 5

Принципы, связанные с обработкой персональных данных

1. Персональные данные должны:

(a) обрабатываться на законных основаниях, справедливым и открытым образом в отношении субъекта данных («правомерность,

[47] ([19]) Директива (ЕС) 2015/1535 Европейского Парламента и Совета ЕС от 9 сентября 2015 г. о процедуре предоставления информации в области технических регламентов, а также правил оказания услуг в информационном обществе. (Официальный Журнал Европейского Союза № L 241, 17.9.2015, С. 1) – *Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).*

справедливость и открытость/траспаренность» – *lawfulness, fairness and transparency*);

(b) собираться для конкретных, ясных и законных целей и не должны в дальнейшем обрабатываться способом, несовместим с этими целями; дальнейшая обработка для достижения целей общественного интереса, научных или исторических исследований, либо для статистических целей, в соответствии со статьей 89 (1), не должна рассматриваться в качестве несовместимой с первоначальными целями («целевое ограничение» – *purpose limitation*);

(c) быть достоверными, соответствующими, а также быть ограничены тем, что необходимо связано с целями, для которых они обрабатываются («минимизация данных» – *data minimisation*);

(d) быть точными и, при необходимости, обновленными; необходимо принимать обоснованные меры для обеспечения своевременного удаления или исправления неточных данных с учетом целей, для которых они были обработаны, были удалены или исправлены без задержки («точность» – *accuracy*);

(e) храниться в форме, которая позволяет идентифицировать субъектов данных, в течение срока, необходимого для целей, для которых персональные данные обработаны; персональные данные могут храниться в течение более длительного периода, если персональные данные будут обрабатываться исключительно в целях общественного интереса, научных или исторических исследований, либо для статистических целей, в соответствии со статьей 89 (1), с учетом применения соответствующих технических и организационных мер, требуемых в соответствии с настоящим Регламентом для защиты прав и свобод субъекта данных («ограничение хранения» – *storage limitation*);

(f) обрабатываться способом, обеспечивающим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери, повреждения или уничтожения, с использованием соответствующих технических и организационных мер («целостность и конфиденциальность» – *integrity and confidentiality*).

2. Контролёр несет ответственность и должен быть способен подтвердить соблюдение требований параграф 1 («подотчетность» – *accountability*).

Статья 6

Правомерность обработки

1. Обработка является правомерной, только если и постольку, поскольку применимо хотя бы одно из следующих условий:

(a) субъект данных дал согласие на обработку его/ее персональных данных для одной или нескольких конкретных целей;

(b) обработка необходима для исполнения договора, в котором субъект данных является одной из сторон, либо для принятия мер по требованию субъекта данных до заключения договора;

(c) обработка необходима для соблюдения правовых обязательств, субъектом которых является контролёр;

(d) обработка необходима для защиты жизненных интересов субъекта данных, либо иного физического лица;

(e) обработка необходима для выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролёра;

(f) обработка необходима для целей обеспечения законных интересов контролёра или третьего лица, за исключением случаев, когда такие интересы не принимают во внимание интересы или основные права и свободы субъекта данных, которые требуют защиты персональных данных, в частности, в случаях, когда субъектом данных является ребенок.

Пункт (f) первого подпараграфа не применяется в отношении обработки, осуществляемой органами власти при осуществлении ими своих задач.

2. Государства-члены могут обеспечивать или закреплять более конкретные положения для применения норм настоящего Регламента в отношении обработки на предмет соответствия пунктам (c) и (e) параграфа 1, путем более четкого определения конкретных требования к обработке, а также к иным мерам, для того, чтобы обеспечить правомерную и справедливую обработку, в том числе для других особых ситуаций обработки, предусмотренных в Главе IX.

3. Основания для обработки, указанные в пункте (c) и (e) параграфа 1, должны устанавливаться:

(a) правом Евросоюза; или

(b) правом государства-члена, которое применимо к контролёру.

Цель обработки должна определяться этими правовыми основаниями или, в отношении обработки, указанной в пункте (e) параграфа 1, должна быть необходима для выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролёра. Такие же правовые основания могут содержать конкретные положения адаптирующие применение норм настоящего Регламента, в том числе: общие условия, регулирующие правомерность обработки контролёром; типы данных, являющиеся предметом обработки; соответствующие субъекты данных; конкретные структуры которым раскрываются персональные данные и конкретные цели раскрытия персональных данных; целевое ограничение; сроки хранения; а также

процедуры обработки и процесс обработки, включая меры обеспечивающие правомерность и справедливость обработки, например, для таких конкретных ситуаций обработки, которые предусмотрены в главе IX. Право Евросоюза или право государства-члена должно удовлетворять цели общественных интересов, а также быть соразмерно поставленной законной цели.

Если обработка с целью, отличной от той, для которой были собраны личные данные, не основана на согласии субъекта данных или на законе Союза или государства-члена, который представляет собой необходимую и соразмерную меру в демократическом обществе для обеспечения целей, указанных в в Статье 23 (1), контролёр должен, чтобы удостовериться, совместима ли обработка для другой цели с целью, для которой первоначально собирались персональные данные, учитывать, в том числе:

(a) любые связи между целями, для которых персональные данные были собраны, и целями предполагаемой последующей обработки;

(b) контекст, для которого собирались персональные данные, в частности, касающийся отношений между субъектами данных и контролёром;

(c) характер персональных данных, в частности, производилась ли обработка особых категорий данных, в соответствии со Статьей 9, либо производилась обработка персональных данных, связанная с осужденными в уголовном порядке и правонарушителями, в соответствии со Статьей 10;

(d) возможные последствия предполагаемой последующей обработки для субъектов данных;

(e) существование соответствующих специальных защитных мер, которые могут охватывать криптографию или псевдонимизацию.

Статья 7

Существенные условия относительно согласия

1. Когда обработка основывается на согласии, контролёр должен быть способен подтвердить, что субъект данных согласен на обработку его/ее персональных данных.

2. Если согласие субъекта данных дается в виде письменного заявления, которое также касается других вопросов, запрос о согласии должен быть представлен способом, который четко отличен от других вопросов в понятной и легкодоступной форме, с использованием ясного и простого языка. Любая часть такого заявления, которая представляет собой нарушение настоящего Регламента, не имеет обязательной силы.

3. Субъект данных должен иметь право в любое время отозвать его/ее согласие. Отзыв согласия не должен влиять на правомерность обработки, основанной на согласии до его отзыва. Отзыв согласия не влияет на правомерность обработки основанной на согласия до отзыва согласия. Прежде чем давать согласие, субъект данных должен быть проинформирован

об этом. Процедура отзыва согласия должна быть такой же простой, как и процедура предоставления согласия.

4. При оценке того, предоставлено ли согласие по доброй воле, основное внимание необходимо уделить тому, в частности, зависит ли выполнение контакта, включая предоставление услуги, от согласия на обработку персональных данных, которые не являются необходимыми для выполнения такого контракта.

Статья 8

Существенные условия, применимые к согласию ребенка, в связи с услугами информационного общества

1. Если применяется пункт (a) Статьи 6 (1) при предоставлении услуг информационного общества непосредственно ребенку, обработка персональных данных ребенка является правомерной, если ребенку исполнилось как минимум 16 лет. Если ребенок еще не достиг возраста 16 лет, такая обработка является правомерной, только если и постольку, поскольку согласие было дано или одобрено лицом, обладающим родительской ответственностью в отношении ребенка.

Государства-члены могут законодательно предусмотреть меньший возраст для указанных целей при условии, что такой возраст не будет ниже 13 лет.

2. Контролёр должен предпринять разумные меры для того, чтобы в таких случаях удостовериться, что согласие было дано или одобрено лицом, обладающим родительской ответственностью в отношении ребенка, с учетом имеющихся технологий.

3. Параграф 1 не затрагивает положения общего права договоров государств-членов, таких как нормы о юридической силе, заключении или сроке действия договора в отношении ребенка.

Статья 9

Обработка особых категорий персональных данных

1. Обработка персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные или философские воззрения, либо членство в профсоюзе, а также обработка генетических данных, биометрических данных для однозначной идентификации физического лица, данных касающихся здоровья, половой жизни или сексуальной ориентации физического лица, запрещена.

2. Параграф 1 не применяется, если применимо одно из следующих положений:

(a) субъект данных дал прямое согласие на обработку указанных персональных данных для одной или нескольких обозначенных целей, кроме случаев, когда право Евросоюза или право государства-члена предусматривает, что запрет, указанный в параграфе 1, не может быть отменен субъектом данных;

(b) обработка является необходимой для целей выполнения обязательств и осуществления конкретных прав контролёра или субъекта данных в сфере занятости и социального обеспечения, а также права социального обеспечения и социальной защиты, в той мере, в какой это допускается правом Евросоюза или правом государства-члена или коллективным договором в соответствии с правом государства-члена, предусматривающее надлежащие средства защиты основных прав и интересов субъекта данных;

(c) обработка является необходимой для защиты жизненных интересов субъекта данных или иного физического лица, если субъект данных физически или юридически не способен дать свое согласие;

(d) обработка осуществляется фондом, ассоциацией или любой иной некоммерческой организацией в рамках их законной деятельности с соответствующими гарантиями в политических, философских, религиозных или профсоюзных целях и при условии, что обработка относится исключительно к членам, бывшим членам организации или лицам, которые осуществляют постоянный контакт с нею в связи с ее целями, и что персональные данные не раскрываются третьим лицам без согласия на это субъекта персональных данных;

(e) обработка связана с персональным данным, которые субъект данных явным образом сделал общедоступными;

(f) обработка является необходимой для предъявления, исполнения или защиты судебных исков или в случаях, когда суды действуют в пределах своей судейской дееспособности;

(g) обработка является необходимой по причинам особого общественного интереса на основе права Евросоюза или права государства-члена, которое соразмерно преследуемой цели, соответствует сути права на защиту данных и предусматривает приемлемые и конкретные меры по защите основных прав и интересов субъекта данных;

(h) обработка является необходимой в целях профилактической или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи или лечения, либо для управления системами и услугами здравоохранения и социального обеспечения на основании права Евросоюза или права государства-члена, а также вытекает из договора с работником здравоохранения при соблюдении условий и гарантий предусмотренных в параграфе 3;

(i) обработка является необходимой по причинам общественного интереса в сфере общественного здравоохранения, например, защиты от серьезных трансграничных угроз здоровью или для обеспечения высоких

стандартов качества и надежности медицинского обслуживания и лекарственных средств или медицинской техники, на основании права Евросоюза или права государства-члена, предусматривающее приемлемые и конкретные меры для защиты прав и свобод субъекта данных, в частности, профессиональной тайны;

(j) обработка является необходимой для архивных целей в общественных интересах, научных или историко-исследовательских целей, либо для статичтических целей в соответствии со Статей 89 (1), основании права Евросоюза или права государства-члена, которая должна быть соразмерна преследуемой цели, должна соответствовать сути права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных.

3. Персональные данные, указанные в параграфе 1, могут обрабатываться для целей, указанных в пункте (h) параграфа 2, когда эти данные обрабатываются специалистом или под его ответственностью, и такой специалист обязан соблюдать профессиональную тайну согласно праву Евросоюза или праву государства-члена, либо в соответствии с нормами, предусмотренными национальными компетентными органами, или, если обработка осуществляется иным лицом, которое обязано соблюдать конфиденциальность согласно праву Евросоюза или праву государства-члена, или согласно правилам, установленным национальными компетентными органами.

4. Государства-члены могут сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных, связанных со здоровьем.

Статья 10

Обработка персональных данных, связанных с уголовными приговорами и правонарушениями

Обработка персональных данных, связанных с уголовными приговорами и правонарушениями или связанных с мерами безопасности, по основаниям статьи 6 (1), осуществляется только под контролем официального органа, либо когда обработка разрешена правом Евросоюза или государства-члена, предусматривающим соответствующие гарантии для прав и свобод субъектов данных. Любой всеобъемлющий реестр уголовных приговоров должен храниться только под контролем официального органа.

Статья 11

Обработка, не требующая идентификации

1. Если цели, для которых контролёр обрабатывает персональные данные, не требуют или уже не требуют идентификации субъекта данных контролёром, этот контролёр не обязан хранить, получать или обрабатывать дополнительную информацию для идентификации субъекта данных с единственной целью соблюсти настоящий Регламент.

2. Когда, в случаях, предусмотренных в параграфе 1 настоящей Статьи, контролёр способен подтвердить, что он не в состоянии идентифицировать субъекта данных, контролёр должен соответственно проинформировать субъекта данных, при наличии соответствующей возможности. В таких случаях Статьи 15-20 не применяются, за тем исключением, когда субъект данных для осуществления его/ее прав, согласно указанным Статьям, предоставляет дополнительную информацию, которая обеспечивает его/ее идентификацию.

ГЛАВА III.
ПРАВА СУБЪЕКТА ДАННЫХ

Раздел 1

ТРАСПАРЕНТНОСТЬ/ПРОЗРАЧНОСТЬ И МЕТОДЫ

Статья 12

Прозрачность информации, сообщения и методы осуществления прав субъектов данных

1. Контролёр должен предпринять соответствующие меры для предоставления субъекту данных любой информации, указанной в Статьях 13 и 14, а также любых сообщений, в соответствии со Статьями 15-22 и Статьей 34, относящиеся к обработке, субъекту данных, в сжатой, открытой, понятной и легкодоступной форме на ясном и простом языке, в том числе относящейся к любой информации, адресованной ребенку. Информация должна предоставляться в письменной форме, либо иными средствами, в том числе, в необходимых случаях, электронными средствами. По просьбе субъекта данных информация может быть предоставлена в устной форме, в том случае, если идентификация субъекта данных подтверждена иными средствами.

2. Контролёр должен содействовать осуществлению прав субъекта данных в соответствии со Статьями 15-22. В случаях, предусмотренных в Статье 11 (2), контролёр не может отказаться действовать по запросу субъекта данных для осуществления его/ее прав в соответствии со Статьями

15-22, кроме случаев, когда контролёр докажет, что он не в состоянии идентифицировать этого субъекта данных.

3. Контролёр должен предоставить информацию о действиях, предпринятых по запросу в соответствии со Статьям 15-22, субъекту данных, без неоправданных задержек, и в любом случае в течение одного месяца после получения такого запроса. Этот срок может быть продлен еще на два месяца, при необходимости, принимая во внимание сложность и количество запросов. Контролёр должен проинформировать субъекта данных о любом таком продлении срока в течение одного месяца после получения этого запроса, вместе с указанием причин этой задержки. В случае, если субъект данных делает запрос электронным способом, информация должна быть предоставлена по возможности электронным способом, кроме случаев, когда субъект данных не запрашивает иной способ передачи информации.

4. Если контролёр не предпринимает действий по запросу субъекта данных, контролёр должен проинформировать субъекта данных незамедлительно, и не позднее одного месяца после получения такого запроса, о причинах непринятия действий, а также о возможности подачи жалобы надзорному органу и о возможности судебных средств защиты прав.

5. Информация, предоставляемая в соответствии со Статьями 13 и 14, а также любые сообщения и любые действия, предпринятые в соответствии со Статьями 15-22 и 34 предоставляются бесплатно. В случае, если запросы от субъекта данных являются явно не обоснованными или чрезмерными, в частности, вследствие их повторяющегося характера, контролёр может либо:

(a) взимать разумную плату, принимая во внимание административные расходы на предоставление информации или сведений, либо за осуществление запрашиваемых действий; или

(b) отказаться действовать в соответствии с этим запросом.

Контролёр несет бремя доказывания явной необоснованности запроса или чрезмерного характера этих запросов.

6. Без ущерба действию Статьи 11, в случае, если у контролёра есть разумные сомнения, связанные с установлением личности физического лица, подающего запрос, в соответствии со Статьям 15-22, контролёр может затребовать предоставление дополнительной информации, необходимой для идентификации этого субъекта данных.

7. Информация, предоставляемая субъектам данных, согласно Статьям 13 и 14, может предоставляться в сочетании со стандартизированными графическими символами с тем, чтобы дать в четкой, ясной, понятной и разборчивой форме общее представление о предполагаемой обработке. В том случае, если графические символы представлены в электронном виде, они должны быть пригодны для машинного считывания.

8. Европейская Комиссия должна быть уполномочена принимать подзаконные акты в соответствии со Статьей 92 в целях определения информации, которая представляется посредством графических обозначений, а также определения процедур для предоставления стандартизированных графических символов.

Раздел 2

ИНФОРМАЦИЯ И ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Статья 13

Предоставляемая информация при сборе персональных данных от субъекта данных

1. В том случае, если персональные данные, относящиеся к субъекту данных, собираются от субъекта данных, контролёр должен, в момент получения персональных данных, предоставить субъекту данных всю следующую информацию:

(a) идентификационную информацию и реквизиты контролёра и, там, где это применимо, представителя контролёра;

(b) реквизиты инспектора по защите персональных данных, там, где это применимо;

(c) цели обработки, для которых предназначены персональные данные, а также правовые основания для такой обработки;

(d) законные интересы контролёра или третьего лица, в случае, если обработка основана на пункте (f) Статьи 6 (1);

(e) получателей или категории получателей персональных данных, если таковые имеются;

(f) намерения контролёра, там, где это применимо, передать персональные данные в третью страну или международную организацию, а также о наличии или отсутствии решения Европейской Комиссии о достаточности мер, или в случае передачи данных, предусмотренных Статьями 46 или 47, а также вторым подпараграфом Статьи 49 (1), ссылку на соответствующие или подходящие гарантии и средства, с помощью которых можно получить копии персональных данных, либо где они могут быть предоставлены.

2. В дополнение к информации, предусмотренной параграфом 1, контролёр должен, в момент получения персональных данных, предоставить дополнительно субъекту данных следующую информацию, необходимую для обеспечения справедливой и прозрачной обработки:

(a) о сроке, в течение которого будут храниться персональные данные или, если это не представляется возможным, критерии для определения такого срока;

(b) о наличии права требования от контролёра доступа к персональным данным, а также исправления или удаления персональных данных, либо ограничения обработки или возражение против обработки, также как и права на переносимость данных;

(c) о наличии права отозвать согласие в любое время, не затрагивая правомерность обработки, выполненную до такого отзыва согласия, если обработка осуществляется в соответствии с пунктом (a) Статьи 6 (1) или пунктом (a) Статьи 9 (2);

(d) о праве подачи жалобы в надзорный орган;

(e) о том, является ли предоставление персональных данных требованием, предусмотренным законом или требованием договора, либо требованием, необходимым для заключения договора, а также о том, обязан ли субъект данных предоставлять персональные данные и о возможных последствиях непредставления таких данных;

(f) о наличии автоматизированного принятия решения, включая составление профиля, в соответствии со Статьей 22 (1) и (4), а также по крайней мере в этих случаях, достоверной информации об имеющем место алгоритме, и о значимости и предполагаемых последствиях обработки для субъекта данных.

3. В случае, если контролёр намерен в дальнейшем обрабатывать персональные данные в иных целях, чем те, для которых персональные данные были получены, этот контролёр должен, до начала такой дальнейшей обработки, предоставить субъекту данных информацию относительно этой иной цели, а также любую дополнительную информацию, согласно параграфу 2.

4. Параграфы 1, 2 и 3 не применимы в случаях, если субъект данных уже располагает соответствующей информацией.

Статья 14

Предоставляемая информация при получении персональных данных не от субъекта данных

1. В случае если персональные данные получены не от субъекта данных, контролёр должен предоставить субъекту данных следующую информацию:

(a) идентификационные и контактные данные контролёра и, там, где это применимо, представителя контролера;

(b) реквизиты инспектора по защите персональных данных, там, где это применимо;

(c) цели обработки, для которых предназначены персональные данные, а также правовые основания обработки;

(d) категории соответствующих персональных данных;

(e) получателей или категории получателей персональных данных, если таковые существуют;

(f) намерение контролёра, там, где это применимо, передать персональные данные получателю в третьей стране или международной организации, и о существовании или отсутствии решения Европейской Комиссии о достаточности мер, либо, в случае передачи персональных данных согласно Статье 46 или 47, или второму подпараграфу Статьи 49 (1), ссылку на соответствующие или подходящие гарантии и средства, с помощью которых можно получить копии персональных данных, или где они могут быть предоставлены.

2. В дополнение к информации, упомянутой в параграфе 1, контролёр должен предоставить субъекту данных следующую информацию, необходимую для обеспечения справедливой и прозрачной обработки в отношении субъекта данных:

(a) срок, в течение которого будут храниться персональные данные, или если это не представляется возможным, критерии, используемые для определения такого срока;

(b) законные интересы контролёра или третьего лица, в случаях, если обработка основана на пункте (f) Статьи 6 (1);

(c) наличие права требования от контролёра доступа к персональным данным, а также исправления или удаления персональных данных, либо ограничения обработки или возражение против обработки, также как и права на переносимость данных;

(d) наличие права отозвать согласие в любое время, не затрагивая правомерность обработки, выполненную до такого отзыва согласия, если обработка осуществляется в соответствии с пунктом (a) Статьи 6 (1) или пунктом (a) Статьи 9 (2);

(e) право подачи жалобы в надзорный орган;

(f) указание из каких источников персональные данные взяты и, если это применимо, взяты ли они из общедоступных источников;

(g) применение автоматизированного способа принятия решения, в том числе составление профиля, согласно Статье 22 (1) и (4), а также, по крайней мере в этих случаях, достоверной информации об имеющем место алгоритме, и о значимости и предполагаемых последствиях обработки для субъекта данных.

3. Контролёр должен предоставить информацию, указанную в параграфах 1 и 2:

(a) в течение разумного периода времени после получения персональных данных, но, как минимум, в пределах одного месяца, исходя из конкретных обстоятельств обработки персональных данных;

(b) не позднее первого обращения к этому субъекту данных, если персональные данные должны использоваться для связи с субъектом данных; или

(c) как минимум в момент первоначального раскрытия персональных данных, если предусмотрено раскрытие информации другому получателю.

4. В случае, если контролёр намерен продолжить обработку персональных данных с целью, отличной от той, для которой персональные данные были получены, контролёр должен предоставить субъекту данных, перед последующей обработкой, информацию об такой иной цели, а также любую соответствующую дополнительную информацию, указанную в параграфе 2.

5. Параграфы 1-4 не применяются в том случае, если:

(a) субъект данных уже обладает информацией;

(b) предоставление такой информации оказывается невозможным или будет сопряжено с непропорциональными усилиями, в частности, для обработки в архивных целях в интересах общества, в целях научных или исторических исследований, либо для статистических целей, при наличии условий и гарантий, предусмотренных Статьей 89 (1), или постольку, поскольку обязанность, указанная в параграфе 1 настоящей Статьи, может стать невозможной или негативно отразиться на достижении целей такой обработки. В таких случаях контролёр должен принять надлежащие меры для защиты прав, свобод и законных интересов субъекта данных, включая доведение информации до всеобщего сведения;

(c) получение или раскрытие информации непосредственно предусмотрено правом Евросоюза или правом государства-члена, под действие которого подпадает контролёр и которое предусматривает соответствующие меры защиты законных интересов субъекта данных; или

(d) персональные данные должны оставаться конфиденциальными, исходя из обязательств по соблюдению профессиональной тайны, в соответствии с правом Евросоюза или правом государства-члена, включая обязательства, вытекающие в силу закона о сохранении секретности.

Статья 15

Право субъекта данных на доступ к данным

1. Субъект данных вправе получать от контролёра подтверждение относительно того, находятся ли персональные данные, касающиеся его/ее в обработке, и в этом случае, он имеет право на доступ к персональным данным, а также к следующей информации:

(a) о цели обработки;

(b) о соответствующих категориях обрабатываемых персональных данных;

(c) о получателях или категории получателей, которым персональные данные были либо будут раскрыты, в том числе, о получателях в третьих странах или о международных организациях;

(d) о предполагаемом сроке, когда это возможно, в течение которого будут храниться персональные данные, или, если это невозможно, о критериях, используемых для определения указанного срока;

(e) о наличии права требовать от контролёра исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки;

(f) о праве подачи жалобы в надзорный орган;

(g) об источнике любой доступной информации, связанной с персональными данными, если они получены не от субъекта данных;

(h) о применении автоматизированного способа принятия решения, в том числе составление профиля, согласно Статье 22 (1) и (4), а также, по крайней мере в этих случаях, достоверной информации об имеющем место алгоритме, также как о значимости и предполагаемых последствиях обработки для субъекта данных.

2. В случае, если персональные данные передаются третьей стране или международной организации, субъект данных вправе получать информацию о соответствующих гарантиях, в соответствии со Статьей 46, относительно такой передачи данных.

3. Контролёр должен предоставить копию персональных данных, проходящих обработку. За любые дополнительные копии, запрашиваемые субъектом данных, контролёр может взимать приемлемую плату в зависимости от административных расходов. Если субъект данных делает запрос электронным способом, информация должна предоставляться в принятой электронной форме, если иное не запрошено субъектом данных.

4. Право на получение копии, предусмотренной параграфом 3, не должно негативно влиять на права и свободы иных лиц.

Раздел 3

ИСПРАВЛЕНИЕ И УДАЛЕНИЕ ДАННЫХ

Статья 16

Право на исправление данных

Субъект данных вправе потребовать от контролёра без неоправданной задержки исправления неточных персональных данных, касающихся его/ее. Принимая во внимание цели обработки, субъект данных должен иметь право дополнить неполные персональные данные, в том числе путем предоставления дополнительного заявления.

Статья 17

Право на удаление данных («право на забвение»)

1. Субъект данных должен иметь право потребовать от контролёра удалить персональные данные, касающихся его/ее без неоправданной задержки, а контролёр обязан удалить персональные данные без неоправданной задержки, в том случае, если применимо одно из следующих оснований:

(a) персональные данные больше не нужны для целей, для которых они были собраны или обработаны иным образом;

(b) субъект данных отозвал свое согласие, на основании которого, согласно пункту (a) Статьи 6 (1) или пункту (a) Статьи 9 (2), осуществлялась обработка, а также если отсутствует иное правовое основание обработки;

(c) субъект данных возражает против обработки в соответствии со Статьей 21 (1), и отсутствуют правовые основания, имеющие преимущественную силу, либо субъект данных возражает против обработки в соответствии со Статьей 21 (2);

(d) персональные данные были обработаны неправомерно;

(e) персональные данные должны быть удалены в соответствии с правовыми обязательствами, вытекающими из права Евросоюза или права государства-члена, действие которых распространяется на контролёра;

(f) персональные данные были собраны в связи с предложением услуг информационного общества, упомянутых в Статье 8 (1).

2. В случае, если контролёр обнародовал персональные данные, а он обязан, согласно параграфу 1, удалить эти персональные данные, контролёр, учитывая имеющиеся технологические возможности и расходы на исполнение, должен предпринять обоснованные меры, включая технические меры, чтобы проинформировать контролёров, обрабатывающих персональные данные, о том, что субъект данных затребовал от таких контролёров удаления любых ссылок на такие персональные данные, или их копирование или тиражирование.

3. Параграфы 1 и 2 не применяться в тех случаях, когда обработка необходима:

(a) для осуществления права на свободу выражения мнения и распространения информации;

(b) для соблюдения правовой обязанности, которая требует обработки в соответствии с правом Евросоюза или правом государства-члена, которое применимо к контролёру, или для выполнения задачи, осуществляемой в общественных интересах, либо при осуществлении официальных полномочий, возложенных на контролёра;

(c) в силу общественных интересов в сфере социального здравоохранения в соответствии с пунктами (h) и (i) Статьи 9 (2) и Статьи 9 (3);

(d) для архивных целей в общественных интересах, научных или исторических исследовательских целях, либо для статистических целей в

соответствии со статьей 89 (1), постольку, поскольку право, предусмотренное в параграфе 1, может сделать невозможным или отрицательно отразиться на достижении целей такой обработки; или

(e) для предъявления, исполнения или защиты правовых притязаний.

Статья 18

Право на ограничение обработки

1. Субъект данных должен иметь право потребовать от контролёра ограничить обработку, если применимо одно из следующих условий:

(a) точность персональных данных оспаривается субъектом данных, в течение срока,

позволяющего контроллеру проверить точность персональных данных;

(b) обработка является неправомерной, и субъект данных возражает против удаления персональных данных, и взамен требует ограничить их использование;

(c) контролёру больше не нужны персональные данные для целей обработки, но они требуются субъекту данных для предъявления, исполнения или защиты правовых притязаний;

(d) субъект данных возражал против обработки в соответствии со Статьей 21 (1), ожидая удостоверения того, преобладают ли правовые основания контролёра таким правовым основаниям субъекта данных.

2. В случае, если обработка была ограничена в соответствии с параграфом 1, такие персональные данные должны, за исключением хранения, обрабатываться только с согласия субъекта данных или для предъявления, исполнения или защиты правовых притязаний, или для защиты прав другого физического или юридического лица, либо по причинам важного общественного интереса Евросоюза или государства-члена.

3. Субъект данных, который добился ограничения обработки, в соответствии с пунктом 1, должен быть проинформирован контролёром до того, как будет отменено ограничение обработки.

Статья 19

Обязательства по уведомлению в отношении исправления или удаления персональных данных или ограничении обработки

Контролёр должен сообщить о любом исправлении или удалении персональных данных, либо ограничении обработки, осуществляемых в соответствии со Статьей 16, Статьей 17 (1) и Статьей 18, каждому получателю, которому были раскрыты персональные данные, кроме случаев, когда это оказывается невозможным или сопряжено с несоразмерными

усилиями. Контролёр должен проинформировать субъекта данных об этих получателях, если субъект данных запрашивает его об этом.

Статья 20

Право на переносимость данных

1. Субъект данных должен иметь право на получение персональных данных, касающихся его/ее, которые он/она предоставил контролёру, в структурированном, обычно используемом и машиночитаемом формате, а также должен иметь право передавать эти данные другому контролёру бес препятствий со стороны контролёра, которому были предоставлены персональные данные, в случае, если:

(а) обработка основывается на согласии в соответствии с пунктом (а) Статьи 6 (1) или пунктом (а) статьи 9 (2), либо по договору в соответствии с пунктом (б) Статьи 6 (1); и
(в) обработка осуществляется с помощью автоматизированных средств.

2. При осуществлении его/ее права на переносимость данных в соответствии с параграфом 1, субъект данных должен иметь право передавать персональные данные непосредственно от одного контролёра к другому, если это технически осуществимо.
3. Осуществление права, упомянутого в параграфе 1 настоящей Статьи, должно действовать без ущерба Статье 17. Это право не применяется к обработке, необходимой для выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, вложенных на контролёра.
4. Право, упомянутое в параграфе 1, не должно отрицательно влиять на права и свободы иных лиц.

Раздел 4

ПРАВО НА ВОЗРАЖЕНИЕ И АВТОМАТИЗИРОВАННОЕ ИНДИВИДУАЛЬНОЕ ПРИНЯТИЕ РЕШЕНИЯ

Статья 21

Право на возражение

1. Субъект данных должен иметь право на возражение, по основаниям, связанным с его/ее конкретной ситуации, в любой момент против обработки персональных данных касающихся его/ее, руководствуясь пунктом (e) или (f) Статьи 6 (1), включая составление профиля, основанное на таких положениях. Контролёр не должен больше обрабатывать персональные данные, кроме случаев, когда он может доказать наличие убедительных правовых оснований для обработки, которые имеют преимущественное юридическое действие над интересами, правами и свободами субъекта данных, или обработка необходима для предъявления, исполнения или защиты правовых притязаний.

2. В случаях, если персональные данные обрабатываются для целей прямого маркетинга, субъект данных должен иметь право на возражение в любой момент против обработки персональных данных, касающихся его/ее для целей такого маркетинга, включая составление профиля, в той мере, в какой это связано с таким прямым маркетингом.

3. Если субъект данных возражает против обработки в целях прямого маркетинга, персональные данные больше не должны обрабатываться для таких целей.

4. Не позднее момента первого общения с субъектом данных, право, указанное в параграфах 1 и 2, должно быть прямо доведено до сведения субъекта данных и должно быть представлено ясно и отдельно от любой иной информации.

5. В контексте использования услуг информационного общества и, невзирая на Директиву 2002/58/ЕС, этот субъект данных может осуществлять его/ее право на на возражение автоматизированным способом с использованием технических средств.

6. В случае, если персональные данные обрабатываются в научных или исторических исследовательских целях, либо для статистических целей в соответствии со Статьей 89 (1), этот субъект данных, по основаниям, относящимся к его/ее конкретной ситуации, должен иметь право возражать против обработки персональных данных, касающихся его/ее, кроме случаев, когда обработка является необходимой для выполнения задачи, осуществляемой по причинам общественного интереса.

Статья 22

Автоматизированное индивидуальное принятие решений, включая составление профиля

1. Субъект данных должен иметь право не подчиняться решению, основанному исключительно на автоматизированной обработке, включая

составление профиля, которое порождает правовые последствия, касающиеся его/ее или аналогичным образом в значительной степени влияют на него/нее.

2. Параграф 1 не применяется, если решение:

(a) является необходимым для заключения или исполнения договора между субъектом данных и контролёром данных;

(b) дозволено правом Евросоюза или правом государства-члена, которому подчиняется контролёр, и которые также устанавливают приемлемые меры защиты прав и свобод субъекта данных и законных интересов; или

(c) основывается на прямом согласии субъекта данных.

3. В случаях, указанных в пунктах (a) и (c) параграфа 2, контролёр данных должен применять надлежащие меры для защиты прав и свобод субъекта данных и законных интересов, и, как минимум, права требовать вмешательства со стороны контролёра, права выражать его/ее точку зрения, а также оспаривать это решение.

4. Решения, упомянутые в параграфе 2, не должны основываться на особых категориях персональных данных, предусмотренных в Статье 9 (1), кроме случаев, когда пункты (a) или (g) Статьи 9 (2) применяются и прияты надлежащие меры защиты прав, свобод и законных интересов субъекта данных.

Раздел 5

ОГРАНИЧЕНИЯ

Статья 23

Ограничения

1. Право Евросоюза или право государства-члена, применимое к контролёру или обработчику, может посредством законодательных мер ограничить объем и содержание обязательств и прав, предусмотренных в Статьях 12-22 и Статье 34, а также в Статье 5, в той мере, в какой эти положения соответствуют правам и обязанностям, предусмотренным в Статьях 12-22, если такие ограничения соответствуют сути основных прав и свобод, а также является необходимой и соразмерной мерой в демократическом обществе для обеспечения:

(a) национальной безопасности;

(b) обороны;

(c) общественной безопасности;

(d) предотвращения, расследования, розыска преследования по уголовным преступлениям или исполнения уголовных наказаний, в том числе защиты и предупреждения угроз общественной безопасности;

(e) иных важных целей интересов неограниченного круга лиц Евросоюза или государства-члена, в частности важных экономических или финансовых интересов Евросоюза или государства-члена, включая денежные, бюджетные и налоговые вопросы, социальное здравоохранение и общественную безопасность;

(f) защиты независимости судебной власти и защиты судебного производства;

(g) предупреждения, расследования, выявления и преследования нарушений этики, касающейся регулируемых профессий;

(h) мониторинга, контрольных и распорядительных функций, связанных, даже периодически, с осуществлением официальных полномочий в случаях, предусмотренных в пунктах (a)-(e) и (g);

(i) защиты субъекта данных или прав и свобод иных лиц;

(j) исполнения решений по гражданско-правовым искам.

2. В частности, любые законодательные меры, упомянутые в параграфе 1, должны содержать конкретные положения, по крайней мере, в соответствующих случаях, относительно:

(a) целей обработки или категорий обработки;

(b) категорий персональных данных;

(c) объема введенных ограничений;

(d) средств защиты предупреждения несанкционированного доступа или передачи (данных);

(e) определения контролёра или категорий контролёров;

(f) сроков хранения и применимых гарантий, принимая во внимание характер, объем и цели обработки или категории обработки;

(g) рисков для прав и свобод субъектов данных; и

(h) прав субъектов данных получать информацию об ограничении, кроме случаев, когда это может нанести ущерб цели ограничения.

ГЛАВА IV.

КОНТРОЛЁР И ОБРАБОТЧИК

Раздел 1

ОБЯЗАТЕЛЬСТВА ОБЩЕГО ХАРАКТЕРА

Статья 24

Ответственность контролёра

1. Принимая во внимание характер, сферу охвата, контекст и цели обработки, равно как и вероятность возникновения рисков и степень опасности для прав и свобод физических лиц, контролёр должен применять соответствующие технические и организационные меры, для того, чтобы обеспечить и быть способным подтвердить, что обработка осуществляется в соответствии с настоящим Регламентом. Такие меры должны пересматриваться и обновляться, в необходимых случаях.

2. В случаях соизмеримости по отношению к обработке данных, меры, предусмотренные в параграфе 1, должны охватывать применение соответствующей политик защиты данных контроллером.

3. Соблюдение утвержденных кодексов поведения, предусмотренных в Статье 40, или утвержденных механизмов сертификации, в соответствии со Статьей 42, может использоваться в качестве параметра, подтверждающего соблюдение обязанностей контролёром.

Статья 25

Защита данных для определенных целей/случаев и по умолчанию

1. Принимая во внимание современное состояние развития техники, затраты на внедрение, а также характер, объем, контекст и цели обработки, в равной степени как и вероятность возникновения рисков, так и опасностей для прав и свобод физических лиц, возникающих при обработке, контролёр должен, и во время определения средств обработки, и во время самой обработки, применять соответствующие технические и организационные меры, такие как псевдонимизация, которые предусмотрены для эффективного осуществления принципов защиты данных, к, примеру, минимизации данных, а также для тесной увязки необходимых средств защиты в обработку данных для того, чтобы соответствовать требованиям настоящего Регламента и обеспечить защиту прав субъектов данных.

2. Контролёр должен осуществлять соответствующие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только персональные данные, которые необходимы для каждой конкретной цели их обработки. Такая обязанность распространяется на собранный массив персональных данных в части, касающейся их обработки, сроку их хранения, а также к доступу к ним. В частности, такие меры должны обеспечивать, что по умолчанию доступ к персональным данным не будет предоставлен неопределенному числу физических лиц без вмешательства этого индивидуума.

3. Утвержденный механизм сертификации в соответствии со Статьей 42, может использоваться в качестве параметра для подтверждения соблюдения требований, предусмотренных в параграфах 1 и 2 настоящей статьи.

Статья 26

Контролёры, действующие совместно

1. В том случае, если два или более контролёров совместно определяют цели и средства обработки, они являются контролёрами, действующие совместно. Они должны открытым (транспарентным) способом определить свои соответствующие функциональные обязанности, на предмет соблюдения обязательств, вытекающих из настоящего Регламента, в частности в отношении осуществления прав субъекта данных, а также их соответствующих обязанностей по предоставлению информации, предусмотренной Статьями 13 и 14, посредством договоренности между ними, за исключением случаев, когда и постольку, поскольку соответствующие обязанности контролёров определены правом Евросоюза или правом государства-члена, которые применимы к контролёрам. Эта договоренность может определять пункт взаимосвязи (*contact point*) для субъектов данных.

2. Договоренность, предусмотренная параграфом 1, должна надлежащим образом отражать соответствующие роли и взаимоотношения контролёров, действующих совместно по отношению к субъектам данных. Существенные условия договоренности должны быть доступны для субъектов данных.

3. Независимо от условий договоренности, предусмотренной параграфом 1, субъект данных может осуществлять его/ее права, вытекающие из настоящего Регламента в отношении каждого контролёра, а также против каждого контролера.

Статья 27

Представители контролёров или обработчиков, не учрежденных в Евросоюзе

1. В том случае, когда применяется Статья 3 (2), контролёр или обработчик должны в форме письменного документа назначить представителя в Евросоюзе.

2. Обязательство, изложенное в параграфе 1 настоящей Статьи, не применяется: в отношении:

(a) к обработке, которая является единичной, не охватывает в больших масштабах обработку особых категорий данных, согласно Статье 9 (1), либо обработку персональных данных, связанных с уголовными приговорами и правонарушениями, согласно Статье 10, а также к обработке персональных данных, которая едва ли обернется рисками для прав и свобод физических лиц, принимая во внимание характер, контекст, цели и задачи этой обработки; или

(b) в отношении органа государственной власти или учреждения.

3. Представитель должен быть учрежден в одном из государств-членов, в котором находятся субъекты данных, персональные данные которых обрабатываются в связи с предложением товаров или услуг, либо в отношении действий которых осуществляется мониторинг.

4. Представитель контролёра или обработчика должен обладать полномочиями, предоставленными ему контролёром или обработчиком и рассматриваться наряду, либо вместо контролёра или обработчика, в частности, надзорными органами и субъектами данных по всем вопросам, связанным с обработкой, в целях обеспечения соблюдения настоящего Регламента.

5. Назначение представителя контролёром или обработчиком не должно наносить ущерба юридическим действиям, которые могут быть возбуждены против самого контролёра или обработчика.

Статья 28

Обработчик

1. В том случае, если обработка осуществляется от имени контролёра, контролёр должен использовать исключительно обработчиков, обеспечивающих надлежащие гарантии применения соответствующих технических и организационных мер таким способом, чтобы обработка отвечала требованиям настоящего Регламента и обеспечивала защиту прав субъекта данных.

2. Обработчик не должен привлекать другого обработчика без предварительного письменного оформленного специального или общего разрешения контролёра. В случае разрешения общего характера, обработчик должен проинформировать контролёра о любых предполагаемых изменениях, касающихся дополнительного привлечения или замены других обработчиков, с тем, чтобы дать контролёру возможность высказать возражения против таких изменений.

3. Обработка данных обработчиком, должна регулироваться договором, либо иным правовым актом в соответствии с правом Евросоюза или права государства-члена, который имеет обязательную силу для обработчика в отношении контролёра, и который определяет предмет и период, в течение которого осуществляется обработка, характер и цель обработки, тип персональных данных и категории субъектов данных, а также обязанности и права контролёра. Такой договор либо иной правовой акт должен, в частности, предусматривать, что обработчик:

(a) обрабатывает персональные данные только на основании документально подтвержденных распоряжений контролёра, в том числе в отношении передачи персональных данных третьей стране или

международной организации, если только этого не требует право Евросоюза или право государств-члена, которое применяется к обработчику; в этом случае обработчик должен проинформировать контролёра об этих правовых требованиях до начала обработки, за исключением случаев, когда такое право запрещает подобное информирование по основаниям общественного интереса;

(b) гарантирует, что лица, уполномоченные обрабатывать персональные данные, взяли на себя обязательства соблюдать конфиденциальность, либо обязательства этих лиц соблюдать конфиденциальность, предусмотрены законом;

(c) предпринимает все меры, требуемые в соответствии со Статьей 32;

(d) соблюдает условия, указанные в параграфах 2 и 4, по привлечению другого обработчика;

(e) принимая во внимание характер обработки, помогает контролёру соответствующими техническими и организационными мерами, насколько это возможно, осуществлять обязанности контролёра отвечать на запросы по осуществлению прав субъекта данных, изложенных в главе III;

(f) содействует контролёру в обеспечении соблюдения обязанностей в соответствии со Статьями 32-36, принимая во внимание характер обработки, а также информацию, доступную для обработчика;

(g) по выбору контролёра, удаляет или возвращает все персональные данные контролёру по завершению предоставления услуг, связанных с обработкой, а также удаляет существующие копии, кроме случаев, когда право Евросоюза или право государства-члена требует хранения персональных данных;

(h) предоставляет в распоряжение контролёра всю информацию, необходимую для того, чтобы подтвердить соблюдение обязанностей, предусмотренных настоящей Статьей, а также дающую возможность и содействующую проведению аудита, включая инспекционные проверки, проводимые контролёром либо иным аудитором, уполномоченным контролёром.

В части, относящейся к пункту (h) первого подпараграфа, обработчик должен незамедлительно информировать контролёра, в случае, если, по его мнению, распоряжения нарушают настоящий Регламент или иные положения по защите данных. Евросоюза или государства-члена.

4. В случае, когда обработчик привлекает другого обработчика для выполнения конкретной деятельности по обработке от имени контролёра, такие же обязательства по защите данных, которые предусмотрены договором или иным правовым актом между контролёром и обработчиком, в соответствии с параграфом 3, должны быть возложены на такого другого обработчика, посредством договора или иного правового акта, согласно праву Евросоюза или права государства-члена, в том числе, обеспечивающие достаточные гарантии применения соответствующих технических и организационных мер с тем, чтобы обработка отвечала требованиям

настоящего Регламента. В случаях, когда другой обработчик не выполняет свои обязательства по защите данных, первоначальный обработчик продолжает нести полную ответственность перед контролёром по обязательствам такого другого обработчика.

5. Соблюдение обработчиком утвержденных кодексов поведения, упомянутых в Статье 40, или утвержденного механизма сертификации, в соответствии со Статьей 42, может использоваться в качестве показателя, позволяющего свидетельствовать о достаточности гарантий, предусмотренных параграфами 1 и 4 настоящей Статьи.

6. Без ущерба действию индивидуального договора, заключенного между контролёром и обработчиком, этот договор или иной правовой акт, указанный в параграфах 3 и 4 настоящей Статьи, может полностью или частично основываться на стандартных договорных положениях, предусмотренных в параграфах 7 и 8 настоящей Статьи, в том числе, когда они являются составной частью сертификата, выданного контроллеру или обработчику, в соответствии со Статьями 42 и 43.

7. Европейская Комиссия может устанавливать стандартные договорные положения по вопросам, указанным в параграфах 3 и 4 настоящей Статьи, и в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

8. Надзорный орган может одобрять стандартные договорные положения по вопросам, указанным в параграфах 3 и 4 настоящей Статьи, и в соответствии с механизмом согласования, предусмотренном Статьей 63

9. Договор или иной правовой акт, упомянутый в параграфах 3 и 4, должен иметь письменную форму, в том числе в электронном виде.

10. Без ущерба для действия Статей 82, 83 и 84, если обработчик нарушает требования настоящего Регламента путем определения целей и способов обработки, этот обработчик должен рассматриваться в качестве контролёра применительно к такой обработки.

Статья 29

Обработка, подконтрольная контролёру или обработчику

Обработчик или любое иное лицо, действующее от лица контролёра или обработчика, которое имеет доступ к персональным данным, не должны обрабатывать такие данные, кроме как по распоряжению контролёра, если этого не требует право Евросоюза или государства-члена.

Статья 30

Отчетные записи обработки данных

1. Каждый контролёр и, когда это применимо, представитель контролёра должен вести учетные записи обработки данных, находящейся под его ответственностью. Такой учет должен содержать всю нижеследующую информацию:

(a) наименование и реквизиты контролёра и, когда это применимо, контролёра, действующего совместно с ним (со-контролёра), представителя контролёра и инспектора по защите персональных данных;

(b) цели обработки;

(c) описание категорий субъектов данных и категорий персональных данных;

(d) категории получателей, которым персональных данные были или будут раскрыты, включая получателей в третьих странах или международных организациях;

(e) о передаче персональных данных, когда это применимо, в третью страну или международную организацию, включая указание этой третьей страны или международной организации, а в случае передачи персональных данных согласно второму подпараграфу Статьи 49 (1), документальное подтверждение надлежащего обеспечения защиты;

(f) предусмотренные сроки удаления различных категорий данных, когда это возможно;

(g) общее описание технических и организационных мер безопасности, предусмотренных в Статье 32 (1), когда это возможно;

2. Каждый обработчик и, когда это применимо, представитель обработчика должны вести учет всех категорий обработки данных, осуществляемой от имени контролёра, содержащий:

(a) наименование и реквизиты обработчика или обработчиков лиц и каждого контролёра, от имени которого действует обработчик и, когда это применимо, представителя контролёра или обработчика, а также и инспектора по защите персональных данных;

(b) категории обработки, осуществляемые от имени каждого контролёра;

(c) передачу персональных данных в третью страну или международную организацию, когда это применимо, включая определение такой третьей страны или международной организации, а в случае передачи упомянутых во втором подпараграфе Статьи 49 (1), документальное подтверждение достаточности гарантий;

(D) общее описание технических и организационных мер безопасности, когда это возможно, предусмотренных в Статье 32 (1).

3. Учетные записи, упомянутые в параграфах 1 и 2, должны храниться в письменной форме, в том числе в электронном виде.

4. Контролёр или обработчик и, когда это применимо, представитель контролёра или обработчика должны предоставлять учетные записи в распоряжение надзорных органов по их требованию.

5. Обязательства, предусмотренные в параграфах 1 и 2, не применяются в отношении предприятия или организации, на которых занято менее 250

человек, кроме случаев, когда осуществляемая обработка может привести к возникновению возможных рисков для прав и свобод субъектов данных, такая обработка не носит случайный характер, либо обработка охватывает специальные категории данных, предусмотренные в Статье 9 (1), или персональные данные касаются судимости или правонарушений, предусмотренные в Статье 10.

Статья 31

Сотрудничество с надзорным органом

Контролёр и обработчик и, когда это применимо, их представители должны сотрудничать с надзорным органом, по запросу, при осуществлении выполнении своих задач.

Раздел 2

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 32

Безопасность обработки

1. Принимая во внимание современный уровень развитие техники, затраты, связанные с внедрением, а также характер, объем, контекст и цели обработки, а равно и вероятностное возникновение рисков и опасности для прав и свобод физических лиц, контролёр и обработчик должны осуществлять соответствующие технические и организационные меры, обеспечивающие надлежащий уровень безопасности соразмерный этим рискам, включая, среди прочего, следующее:

(a) псевдонимизация и криптографическая защита персональных данных;

(b) средства для обеспечения постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки и услуг;

(c) средства своевременного восстановления доступности и доступа к персональным данным в случае природного или технического инцидента;

(d) процедура регулярной проверки и оценки эффективности технических и организационных мер, обеспечивающая безопасность обработки.

2. При определении надлежащего уровня безопасности, в расчет должны приниматься в том числе риски, которые представляет собой сама обработка, в особенности риски от случайного или неправомерного

уничтожения, потери, изменения, несанкционированного раскрытия или доступа к персональным данным переданным, сохраненным либо или иным образом обработанным.

3. Соблюдение принятого кодекса поведения, предусмотренного в Статье 40, или принятого механизма сертификации, предусмотренного в Статье 42, может быть использовано как показатель, свидетельствующий о соблюдении требований, установленных в параграфе 1 настоящей Статьи.

4. Контролёр и обработчик должны предпринять меры для обеспечения того, чтобы любое физическое лицо, подчиняющееся контролёру или обработчику, которое имеет доступ к персональным данным, не обрабатывало их, за исключением распоряжений контролёра, кроме случаев, когда он/она обязаны действовать так согласно праву Евросоюза или государства-члена.

Статья 33

Уведомление надзорного органа об утечке персональных данных

1. В случае утечки персональных данных контролёр, без неоправданной задержки и, при наличии соответствующей возможности, не позднее чем через 72 часа после того, как он узнает об этом, уведомляет об утечке персональных данных компетентный надзорный орган в соответствии со Статьей 55, кроме случаев, когда эта утечка персональных данных едва ли обернется рисками для прав и свобод физических лиц. В случае если уведомление надзорного органа не произведено в течение 72 часов, в нем должны быть указать причины задержки.

2. Обработчик должен уведомить контролёра без неоправданной задержки об утечке персональных данных как только ему стало известно об утечке персональных данных.

3. Уведомление, предусмотренное параграфом 1, должно как минимум:

(a) описывать характер утечки персональных данных, в том числе, когда это возможно, категории и приблизительное количество соответствующих субъектов данных, а также категории и приблизительное количество соответствующих записей персональных данных;

(b) сообщать наименование и реквизиты инспектора по защите персональных данных или иного контактного пункта, где может быть получена более подробная информация;

(c) описывать вероятные последствия утечки персональных данных;

(d) описывать меры, предпринятые или предполагаемые к принятию контролёром в ответ на утечки персональных, в том числе, в необходимых случаях, меры по смягчению возможных неблагоприятных последствий таких утечек.

4. Если, и в том случае когда, невозможно предоставить информацию единовременно, эта информация может предоставляться поэтапно без неоправданной дальнейшей задержки.

5. Контролёр должен документировать любые утечки персональных данных, содержащие факты, касающиеся утечки персональных данных, их последствий, а также предпринятых меры по устранению последствий. Такая документация должна позволять надзорному органу проверить соблюдение настоящей Статьи.

Статья 34

Сообщение субъекту данных об утечке персональных данных

1. В тех случаях, когда утечка персональных данных, вероятнее всего приведет к высокому риску для прав и свобод физических лиц, контролёр должен сообщить субъекту данных об утечке персональных данных, без необоснованной задержки.

2. Сообщение субъекту данных, предусмотренное параграфом 1 настоящей Статьи, должно излагать ясным и простым языком характер утечки персональных данных, а также содержать как минимум информацию и меры, предусмотренные в пунктах (b), (c) и (d) Статьи 33(3).

3. Сообщение субъекту данных, предусмотренное параграфом 1, не требуется, если выполнено любое из следующих условий:

(a) контролёр принял надлежащие технические и организационные защитные меры защиты, и такие меры были применены в отношении персональных данных, затронутых утечкой, в том числе и такие меры, которые отображают персональные данные в непонятном виде для любого лица, которое не имеет права доступа к ним, среди которых криптографическая защита;

(b) контролёр предпринял последующие меры, которые гарантируют, что высокий риск для прав и свобод субъектов данных, упомянутых в параграфе 1, больше не способен получить вероятную реализацию;

(c) требуются несоразмерные усилия. В этом случае, вместо этого делается сообщение для всеобщего сведения либо предпринимается аналогичная мера, посредством которой субъекты данных информируются равнодействующим способом.

4. Если контролёр еще не сообщил субъекту данных об утечке персональных данных, надзорный орган, рассмотрев возможные последствия высокой степени риска для прав и свобод физических лиц, может потребовать сделать такое сообщение, либо может решить, что любое из условий, предусмотренных параграфом 3, выполнены.

Раздел 3

ОЦЕНКА ВОЗДЕЙСТВИЯ НА ЗАЩИТУ ДАННЫХ И ПРЕДВАРИТЕЛЬНАЯ КОНСУЛЬТАЦИЯ

Статья 35

Оценка воздействия на защиту данных

1. В тех случаях, когда тип обработки данных, в частности при использовании новых технологий, а также принимая во внимание характер, объем, контекст и цели обработки, вероятнее всего приведет к высокому риску для прав и свобод физических лиц, контролёр должен, до этой обработки, осуществить оценку воздействия предусмотренных операций обработки на защиту персональных данных. Отдельная оценка может быть проведена в отношении ряда аналогичных операций обработки, который представляет подобные высокие риски.

2. Контролёр должен посоветоваться с инспектором по защите персональных данных, в случае если он назначен на должность, при проведении оценки воздействия на защиту данных.

3. Оценка воздействия на защиту данных, предусмотренная параграфом 1, требуется, в том числе, в случае:

(a) системной и масштабной оценки персональных особенностей, касающихся физических лиц, которая основана на автоматизированной обработке, включая составление профиля, и на которых основаны решения, порождающие правовые последствия, связанные с физическим лицом, либо подобным образом значительно влияют на физическое лицо;

(b) масштабной обработки особых категорий данных, предусмотренных Статьей 9 (1), либо персональных данных, связанных с уголовными приговорами и правонарушениями, в соответствии со Статьей 10; или

(c) систематического мониторинга сфер, открытых для всех пользователей в широких масштабах.

4. Надзорный орган должен устанавливать и доводить до сведения широкой общественности перечень видов обработки данных, которые являются предметом требований оценки воздействия на защиту данных, в соответствии с параграфом 1. Надзорный орган должен передать такие списки Совету, указанному в Статье 68.

5. Надзорный орган может также устанавливать и доводить до сведения широкой общественности перечень видов обработки данных, для которых не требуется оценка воздействия на защиту данных. Надзорный орган должен передать такие перечни Совету.

6. До принятия перечней, предусмотренных параграфами 4 и 5, компетентный надзорный орган должен применить механизм согласования,

предусмотренный Статьей 63, когда такие перечни охватывают обработку данных, которая связана с предложением товаров и услуг субъектам данных, или с мониторингом их действий в нескольких государствах-членах, либо могут существенно влиять на свободное перемещение персональных данных на территории Евросоюза.

7. Оценка должна содержать как минимум:

(a) систематизированное описание предусмотренных операций обработки данных, а также целей обработки, в том числе, когда это применимо, законные права, осуществляемые контролёром;

(b) оценку необходимости и соразмерности операций обработки по отношению к целям;

(c) оценку рисков в отношении прав и свобод субъектов данных, предусмотренных параграфом 1; и

(d) меры, предусмотренные в отношении рисков, в том числе гарантии, меры безопасности, а также механизмы для обеспечения защиты персональных данных и подтверждения соблюдения настоящего Регламента, принимая во внимание права и законные интересы субъектов данных и иных заинтересованных лиц.

8. Соблюдение принятых кодексов поведения, упомянутых в Статье 40 соответствующими контролёрами или обработчиками, должно быть учтено при оценке воздействия операций по обработке, осуществляемые такими контролёрами или обработчиками, в том числе для целей оценки воздействия на защиту данных.

9. В соответствующих случаях, контролёр должен узнать мнения субъектов данных или их представителей относительно предполагаемой обработки, без ущерба для защиты коммерческих или общественных интересов, либо безопасности обработки данных.

10. В случае, когда обработка, согласно пункту (c) или (e) Статьи 6 (1), имеет правовые основания по праву Евросоюза или государства-члена, которое применимо к контролёру, такое право регулирует конкретную операцию обработки, либо ряд соответствующих операций, а также оценку воздействия защиты данных проведенную ранее, как часть общей оценки воздействия в контексте применения таких правовых оснований, параграфы 1-7 не применяются, кроме случаев, когда государства-члены рассматривают их необходимыми для осуществления такой оценки до начала обработки данных.

11. В необходимых случаях контролёр должен провести анализ для того, чтобы оценить, осуществлена ли обработка в соответствии с оценкой воздействия на защиту данных, по крайней мере когда существует изменение риска, представленного операциями обработки.

Статья 36

Предварительная консультация

1. Контролёр должен проконсультироваться с надзорным органом до начала обработки, когда оценка воздействия на защиту данных в соответствии со Статьей 35 показывает, что эта обработка предполагает высокий риск в отсутствии мер, предпринятых контролёром для минимизации последствий этого риска.

2. В случаях, когда надзорный орган считает, что предполагаемая обработка, предусмотренная параграфом 1, могла бы нарушить положения настоящего Регламента, в том числе, когда контролёр в недостаточной степени определил или минимизировал последствия риска, надзорный орган должен, в срок не превышающий восьми недель с момента получения запроса о проведении консультации, предоставить контролёру письменные рекомендации и, в случаях когда это применимо, обработчику, а также может использовать любые свои полномочия, предусмотренные в Статье 58. Указанный срок может быть увеличен на шесть недель, принимая во внимание сложность предполагаемой обработки. Надзорный орган должен проинформировать контролёра и, когда это применимо, обработчика, о любых таких увеличениях сроков в течение одного месяца с момента получения запроса о консультации, вместе с указанием причин этой задержки. Обозначенные сроки могут быть приостановлены до тех пор, пока надзорный орган не получит информацию, запрашиваемую им для целей консультации.

3. При консультировании надзорным органом, в соответствии с параграфом 1, контролёр должен предоставить надзорному органу:

(a) когда это применимо, сведения об обязанностях контролёра, контролёрах действующих совместно, и обработчиках, вовлеченных в обработку, в частности, по обработке в рамках группы компаний;

(b) сведения о цели и способах предполагаемой обработки;

(c) сведения о мерах и средствах защиты прав и свобод субъектов данных в соответствии с настоящим Регламентом;

(d) когда это применимо, реквизиты инспектора по защите персональных данных;

(e) оценку воздействия на защиту данных в соответствии со Статьей 35; и

(f) любую иную информацию, по требованию надзорного органа.

4. Государства-члены должны консультироваться с надзорным органом при подготовке предложения о принятии законодательных мер национальным Парламентом, либо мер регулирования, основанных на таких законодательных мерах, которые связаны с обработкой.

5. Несмотря на параграф 1, право государства-члена может обязать контролёров консультироваться с надзорным органом и получать предварительное разрешение от надзорного органа в отношении обработки, осуществляемой контролёром для задач общественных интересов, включая обработку, связанную с социальной защитой и здравоохранением.

Раздел 4

ИНСПЕКТОР ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 37

Назначение на должность инспектора по защите персональных данных

1. Контролёр и обработчик должны назначить инспектора по защите персональных данных при любых обстоятельствах, в случае когда:

(a) обработка осуществляется органом власти или учреждением, за исключением судов, действующих в рамках своей судейской дееспособности;

(b) ключевая деятельность контролёра или обработчика заключается в обработке данных, которая в силу своего характера, своего объема и/или целей, требует регулярного и систематического мониторинга субъектов данных в больших масштабах; или

(c) ключевая деятельность контролёра или обработчика заключается в масштабной обработке особых категорий данных, в соответствии со Статьей 6, а также персональных данных, касающихся осужденнных в уголовном порядке и правонарушителей в соответствии со Статьей 10.

2. Группа компаний может назначить единого инспектора по защите персональных данных, при условии, что инспектор по защите персональных данных может быть легко доступен для каждой компании.

3. В случае если контролёр или обработчик является государственным органом или учреждением, единый инспектор по защите персональных данных может быть назначен для нескольких таких органов власти или учреждений, принимая во внимание их организационную структуру и количественный состав.

4. В случаях, иных чем те, которые указаны в параграфе 1, контролёр, или обработчик, или ассоциации и иные органы, представляющие категории контролёров или обработчиков, могут, или если этого требует право Евросоюза или право государства-члена, должны назначить инспектора по защите персональных данных. Инспектор по защите персональных данных может действовать от лица указанных ассоциаций и иных органов, представляющих контролёров или обработчиков.

5. Инспектор по защите персональных данных должен назначаться на основе профессиональных качеств и, в том числе, на основе экспертных знаний в сфере права защиты данных и практики, а также способности осуществлять задачи, предусмотренные Статьей 39.

6. Инспектор по защите персональных данных может являться сотрудником контролёра или обработчика, или осуществлять задачи на основании договора об оказании услуг.

7. Контролёр или обработчик должны опубликовать реквизиты инспектора по защите персональных данных и сообщить их надзорному органу.

Статья 38

Должность инспектора по защите персональных данных

1. Контролёр и обработчик должны обеспечить, чтобы инспектор по защите персональных данных участвовал в установленном порядке и согласно указанным срокам во всех делах, которые относятся к защите персональных данных.

2. Контролёр и обработчик должны оказывать содействие инспектору по защите персональных данных в осуществлении задач, предусмотренных в Статье 39, посредством средств, необходимых для осуществления таких задач, а также предоставлением доступа к персональным данным и операциям обработки, и поддерживать его/ее экспертную осведомленность.

3. Контролёр и обработчик должны следить за тем, чтобы инспектор по защите персональных данных не получал каких-либо указаний относительно осуществления таких задач. Он/она не должны быть уволены или наказаны контролёром или обработчиком за осуществление их задач. Инспектор по защите персональных данных должен напрямую отчитываться перед руководством высшего уровня контролёра или обработчика.

4. Субъекты данных могут обращаться к инспектору по защите персональных данных относительно всех вопросов, связанных с обработкой их персональных данных, а также связанных с осуществлением их прав в соответствии с настоящим Регламентом.

5. Инспектор по защите персональных данных должен быть связан с соблюдением тайны или конфиденциальности, в отношении осуществления его/ее задач, в соответствии с правом Евросоюза или правом государства-члена.

6. Инспектор по защите персональных данных может выполнять иные задачи и обязанности. Контролёр или обработчик должны следить за тем, чтобы любые такие задачи и обязанности не приводили к конфликту интересов.

Статья 39

Задачи инспектора по защите персональных данных

1. Инспектор по защите персональных должен выполнять, как минимум следующие задачи:

(а) информировать и давать советы контролёру или обработчику, а также сотрудникам, которые осуществляют обработку, относительно их

обязанностей по настоящему Регламенту и иным положениям о защите данных Евросоюза или государства-члена;

(b) осуществлять мониторинг соблюдения настоящего Регламента, иных положений Евросоюза или государства-члена о защите данных, и политик контролёра или обработчика в отношении защиты персональных данных, в том числе распределения обязанностей, повышения осведомленности и обучения персонала, занятого в обработке данных, а также относительно аудита.

(c) давать рекомендации, когда они запрашиваются, относительно оценки воздействия на защиту данных, а также осуществлять мониторинг их выполнения, в соответствии со Статей 35;

(d) сотрудничать с надзорным органом;

(e) действовать в качестве контактного центра для надзорного органа по вопросам, относящимся к обработке, в том числе по предварительному консультированию, предусмотренному Статей 36, а также давать советы, в соответствующих случаях, в относительно иных вопросов;

2. Инспектор по защите персональных данных при выполнении его/ее задач должен соответствующим образом учитывать риск, связанный с операциями обработки, принимая во внимание характер, объем, контекст и цели обработки.

Раздел 5

КОДЕКСЫ ПОВЕДЕНИЯ И СЕРТИФИКАЦИЯ

Статья 40

Кодексы поведения

1. Государства-члены, надзорные органы, Совет и Европейская Комиссия должны содействовать разработке кодексам поведения, предназначенных для надлежащего применения настоящего Регламента, принимая во внимание специфические характеристики различных секторов обработки, а также специфические потребности микро, малых и средних предприятий.

2. Ассоциации и иные организации, представляющие категории контролёров или обработчиков, могут разрабатывать кодексы поведения, либо вносить изменения или распространять такие кодексы, в целях уточнения требований применения настоящего Регламента, к примеру, касающиеся:

(a) справедливой и прозрачной (транспарентной) обработки;

(b) законных интересов контролёров в конкретных условиях;

(c) сбора персональных данных;

(d) псевдонимизации персональных данных;

(e) информации, предоставляемой общественности и субъектам данных;

(f) осуществления прав субъектов данных;

(g) информации, предоставляемой детям и защиты детей от информации, а также способа, с помощью которого получено согласие лиц, обладающих родительской ответственностью над детьми;

(h) мер и процедур, предусмотренных Статьями 24 и 25, а также мер для обеспечения безопасности обработки в соответствии со Статей 32;

(i) уведомления надзорных органов об утечке персональных данных и сообщение о таких утечках персональных данных субъектам данных;

(j) передачи персональных данных третьим странам или международным организациям; или

(k) внесудебных процедур, а также иных процедур рассмотрения споров, разрешающих споры между контролёрами и субъектами данных, связанных с обработкой, без ущерба правам субъектов данных в соответствии со Статьями 77 и 79.

3. В дополнение к точному соблюдению контролёрами или обработчиками, на которых распространяется настоящий Регламент, кодексы поведения, одобренные в соответствии с параграфом 5 настоящей Статьи, и обладающие общим характером действия в соответствии с параграфом 9 настоящей Статьи, могут также соблюдаться контролёрами или обработчиками, на которых не распространяется настоящий Регламент, согласно Статье 3, для того, чтобы обеспечить надлежащую защиту в контексте передачи персональных данных третьим странам или международным организациям, как это предусмотрено в пункте (e) Статьи 46 (2). Указанные контролёры или обработчики должны придать обязательную и принудительную силу договорным или иным законным образом обязывающим документам, для того, чтобы применять такую надлежащую защиту, в том числе в отношении прав субъектов данных.

4. Кодекс поведения, предусмотренный параграфом 2 настоящей Статьи, должен содержать механизмы, которые позволят органу, указанному в Статье 41 (1), осуществлять обязательный мониторинг соблюдения его положений контролёрами или обработчиками, которые берут на себя обязательства применять его, без ущерба задачам и полномочиям надзорных органов, компетентных в соответствии со Статьей 55 или 56.

5. Ассоциации и иные органы, указанные в параграфе 2 настоящей Статьи, которые намерены разработать кодекс поведения, или изменить, либо расширить существующий кодекс, должны представить проект кодекса, поправки или его расширение надзорному органу, который компетентен в соответствии со Статьей 55. Надзорный орган должен предоставить заключение о том, соответствует ли проект кодекса, изменение или расширение настоящему Регламенту, а также должен утвердить такой проект кодекса, его изменения или расширение, если посчитает, что это обеспечит достаточную надлежащую защиту.

6. Когда проект кодекса, или поправки или расширение утвержден в соответствии с параграфом 5 и рассматриваемый кодекс поведения не связан с обработкой данных в нескольких государствах-членах, надзорный орган должен зарегистрировать и опубликовать кодекс.

7. В случае, когда проект кодекса связан с обработкой данных в нескольких государствах-членах, надзорный орган, компетентный согласно Статье 55, должен, до утверждения проекта кодекса, изменений или расширений, передать его в соответствии с процедурой, указанной в Статье 63, Совету (Board), который должен дать заключение о соответствии проекта кодекса, поправок или расширений, настоящему Регламенту, либо, в случае, указанном в параграфе 3 настоящей Статьи, предусматривает ли он соответствующую защиту.

8. В случае, когда заключение, предусмотренное параграфом 7, подтверждает, что проект кодекса, его изменения или расширение соответствует настоящему Регламенту, или в случае, указанном в параграфе 3, предусматривает соответствующую защиту, Совет должен представить свое заключение Европейской Комиссии.

9. Европейская Комиссия может посредством имплементирующих актов принять решение о том, что утвержденный кодекс поведения, поправки или расширения, предоставленные ему на рассмотрение в соответствии с пунктом 8 настоящей Статьи, имеют общий характер действия на территории Евросоюза. Такие имплементирующие акты утверждаются в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

10. Европейская Комиссия должна обеспечить размещение в открытом доступе утвержденных кодексов, которые были определены как обладающие общим характером действия в соответствии с параграфом 9.

11. Совет (Board) сводит в реестр все утвержденные кодексы, изменения и распространения, и доводит их до всеобщего сведения посредством соответствующих мер.

Статья 41

Мониторинг утвержденных кодексов поведения

1. Без ущерба для задач и полномочий компетентного надзорного органа в соответствии со Статьями 57 и 58 мониторинг соответствия кодекса поведения, согласно Статьей 40, может осуществляться органом, обладающим соответствующим уровнем квалификации в отношении предметной составляющей кодекса, а также аккредитован для таких целей компетентным надзорным органом.

2. Орган, указанный в параграфе 1, может быть аккредитован для мониторинга соответствия кодекса поведения, когда такой орган:

(a) продемонстрировал свою независимость и квалификацию в отношении предметной составляющей кодекса во исполнение требований компетентного надзорного органа;

и которая удовлетворила требования компетентного надзорного органа;

(b) установил процедуры, которые позволяют ему оценивать, пригодность соответствующих контролёров и обработчиков применять кодекс, осуществлять мониторинг их соответствия положениям кодекса, а также проводить периодическую проверку их действий;

(c) определил процедуры и структуры для рассмотрения жалоб о нарушениях кодекса, либо способов, с помощью которых применялся или применяется кодекс контролёром или обработчиком, а также а также для того чтобы сделать указанные процедуры и структуры прозрачными для субъектов данных и общественности; и

(d) продемонстрировал компетентному надзорному органу, что его задачи и обязанности не приведут к конфликту интересов.

3. Компетентный надзорный орган должен представить проект критериев для аккредитации органа, предусмотренного параграфом 1 настоящей Статьи, Совету согласно **механизму согласования**, в соответствии со Статьей 63.

4. Без ущерба для задач и полномочий компетентного надзорного органа, а также положениям Главы VIII, орган, предусмотренный параграфом 1 настоящей Статьи, при условии соблюдения надлежащих гарантий, должен предпринимает соответствующие действия в случаях нарушения кодекса контролёром или обработчиком, в том числе отстранение или исключение соответствующего контролёра или обработчика от кодекса. Он должен проинформировать компетентный надзорный орган о таких действиях и причинах их принятия.

5. Компетентный надзорный орган должен отозвать аккредитацию органа, указанного в параграфе 1, если условия аккредитации не соблюдаются или больше не выполняются, либо когда действия, предпринятые органом, нарушают настоящий Регламент.

6. Настоящая Статья не должна применяться в отношении обработки, осуществляемой компетентными государственными органами или учреждениями.

Статья 42

Сертификация

1. Государства-члены, надзорные органы, Совет и Европейская Комиссия должны содействовать, в частности на уровне Евросоюза, внедрению механизмов сертификации защиты данных, а также печатей и маркировочных знаков для защиты данных с целью подтверждения соблюдения настоящего Регламента при операциях обработки, контролёрами

и обработчиками. Конкретные потребности микро, малых и средних предприятий должны быть приняты во внимание.

2. В дополнение к точному соблюдению контролёрами или обработчиками, на которых распространяется настоящий Регламент, механизмы сертификации защиты данных, печати или маркировочные знаки, утвержденные в соответствии с параграфом 5 настоящей Статьи, могут устанавливаться с целью подтверждения наличия соответствующих гарантий, предоставляемых контролёрами или обработчиками, которые не подпадают под действие настоящего Регламента согласно Статье 3, в контексте передачи персональных данных третьим странам или международным организациям, согласно пункту (f) Статьи 46 (2). Указанные контролёры или обработчики должны придать обязательную и принудительную силу договорным или иным законным образом обязывающим документам, для того, чтобы применять такие надлежащие гарантии, в том числе в отношении прав субъектов данных.

3. Сертификация должна быть добровольной и доступной посредством прозрачного (транспарентного) процесса.

4. Сертификация, согласно настоящей Статье, не уменьшает ответственности контролёра или обработчика по соблюдению настоящего Регламента и действует без ущерба задачам и полномочиям надзорного органа, который обладает компетенцией в соответствии со Статьей 33 или 56.

5. Сертификация, в соответствии с настоящей Статье, должна осуществляться органами сертификации, указанными в Статьей 43, или компетентным надзорным органом на основе критериев, утвержденных таким компетентным надзорным органом, согласно Статье 58 (3), либо Советом, в соответствии со Статьей 63. Если критерии утверждены Советом, это может означать общую сертификацию, Европейский сертификат защиты данных[48].

6. Контроллер или обработчик, который направляет на рассмотрение свою обработку для проведения механизма сертификации, должен предоставить органу сертификации, предусмотренному Статьей 43, или, когда это применимо, компетентному надзорному, органу всю информацию, а также доступ к обработке данных, которые являются необходимыми для проведения процедуры сертификации.

7. Сертификация должна предоставляться контролёру или обработчику на максимальный трехлетний срок, и может быть продлена на тех же условиях, в том случае, если соответствующие требования продолжают соблюдаться. Сертификация должна быть отозвана, когда это применимо, органами сертификации, указанными в Статье 43, или компетентным надзорным органом, в том случае, когда требования сертификации не соблюдены, или больше не соблюдаются.

[48] *European Data Protection Seal*

8. Совет[49] должен свести все механизмы сертификации, а также печати защиты данных и маркировочные знаки в реестр, а также довести их до всеобщего сведения посредством любых соответствующих мер.

Статья 43

Органы сертификации

1. Без ущерба для задач и полномочий компетентного надзорного органа, согласно Статьям 57 и 58, органы сертификации, обладающие надлежащим уровнем квалификации в отношении защиты данных, после информирования надзорного органа, для того, чтобы содействовать ему в осуществлении им своих полномочий, в соответствии с пунктом (h) Статьи 58 (2), когда это необходимо, должны выдавать и возобновлять сертификацию. Государства-члены должны обеспечить, чтобы такие органы сертификации были аккредитованы одним или обоими из следующих органов:

(a) надзорным органом, компетентным в соответствии со Статьями 55 или 56; и/или

(b) национальным органом по аккредитации, упомянутым в Регламенте (ЕС) № 765/2008 Европейского Парламента и Совета[50], соответственно EN-ISO/IEC 17065/2012, а также согласно дополнительным требованиям, установленными надзорным органом, являющимся компетентным органом в соответствии со Статьей 55 или 56.

2. Органы сертификации, предусмотренные параграфом 1, должны быть аккредитованы в соответствии с этим параграфом только, там, где они:

(a) продемонстрировали свою независимость и квалификацию в отношении предметной сферы сертификации во исполнение требований компетентного надзорного органа;

(b) обязались соблюдать критерии, предусмотренные в Статье 42 (5), и одобренные надзорным органом, который является компетентным в соответствии со Статьей 55 или 56 или Советом, согласно Статье 63;

(c) установили процедуры выдачи, периодического рассмотрения и отзыва сертификации защиты данных, печатей и знаков;

(d) определили процедуры и структуры для рассмотрения жалоб о нарушениях сертификации, или о способе которым такая сертификация была осуществлена или осуществляется контролёром или обработчиком, а также и сделали такие процедуры и структуры прозрачными для субъектов данных и общественности; и

---

[49] *Board*

[50] Регламент (ЕС) 765/2008 Европейского Парламента и Совета ЕС от 9 июля 2008 г., устанавливающий требования к аккредитации и надзору в отношении продукции, размещаемой на рынке ЕС, и отменяющий Регламент (ЕЭС) 339/93. (Официальный Журнал Европейского Союза № L 218, 13.08.2008, С. 30). *Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).*

(e) продемонстрировали во исполнение требований компетентного надзорного органа, что их задачи и обязанности не приведут к конфликту интересов.

3. Аккредитация органов сертификации, согласно параграфам 1 и 2 настоящей Статьи, должна осуществляться на основе критериев, утвержденных надзорным органом, который является компетентным в соответствии со Статей 55 или 56, либо Советом согласно Статье 63. В случае аккредитации в соответствии с пунктом (b) параграфа 1 настоящей Статьи, указанные требования должны дополнять те требования, которые предусмотрены в Регламенте (ЕС) № 765/2008, а также технические нормы, которые описывают методы и процедуры органов сертификации.

4. Органы сертификации, предусмотренные параграфом 1, должны быть ответственны за надлежащую оценку, которая лежит в основе сертификации или отмены этой сертификации, без ущерба ответственности контролёра или обработчика за соблюдение настоящего Регламента. Аккредитация должна выдаваться на максимальный срок в пять лет и может быть возобновлена на тех же условиях, в случае, если орган по сертификации отвечает требованиям, установленным настоящей Статьей.

5. Органы сертификации, предусмотренные параграфом 1, должны предоставить компетентным надзорным органам причины выдачи или отзыва запрашиваемой сертификации.

6. Требования, предусмотренные параграфом 3 настоящей Статьи, и критерии, предусмотренные Статьей 42 (5), должны быть обнародованы надзорным органом в легкодоступной форме. Эти надзорные органы должны также передать такие требования и критерии Совету. Совет должен внести все механизмы сертификации и печати защиты данных в реестр, а также довести их до всеобщего сведения посредством любых соответствующих мер.

7. Без ущерба для положений Главы VIII, компетентный надзорный орган или национальный орган по аккредитации должны отозвать аккредитацию органа сертификации, согласно параграфу 1 настоящей Статьи, в случаях, когда условия для аккредитации не выполнены, либо не больше не выполняются, или когда действия принятые органом сертификации, нарушают настоящий Регламент.

8. Европейская Комиссия уполномочена принимать подзаконные акты в соответствии со Статьей 92 в целях уточнения требований, которые необходимо принять во внимание для механизмов сертификации защиты данных, упомянутых в Статье 42 (1).

9. Европейская Комиссия может принять имплементирующие акты, устанавливающие технические стандарты для механизмов сертификации, а также печатей защиты данных и знаков, а равно механизмы способствующие и признающие такие механизмы сертификации, печати и знаки. Такие имплементирующие акты должны приниматься в соответствии с процедурой проверки, указанной в статье 93 (2).

ГЛАВА V.

ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ СТРАНАМ ИЛИ МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ

Статья 44

Общие принципы передачи

Любая передача персональных данных, подвергшихся обработке или предназначенные для обработки, после передачи третьей стране или международной организации, должна проводиться лишь в случаях, когда это допускается другими положениями настоящего Регламента, если условия, предусмотренные в этой Главе, соблюдаются контролёром или обработчиком, включая последующую передачу персональных данных из третьей страны или международной организации в другую третью страну или в другую международную организацию. Все положения настоящей Главы должны применяться с целью обеспечения того, чтобы уровень защиты физических лиц, гарантированный настоящим Регламентом, не был подорван.

Статья 45

Передача данных на основе решения достаточности мер

1. Передача персональных данных третьей стране или международной организации может иметь место, когда Европейская Комиссия приняла решение, что третья страна, территория, или один или несколько особых секторов третьей страны, либо соответствующая международная организация обеспечивают надлежащий уровень гарантий. Такая передача не должна требовать какого-либо специального разрешения.

2. При оценке надлежащего уровня защиты Европейская Комиссия должна, в частности, принять во внимание следующие параметры:

(а) верховенство права, уважение прав человека и основных свобод, соответствующее законодательство, как общее, так и отраслевое, в том числе относящееся к общественной безопасности, обороне, национальной безопасности и уголовному праву, и доступу органов власти к персональным данным, а также применение такого законодательства, правил защиты данных, профессиональных правил и мер безопасности, включая правила

последующей передачи персональных данных в другую третью страну или международную организацию, которые соблюдаются в этой третьей стране или международной организации, прецедентное право, а равно действующие и имеющие законную силу права субъекта данных и эффективные административные и судебные средства возмещения вреда субъекту данных, чьи персональные данные передаются;

(b) наличие и эффективное функционирование одного или нескольких самостоятельных надзорных органов в третьей стране, или которым подчинена международная организация, курирующие вопросы гарантий и принудительного обеспечения соблюдения норм защиты данных, в том числе соблюдение надлежащих полномочий в сфере правоприменения, для содействия и консультирования субъектов данных при осуществлении ими своих прав, а также для сотрудничества с надзорными органами государств-членов; и

(c) международные обязательства третьей страны или соответствующей международной организации, которые они взяли на себя, или иные обязательства, вытекающие из конвенций или международных документов, имеющие обязательную юридическую силу, а равно и из их участия в многосторонних или региональных системах, в том числе имеющих отношение к защите персональных данных.

3. Европейская Комиссия, после оценки достаточности уровня защиты, может принять решение, посредством имплементирующего акта, о том, что третья страна, территория, или один или несколько особых секторов третьей страны либо международная организация, обеспечивают надлежащий уровень защиты в соответствии со смыслом положений параграфа 2 настоящей Статьи. Этот имплементирующий акт должен предусматривать механизм периодического обзора, как минимум каждые четыре года, который должен принять во внимание все имеющие значение изменения в третьей стране или международной организации. Этот имплементирующий акт должен устанавливать его территориальное или отраслевое применение и, когда это применимо, определять надзорный орган или органы, предусмотренные пунктом (b) параграфа 2 настоящей Статьи. Этот имплементирующий акт должен быть принят в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

4 Европейская Комиссия должна, на регулярной основе, осуществлять мониторинг изменений в третьих странах и международных организациях, которые могут повлиять на выполнение решений, принятых согласно параграфу 3 настоящей Статьи, а также решений, принятых на основе Статьи 25 (6) Директивы 95/46/ЕС.

5. Европейская Комиссия, при наличии выявленной информации, в том числе руководствуясь рассмотрением, предусмотренным параграфом 3 настоящей Статьи, о том, что третья страна, территория, или один или несколько особых секторов третьей страны либо международная организация, больше не обеспечивают надлежащий уровень защиты в

соответствии со смыслом положений параграфа 2 настоящей Статьи, в той мере в какой это необходимо, должна отменить, изменить или приостановить решение, упомянутое в параграфе 3 настоящей Статьи, посредством имплементирующих актов, не имеющих обратную силу. Такие имплементирующие акты должны приниматься в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

При соответствующей обоснованной настоятельной необходимости Европейская Комиссия должна принять имплементирующие акты прямого действия в соответствии с процедурой, упомянутой в статье 93 (3).

6. Европейская Комиссия должна начать консультации с третьей страной или международной организацией в целях исправления ситуации, которая способствовала принятию решения в соответствии с параграфом 5.

7. Решение, принятое в порядке параграфа 5 настоящей Статьи, действует без ущерба передаче персональных данных третье стране, территории, или одной или нескольким особым секторам третьей страны либо соответствующей международной организации, в соответствии со Статьями 46-49.

8. Европейская Комиссия должна опубликовать в Официальном Журнале Европейского Союза[51], а также на своем веб-сайте список третьих стран, территорий и особых секторов третьей страны и международных организаций, в отношении которых она приняла решение о том, что надлежащий уровень защиты существует, либо больше не обеспечивается.

9. Решения, принятые Европейской Комиссией на основании Статьи 25 (6) Директивы 95/46/ЕС, остаются в силе до тех пор, пока они не изменены, заменены или утратили силу Решением Европейской Комиссии, принятого в соответствии с параграфом 3 или 5 настоящей Статьи.

Статья 46

Передача при наличии надлежащих гарантий

1. При отсутствии решения в порядке Статьи 45(3), контролёр или обработчик могут передать персональные данные третьей стране или международной организации только, если контролёр или обработчик предоставляют надлежащие гарантии, а также при условии, что имеющие законную силу права субъекта данных и действующие средства правовой защиты субъекта данных являются доступными.

2. Эти надлежащие гарантии, упомянутые в параграфе 1, могут предоставляться без специального разрешения надзорного органа посредством:

(a) документов, носящих юридически обязательный характер и подлежащих принудительному применению между органов власти или учреждений;

[51] *Official Journal of the European Union*

(b) обязательных корпоративных правил в соответствии со Статьей 47;

(c) стандартных условий защиты данных, одобренных Европейской Комиссией в соответствии с процедурой проверки, предусмотренной Статьей 93 (2);

(d) стандартных условий защиты данных одобренных надзорным органом, а также одобренных Европейской Комиссией в порядке процедуры проверки, предусмотренной Статьей 93 (2);

(e) утвержденных кодексов поведения, в соответствии со Статьей 40, вместе с юридически обязывающими и подлежащими принудительному исполнению обязательствами контролёра или обработчика в третьей стране в целях применения надлежащих гарантий, в том числе в отношении прав субъектов данных; или

(f) утвержденного механизма сертификации, в порядке Статьи 42, вместе с юридически обязывающими и подлежащими принудительному исполнению обязательствами контролёра или обработчика в третьей стране в целях применения надлежащих гарантий, в том числе в отношении прав субъектов данных.

3. На основании и в соответствии с разрешением компетентного надзорного органа надлежащие гарантии, упомянутые в параграфе 1, могут быть также предоставлены, в частности, посредством:

(a) условий контракта между контролёром или обработчиком, а также между контролёром, обработчиком или получателем персональных данных в третьей стране, или международной организации; или

(b) положений, внесенных в административные договоренности с органами государственной власти или учреждениями, которые включают в себя обеспеченные и действующие права субъектов данных.

4. Надзорный орган должен применять механизм согласования, предусмотренный Статьей 63, в случаях, установленных параграфом 3 настоящей Статьи.

5. Разрешения государства-члена или надзорного органа на основании Статьи 26 (2) Директивы 95/46/ЕС, остаются в силе до изменения, заменены или отменены, при необходимости, этим надзорным органом. Решения, принятые Европейской Комиссией на основании Статьи 26 (4) Директивы 95/46/ЕС, остаются в силе до изменения, заменены или отменены, при необходимости, Решением Европейской Комиссии, принятом в соответствии с параграфом 2 настоящей Статьи.

Статья 47

Обязательные корпоративные правила

1. Компетентный надзорный орган должен утвердить обязательные корпоративные правила в соответствии с механизмом согласования, установленным Статьей 63, при условии, что они:

(a) являются юридически обязательными, а также применяются и принудительно обеспечиваются каждым заинтересованным членом группы компаний или группы предприятий, осуществляющих совместную экономическую деятельность, включая их сотрудников;

(b) явным образом наделяют субъектов данных правами, обеспеченными правовой защитой, в отношении обработки их персональных данных; и

(c) отвечают требованиям, изложенным в параграфе 2.

2. Обязательные корпоративные правила, упомянутые в параграфе 1, должны устанавливать как минимум:

(a) структуру и реквизиты группы компаний или группы предприятий, осуществляющих совместную экономическую деятельность, а также каждого из их членов;

(b) передачу данных или ряд таких передач, в том числе категории персональных данных, тип обработки и их цели, тип затронутых субъектов данных и наименование соответствующей третьей страны или стран;

(c) их юридически обязательных характер, как внутренний, так и внешний;

(d) применение общих принципов защиты данных, в том числе, целевое ограничение, минимизация данных, ограничение сроков хранения, качество данных, защита данных для определенных целей/случаев и по умолчанию, правовые основания для обработки, обработка специальных категорий персональных данных, меры обеспечения безопасности данных, а также требования, касающиеся дальнейшей передачи данных органам, не связанные обязательными корпоративными правилами;

(e) права субъектов данных в отношении обработки и средства осуществления этих прав, в том числе право не зависеть от решений, основанных исключительно на автоматизированной обработке, включая составление профиля, в соответствии со Статей 22, а также право на подачу жалобы компетентному надзорному органу и в компетентные суды государств-членов, согласно Статье 79, и право на получение возмещения и, при необходимости, компенсации за нарушение обязательных корпоративных правил;

(f) принятие ответственности контролёром или обработчиком, учрежденных на территории государства-члена, за любые нарушения обязательных корпоративных правил любым заинтересованным членом, не учрежденным в Евросоюзе; контролёр или обработчик полностью или частично освобождаются от указанной ответственности, только тогда, когда они докажут, что такой член не несет ответственности за событие, повлекшее за собой ущерб;

(g) каким образом информация об обязательных корпоративных правилах, в частности о положениях, указанных в пунктах (d), (e) и (f) настоящего параграфа, предоставляется субъектам данных в дополнение к Статьям 13 и 14;

(h) задачи любого инспектора по защите данных, назначенного в соответствии со Статьей 37, или любого иного лица или организации, ответственных за мониторинг соблюдения обязательных корпоративных правил в группе компаний или группе предприятий, осуществляющих совместную экономическую деятельность, а также мониторинг подготовки и обработки жалоб;

(i) процедуры рассмотрения жалоб;

(j) механизмы в рамках группы компаний или группы предприятий, осуществляющих совместную экономическую деятельность, для проверки соблюдения обязательных корпоративных правил. Такие механизмы должны охватывать аудиты защиты данных и методы, обеспечивающие устранение нарушений защиты прав субъектов данных. Результаты такой проверки должны быть представлены лицу или организации, указанных в пункте (h), и руководству, которое контролирует группу компаний или группу предприятий, осуществляющих совместную экономическую деятельность, а также должны быть доступны компетентному надзорному органу по его запросу;

(k) механизмы отчетности и учета изменений правил, а также представления отчетности о таких изменениях в надзорный орган;

(l) механизм сотрудничества с надзорным органом для обеспечения соблюдения любым членом группы компаний или группы предприятий, осуществляющих совместную экономическую деятельность, в том числе, посредством предоставления надзорному органу результатов проверок мер, предусмотренных пунктом (j);

(m) механизмы отчетности для компетентных надзорных органов по любым правовым требованиям, применимым к членам группы компаний или группы предприятий, осуществляющих совместную экономическую деятельность, в третьей стране, и которые могут иметь существенное неблагоприятное воздействие по гарантиям, предусмотренным обязательными корпоративными правилами; и

(n) соответствующее обучение по защите данных персонала, имеющего постоянный или регулярный доступ к персональным данным.

3. Европейская Комиссия может детализировать формат и процедуры обмена информацией между контролёрами, обработчиками и надзорными органами относительно обязательных корпоративных правил в соответствии со смыслом настоящей Статьи. Такие имплементирующие акты должны быть приняты в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

Статья 48

Передача данных или раскрытие не утвержденная согласно праву Евросоюза

Любое решение суда или арбитражного органа, а также любое решение административного органа третьей страны, требующее от контролёра или обработчика передачи или раскрытия персональных данных, может быть признано или может подлежать принудительному исполнению любым способом, только если оно основано на международном соглашении, таком как договор о взаимной правовой помощи, действующий между запрашивающей третьей страной и Евросоюзом либо государством-членом, без ущерба иным основаниям для передачи, в соответствии с настоящей Главой.

Статья 49

Изъятия для конкретных случаев

1. В случае отсутствия решения о достаточности мер в порядке Статьи 45 (3) или надлежащих гарантий согласно Статьи 46, включая обязательные корпоративные правила, передача или ряд передач персональных данных третьей стране или международной организации должна иметь место только при соблюдении одного из следующих условий:

(a) субъект данных прямо согласился с предлагаемой передачей после того, как был проинформирован о возможных рисках такой передачи для субъекта данных в связи с отсутствием решения о достаточности мер и надлежащих гарантий;

(b) передача требуется для исполнения договора между субъектом данных и контролёром либо для выполнения преддоговорных мероприятий, предпринятых по запросу субъекта данных;

(c) передача требуется для заключения договора или для исполнения договора, заключенного в интересах субъекта данных между контролёром и иным физическим или юридическим лицом;

(d) передача требуется по веским причинам общественного интереса;

(e) передача требуется для предъявления, осуществления или защиты по предъявленным требованиям и искам;

(f) передача требуется для того, чтобы защитить жизненно важные интересы субъекта данных или иных лиц, в том случае, когда субъект данных физически или юридически не может дать свое согласие;

(g) передача осуществляется из реестра, который, в соответствии с правом Евросоюза или правом государства-члена, предназначен для предоставления информации неограниченному кругу лиц и которая является открытой для ознакомления и широкой общественности в целом, и любого лица, которое может подтвердить наличие законного интереса, но только в той мере, в какой соблюдаются условия, установленные правом Евросоюза или правом государства-члена, для ознакомления, реализуемого в этом конкретном случае.

Когда передача не может основываться на положениях Статьей 45 или 46, в том числе на положениях обязательных корпоративных правил, и ни одно из изъятий для конкретных случаев, предусмотренных первым подпараграфом настоящего параграфа не применимо, передача данных третьей стране или международной организации может иметь место только, если передача не носит повторяющийся характер, касается ограниченного числа субъектов данных, требуется в целях обоснования законных интересов контролёра, которые не имеют преимущественную юридическую силу над интересами или правами и свободами субъекта данных и контролёр оценил все сопутствующие обстоятельства передачи данных, и, на основании такой оценки, предоставил надлежащие гарантии, применительно к защите персональных данных.

Контролёр должен проинформировать о передаче надзорный орган. Контролёр должен, помимо предоставленной информации, указанной в Статьях 13 и 14, проинформировать субъекта данных о передаче данных, а также об обоснованных законных интересах, которые он реализует.

2. Передача в порядке пункта (g) первого подпараграфа параграфа 1 не должна охватывать все персональные данные либо целые категории персональных данных, содержащихся в реестре. Когда реестр предназначен для ознакомления лиц, имеющих законный интерес, передача осуществляется только по запросу таких лиц или если такие лица являются получателями данных.

3. Пункты (a), (b) и (c) первого подпараграфа параграфа 1, а также второй подпараграф параграфа 1 не применяются к деятельности, осуществляемой органами власти при выполнении ими своих публичных полномочий.

4. Общественный интерес, упомянутый в пункте (d) первого подпараграфа параграфа 1, должен быть признан в праве Евросоюза или в праве государства-члена, которое применимо к контролёру.

5. В случае отсутствия решения о достаточности мер, право Евросоюза или право государство-члена может по веским основаниям общественного интереса, прямо устанавливать ограничения на передачу конкретных категорий персональных данных третьей стране или международной организации. Государства-члены должны о таких положениях уведомить Европейскую Комиссию.

6. Контролёр или обработчик должны документировать оценку, также как и достаточность гарантий, упомянутых вторым подпараграфом параграфа 1 настоящей Статьи, в учетных записях, предусмотренных Статьей 30.

Статья 50

Международное сотрудничество по защите персональных данных

В отношении третьих стран и международных организаций, Европейская Комиссия и надзорные органы должны принимать необходимые меры для того, чтобы:

(a) совершенствовать международные механизмы сотрудничества для содействия эффективному применению законодательства о защите персональных данных;

(b) оказывать международную взаимную помощь в обеспечении соблюдения законодательства о защите персональных данных, в том числе посредством уведомлений, передач жалоб на рассмотрение, помощи в расследовании, а также обмена информацией, с учетом соответствующих гарантий защиты персональных данных и других основных прав и свобод;

(c) привлекать соответствующих заинтересованных участников (стейкхолдеров) к обсуждению и мероприятиям, направленных на содействие международному сотрудничеству в обеспечении соблюдения законодательства о защите персональных данных;

(d) содействовать обмену и выдаче документов о законодательстве по защите персональных данных и правоприменительной практике, в том числе в отношении конфликта юрисдикций с третьими странами.

ГЛАВА VI.

САМОСТОЯТЕЛЬНЫЕ НАДЗОРНЫЕ ОРГАНЫ

Раздел 1

САМОСТОЯТЕЛЬНЫЙ СТАТУС

Статья 51

Надзорный орган

1. Каждое государство-член должно предусмотреть существование одного или нескольких самостоятельных полномочных государственных органов, являющихся ответственными за мониторинг применения настоящего Регламента, для того, чтобы обеспечить защиту основных прав и свобод физических лиц в отношении обработки, а также свободного движения персональных данных на территории Евросоюза (далее – «Надзорный орган»).

2. Каждый Надзорный орган должен внести свой вклад в согласованное применение настоящего Регламента на территории всего Евросоюза. В этих целях Надзорные органы должны сотрудничать друг с другом, а также с Европейской Комиссией согласно Главе VII.

3. В случае, когда в государстве-члене учреждается более одного Надзорного органа, такое государство-член назначает Надзорный орган,

который представляет эти органы в Совете, а также должно установить механизм обеспечения соблюдения другими ведомствами норм, относящихся к механизму согласования, предусмотренного в Статье 63.

4. Каждое государство-член должно уведомить Европейскую Комиссию о нормативных положениях своего права, которые приняты в соответствии с настоящей Главой, к 25 мая 2018 г., а также, без промедления уведомлять о любых последующих поправках, затрагивающих нормативные положения.

Статья 52

Самостоятельность

1. Каждый Надзорный орган действует с полной самостоятельностью при осуществлении своих задач и выполнении своих полномочий в соответствии с настоящим Регламентом.

2. Член или члены каждого Надзорного органа должны, при выполнении своих задач и осуществлении своих полномочий в соответствии с настоящим Регламентом, оставаться свободными от внешнего воздействия, будь то прямое или косвенное, а также не должны искать или получать указания от кого бы то ни было.

3. Член или члены каждого Надзорного органа должны воздерживаться от любых действий, несовместимых с их обязанностями, а также не должны, в течение срока их полномочий, заниматься любым иным несовместимым видом деятельности, оплачиваемым или неоплачиваемым.

4. Каждое государство-член должно обеспечить, чтобы каждому Надзорному органу были предоставлены кадровые, технические и финансовые ресурса, помещения и инфраструктура, необходимые для эффективного выполнения его задач и осуществления его полномочий, в том числе те, которые осуществляются контексте взаимной помощи, сотрудничества и участия в Совете.

5. Каждое государство-член должно обеспечить, чтобы каждый Надзорный орган выбирал и располагал своим собственным персоналом, который находится в непосредственном подчинении члена или членов заинтересованного надзорного органа.

6. Каждое государство-член должно обеспечить, чтобы каждый Надзорный орган подвергался финансовому контролю, который не влияет на его самостоятельность, и что он обладает отдельным, открытым годовым бюджетом, который может являться частью общего или национального бюджета.

Статья 53

Общие условия для членов Надзорного органа

1. Государство-член должно обеспечить, чтобы каждый член его Надзорного органа был назначен посредством прозрачной процедуры:

– его Парламентом;

– его Правительством;

– его Главой государства; или

– самостоятельным учреждением, на которое возложены обязанности по назначению согласно праву государства-члена.

2. Каждый член должен обладать квалификацией, опытом и знаниями, в том числе в сфере защиты персональных данных, требуемых для выполнения своих обязанностей и осуществления своих полномочий.

3. Обязанности члена должны прекращаться в случае истечения срока полномочий, отставки или обязательного выхода на пенсию, в соответствии с правом конкретного государства-члена.

4. Член должен быть освобожден от должности только в случае серьезного нарушения или если он больше не соблюдает условия, необходимые для выполнения обязанностей.

Статья 54

Правила учреждения Надзорного органа

1. Каждое государство-член должно предусмотреть законодательно всё нижеследующее:

(a) создание каждого Надзорного органа;

(b) квалификации и условия приемлемости, требуемые для назначения в качестве члена каждого Надзорного органа;

(c) правила и процедуры назначения члена или членов каждого надзорного органа;

(d) продолжительность срока полномочий члена или членов каждого надзорного органа не менее четырех лет; за исключением первого назначения после 24 мая 2016 года, часть которого может иметь место на более короткий период, когда это необходимо для обеспечения самостоятельности Надзорного органа с помощью использования ступенчатой процедуры назначения;

(e) могут ли, и если да, на какой срок член или члены каждого Надзорного органа обладать правом на повторное назначение*;*

(f) положения, регулирующие обязанности члена или членов, а также персонала каждого Надзорного органа, запреты на несовместимость действий, видов деятельности и выплат в течение и по окончании срока полномочий, равно как и правила, регулирующие прекращение службы.

2. Член или члены, а также персонал каждого Надзорного органа должны, в соответствии с правом Евросоюза или правом государства-члена, подпадать под действие обязанности соблюдения профессиональной тайны,

как во время, так и после истечения срока их полномочий, в отношении любой конфиденциальной информации, которая стала известна им в ходе выполнения своих задач или осуществления своих полномочий. В течение срока их полномочий такая обязанность соблюдения профессиональной тайны должна, в том числе, применяться к сообщениям физических лиц о нарушениях настоящего Регламента.

Раздел 2

КОМПЕТЕНЦИЯ, ЗАДАЧИ И ПОЛНОМОЧИЯ

Статья 55

Компетенция

1. Каждый надзорный орган должен обладать компетенцией по выполнению задач, возложенных на него, и осуществлению полномочий, предоставленных ему в соответствии с настоящим Регламентом, на территории его собственного государства-члена.

2. В случае, когда обработка осуществляется государственными органами или частными организациями, действующими на основании пункта (c) или (e) Статьи 6 (1), Надзорный орган соответствующего государства-члена должен являться компетентным органом. В таких случаях Статья 56 не применима.

3. Надзорные органы не обладают компетенцией по контролю операций обработки данных судами в рамках их судейской дееспособности.

Статья 56

Компетенция руководящего надзорного органа

1. Без ущерба для действия Статьи 55, Надзорный орган главного учреждения или единственного учреждения контролёра или обработчика должен обладать компетенцией действовать как руководящий надзорный орган для трансграничной обработки, осуществляемой таким контроллером или обработчиком в соответствии с процедурой, предусмотренной в Статье 60.

2. В порядке изъятия из параграфа 1, каждый Надзорный орган должен быть компетентен рассматривать поданные ему жалобы или вероятное нарушение настоящего Регламента, если предмет имеет отношение только к

учреждению в его государстве-члене или существенно влияет на субъектов данных только в его государстве-члене.

3. В случаях, упомянутых в параграфе 2 настоящей Статьи, Надзорный орган должен незамедлительно проинформировать руководящий надзорный орган на этот счет. В течение трех недельного срока после получения соответствующей информации руководящий надзорный орган должен приять решение о том, будет или не будет он рассматривать заявление в соответствии с процедурой, предусмотренной в Статье 60, принимая во внимание то, находится или нет учреждение контролёра или обработчика в государстве-члене, Надзорный орган которого проинформировал его.

4. В том случае, когда руководящий надзорный орган решает рассмотреть заявление, применяется процедура, предусмотренная Статьей 60. Надзорный орган, который проинформировал руководящий надзорный орган, может представить руководству надзорного органа проект решения. Руководящий надзорный орган должен максимально учесть этот проект при подготовке проекта решения, упомянутого в Статье 60 (3).

5. Когда руководящий надзорный орган решает не рассматривать заявление, надзорный орган, который проинформировал руководящий надзорный орган, должен решить его в соответствии со Статьями 61 и 62.

6. Руководящий надзорный орган должен быть единственным посредником контролёра или обработчика при трансграничной обработке, осуществляемой таким контролёром или обработчиком.

Статья 57

Задачи

1. Без ущерба для других задач, установленных настоящим Регламентом, каждый надзорный орган на своей территории должен:

(a) осуществлять мониторинг применения настоящего Регламента;

(b) содействовать повышению осведомленности общественности и разъяснению относительно рисков, норм, гарантий и прав, касающихся обработки. Мероприятиям, адресованные детям, должно уделяться особое внимание;

(c) консультировать в соответствии с правом государства-члена, национальный Парламент, Правительство и иные учреждения и органы в отношении законодательных и административных мер, относящихся к защите прав и свобод физических лиц, касающихся обработке данных;

(d) содействовать повышению осведомленности контролёров и обработчиков относительно их обязательств по настоящему Регламенту;

(e) предоставлять информацию, по запросу, любому субъекту данных, касающуюся осуществления их прав согласно настоящему Регламенту и, при необходимости, сотрудничать с надзорными органами в других государствах-членах в этих целях;

(f) рассматривать жалобы, поданные субъектом данных или органом, организацией, либо ассоциацией в соответствии в соответствии со Статьей 80, а также разбирать, в тех случаях, когда это уместно, предмет жалобы и информировать заявителя о ходе и результатах разбирательства в разумный срок, в частности, о дальнейшем разбирательстве или координация с другим надзорным органом при необходимсти;

(g) сотрудничать, включая обмен информацией и предоставление взаимной помощи, с другими надзорными органами, в целях обеспечения согласованного применения и обеспечения соблюдения настоящего Регламента;

(h) проводить разбирательства по применению настоящего Регламента, в том числе на основе информации, полученной от другого надзорного органа или другого органа власти;

(i) осуществлять мониторинг соответствующих изменений, в той части в которой они влияют на защиту персональных данных, в том числе на развитие информационно-коммуникационных технологий и коммерческих практик;

(j) утверждать стандартные условия договоров, предусмотренные в Статье 28 (8) и в пункте (d) Статьи 46 (2);

(k) устанавливать и вести список в отношении требования оценки воздействия защиты данных в соответствии со Статьей 35 (4);

(l) консультировать по операциям обработки данных, предусмотренных Статьей 36 (2);

(m) поощрять разработку кодексов поведения в порядке Статьи 40 (1), а также давать заключения и утверждать такие кодексы поведения, которые обеспечивают достаточные гарантии в соответствии со Сатьей 40 (5);

(n) поощрять создание механизмов сертификации защиты данных, а также печатей и знаков защиты данных в порядке Статьи 42 (1) и утверждать критерии сертификации в порядке Статьи 42 (5);

(o) проводить, когда это применимо, периодическую проверку сертификатов, выданных в порядке Статьи 42 (7);

(p) составлять и публиковать критерии аккредитации органа по осуществлению мониторинга за соблюдением кодексов поведения в порядке Статьи 41 и органа по сертификации в порядке Статьи 43;

(q) проводить аккредитацию органа по осуществлению мониторинга за соблюдением кодексов поведения контролю за соблюдением норм поведения в соответствии со Статьей 41 и органа по сертификации в соответствии со Статьей 43;

(r) утверждать договорные условия и положения, предусмотренные в Статьей 44 (3);

(s) утверждать обязательные корпоративные правила, согласно Статьей 47;

(t) содействовать деятельности Совета;

(u) вести внутренний учет нарушений настоящего Регламента и мер, принятых в соответствии со Статьей 58 (2); и

(v) выполнять любые иные задачи, относящиеся к защите персональных данных.

2. Каждый надзорный орган должен облегчать подачи жалоб, указанных в пункте (f) параграфа 1, посредством таких мер как предоставление форм подачи жалоб, которые также могут быть заполнены в электронном виде, без исключения использования иных средств связи.

3. Осуществление задач каждого надзорного органа осуществляется на безвозмездной основе для субъекта данных и, когда это применимо, для инспектора по защите персональных данных.

4. Когда запросы являются явно необоснованными или чрезмерными, в том числе из-за их повторяющегося характера, надзорный орган может взимать разумную плату в зависимости от административных расходов или отказаться действовать по запросу. Надзорный орган должен нести бремя доказывания необоснованного или чрезмерного характера запроса.

Статья 58

Полномочия

1. Каждый надзорный орган должен располагать всеми нижеследующими следующими полномочиями по разбирательствам:

(a) поручать контролёру и обработчику и, кода это применимо, представителю контролёра и обработчика, предоставить любую информацию, требуемую для выполнения его задач;

(b) осуществлять разбирательства в форме аудиторских проверок защиты данных;

(c) проводить обзор сертификаций, выданных в порядке Статьи 42 (7);

(d) уведомлять контролёра или обработчика о предполагаемом нарушении настоящего Регламента;

(e) получать от контролёра и обработчика доступ ко всем персональным данным, а также ко всей информации, необходимой для выполнения своих задач;

(f) получать доступ к любым помещениям контролёра и обработчика, включая любое оборудование и средства для обработки данных, в соответствии с процессуальным правом Евросоюза или процессуальным правом государства-члена.

2. Каждый надзорный орган должен располагать всеми нижеследующими следующими полномочиями по устранению недостатков:

(a) выносить предупреждения контролёру или обработчику о том, что предполагаемая обработка данных способна нарушить положения настоящего Регламента;

(b) объявлять выговор контролёру или обработчику, если операция обработки нарушила положения настоящего Регламента;

(c) предписывать контролёру или обработчику соблюдать запросы субъекта данных относительно осуществления его/ее прав по настоящему Регламенту;

(d) предписывать контролёру или обработчику вести операции обработки в соответствии с положениями настоящего Регламента, когда это применимо, в установленном порядке в течение определенного срока;

(e) предписывать контролёру сообщить субъекту данных об утечке персональных данных;

(f) налгать временные или окончательные ограничения, включая запрет обработки;

(g) предписывать исправить или удалить персональные данные, либо ограничить обработку в порядке Статей 16, 17 и 18, а также уведомить об указанных мерах получателей, которым были раскрыты персональные данные в соответствии со Статьей 17 (2) и Статьей 19;

(h) отозывать сертификат или предписывать органу сертификации отозвать сертификат, выданный в соответствии со Статьями 42 и 43, либо предписать органу сертификации не выдавать сертификат, если требования к сертификации отсутствуют или больше не выполняются;

(i) налагать административный штраф в порядке Статьи 83 в дополнение или вместо мер, предусмотренных в настоящем параграфе, в зависимости от обстоятельств каждого конкретного дела;

(j) предписывать приостановку перемещения потока данных получателю в третьей стране или международной организации.

3. Каждый надзорный орган должен обладать всеми нижеследующими полномочиями, связанными с выдачей разрешений и консультативными полномочиями:

(a) консультировать контролёра в соответствии с процедурой предварительной консультации, предусмотренной Статьей 36;

(b) выдавать заключения, по собственной инициативе или по запросу, для национального Парламента, Правительства государства-члена или, в соответствии с правом государства-члена, иным учреждениям и органам, а также для общественности по любому вопросу, относящемуся к защите персональных данных;

(c) разрешать обработку, упомянутую в Статье 36 (5), если право государства-члена требует такого предварительного разрешения;

(d) выдавать заключения и утверждать кодексы поведения в порядке Статьи 40 (5);

(e) осуществлять аккредитацию органов сертификации в порядке Статьи 43;

(f) выдавать сертификаты и утверждать критерии сертификации в соответствии со Статьей 42 (5);

(g) утверждать стандартные условия защиты данных, предусмотренные Статьей 28 (8) и в пунктом (d) Статьи 46 (2);

(h) утверждать договорные условия, предусмотренные пунктом (a) Статьи 46 (3);

(i) утверждать административные договоренности, предусмотренные пунктом (b) Статьи 46 (3);

(j) утверждать обязательные корпоративные правила в соответствии со Статьей 47.

4. Осуществление полномочий, предоставленных надзорному органу в порядке настоящей Статьи, должно подпадать под действие соответствующих гарантий, включая эффективные средства судебной защиты и процессуальные гарантии, закрепленные в праве Евросоюза и в праве государства-члена в соответствии с Хартией.

5. Каждое государство-член должно законодательно предусмотреть, что его надзорный орган обладает полномочиями довести до сведения органов судебной власти о нарушении настоящего Регламента и, когда это применимо, вправе возбудить судебное производство или иным образом участвовать в нем, для того, чтобы обеспечить соблюдение положений настоящего Регламента.

6. Каждое государство-член может законодательно предусмотреть, что его надзорный орган обладает дополнительными полномочиями, по отношению к тем, которые предусмотрены параграфами 1, 2 и 3. Осуществление этих полномочий не нарушает действенного функционирования Главы VII.

Статья 59

Отчет о деятельности

Каждый надзорный орган подготавливает ежегодный отчет о своей деятельности, который может включать список типов зарегистрированных нарушений, а также виды мероприятий, принятых в соответствии со Статьей 58 (2). Такие отчеты должны передаваться национальному Парламенту, Правительству и иным органам, как это предусмотрено правом государства-члена. Они должны быть доступны для общественности, Европейской Комиссии и Совету.

ГЛАВА VII.

СОТРУДНИЧЕСТВО И СОГЛАСОВАНИЕ

Раздел 1

СОТРУДНИЧЕСТВО

Статья 60

Сотрудничество между руководящим надзорным органом и иными заинтересованными надзорными органами

1. Руководящий надзорный орган должен сотрудничать с иными заинтересованными надзорными органами в соответствии с настоящей Статьей в стремлении достигнуть консенсуса. Руководящий надзорный орган и заинтересованные надзорные органы должны обмениваться всей существенной информацией друг с другом.

2. Руководящий надзорный орган может запросить в любое время иные заинтересованные надзорные органы оказать взаимную помощь в порядке Статьи 61, а также может проводить совместные операции в соответствии со Статьей 62, в частности для проведения рассмотрения или осуществления мониторинга использования мер, качающихся контролёра или обработчика, учрежденных в другом государстве-члене.

3. Руководящий надзорный орган должен незамедлительно передать соответствующую информацию по вопросу другим заинтересованным надзорным органам. Он без промедления должен представить проект решения другим заинтересованным надзорным органам для их заключения и должен учесть их позицию.

4. В случае, когда другой заинтересованных надзорных органов в течение четырех недель после проведения консультаций, согласно параграфу 3 настоящей Статьи, выскажет соответствующее и мотивированное возражение против этого проекта решения, руководящий надзорный орган, если он не поддержит соответствующее и мотивированное возражение, либо посчитает, что возражение не является соответствующим или не мотивированным, передает такой вопрос на **механизм согласования**, предусмотренный Статьей 63.

5. Когда руководящий надзорный орган намерен поддержать соответствующее и мотивированное возражение, он передает иным заинтересованным надзорным органам доработанный проект решения для их заключения. Такой доработанный проект решения подлежит **процедуре,** указанной в параграфе 4, в двух недельный срок.

6. Если ни один из других заинтересованных надзорных органов не возражает против проекта решения, который был представлен руководящим надзорным органом в течение срока, указанного в параграфах 4 и 5, руководящий надзорный орган и заинтересованные надзорные органы считаются согласными с таким проектом решения и должны быть связаны таким проектом решения.

7. Руководящий надзорный орган должен принять решение и уведомить о нем главное учреждение или единственное учреждение контролёра или

обработчика, сообразно обстоятельствам, а также проинформировать другие заинтересованные надзорные органы и Совет относительно соответствующего решения, включая краткое изложение соответствующих фактов и оснований. Надзорный орган, которому подана жалоба, информирует заявителя о таком решении.

8. В порядке изъятия из параграфа 7, в случае, когда отказано в удовлетворении жалобы или она отклонена, надзорный орган, которому она была подана, должен принять решение и уведомить о нем заявителя, а также проинформировать соответствующего контролёра.

9. В случае, когда руководящий надзорный орган и заинтересованные надзорные органы соглашаются отказать в удовлетворении жалобы или отклонить часть жалобы, и предпринимают действия по другим частям такой жалобы, должно быть принято отдельное решение по каждым отдельным частям жалобы. Руководящий надзорный орган должен принять решение относительно той части, касающейся действий, связанных с контролёром, должен уведомить о нем главное учреждение или единственное учреждение контролёра или обработчика на территории своего государства-члена, а также должен проинформировать об этом соответствующего заявителя, при этом надзорный орган заявителя должен вынести решение относительно части, связанной с отказом в удовлетворении жалобы или с ее отклонением, и должен уведомить об этом заявителя и проинформировать контролёра или обработчика.

10. После получения уведомления о решении руководящего надзорного органа в порядке параграфов 7 и 9, контролёр или обработчик должны предпринять необходимые меры для обеспечения соблюдения решения касательно обработки данных в отношении всех своих учреждений в Евросоюзе. Контролёр или обработчик должны уведомить руководящий надзорный орган о мерах, препринятых для соблюдения этого решения, который информирует об этом иные заинтересованные надзорные органы.

11. Когда, в исключительных случаях, заинтересованный надзорный орган имеет основания полагать, что существует настоятельная необходимость действовать в целях защиты интересов субъектов данных, применяется процедура безотлагательности, предусмотренная Статьей 66.

12. Руководящий надзорный орган и иные заинтересованные надзорные органы предоставляют информацию, требуемую в соответствии с настоящей Статьей друг другу, электронным способом, с использованием стандартных форм.

Статья 61

Взаимная помощь

1. Надзорные органы должны предоставлять друг другу соответствующую информацию и оказывать взаимную помощь в целях

единообразного осуществления и применения настоящего Регламента, и должны принимать меры для эффективного сотрудничества друг с другом. Взаимная помощь должна распространяться, в том числе, на информационные запросы и меры надзора, такие как запросы относительно предварительных разрешений и консультаций, проверок и рассмотрений.

2. Каждый надзорный орган должен предпринять все соответствующие меры, требующиеся для ответа на запрос другого надзорного органа без неоправданной задержки, и не позднее одного месяца после получения такого запроса. Такие меры могут включать в том числе передачу соответствующей информации о проведении рассмотрения.

3. Запросы об оказании помощи должны содержать всю необходимую информацию, включая цели и причины запроса. Обмен информацией должен использоваться только для цели, которая была указана в запросе.

4. Запрашиваемый надзорный орган не должен отказываться от рассмотрения запроса кроме тех случаев, когда:

(a) он не компетентен в отношении вопросов, составляющих предмет запроса либо таких мер, которые затребованы к исполнению; или

(b) согласие на рассмотрение запроса могло бы нарушить положения настоящего Регламента, либо право Евросоюза или право государства-члена, которому подчиняется надзорный орган, получивший запрос.

5. Запрошенный надзорный орган должен проинформировать запрашивающий надзорный орган о результатах, либо в зависимости от ситуации, о ходе выполнения мероприятий, предпринятых в ответ этот запрос. Запрошенный надзорный орган должен указать причины любого отказа в выполнении запроса в соответствии с параграфом 4.

6. Запрошенные надзорные орган должны, как правило, предоставить информацию, требуемую другими надзорными органами электронным способом, с использованием стандартных форм.

7. Запрошенные надзорные органы не должны взимать плату за любые действия, предпринятые им в соответствии с запросом о взаимной помощи. Надзорные органы могут согласовать правила возмещения друг другу особых затрат, возникших в результате предоставления взаимной помощи в исключительных случаях.

8. В случаях, когда надзорный орган не предоставляет информацию, предусмотренную параграфом 5 настоящей Статьи, в течение одного месяца после получения запроса другого надзорного органа, запрашивающий надзорный орган может принять временную меру на территории своего государства-члена в соответствии со Статьей 55 (1). В этом случае безотлагательная необходимость действовать в соответствии со Статьей 66 (1), должна презюмироваться, чтобы обеспечить и принять безотлагательное обязывающее решение Совета в соответствии со Статьей 66 (2).

9. Европейская Комиссия посредством имплементирующих актов может определить формат и процедуры взаимной помощи, предусмотренной в настоящей Статье, а также порядок обмена информацией электронными

средствами между надзорными органами, и между надзорными органами и Советом, в том числе с использованием стандартных форм, упомянутые в параграфе 6 настоящей Статьи. Такие имплементирующие акты должны приниматься в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

Статья 62

Совместные действия надзорных органов

1. Надзорные органы должны, когда это применимо, проводить совместные действия, в том числе совместные рассмотрения и совместные принудительные меры, в которых принимают участие члены или персонал надзорных органов других государств-членов.

2. В то случае, когда контролёр или обработчик учреждены в нескольких государствах-членах, либо если значительное число субъектов данных в более чем в одном государстве-члене вероятно будут в значительной степени подвергнуты операции обработки, надзорный орган каждого из этих государств-членов должен иметь право участвовать в совместных действиях. Надзорный орган, который является компетентным в соответствии со Статьей 56 (1) или (4), должен пригласить надзорный орган каждого из этих государств-членов принять участие в совместных действиях, а также должен безотлагательно дать ответ на запрос надзорного органа относительно участия.

3. Надзорный орган, в соответствии с правом государства-члена и с разрешения надзорного органа, оказывающего содействие, может наделить полномочиями, в том числе полномочиями по рассмотрению, членов или персонал участвующих в совместных действиях, либо в той мере, в какой право государства-члена принимающего надзорного органа разрешает, может позволить членам или персоналу надзорного органа, оказывающего содействие, осуществлять их полномочия по устранению недостатков в соответствии с правом государства-члена, надзорного органа, оказывающего содействие. Такие полномочия по устранению недостатков могут осуществляться только под руководством и в присутствии членов или персонала принимающего надзорного органа. Члены или персонал, надзорного органа, оказывающего содействие, подчиняются праву государства-члена принимающего надзорного органа.

4. В случае, когда, в соответствии с параграфом 1, персонал надзорного органа, оказывающего содействие, осуществляет свою деятельность в другом государстве-члене, государство-член принимающего надзорного органа должно взять на себя ответственность за их действия, в том числе обязательства за любой ущерб, причиненный ими в результате их деятельности, в соответствии с правом государства-члена, на территории которого они осуществляют свою деятельность.

5. Государство-член, на территории которого был причинен ущерб, должно возместить такой ущерб, с соблюдением условий, применимым в отношении ущерба, причиненного его собственным персоналом. Государство-член надзорного органа, оказывающего содействие, персонал которого причинил ущерб любому лицу на территории другого государства-члена, должно возместить такому другому государству-члену в полном размере любые суммы, выплаченные лицам, управомоченным от их имени.

6. Без ущерба осуществлению своих прав в отношении третьих сторон и за исключением параграфа 5, каждое государство-член, в случае, предусмотренном в параграфе 1, должно воздерживаться от требований возмещения от другого государства-члена относительно ущерба, упомянутого в параграфе 4.

7. В случае, когда предполагаются совместные действия и надзорный орган в течение одного месяца не выполняет обязательства, предусмотренные во втором предложении параграфа 2 настоящей Статьи, другие надзорные органы могут принять временную меру на территории своего государства-члена в соответствии со Статьей 55. В этом случае безотлагательная необходимость действовать в соответствии со Статьей 66 (1), должна презюмироваться, чтобы обеспечить и принять безотлагательное обязывающее решение Совета в соответствии со Статьей 66 (2).

Раздел 2

СОГЛАСОВАНИЕ

Статья 63

Механизм согласования

Для того, чтобы содействовать согласованному применению настоящего Регламента на территории всего Евросоюза, надзорные органы должны сотрудничать друг с другом и, в соответствующих случаях, с Европейской Комиссией посредством механизма согласования, как это предусмотрено в настоящем Разделе.

Статья 64

Заключение Совета

1. Совет должен дать свое заключение, в котором компетентный надзорный орган намерен принять любую из нижеуказанных мер. В этих

целях, компетентный надзорный орган передает Совету проект решения, когда оно:

(a) имеет целью принять перечень операций обработки, с учетом требований оценки воздействия на защиту данных в соответствии со Статьей 35 (4);

(b) затрагивает вопросы, предусмотренные Статьей 40 (7), соответствует ли проект кодекса поведения, или поправок, или расширение, настоящему Регламенту;

(c) имеет целью одобрить критерии аккредитации организаций, согласно Статье 41 (3), или органа сертификации согласно Статье 43 (3);

(d) имеет целью установить стандартные условия защиты данных, указанные в пункте (d) Статьи 46 (2) и Статьи 28 (8);

(e) имеет целью утвердить договорные условия, указанные в пункте (a) Статьи 46(3); или

(f) имеет целью принять обязательные корпоративные правила в соответствии со смыслом Статьи 47.

2. Любой надзорный орган, Председатель Совета или Европейская Комиссия могут потребовать, чтобы любой вопрос общего применения или порождающий последствия в нескольких государствах-членах, был изучен Советом на предмет получения заключения, в том числе когда компетентный надзорный орган не выполняет обязательств по оказанию взаимной помощи в соответствии со Статьей 61 или по совместным действиям в соответствии со Статьей 62.

3. В случаях, указанных в параграфах 1 и 2, Совет должен дать заключение по вопросу, представленному ему на рассмотрение, при условии, что он уже не дал свое заключение по тому же самому вопросу. Такое заключение должно быть принято в течение восьми недель простым большинством голосов членов Совета. Этот срок может быть продлен еще на шесть недель, принимая во внимание сложность предмета вопроса. При рассмотрении проекта решения, предусмотренного пунктом 1, направленное членам Совета, в соответствии с пунктом 5, то член, который не высказал возражения в течение разумного срока, установленного Председателем, считается согласным с проектом решения.

4. Надзорные органы и Европейская Комиссия, должны без необоснованной задержки, передать Совету электронным способом, с использованием стандартизированного формата, любую информацию по данному вопросу, в том числе сообразно обстоятельствам, краткое изложение фактов, проект решения, основания для принятия необходимой меры, а также позиции других заинтересованных надзорных органов.

5. Президиум Совета, без необоснованной задержки, электронным способом информирует:

(a) членов Совета и Европейскую Комиссию о любой направленной ему информации по данному вопросу с использованием стандартизированного

формата. Секретариат Совета, в необходимых случаях, обеспечивает письменный перевод информации по данному вопросу; и

(b) надзорный орган, указанный, в зависимости от ситуации, в параграфах 1 и 2, а также Европейскую Комиссию, о своем заключении и опубликовывает его.

6. Компетентный надзорный орган не принимает свой проект решения, упомянутый в параграфе 1, в течение срока, указанного в параграфе 3.

7. Надзорный орган, упомянутый в параграфе 1, должен в максимальной степени принять во внимание заключение Совета, и, в течение двух недель после получения заключения, сообщить Президиуму Совета электронным способом, оставит ли он свой проект решения без изменений или изменит его, и, если таковой последует, передать измененный проект решения с использованием стандартизированного формата.

8. В случае, когда заинтересованный надзорный орган информирует Президиум Совета, в течение срока, упомянутого, в параграфе 7 настоящей Статьи, что он не намерен следовать заключению Совета, в полном объеме или частично, с указанием соответствующих причин, применяется Статья 65 (1).

Статья 65

Урегулирование Советом спорных вопросов

1. Для того чтобы обеспечить надлежащее и согласованное применение настоящего Регламента, в конкретных случаях, Совет должен принять обязательное для исполнения решение в следующих случаях:

(a) когда, в случае, упомянутом в статье 60 (4), заинтересованный надзорный орган выдал соответствующее и мотивированное **в**озражение против проекта решения руководящего органа, либо руководящий орган отклонил такое возражение как не соответствующее и не мотивированное. Обязательное для исполнения решение должно касаться всех вопросов, которые являются предметом соответствующего и мотивированного возражения, в том числе по вопросу существуют ли нарушения настоящего Регламента;

(b) когда существуют противоречивые позиции относительно того, какой из заинтересованных надзорных органов является компетентным для главного учреждения;

(c) когда компетентный надзорный орган не запрашивает заключение Совета по вопросам, указанным в Статье 64 (1), либо не следует заключению Совета, выданного в соответствии со Статьей 64. В этом случае любой заинтересованный надзорный орган или Европейская Комиссия могут передать этот вопрос Совету.

2. Решение, упомянутое в параграфе 1, должно приниматься в течение одного месяца с момента направления существа вопроса на рассмотрение большинством в две трети голосов членов Совета. Этот срок может быть продлен еще на один месяц, исходя из сложности предмета рассмотрения. Решение, упомянутое в параграфе 1, должно быть обоснованным и направляться руководящему надзорному органу, а также всем заинтересованным надзорным органам, и быть обязательным к исполнению этими органами.

3. В случаях, когда Совет не смог принять решение в сроки, указанные в параграфе 2, он должен принять свое решение в течение двух недель после истечения второго месяца, указанного в параграфе 2, простым большинством членов Совета. Если члены Совета разошлись во мнениях, решение принимается голосованием его Президиума.

4. Заинтересованные надзорные органы не должны принимать решение по существу вопроса, представленному Совету согласно параграфу 1, в течение сроков, предусмотренных в параграфах 2 и 3.

5. Президиум Совета должен уведомить, без необоснованных задержек, о решении, предусмотренном параграфом 1, заинтересованные надзорные органы. Он должен проинформировать о таком решении Европейскую Комиссию. Это решение должно быть опубликовано на веб-сайте Совета без промедления после утверждения надзорным органом окончательного решения, упомянутого в параграфе 6.

6. Руководящий надзорный орган или, в зависимости от обстоятельств, надзорный орган, которому была подана жалоба, должен принять свое окончательное решение на основании решения, предусмотренного параграфом 1 настоящей Статьи, без необоснованных задержек, и, не позднее одного месяца после того, как Совет уведомил о своем решении. Руководящий надзорный орган или, в зависимости от обстоятельств, надзорный орган, которому была подана жалоба, должен проинформировать Совет о дате, когда его окончательное решение доведено до сведения соответственно контролёра или обработчика, или субъекта данных. Окончательное решение заинтересованных надзорных органов должно быть принято в порядке Статей 60(7), (8) и (9). Окончательное решение должно ссылаться на решение, предусмотренное параграфом 1 настоящей Статьи, а также должно устанавливать, что решение, упомянутое в этом параграфе, будет опубликовано на веб-сайте Совета в соответствии с параграфом 5 настоящей Статьи. К окончательному решению должно прилагаться решение, указанное в параграфе 1 настоящей Статьи.

Статья 66

Процедура безотлагательности

1. В исключительных обстоятельствах, когда заинтересованный надзорный орган считает, что существует настоятельная необходимость действовать в целях защиты прав и свобод субъектов данных, он может, путем изъятия из механизма согласования, указанного в Статьях 63, 64 и 65, или от процедуры в прядке Статьи 60, незамедлительно принять обеспечительные меры, порождающие правовые последствия на его собственной территории, с установлением срока их действия, который не должен превышать трех месяцев. Надзорный орган должен, незамедлительно, сообщить об этих мерах, а также о причинах их принятия, другим заинтересованным надзорным органам, Совету и Европейской Комиссии.

2. Когда надзорный орган принял меру в соответствии с параграфом 1, и считает, что в срочном порядке необходимо принять решающие меры, он может запросить от Совета срочного заключения или срочного решения обязательного для исполнения, указав причины для требования такого заключения или решения.

3. Любой надзорный орган может запросить от Совета срочного заключения или срочного решения обязательного для исполнения, в зависимости от обстоятельств, в том случае, если компетентный надзорный орган не принимает соответствующие меры в ситуации наличия настоятельной необходимости действовать в целях защиты прав и свобод субъектов данных, указав причины для требования такого заключения или решения, в том числе настоятельную необходимость действовать.

4. В изъятия из Статьи 64 (3) и Статьи 65 (2), срочное заключение или срочное решение обязательное для исполнения, предусмотренные параграфами 2 и 3 настоящей Статьи, должны быть приняты в течение двух недель простым большинством голосов членов Совета.

Статья 67

Обмен информацией

Европейская Комиссия может принимать имплементирующие акты общей сферы применения для того, чтобы определить меры по обеспечению обмена информацией электронными средствами между надзорными органами, а также между надзорными органами и Советом, в том числе стандартизированный формат, предусмотренный Статьей 64.

Такие имплементирующие акты должны быть приняты в соответствии с процедурой проверки, предусмотренной Статьей 93 (2).

Раздел 3

ЕВРОПЕЙСКИЙ СОВЕТ ПО ЗАЩИТЕ ДАННЫХ

Статья 68

Европейский совет по защите данных

1. Европейский совет по защите данных[52] (далее – «Совет») настоящим учреждается в качестве органа Евросоюза и обладает правами юридического лица.

2. Совет должен быть представлен своим Президиумом.

3. Совет должен состоять из руководителей одного надзорного органа каждого государства-члена, а также Европейского инспектора по защите данных[53] или их соответствующих представителей.

4. В случае, когда в государстве-члене более одного надзорного органа, являющихся ответственными за мониторинг применения положений в порядке настоящего Регламента, должен быть назначен единый представитель, в соответствии с правом такого государства-члена.

5. Европейская Комиссия должна обладать правом принимать участие в деятельности и заседаниях Совета без права голоса. Европейская Комиссия должна назначить представителя. Президиум Совета должен сообщать Европейской Комиссии о деятельности Совета.

6. В случаях, предусмотренных в Статье 65, Европейский инспектор по защите данных должен обладать правом голоса только по решениям, которые касаются принципов и норм, применимых к учреждениям, органам, ведомствам и агентствам Евросоюза, которые соответствуют содержанию настоящего Регламента.

Статья 69

Независимость

1. Совет должен действовать независимо при выполнении своих задач или осуществлении своих полномочий, в соответствии со Статьями 70 и 71.

2. Без ущерба требованиям Европейской Комиссии, упомянутых в пункте (b) статьи 70 (1) и в статье 70 (2), Совет, при выполнении своих задач или осуществлении своих полномочий, не должен ни стремиться получить, ни получать указания от кого бы то ни было.

Статья 70

Задачи Совета

[52] *European Data Protection Board*

[53] *European Data Protection Supervisor*

1. Совет должен обеспечить согласованное применение настоящего Регламента. В этих целях Совет должен по собственной инициативе, или при необходимости, по требованию Европейской Комиссии, в том числе:

(a) осуществлять мониторинг и обеспечивать надлежащее применение настоящего Регламента в случаях, предусмотренных в Статях 64 и 65, без ущерба задачам национальных надзорных органов;

(b) консультировать Европейскую Комиссию по любым вопросам, относящимся к защите персональных данных в Евросоюзе, включая любые предполагаемые изменения настоящего Регламента;

(c) консультировать Европейскую Комиссию относительно формата и порядка осуществления обмена информацией между контролёрами, обработчиками, а также надзорными органами в отношении обязательных корпоративных правил;

(d) издавать директивные указания, рекомендации и лучшие практики по процедурам удаления ссылок, копирования или тиражирования персональных данных из общедоступных служб связи, указанных в Статье 17 (2);

(e) рассматривать, по собственной инициативе, по запросу одного из своих членов либо по требованию Европейской Комиссии, любые вопросы, связанные с применением настоящего Регламента, а также издавать директивные указания, рекомендации и лучшие практики для того, чтобы содействовать согласованному применению настоящего Регламента;

(f) издавать директивные указания, рекомендации и лучшие практики в соответствии с пунктом (e) настоящего параграфа для дальнейшего уточнения критериев и условий для решений, основанных на составленном профиле в порядке Статьи 22 (2);

(g) издавать директивные указания, рекомендации и лучшие практики в соответствии с пунктом (e) настоящего параграфа для выявления утечек персональных данных и определения неоправданных задержек, упомянутых в Статье 33 (1) и (2), а также в отношении конкретных обстоятельств, при которых контролёр или обработчик должны уведомить об утечке персональных данных;

(h) издавать директивные указания, рекомендации и лучшие практики в соответствии с пунктом (e) настоящего параграфа применительно к обстоятельствам, при которых утечка персональных данных способна с большей вероятностью привести к высоким рискам для прав и свобод физических лиц, упомянутых в Статье 34 (1);

(i) издавать директивные указания, рекомендации и лучшие практики в соответствии с пунктом (e) настоящего параграфа, в целях дальнейшего уточнения критериев и требований для передачи персональных данных, основанных на обязательных корпоративных правилах, соблюдаемых контролёрами, и обязательных корпоративных правилах соблюдаемых обработчиками, а также дополнительных необходимых требованиях, для

обеспечения защиты персональных данных соответствующих субъектов данных согласно Статье 47;

(j) издавать директивные указания, рекомендации и лучшие практики в соответствии с пунктом (e) настоящего параграфа, в целях дальнейшего уточнения критериев и требований относительно передачи персональных данных на основании Статьи 49 (1);

(k) разрабатывать директивы для надзорных органов, касающиеся применения мер, упомянутых казанных в Статье 58 (1), (2) и (3), а также установления административных штрафов в порядке Статьи 83;

(l) рассматривать практическое применение директивных указаний, рекомендаций и лучших практик, упомянутых в пунктах (e) и (f);

(m) издавать директивные указания, рекомендации и лучшие практики в соответствии с пунктом (e) настоящего параграфа устанавливающие единый порядок представления сообщений физическим лицам о нарушениях настоящего Регламента в порядке Статьи 54 (2);

(n) содействовать разработке кодексов поведения и установлению механизмов сертификации защиты данных, а также печатей защиты данных и знаков в соответствии со Статьями 40 и 42;

(o) осуществлять аккредитацию органов сертификации и их регулярную проверку, в соответствии со Статьей 43, и вести открытый реестр аккредитованных органов в соответствии со Статьей 43 (6), а также аккредитованных контролёров или обработчиков, учрежденных в третьих странах в соответствии со Статьей 42 (7);

(p) определять требования, указанные в Статьей 43 (3), в целях аккредитации органов сертификации согласно Статьей 42;

(q) представлять Европейской Комиссии заключение относительно требований по сертификации, предусмотренных в Статье 43 (8);

(r) представлять Европейской Комиссии заключение относительно графических обозначений, указанных в Статьей 12 (7);

(s) представлять Европейской Комиссии заключение по оценке соответствия уровня защиты в третьей стране или в международной организации, в том числе оценку того, что третья страна, территория, или один или несколько особых секторов в этой третьей стране, или международная организация, больше не обеспечивают надлежащий уровень защиты. В этих целях Европейская Комиссия должна представить Совету всю необходимую документацию, включая переписку с правительством третьей страны, в отношении этой третьей страны, территории или особого сектора, или с международной организацией.

(t) давать заключения по проектам решений надзорных органов согласно механизму согласования, предусмотренному в Статье 64 (1), по вопросам, представленным в соответствии со Статьей 64 (2), а также принимать решения, обязательные для исполнения в порядке Статьи 65, в том числе в случаях, упомянутых в статье 66;

(u) содействовать сотрудничеству, а также эффективному двустороннему и многостороннему обмену информацией и лучшими практиками между надзорными органами;

(v) содействовать общим программам обучения, а также способствовать обмену персоналом между надзорными органами и, при необходимости, с надзорными органами третьих стран или с международными организациями;

(w) содействовать обмену знаниями и документацией относительно законодательства по защите данных и практики с органами по надзору защиты данных в любой стране мира;

(x) давать заключения относительно кодексов поведения, разработанных на уровне Евросоюза, в порядке Статьи 40 (9); и

(y) поддерживать общедоступный электронный реестр решений, принятых надзорными органами и судами по вопросам, обработанным в рамках механизма согласования.

2. В случае если Европейской Комиссии требует консультации от Совета, она может установить предельно допустимый срок, принимая во внимание безотлагательность вопроса.

3. Совет должен передать свои заключения, директивные указания, рекомендации и лучшие практики Европейской Комиссии и комитету, указанному в Статье 93, и обнародовать их.

4. Совет, в случае необходимости, должен консультировать заинтересованные стороны и давать им возможность сделать комментарии в течение разумного срока. Совет, должен без ущерба для Статьи 76, довести результаты консультаций до всеобщего сведения.

Статья 71

Отчеты

1. Совет должен составлять ежегодный отчет о защите физических лиц относительно обработки данных в Евросоюзе и, в соответствующих случаях, в третьих странах и международных организациях. Отчет должен быть обнародован и передан Европейскому Парламенту, Европейскому Совету и Европейской Комиссии.

2. Ежегодный отчет должен включать обзор практического применения директивных указаний, рекомендаций и лучших практик, упомянутых в пункте (1) Статьи 70 (1), а также решений, **обязательных для исполнения,** предусмотренных в Статье 65.

Статья 72

Процедура

1. Совет должен принимать решения простым большинством голосов своих членов, если иное не предусмотрено настоящим Регламентом.

2. Совет должен принять свои собственные правила процедур большинством в две трети голосов своих членов и проводить свою собственную оперативную деятельность.

Статья 73

Президиум

1. Совет должен выбрать выбрать Председателя и двух заместителей председателя из числа своих членов простым большинством голосов.

2. Срок полномочий Председателя и его заместителей должен составлять пять лет, с допуском однократного возобновления.

Статья 74

Задачи Президиума

1. Президиум должен выполнять следующие задачи:

(a) созывать совещания Совета и готовить их повестку дня;

(b) уведомлять о решениях, принятых Советом, в порядке Статьи 65, руководящий надзорный орган и заинтересованные надзорные органы;

(c) обеспечивать своевременное осуществление задач Совета, в том числе, в отношении механизма согласования, предусмотренного Статьей 63.

2. Совет должен установить распределение задач между Председателем и его заместителями в своих правилах процедур.

Статья 75

Секретариат

1. Совет должен иметь секретариат, который должен быть представлен Европейским инспектором по защите данных.

2. Секретариат должен выполнять свои задачи только на основании указаний Президиума Совета.

3. Персонал Европейского инспектора по защите данных, участвующий в выполнении задач, возложенных на Совет согласно настоящему Регламенту, подлежат отдельному порядку отчетности, от персонала, участвующего в выполнении задач, осуществляемых Европейским инспектором по защите данных.

4. В соответствующих случаях Совет и Европейский инспектор по защите данных должны составлять и публиковать Меморандум о

взаимопонимании, имплементирующий настоящую Статью, определяющий условия их сотрудничества, и применимый к персоналу Европейского инспектора по защите данных, участвующему в осуществлении задач, возложенных на Совет в соответствии с настоящим Регламентом.

5. Секретариат должен оказывать Совету аналитическую, административную и логистическую поддержку.

6. Секретариат должен нести ответственность, в том числе за:

(a) повседневную деятельность Совета;

(b) информационное взаимодействие между членами Совета, его Президиумом и Европейской Комиссией;

(c) связь с иными учреждениями и общественностью;

(d) использование электронных средств для внутренней и внешней связи;

(e) письменный перевод соответствующей информации;

(f) за подготовку и последовательное выполнение заседаний Совета;

(g) за подготовку, составление проектов и публикацию заключений, решений об урегулировании спорных вопросов между надзорными органами, а также иных документов, принятых Советом.

Статья 76

Конфиденциальность

1. Обсуждения Совета должны быть конфиденциальными, если Совет сочтет это необходимым, в соответствии с порядком, предусмотренным его правилам процедур.

2. Доступ к документам, представленным на рассмотрение членам Совета, экспертам и представителям третьих сторон, регулируется Регламентом (ЕС) 1049/2001 Европейского Парламента и Совета ЕС[54].

ГЛАВА VIII.

СРЕДСТВА ПРАВОВОЙ ЗАЩИТЫ, ОТВЕТСТВЕННОСТЬ И САНКЦИИ

Статья 77

Право подавать жалобу в надзорный орган

1. Без ущерба любым иным административным или судебным средствам защиты, каждый субъект данных должен обладать правом подачи жалобы в

[54] (1) Регламент (ЕС) 1049/2001 Европейского Парламента и Совета ЕС от 30 мая 2001 г. о доступе общественности к документам Европейского Парламента, Совета ЕС и Европейской Комиссии. *Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.*

надзорный орган, в том числе, в государстве-члене его/ее обычного места проживания, места работы или места предполагаемого нарушения, если субъект данных считает, что обработка относящихся к нему/ней персональных данных нарушает настоящий Регламент.

2. Надзорный орган, в который была подана жалоба, должен проинформировать заявителя о ходе и результатах жалобы, включая возможность судебной защиты прав в порядке Статьи 78.

Статья 78

Право на эффективные средства судебной защиты против надзорного органа

1. Без ущерба любым иным административным или вне-судебным средствам защиты, каждое физическое или юридическое лицо должно иметь право на эффективные средства судебной защиты против юридически обязательного решения надзорного органа, касающихся их.

2. Без ущерба любым иным административным или вне-судебным средствам защиты каждый субъект данных должно иметь право на эффективные средства судебной защиты, в случае, когда надзорный орган, который является компетентным в соответствии со Статьями 55 и 56, не рассматривает жалобу или не сообщает субъекту данных, в течение трех месяцев, о ходе или результатах рассмотрения жалобы, поданной в соответствии со Статей 77.

3. Производство против надзорного органа должно передаваться в суд государства-члена, в котором надзорный орган учрежден.

4. В случае, когда производство по делу возбуждено в отношении решения надзорного органа, которому предшествовало заключение, либо решение Совета в рамках механизма **согласования**, надзорный орган направляет такое заключение или решение в суд.

Статья 79

Право на эффективные средства судебной защиты в отношении контролёра или обработчика

1. Без ущерба любым иным административным или вне-судебным средствам защиты, в том числе праву подачи жалобы в надзорный орган, согласно Статье 77, каждый субъект данных должен иметь право на эффективные средства судебной защиты, если он/она считает, что его/ее права по настоящему Регламенту, были нарушены в результате обработки его/ее персональных данных в нарушение требований настоящего Регламента.

2. Производство против контролёра или обработчика должно быть передано в суд государства-члена, где контролёр или обработчик имеют учреждение. Как альтернативный вариант, такое производство может быть передано в суд государства-члена, где субъект данных имеет его/ее обычное место жительства, кроме тех случаев, когда контролёр или обработчик является органом власти государства-члена, действуя при осуществлении им публичных полномочий.

Статья 80

Представительство субъектов данных

1. Субъект данных вправе поручить некоммерческой корпорации, организации либо ассоциации, которые были должным образом учреждены в соответствии с правом государства-члена, имеют уставные задачи в сфере общественного интереса, а также действуют в сфере защиты прав и свобод субъектов данных, в части защиты их персональных данных, подавать жалобу от его имени, осуществлять права, указанные в Статьях 77, 78, и 79, от его имени, и иметь право на получение компенсации согласно Статье 82, от его имени в случаях, предусмотренных правом государства-члена.

2. Государства-члены могут предусмотреть, что любая корпорация, организация либо ассоциация, предусмотренные параграфом 1 настоящей Статьи, независимо от поручения субъекта данных, имеет право подавать в указанном государстве-члене жалобу в надзорный орган, компетентный в соответствии со Статьей 77, а также осуществлять права, указанные в Статьях 78, и 79, если он считает, что права субъекта данных, согласно настоящему Регламенту, были нарушены в результате обработки данных.

Статья 81

Приостановление судебного разбирательства

1. В случае если компетентный суд государства-члена обладает информацией о судебном разбирательстве касающегося того же вопроса по поводу обработки тем же самым контролёром или обработчиком, и что оно рассматривается в суде другого государства-члена, он должен связаться с этим судом в другом государстве-члене, для того чтобы подтвердить наличие такого разбирательства.

2. В случае если судебное разбирательство, касающееся того же вопроса по поводу обработки тем же самым контролёром или обработчиком, рассматривается в суде другого государства-члена, любой компетентный суд, иной чем суд, рассматривающий дело первым, может приостановить производство по этому делу.

3. В случае, если такое судебное разбирательство находится в процессе рассмотрения по первой инстанции, любой суд, иной, чем суд,

рассматривающий дело первым, может также, по заявлению одной из сторон, отказаться от юрисдикции, если суд, рассматривающий дело первым, обладает юрисдикцией в отношении соответствующих действий, и его право разрешает объединение исков.

Статья 82

Право на компенсацию и ответственность

1. Любое лицо, которое понесло материальный или нематериальный ущерб в результате нарушения положений настоящего Регламента, обладает правом на получение компенсации от контролёра или обработчика за понесенный ущерб.

2. Любой контролёр, участвующий в обработке данных, должен нести ответственность за ущерб, вызванный обработкой данных, которая нарушает настоящий Регламент. Обработчик должен нести ответственность за ущерб, вызванный обработкой данных, только если он не выполнил обязательства по настоящему Регламенту, конкретно направленные на обработчиков или когда он действовал вне пределов или в нарушение законных предписаний контролёра.

3. Контролёр или обработчик освобождается от ответственности в соответствии с параграфом 2, если он докажет, что он никоим образом не несет ответственность за событие, которое повлекло за собой ущерб.

4. В случае, когда более одного контролёра или обработчика, либо когда контролёр и обработчик задействованы оба в одной и той же обработке данных, а также в случае, когда они, в соответствии с параграфом 2 и 3, ответственны за любой ущерб, вызванный обработкой, каждый контролёр или обработчик должны нести ответственность за ущерб в полном объеме, для того, чтобы обеспечить эффективную компенсацию субъекту данных.

5. Если контролёр или обработчик полностью возместили, в соответствии с параграфом 4, за нанесенный ущерб, такой контролёр или обработчик вправе требовать от других контролёров или обработчиков, участвующих в той же самой обработке, возврата части компенсации, соответствующей их части ответственности за ущерб, в соответствии с условиями, предусмотренными параграфом 2.

6. Судебное разбирательство в отношении осуществления права на получение компенсации должно быть передано в суд, компетентный в соответствии с правом государства-члена, упомянутого в Статье 79 (2).

Статья 83

Общие условия наложения административных штрафов

1. Каждый надзорный орган должен обеспечить, чтобы наложение административных штрафов, в порядке настоящей Статьи в отношении нарушений положений настоящего Регламента, предусмотренных в параграфах 4, 5 и 6, в каждом отдельном случае, было эффективным, соразмерным и имело сдерживающее воздействие.

2. Административные штрафы, в зависимости от обстоятельств каждого конкретного случая, должны налагаться в дополнение, либо вместо мер, предусмотренных пунктами (a)-(h) и (j) Статьи 58 (2). При принятии решения по вопросу наложения административного штрафа и решения о размере административного штрафа, в каждом отдельном случае должно подлежать учету следующее:

(a) характер, тяжесть и продолжительность нарушения, принимая во внимание характер, объем и цели соответствующей обработки, также как и количество затронутых субъектов данных, а равно и размер ущерба, понесенного ими;

(b) умышленный или неосторожный характер нарушения;

(c) любые меры, предпринятые контролёром или обработчиком, для смягчения ущерба, полученного субъектами данных;

(d) степень ответственности контролёра или обработчика, принимая во внимание технические и организационные меры, осуществляемые ими в соответствии со Статьями 25 и 32;

(e) любые соответствующие предыдущие нарушения контролёра или обработчика;

(f) степень сотрудничества с надзорным органом для того, чтобы устранить нарушения и смягчить возможные неблагоприятные последствия нарушений;

(g) категории персональных данных, затронутых нарушением;

(h) способ, посредством которого надзорному органу стало известно о нарушении, в том числе, уведомил ли контролёр или обработчик об этом нарушении, и если да, то в какой степени;

(i) соблюдение мер, предусмотренных Статьей 58 (2), ранее было предписано против соответствующего контролёра или обработчика в отношение того же вопроса;

(j) соблюдение утвержденных кодексов поведения в соответствии со Статьей 40, или утвержденных механизмов сертификации, в соответствии со Статьей 42; и

(k) любые иные отягчающие или смягчающие факторы, применимые к обстоятельствам дела, например, полученные финансовые выгоды или избежание потерь, прямо или косвенно связанных с нарушением.

3. Если контролёр или обработчик умышленно или по неосторожности, по тем же самым или связанным с обработкой данных, нарушают несколько положения настоящего Регламента, общий размер административного штрафа не должен превышать размер, установленный для самого тяжкого нарушения.

4. Нарушения следующих положений должны, в соответствии с параграфом 2, подпадать под административные штрафы в размере до 10 000 000 Евро, или применительно к хозяйствующему субъекту, в размере до 2% от «обще-странового» годового оборота хозяйствующего субъекта за весь предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) обязательства контролёра и обработчика в соответствии со Статьями 8, 11, 25-39 и 42 и 43;

(b) обязательства органа сертификации в соответствии со Статьями 42 и 43;

(c) обязательства органов, надзорного органа в соответствии со Статьей 41 (4).

5. Нарушения следующих положений, в соответствии с параграфом 2, должны подпадать под административные штрафы в размере до 20 000 000 Евро или применительно к хозяйствующему субъекту в размере до 4% от «обще-странового» годового оборота за весь предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) нарушение основных принципов обработки, в том числе условий, в отношении согласия, согласно Статьям 5, 6, 7 и 9;

(b) прав субъектов данных, предусмотренных с Статьях 12-22;

(c) передачи персональных данных получателю в третьей стране или международной организации, предусмотренной Статьями 44-49;

(d) любых обязанностей в соответствии с правом государства-члена, принятому в рамках Главы IX;

(e) несоблюдения предписания, или временного или окончательного ограничения на обработку, или приостановление потоков данных надзорным органом в соответсвтии со Статьей 58 (2), либо отказ в предоставлении доступа в нарушение Статьи 58 (1).

6. Нарушения предписаний надзорного органа, в соответствии со Статьей 58 (2), должны, в соответствии с параграфом 2, подпадать под административные штрафы в размере не более 20 000 000 Евро или, применительно к хозяйствующему субъекту, в размере до 4% от «обще-странового» годового оборота хозяйствующего субъекта за весь предыдущий финансовый год, в зависимости от того, какая сумма больше.

7. Без ущерба полномочиям надзорных органов по устранению недостатков, в соответствии со Статьей 58 (2), каждое государство-член может установить правила относительно того, могут ли и в какой мере административные штрафы налагаться на органы государственной власти и учреждения, существующие в этом государстве-члене.

8. Осуществление надзорным органом своих полномочий в соответствии с настоящей Статьей, должно подпадать под действие соответствующих процессуальных гарантий в соответствии с правом Евросоюза и правом государства-члена, включая эффективные средства судебной защиты и надлежащую правовую процедуру.

9. В случае, когда правовая система государства-члена не предусматривает административные штрафы, настоящая Статья может применяться таким образом, чтобы наложение штрафа инициировалось компетентным надзорным органом, а штраф налагался компетентными национальными судами, при этом гарантируя, что такие средства правовой защиты являются эффективными и обладают аналогичным эффектом как и административные штрафы, налагаемые надзорными органами. Во всяком случае, налагаемые штрафы должны быть эффективными, пропорциональными и должны оказывать сдерживающее воздействие. Такие государства-члены должны уведомить Европейскую Комиссию о положениях своего законодательства, которые они принимают в соответствии с настоящим параграфом, до 25 мая 2018 г., а также незамедлительно уведомить о любых последующих изменениях законодательства или поправках, затрагивающих такие положения.

Статья 84

Санкции

1. Государства-члены могут должны установить нормы относительно иных санкций, применимых за нарушения настоящего Регламента, в том числе за нарушения, которые не подпадают под административные штрафы в порядке Статьи 83, а также принять все меры, для того, чтобы обеспечить их применение. Такие санкции должны быть эффективными, соизмеримыми и должны оказывать сдерживающее воздействие.

2. Каждое государство-член должно уведомить Европейскую Комиссию о положениях своего права, которые оно принимает в соответствии с параграфом 1, до 25 мая 2018 г., а также незамедлительно уведомляют о любых последующих изменениях, затрагивающих такие положения.

ГЛАВА IX.

ПОЛОЖЕНИЯ В ОТНОШЕНИИ КОНКРЕТНЫХ СЛУЧАЕВ ОБРАБОТКИ

Статья 85

Обработка и свобода выражения мнений и распространения информации

1. Государства-члены в законодательном порядке должны гармонично согласовать право на защиту персональных данных в порядке настоящего Регламента и право на свободу выражения мнений и распространения информации, в том числе обработку, для публицистических, а также в научных, художественных и литературных целях.

2. Для обработки, осуществляемой в публицистических, научных, художественных и литературных целях, государства-члены должны предусмотреть исключения и изъятия из Главы II (принципы), Главы III (права субъекта данных), Главы IV (контролёр и обработчик), Главы V (передача персональных данных третьим странам и международным организациям), Главы VI (самостоятельные надзорные органы), Главы VII (сотрудничество и согласованность) и Главы IX (конкретные случаи обработки), если они необходимы для того, чтобы гармонично сочетать право на защиту персональных данных со свободой выражения мнений и распространения информации.

3. Каждое государство-член должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно приняло согласно параграфу 2, а также без необоснованных задержек уведомить о любых последующих изменениях законодательства или о поправках, затрагивающих такие положения.

Статья 86

Обработка и доступ общественности к официальным документам

Персональные данные в официальных документах, находящихся в ведении органов, или государственных учреждениях, или частных организациях для осуществления задачи, осуществляемой в общественных интересах, могут быть раскрыты органом власти или учреждением в соответствии с правом Евросоюза или правом государства-члена, применимого к органу власти или учреждению, для того чтобы согласовать доступ общественности к официальным документам с правом на защиту персональных данных в порядке настоящего Регламента.

Статья 87

Обработка национального идентификационного номера

Государства-члены должны способствовать определению конкретных условий обработки национального идентификационного номера или любого другого идентификатора общего назначения. В этом случае национальный идентификационный номер или любой другой идентификатор общего назначения должен использоваться только при обеспечении надлежащих гарантий для прав и свобод субъекта данных в порядке настоящего Регламента.

Статья 88

Обработка применительно к трудовым отношениям

1. Государства-члены могут законодательно или посредством коллективных договоров предусмотреть более конкретные нормы для обеспечения защиты прав и свобод обработки персональных данных работников при выполнении должностных обязанностей, в том числе для целей приема на работу, выполнения трудового договора, включая освобождение от обязательств, установленных законодательством или коллективными договорами, в целях управления, планирования и организации работы, равноправия и разнообразия на рабочем месте, охраны труда и безопасности на производстве, защиты собственности работодателя или клиента, а также в целях осуществления связанных с занятостью индивидуальных или коллективных прав и льгот, связанных с занятостью, и с целью прекращения трудовых отношений

2. Такие нормы должны включать в себя надлежащие и конкретные меры для защиты человеческого достоинства субъекта данных, законные интересы и основные права, с особым учетом прозрачности обработки, передачи персональных данных в рамках группы компаний или группы предприятий, занимающихся совместной экономической деятельностью, а также в отношении систем мониторинга на рабочем месте.

3. Каждое государство-член должно уведомить Европейскую Комиссию о таких нормах своего права, которые она принимает в соответствии параграфу 1, до 25 мая 2018 г., а также без необоснованных задержек уведомляет о любых последующих изменениях, затрагивающих такие положения.

Статья 89

Гарантии и изъятия касающиеся обработки
для архивных целей в общественных интересах, для целей научного или исторического исследования или в статистических целях

1. Обработка для архивных целей в общественных интересах, для целей научного или исторического исследования или в статистических целях подлежит соответствующим гарантиям, согласно настоящему Регламенту, в отношении прав и свобод субъекта данных. Такие гарантии должны обеспечивать, чтобы технические и организационные меры были приняты, в частности, для того, чтобы обеспечить соблюдение принципа минимизации данных. Названные меры могут охватывать псевдонимизацию при условии, что эти цели могут соблюдаться таким способом. В случае, когда обозначенные цели могут достигаться путем дальнейшей обработки, которая не позволяет или больше не позволяет идентификацию субъектов данных, эти цели должны осуществляться этим способом.

2. В случае если персональные данные обрабатываются для архивных целей в общественных интересах, для целей научного или исторического исследования или в статистических целях, право Евросоюза или право государства-члена может предусматривать изъятия из прав, предусмотренных в Статьях 15,16,18 и 21, с учетом условий и гарантий, предусмотренных параграфом 1 настоящей Статьи, в той мере, в которой такие права могут сделать невозможным или серьезно нарушить достижение конкретных целей, и такое изъятие необходима для достижения поставленных целей.

3. В случае если персональные данные обрабатываются для архивных целей, право Евросоюза или право государства-члена может предусматривать изъятие из прав, предусмотренных в Статьях 15,16,18, 19 и 20, с учетом условий и гарантий, предусмотренных параграфом 1 настоящей Статьи, в той мере, в которой такие права могут сделать невозможным или серьезно нарушить достижение конкретных целей, и такое изъятие необходима для достижения поставленных целей.

4. В случае если обработка, предусмотренная в параграфах 2 и 3, одновременно служит для другой цели, дерогация должна применяться только в отношении обработки для целей, предусмотренных в названных параграфах.

Статья 90

Обязательства сохранения секретности

1. Государства-члены могут принять конкретные нормы для определения полномочий надзорных органов предусмотренных пунктами (e) и (f) Статьи 58 (1), в отношении контролёров или обработчиков, на которых, в соответствии с правом Евросоюза или правом государства-члена, либо норм, установленных национальными компетентными органами, возложены обязательства соблюдения профессиональной тайны или других равноценных обязательств секретности, когда это необходимо и соразмерно для поддержания баланса между правом на защиту персональных данных и обязательствами сохранения секретности. Такие нормы должны применяться только в отношении персональных данных, которые контролёр или обработчик получили благодаря деятельности или приобрели в ходе деятельности, предусматривающей такие обязательства сохранения секретности.

2. Каждое государство-член должно уведомить Европейскую Комиссию о нормах, принятых в соответствии с параграфом 1 до 25 мая 2018 г., а также без необоснованных задержек уведомить о любых последующих изменениях, затрагивающих такие нормы.

Статья 91

Действующие нормы защиты данных
церквей и религиозных организаций

1. В случае, когда в государстве-члене церкви и религиозные организации или общины, на дату вступления в силу настоящего Регламента, применяют комплексные нормы, относящиеся к защите физических лиц при обработке данных, такие нормы могут оставаться в силе, при условии если они приведены в соответствие с настоящим Регламентом.

2. Церкви и религиозные организации, которые применяют комплексные нормы, согласно параграфу 1 настоящей Статьи, должны подлежать надзору со стороны самостоятельного надзорного органа, который может быть строго определенным надзорным органом, при условии, что он соблюдает условия, изложенные в Главе VI настоящего Регламента.

ГЛАВА X.

ПОДЗАКОННЫЕ АКТЫ И ИМПЛЕМЕНТИРУЮЩИЕ АКТЫ

Статья 92

Осуществление полномочий относительно подзаконных актов

1. Полномочие принятия подзаконных актов предоставляется Европейской Комиссии в соответствии с условиями, предусмотренными в настоящей Статье.

2. Полномочия относительно подзаконных актов, предусмотренных в Статье 12 (8) и в Статье 43 (8), предоставляется Европейской Комиссии на неопределенный срок, начиная с 24 мая 2016 г.

3. Полномочия по принятию подзаконных актов, предусмотренных в Статье 12 (8) и в Статье 43 (8), может быть отменено в любое время Европейским Парламентом или Европейским Советом. Решение об отмене должно прекращать полномочия по принятию подзаконных актов, предусмотренным таким решением. Оно вступает в силу на следующий день после публикации решения в Официальном Журнале Европейского Союза или в более поздний срок, установленный в принятом решении. Оно не влияет на действительность любых подзаконных актов, уже вступивших в силу.

4. Одновременно с принятием подзаконного акта Европейская Комиссия должна уведомить об этом Европейский Парламент и Европейский Совет.

5. Подзаконный акт, принятый в соответствии со Статьей 12 (8) и Статьей 43 (8), должен вступать в силу только в случае, если ни Европейский Парламент, ни Совет ЕС не представили возражения в течение трех месяцев с

момента уведомления относительно этого акта, и если до истечения указанного срока Европейский Парламент и Европейский Совет оба проинформировали Европейскую Комиссию о том, что они не представят возражения. Указанный срок должен быть продлен на три месяца по инициативе Европейского Парламента или Европейского Совета.

Статья 93

Процедура Комитета

1. Европейская Комиссия должна оказывать содействие Комитету. Такой Комитет должен являться комитетом в значении Регламента (ЕС) 182/2011.
2. В случае, когда сделана ссылка на настоящий параграф, должна применяться Статья 5 Регламента (ЕС) 182/2011.
3. В случае, когда сделана ссылка на настоящий параграф, должна применяться Статья 8 Регламента (ЕС) 182/2011 во взаимосвязи с положениями Статьи 5 названного Регламента.

ГЛАВА XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 94

Отмена Директивы 95/46/ЕС

1. Отмена Директивы 95/46/ЕС вступает в силу с 25 мая 2018 г.
2. Ссылки на отмененную Директиву должны рассматриваться как ссылки на настоящий Регламент. Ссылки на Рабочую группу по защите физических лиц при обработке персональных данных, учрежденную согласно Статье 29 Директивы 95/46/ЕС, должны рассматриваться как ссылки на Европейский совет по защите данных[55], учрежденный настоящим Регламентом.

Статья 95

Соотношение с Директивой 2002/58/ЕС

Настоящий Регламент не должен налагать дополнительных обязательств на физических и юридических лиц в отношении обработки данных в контексте предоставления общедоступных услуг электронной связи услугах связи в коммуникационных сетях общего пользования в Евросоюзе, касающихся вопросов, в отношении которых они являются субъектами конкретных обязательств, в тех же целях установленную Директивой 2002/58/ЕС.

[55] *European Data Protection Board*

Статья 96

Соотношение с ранее заключенными соглашениями

Международные договоры, касающиеся передачи персональных данных третьим странам или международным организациям, которые были заключены государствами-членами до 24 мая 2016 г. и которые соответствуют праву Евросоюза, применявшемуся до указанной даты, должны сохранять свою силу до их изменения, поправок или отменены.

Статья 97

Отчеты Европейской Комиссии

1. До 25 мая 2020 г. и каждые четыре года впоследствии Европейская Комиссия должна направлять отчет об оценке и анализе настоящего Регламента в Европейский Парламент и Европейский Совет. Этот должен быть опубликован.

2. В контексте оценки и анализа, предусмотренного параграфом 1, Европейская Комиссия должна проверить, в том числе, применение и действие:

(a) Главы V о передаче персональных данных третьим странам или международным организациям, в особенности, с учетом решений, принятых в порядке Статья 45 (3) настоящего Регламента, а также решений, принятых в порядке Статьи 25 (6) Директивы 95/46/ЕС;

(b) Главы VII о сотрудничестве и согласовании.

3. Для цели параграфа 1 Европейская Комиссия может запрашивать информацию у государств-членов и надзорных органов.

4. При осуществлении оценки и анализа в порядке параграфов 1 и 2 Европейская Комиссия должна принимать во внимание позиции и выводы Европейского Парламента, Европейского Совета, а также иных соответствующих органов или источников.

5. Европейская Комиссия должна, в случае необходимости, внести соответствующие предложения по изменению настоящего Регламента, в том числе принимая во внимание развитие информационных технологий, а также имея в виду состояние развития в информационном обществе.

Статья 98

Пересмотр иных правовых актов Евросоюза о защите данных

Европейская Комиссия, в случае необходимости, должна представить внести законодательные предложения с целью изменения иных правовых актов Евросоюза о защите персональных данных, для того чтобы обеспечить единообразную и согласованную защиту физических лиц, относящихся к обработке данных. Они должны, в том числе, относиться к нормам, касающимся защиты физических лиц при обработке данных учреждениями, органами, ведомствами и агентствами Евросоюза, а также норм о свободном перемещении таких данных.

Статья 99

Вступление в силу и применение

1. Настоящий Регламент вступает в силу на двадцатый день после своего опубликования в Официальном Журнале Европейского Союза.

2. Он должен применяться с 25 мая 2018 г.

Настоящий Регламент является обязательным в полном объеме и подлежит прямому применению в государствах-членах.

Совершено в Брюсселе 27 апреля 2016 г.

(Подписи)

(Брюссель, 27 апреля 2016 года)