Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR)

Регламент Европейского Парламента и Совета Европейского Союза
2016/679 от 27 апреля 2016 г.
о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС
(Общий Регламент о защите персональных данных)[1]
(General Data Protection Regulation)
(GDPR)

(Действие Регламента распространяется на Европейское экономическое пространство)

Европейский Парламент и Совет Европейского Союза,

Руководствуясь Договором о функционировании Европейского Союза, и, в частности, Статьей 16 Договора,

На основании предложения Европейской Комиссии,

После передачи проекта законодательного акта национальным парламентам,

На основании заключения Европейского комитета по экономическим и социальным вопросам[2],

На основании заключения Комитета регионов[3],

Действуя в соответствии с обычной законодательной процедурой[4],

Принимая во внимание следующие обстоятельства:

(1) Защита физических лиц при обработке персональных данных является основным правом. Статья 8(1) Хартии Европейского Союза об основных правах ("Хартия") и Статья 16(1) Договора о функционировании Европейского Союза (TFEU) предусматривают, что каждый человек имеет право на защиту относящихся к нему персональных данных.

(2) Принципы и правила защиты физических лиц при обработке их персональных данных вне зависимости от гражданства или места жительства лица должны соответствовать основным правам и свободам, в частности, праву на защиту персональных данных. Целью настоящего Регламента является содействие формированию пространства свободы, безопасности и правосудия и экономического союза, содействие экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействие благосостоянию физических лиц.

(3) Целью Директивы 95/46/ЕС Европейского Парламента и Совета ЕС[5] является гармонизация положений о защите основных прав и свобод физических лиц при обработке данных, а также гарантия свободного движения персональных данных между государствами-членами ЕС.

(4) Целью обработки персональных данных является служба человечеству. Право на защиту персональных данных не является абсолютным правом; его необходимо рассматривать относительно его функции в обществе, оно должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности. Настоящий Регламент соблюдает все основные права, свободы и принципы, признанные в Хартии и закрепленные в Договорах, в частности, уважение частной и семейной жизни, жилища и переписки, защиту персональных данных, свободу мысли, совести и вероисповедания, свободу выражения мнения и распространения информации, право ведения хозяйственной деятельности, право на эффективное средство правовой защиты и на справедливое судебное разбирательство, культурное, религиозное и языковое разнообразие.

(5) Экономическая и социальная интеграция, явившаяся следствием функционирования

внутреннего рынка, привела к существенному увеличению трансграничного потока персональных данных. Обмен персональными данными между государственными и негосударственными субъектами, в том числе физическими лицами, объединениями и предприятиями на территории Союза, увеличился. Национальные органы в государствах-членах ЕС призваны в соответствии с законодательством Союза сотрудничать и обмениваться персональными данными в целях выполнения своих обязанностей или осуществления задач от имени органа власти другого государства-члена ЕС.

(6) В связи с быстрым развитием технологий и глобализацией появились новые проблемы, связанные с защитой персональных данных. Масштаб сбора и обмена персональными данными существенно увеличился. Технологии позволяют частным компаниям и органам государственной власти в рамках осуществления своей деятельности использовать персональные данные в беспрецедентном масштабе. В последнее время физические лица все чаще делают доступной личную информацию. Технологии изменили экономическую и социальную жизнь, они должны и далее облегчать свободное движение персональных данных в Союзе, а также их передачу третьим странам и международным организациям, при этом необходимо обеспечить высокий уровень защиты персональных данных.

(7) Указанные достижения требуют наличия надежной, более согласованной правовой базы в области защиты данных в Союзе, опирающейся на строгое исполнение, так как это имеет существенное значение для создания атмосферы доверия, которая позволит цифровой экономике развиваться в рамках внутреннего рынка. Физические лица должны иметь право распоряжаться своими собственными персональными данными. Необходимо повысить уровень правовой определенности и практической достоверности для физических лиц, субъектов экономической деятельности и органов государственной власти.

(8) Если в настоящем Регламенте предусмотрены спецификации или ограничения его положений законодательством государства-члена ЕС, государства-члены ЕС могут по мере необходимости инкорпорировать элементы настоящего Регламента в свое национальное законодательство для обеспечения согласованности, а также для того, чтобы сделать национальные положения более доступными для лиц, в отношении которых они применяются.

(9) Цели и принципы Директивы 95/46/ЕС по-прежнему сохраняют юридическую силу, но она не препятствует фрагментации при имплементации защиты данных в Союзе, правовой неопределенности или распространенному общественному мнению относительно того, что имеются существенные риски для защиты физических лиц, в частности, относительно сетевой активности. Различия в уровне защиты прав и свобод физических лиц, в особенности права на защиту персональных данных при обработке персональных данных в государствах-членах ЕС, могут препятствовать свободному движению персональных данных на территории Союза. В связи с этим указанные различия представляют собой препятствие для осуществления экономической деятельности на уровне Союза, нарушают свободу конкуренции и затрудняют органам власти исполнение их обязанностей согласно законодательству Союза. Указанное различие в уровнях защиты является результатом существования различий в имплементации и применении Директивы 95/46/ЕС.

(10) Для обеспечения согласованного и высокого уровня защиты физических лиц и для устранения препятствий движению персональных данных в Союзе уровень защиты прав и свобод физических лиц при обработке указанных данных должен быть эквивалентным во всех государствах-членах ЕС. На всей территории Союза необходимо гарантировать согласованное и однородное применение положений о защите основных прав и свобод физических лиц при обработке персональных данных. В том, что касается обработки персональных данных для соблюдения правовых обязательств, для выполнения задачи в защиту общественных интересов или при осуществлении полномочий, закрепленных за контролером, государствам-членам ЕС необходимо разрешить сохранять или вводить национальные положения для дальнейшего применения положений настоящего Регламента. В совокупности с общим и горизонтальным

законодательством относительно защиты данных, имплементирующим Директиву 95/46/ЕС, государства-члены ЕС располагают несколькими специфическими нормами в областях, которые требуют более специфических положений. Настоящий Регламент также предлагает государствам-членам ЕС свободу действия в целях определения предписаний, в том числе для обработки особых категорий персональных данных ("конфиденциальные сведения"). В связи с этим настоящий Регламент не исключает законодательство государства-члена ЕС, которое устанавливает обстоятельства для особых ситуаций обработки, в том числе более точное определение условий, при которых обработка персональных данных будет основываться на принципе законности.

(11) Эффективная защита персональных данных на территории Союза требует усиления и точного установления прав субъектов персональных данных и обязанностей тех, кто обрабатывает и определяет обработку персональных данных, а также эквивалентные полномочия по контролю и обеспечению соблюдения положений для защиты персональных данных и равнозначных санкций за нарушение в государствах-членах ЕС.

(12) Статья 16(2) TFEU предписывает Европейскому Парламенту и Совету ЕС установить правила в отношении защиты физических лиц при обработке персональных данных и правила в отношении свободного обращения персональных данных.

(13) Для того чтобы гарантировать соответствующий уровень защиты физических лиц на территории Союза и предупредить возникновение отклонений, мешающих свободному обращению персональных данный в рамках внутреннего рынка, Регламент необходим для обеспечения правовой определенности и прозрачности для субъектов экономической деятельности, включая микропредприятия, малые и средние предприятия, а также для обеспечения физических лиц во всех государствах-членах ЕС таким же уровнем юридически действительных прав, обязанностей и ответственности для контролеров и лиц, осуществляющих обработку, для того, чтобы гарантировать соответствующий мониторинг процесса обработки персональных данных, и равнозначных санкций во всех государствах-членах ЕС, а также плодотворное сотрудничество между надзорными органами различных государств-членов ЕС. Надлежащее функционирование внутреннего рынка требует того, чтобы свободное обращение персональных данных в Союзе не было ограничено или запрещено по причинам, связанным с защитой физических лиц при обработке персональных данных. Для того чтобы принять во внимание специфическую ситуацию микропредприятий, малых и средних предприятий, настоящий Регламент включает в себя частичное отступление в отношении ведения учета для организаций, на которых занято менее 250 работников. В дополнение к этому институты и органы Союза, государства-члены ЕС и их надзорные органы могут учитывать специфические нужды микропредприятий, малых и средних предприятий при применении настоящего Регламента. Понятие "микропредприятия, малые и средние предприятия" указано в Статье 2 Приложения к Рекомендации 2003/361/ЕС Европейской Комиссии[6].

(14) Защита, предусмотренная настоящим Регламентом, должна применяться в отношении физических лиц вне зависимости от их гражданства или места жительства при обработке их персональных данных. Настоящий Регламент не охватывает обработку персональных данных юридических лиц и, в частности, предприятий, учрежденных в качестве юридических лиц, включая наименование и форму юридического лица, а также контактную информацию юридического лица.

(15) Для предотвращения серьезного риска обхода положений защита физических лиц должна быть технически нейтральной и не должна зависеть от используемых технических средств. Защита физических лиц должна применяться в отношении обработки персональных данных при помощи автоматизированных средств, а также в отношении ручной обработки, если персональные данные содержатся или должны будут содержаться в файловой системе. Файлы или группы файлов, а также их титульные страницы, которые не структурированы в соответствии со специальными критериями, не должны подпадать под сферу применения настоящего Регламента.

(16) Настоящий Регламент не распространяется на вопросы, связанные с защитой фундаментальных прав и свобод или со свободным движением персональных данных в отношении деятельности, которая не подпадает под действие законодательства Союза, например деятельности,

связанной с национальной безопасностью. Настоящий Регламент не распространяется на обработку персональных данных государствами-членами ЕС при осуществлении деятельности, касающейся общей внешней политики и политики безопасности Союза.

(17) Регламент (ЕС) 45/2001 Европейского Парламента и Совета ЕС[7] применяется в отношении обработки персональных данных институтами, органами, учреждениями и агентствами Союза. Регламент (ЕС) 45/2001 и другие законодательные акты Союза в области обработки персональных данных должны быть изменены в соответствии с принципами и нормами, установленными в настоящем Регламента, и должны применяться в контексте настоящего Регламента. В целях обеспечения четкой и согласованной базы по защите данных в Союзе после принятия настоящего Регламента следует внести необходимые изменения в Регламент (ЕС) 45/2001 для того, чтобы обеспечить возможность его применения одновременно с применением настоящего Регламента.

(18) Настоящий Регламент не применяется в отношении обработки персональных данных физическими лицами в ходе осуществления исключительно личной или бытовой деятельности, не связанной с профессиональной или коммерческой деятельностью. Личная или бытовая деятельность может включать в себя переписку и сохранение адресов или взаимодействие через социальные сети и сетевую активность, осуществляемые в контексте такой деятельности. Однако настоящий Регламент применяется в отношении контролеров или лиц, осуществляющих обработку, которые обеспечивают 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, выявления уголовных преступлений или привлечения к ответственности, или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности, а также свободное обращение таких данных являются предметом отдельного законодательного акта Союза. Вследствие этого настоящий Регламент не применяется в отношении обработки данных для указанных целей. Однако обрабатываемые органами государственной власти в рамках настоящего Регламента персональные данные, если они используются для указанных целей, должны регулироваться более конкретным законодательным актом Союза, а именно Директивой (ЕС) 2016/680 Европейского Парламента и Совета ЕС[8]. Государства-члены ЕС могут поручить компетентным органам в значении Директивы (ЕС) 2016/680 выполнение задач, которые необязательно осуществляются в целях предупреждения, расследования, выявления уголовных преступлений или привлечения к ответственности или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности, для того чтобы обработка персональных данных для указанных иных целей, постольку, поскольку она находится в рамках законодательства Союза, подпадала под действие настоящего Регламента.

При обработке персональных данных компетентными органами в целях, подпадающих под действие настоящего Регламента, государства-члены ЕС должны иметь возможность сохранять или вводить более конкретные положения для адаптации к применению норм настоящего Регламента. Такие положения могут определять более точные требования для обработки персональных данных указанными компетентными органами для указанных иных целей, с учетом конституционной, организационной и административной структуры соответствующего государства-члена ЕС. Если обработка персональных данных частными организациями попадает под действие настоящего Регламента, настоящий Регламент должен обеспечивать возможность государствам-членам ЕС при наличии определенных оснований законодательно ограничивать определенные обязанности и права, если такое ограничение представляет собой необходимую и пропорциональную меру в демократическом обществе для защиты специфических важных интересов, включая общественную безопасность и предупреждение, расследование, выявление уголовных преступлений или привлечение к ответственности или приведение в исполнение уголовных наказаний, в том числе защиту и предотвращение угроз общественной безопасности. Например, это имеет существенное

значение в рамках противодействия отмыванию доходов, полученных преступным путем, или в рамках деятельности лабораторий судебной экспертизы.

(20) Поскольку настоящий Регламент применяется inter alia в отношении деятельности судов и других судебных органов, законодательство Союза или государства-члена ЕС могло бы определить процесс и процедуры обработки данных в отношении обработки персональных данных судами и другими судебными органами. Для того чтобы обеспечить независимость судебной системы при осуществлении судебных задач, включая процесс принятия решения, компетенция надзорных органов не должна охватывать обработку персональных данных, если суды действуют в пределах своей судейской дееспособности. Необходимо обеспечить возможность передачи контроля над процессом обработки данных особым органам в рамках судебной системы государства-члена ЕС, которые должны, в частности, гарантировать соблюдение норм настоящего Регламента, повысить осведомленность среди представителей судебно-прокурорской системы относительно их обязанностей согласно настоящему Регламенту и рассматривать жалобы в отношении указанного процесса обработки данных.

(21) Настоящий Регламент действует без ущерба применению Директивы 2000/31/ЕС Европейского Парламента и Совета ЕС[9], и, в частности, применению норм Статей 12 - 15 указанной Директивы об ответственности поставщиков посреднических услуг. Указанная Директива ориентирована на содействие нормальному функционированию внутреннего рынка и обеспечивает свободное обращение услуг информационного общества среди государств-членов ЕС.

(22) Любая обработка персональных данных в контексте деятельности об учреждении контролера или лица, обрабатывающего данные, в Союзе должна осуществляться в соответствии с настоящим Регламентом, вне зависимости от того, проводится ли обработка данных на территории Союза. Учреждение подразумевает эффективное и реальной осуществление деятельности посредством установившихся договоренностей. В этой связи юридическая форма таких договоренностей, вне зависимости от того, идет ли речь об отделении или дочернем предприятии с правосубъектностью, не является определяющим фактором.

(23) В целях гарантии того, что физические лица не лишены предоставляемой согласно настоящему Регламенту защиты, обработка персональных данных субъектов данных, находящихся в Союзе, не учрежденными в Союзе контролером или обрабатывающим данные лицом должна подпадать под действие настоящего Регламента, если обработка данных имеет отношение к предложению товаров или услуг таким субъектам данным, вне зависимости от внесения платы. Для того чтобы определить, предлагает ли такой контролер или обрабатывающее данное лицо товары или услуги субъектам данным, которые находятся в Союзе, необходимо установить очевидность того, что контролер или обрабатывающее данное лицо намеревается предложить услуги субъектам данным в одном или нескольких государствах-членах ЕС в Союзе. В свою очередь явная доступность интернет-сайта контролера, обрабатывающего данные лица или посредника в Союзе, адреса электронной почты или иных контактных данных, или использование языка, принятого в третьей стране, в которой учрежден контролер, недостаточны для установления такого намерения, такие факторы как использование языка или валюты, распространенной в одном или нескольких государствах-членах ЕС, в совокупности с возможностью заказа товаров или услуг на данном языке, или упоминание покупателей или пользователей, находящихся в Союзе, указывают на то, что контролер намерен предложить товары или услуги субъектам данных в Союзе.

(24) Обработка персональных данных субъектов данных, находящихся в Союзе, не учрежденными в Союзе контролером или обрабатывающим данные лицом также подпадает под действие настоящего Регламента, если она связана с мониторингом поведенческой активности указанных субъектов данных постольку, поскольку их поведенческая активность имеет место в Союзе. Для того чтобы определить, может ли обработка данных рассматриваться в целях мониторинга поведенческой активности субъектов данных, необходимо установить, прослеживается ли деятельность физических лиц в сети интернет, включая возможное последующее использование способов обработки персональных данных, посредством которых составляется

профиль физического лица, особенно для принятия относящихся к нему решений или для анализа или прогнозирования его/ее личных предпочтений, форм поведения и жизненных позиций.

(25) Если законодательство государства-члена ЕС применяется в силу действия международного публичного права, как например, в дипломатическом представительстве или консульском учреждении государства-члена ЕС, настоящий Регламент должен также применяться в отношении контролера, не учрежденного в Союзе.

(26) Принципы защиты данных должны применяться в отношении любой информации, касающейся идентифицированного или идентифицируемого физического лица. Подвергнутые псевдонимизации персональные данные, которые могут быть соотнесены с физическим лицом посредством использования дополнительной информации, должны рассматриваться в качестве информации об идентифицируемом физическом лице. В целях установления того, является ли физическое лицо идентифицируемым, следует принять во внимание все средства, с высокой степенью вероятности используемые контролером или иным лицом, для того чтобы прямо или косвенно идентифицировать физическое лицо, например, выявление. При определении того, используются ли средства с достаточной степенью вероятности для идентификации физического лица, следует обратить внимание на все объективные факторы, такие как расходы на идентификацию и количество времени, необходимого для идентификации, с учетом имеющихся на момент обработки технологий и технологических разработок. Вследствие этого принципы защиты данных не применяются в отношении анонимной информации, а именно информации, которая не относится к идентифицированному или идентифицируемому физическому лицу, или в отношении персональных данных, предоставленных анонимно таким образом, что субъект данных не идентифицируется. Настоящий Регламент не касается обработки указанной анонимной информации, в том числе в статистических или исследовательских целях.

(27) Настоящий Регламент не применяется в отношении персональных данных умерших лиц. Государства-члены ЕС могут предусмотреть положения в области обработки персональных данных умерших лиц.

(28) Применение псевдонимизации в отношении персональных данных может снизить риски для субъектов данных и помочь контролерам и лицам, обрабатывающим данные, при выполнении ими своих обязанностей по защите данных. Прямое введение "псевдонимизации" в настоящем Регламенте не исключает использование любых других мер по защите данных.

(29) В целях создания стимулов для применения псевдонимизации при обработке персональных данных меры псевдонимизации, допускающие проведение общего анализа, должны быть возможны у того же контролера, если указанный контролер принял технические и организационные меры, необходимые в целях обеспечения, для соответствующей обработки, имплементации настоящего Регламента и гарантии того, что дополнительная информация для соотнесения персональных данных с определенным субъектом данных хранится отдельно. Контролер, обрабатывающий персональные данные, должен указать уполномоченных лиц у того же самого контролера.

(30) Физические лица могут быть связаны с сетевыми идентификаторами, предусмотренными их устройствами, приложениями, программными средствами и протоколами, как например, IP-адреса, идентификаторы типа куки-файлы или иные идентификаторы, например метки радиочастотной идентификации. Это может оставлять следы, которые, особенно в сочетании с уникальными идентификаторами и другой полученной серверами информацией, могут быть использованы для создания профилей физических лиц и для их идентификации.

(31) Органы государственной власти, которым раскрываются персональные данные в соответствии с юридической обязанностью по осуществлению официального представительства, например, налоговые органы и органы таможенного контроля, отделы финансовых расследований, независимые административные органы или службы по надзору за финансовым рынком, ответственные за регулирование и надзор за фондовыми рынками, не должны считаться получателями, если они получают персональные данные, которые в соответствии с

законодательством Союза или государства-члена ЕС необходимы для осуществления конкретного исследования в интересах общества. Запрос на раскрытие данных, направленный органами государственной власти, всегда должен осуществляться в письменной форме, быть обоснованным и носить случайный характер, он не должен касаться целостности файловой системы или вести к объединению файловых систем. Обработка персональных данных указанными органами государственной власти должна соответствовать применимым нормам по защите данных согласно целям обработки.

(32) Согласие должно быть дано посредством четкого утвердительного действия, при помощи которого субъект данных демонстрирует добровольное, определенное и однозначное согласие на обработку относящихся к нему персональных данных, например, посредством письменного заявления, в том числе поданного электронным способом, или устного заявления. Сюда может относиться простановка галочки/крестика при посещении интернет-сайта, выбор технических настроек для услуг информационного общества или иное заявление или способ поведения, который четко указывает на то, что субъект данных в указанном контексте согласен на запланированную обработку своих персональных данных. Молчание, уже проставленная галочка/крестик или бездействие лица не является согласием. Согласие должно охватывать всю обработку, осуществляемую для той же самой цели или целей. Если обработка служит нескольким целям, согласие должно быть дано для каждой из них. Если согласие субъекта данных должно быть дано электронным способом, запрос должен быть сделан в четкой и лаконичной форме, без ненужного прекращения услуги, для которой предоставляется согласие.

(33) Не всегда имеется возможность полностью идентифицировать цель обработки персональных данных для целей научного исследования во время сбора персональных данных. Вследствие этого, субъектам данных необходимо разрешить давать свое согласие в отношении определенных областей научного исследования в соответствии с признанными этическими стандартами научных исследований. Субъекты данных должны иметь возможность давать свое согласие только в отношении определенных областей исследования или частей исследовательских проектов в той мере, в какой это допустимо в рамках запланированной цели.

(34) Генетические данные должны определяться как персональные данные в отношении унаследованных или приобретенных характеристик физического лица, которые были получены в результате анализа биологического образца соответствующего лица, в частности, в результате хромосомного анализа, анализа ДНК или РНК, или анализа иных элементов, позволяющего получить эквивалентную информацию.

(35) Связанные со здоровьем персональные данные должны включать в себя все данные, которые относятся к состоянию здоровья субъекта данных и раскрывают информацию о прошлом, текущем и будущем физическом или психологическом состоянии здоровья субъекта данных. Сюда относится информация о физическом лице, собранная в ходе регистрации или предоставления медицинских услуг согласно Директиве 2011/24/ЕС Европейского Парламента и Совета ЕС[10] указанному физическому лицу; номер, символ или знак, присвоенные физическому лицу для однозначной идентификации указанного лица в целях здоровья; информация, полученная в результате исследования или обследования части тела или телесного материала, включая генетические данные и биологические образцы; а также любая информация, например, о заболевании, инвалидности, риске заболевания, медицинском анамнезе, клиническом лечении или о физиологическом или медико-биологическом состоянии субъекта данных, независимо от источника данных, например, они могут быть получены от врача или другого медицинского работника, больницы, медицинского оборудования или в результате диагностики в лабораторных условиях.

(36) Основное учреждение контролера в Союзе должно являться местом его центральной администрации в Союзе за исключением случаев, когда решения о целях и средствах обработки персональных данных принимаются в ином учреждении контролера в Союзе, в таком случае указанное другое учреждение должно считаться основным учреждением. Для определения основного учреждения контролера в Союзе необходимо использовать объективные критерии, при

этом предполагается эффективное и реальное осуществление управленческой деятельности, в рамках которой принимаются основные решения относительно целей и средств обработки посредством четких договоренностей. Указанный критерий не должен зависеть от того, осуществляется ли обработка персональных данных в указанном месте. Наличие и использование технических средств и методов для обработки персональных данных или деятельности, связанной с обработкой, само по себе не образует основное учреждение и вследствие этого не является определяющим критерием для основного учреждения. Основное учреждение обрабатывающего данные лица должно являться местом его центральной администрации в Союзе или, если в Союзе у него нет центральной администрации, местом, где в Союзе осуществляется связанная с обработкой основная деятельность. Если в обработке участвует контролер и обрабатывающее данные лицо, компетентным главным надзорным органом должен оставаться надзорный орган государства-члена ЕС, в котором находится основное учреждение контролера, а надзорный орган обрабатывающего данные лица должен считаться соответствующим надзорным органом, и указанный надзорный орган должен участвовать в предусмотренной настоящим Регламентом процедуре сотрудничества. В любом случае, надзорные органы государства-члена ЕС или государств-членов ЕС, в которых обрабатывающее данные лицо имеет один или несколько учреждений, не должны считаться соответствующими надзорными органами, если проект решения касается только контролера. Если обработка осуществляется группой предприятий, основное учреждение контролирующего предприятия должно считаться основным учреждением группы предприятий, за исключением случаев, когда цели и средства обработки определяются другим предприятием.

(37) Группа предприятий должна включать в себя контролирующее предприятие и подконтрольные ему предприятия; при этом контролирующее предприятие должно являться предприятием, которое может оказывать решающее воздействие на другие предприятия в силу, например, имущественных отношений, финансового участия или предписаний, которые его регулируют, или полномочия на имплементацию норм о защите персональных данных. Предприятие, которое контролирует обработку персональных данных на предприятиях, входящих в его состав, совместно с указанными предприятиями должны рассматриваться в качестве группы предприятий.

(38) Дети нуждаются в особой защите своих персональных данных, так как они в меньшей степени осознают риски, последствия, соответствующие гарантии и права при обработке персональных данных. Указанная особая защита должна, в частности, применяться в отношении использования персональных данных детей в целях маркетинга или создания личностного профиля или профиля пользователя и сбора персональных данных детей при использовании услуг, предлагаемых непосредственно детям. Согласие лиц, обладающих родительской ответственностью, не является необходимым в контексте профилактических мероприятий и консультационных услуг, предлагаемых непосредственно ребенку.

(39) Любая обработка персональных данных должна быть законной и справедливой. Для физических лиц прозрачность обработки состоит в том, что относящиеся к ним персональные данные собираются, используются, просматриваются или иным образом обрабатываются, а также в том, в какой степени персональные данные обрабатываются или будут обрабатываться. Принцип прозрачности требует, чтобы любая информация или сообщения в отношении обработки указанных персональных данных были легкодоступны и понятны и составлены на ясном и простом языке. Указанный принцип касается, в частности, информации относительно личности контролера и целей обработки, а также иной информации, которая гарантирует справедливую и прозрачную обработку в 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, нормах, гарантиях и правах в отношении обработки персональных данных и о том, как осуществлять свои права в отношении указанной обработки. В частности, определенные цели, для которых обрабатываются персональные данные, должны быть ясными и законными, они должны определяться в ходе сбора персональных данных. Персональные

данные должны быть соответствующими, уместными и ограниченными тем, что необходимо для целей, относительно которых они обрабатываются. В частности, это требует гарантии того, что срок, в течение которого хранятся персональные данные, был ограничен строгим минимумом. Персональные данные должны обрабатываться только, если цель обработки не могла быть достигнута иным способом. Для того чтобы гарантировать, что персональные данные не хранятся дольше положенного, контролер должен установить сроки для их уничтожения или для периодического пересмотра. Необходимо принять обоснованные меры, чтобы гарантировать, что неточные персональные данные были исправлены или удалены. Персональные данные должны обрабатываться таким образом, чтобы гарантировать их соответствующую защиту и конфиденциальность, включая предотвращение несанкционированного доступа или использования персональных данных и оборудования, используемого для обработки.

(40) Для того чтобы обработка была законной, персональные данные должны обрабатываться на основании согласия соответствующего субъекта данных или на ином законном основании, установленном или в настоящем Регламенте, или в другом законодательстве Союза или государства-члена ЕС, указанном в настоящем Регламенте, включая необходимость соблюдать законное обязательство, под действие которого подпадает контролер, или необходимость исполнять договор, одной из сторон которого является субъект данных, или для принятия мер по запросу субъекта данных до заключения договора.

(41) В случае если в настоящем Регламенте делается ссылка на законное основание или законодательную меру, это не обязательно требует принятия парламентом законодательного акта, без ущерба требованиям согласно конституционному строю соответствующего государства-члена ЕС. Однако указанное законное основание или законодательная мера должны быть ясными и точными, их применение должно быть заранее предсказуемо для лиц, которых они касаются, в соответствии с судебной практикой Суда Европейского Союза ("Суд") и Европейского суда по правам человека.

(42) В случае если обработка основывается на согласии субъекта данных, контролер должен быть в состоянии подтвердить, что субъект данных дал свое согласие на обработку. В частности, в рамках письменного заявления по другому вопросу гарантии должны обеспечивать, что субъект данных осознает факт того, что он дает свое согласие и в каком объеме указанное согласие дается. В соответствии с Директивой 93/13/ЕЭС Совета ЕС[11] заявление о согласии, предварительно сформулированное контролером, должно предоставляться в понятной и легкодоступной форме, с использованием ясного и простого языка, оно не должно содержать несправедливых условий. Для того чтобы проинформировать о согласии, субъект данных должен знать, как минимум, идентификационные данные контролера и цели обработки персональных данных. Согласие не считается данным добровольно, если у субъекта данных нет подлинного и свободного выбора или он не в состоянии без ущерба отказаться или аннулировать свое согласие.

(43) Для того чтобы гарантировать, что согласие дается добровольно, оно не должно создавать юридическое основание для обработки персональных данных в особых случаях, когда между субъектом данных и контролером существует явный дисбаланс, в частности, если контролер является органом государственной власти и вследствие этого с учетом всех обстоятельств указанной особой ситуации маловероятно, что согласие было дано добровольно. Предполагается, что согласие не дано добровольно, если отдельное согласие не может быть дано в отношении разных видов обработки персональных данных, несмотря на то, что в отдельном случае это является оправданным, или если исполнение договора, включая предоставление услуги, зависит от согласия, несмотря на то, что указанное согласие не является необходимым для исполнения договора.

(44) Обработка данных должна основываться на принципах законности, если она необходима для исполнения договора или для запланированного заключения договора.

(45) В случае если обработка осуществляется в соответствии с законной обязанностью, под действие которой подпадает контролер, или если обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий, она должна основываться на

законодательстве Союза или государства-члена ЕС. Настоящий Регламент не требует специального законодательства в отношении каждого отдельного вида обработки. Законодательства в качестве основания для нескольких видов обработки может быть достаточно, если обработка данных основана на законной обязанности, под действие которой подпадает контролер, или если обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий. В законодательстве Союза или государства-члена ЕС также должна быть определена цель обработки. Кроме этого, указанное законодательство может уточнять общие условия настоящего Регламента, регулирующие законность обработки персональных данных, может устанавливать спецификации для определения контролера, типы подлежащих обработке персональных данных, соответствующие субъекты данных, организации, которым персональные данные могут раскрываться, целевые ограничения, срок хранения и другие меры для гарантии законной и справедливой обработки. Также в законодательстве Союза или государства-члена ЕС необходимо определить, должен ли контролер, выполняющий задачу в интересах общества или при исполнении должностных полномочий, являться органом государственной власти или другим физическим или юридическим лицом, подпадающим под действие публичного права или при условии, что это оправдано с точки зрения интересов общества, в том числе в целях здоровья, например, общественного здравоохранения, социальной защиты и управления медицинскими услугами, под действие частного права, например, в качестве профессионального объединения.

(46) Обработка персональных данных также считается законной, если она необходима для защиты жизненно важных интересов субъекта данных или другого физического лица. Обработка персональных данных, основанная на жизненном интересе другого физического лица, должна в принципе осуществляться только, если она не может быть проведена на ином законном основании. Некоторые типы обработки могут служить как важным основаниям общественного интереса, так и жизненно важным интересам субъекта данных, например, если обработка необходима в гуманитарных целях, в том числе для контроля эпидемий и их распространения или в чрезвычайных ситуациях гуманитарного характера, в частности, во время техногенных или природных катастроф.

(47) Законные интересы контролера, включая контролера, которому могут быть раскрыты персональные данные, или третьей стороны могут создать законное основание для обработки, при условии, что они не превалируют над интересами или основными правами и свободами субъекта данных, с учетом разумных ожиданий субъектов данных, основанных на взаимоотношении с контролером. Указанный законный интерес может иметь место, например, если между субъектом данных и контролером существуют соответствующие отношения в ситуациях, когда субъект данных является клиентом или состоит на службе контролера. 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, превалировать над интересом контролера данных, если персональные данные обрабатываются в условиях, когда субъекты данных обоснованно не ожидают проведения дальнейшей обработки. Так как законодатель обязан на уровне законодательного акта предусмотреть законное основание для обработки персональных данных органами государственной власти, указанное законное 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 контролера данных. Обработка персональных данных в целях адресного маркетинга может рассматриваться в качестве обработки, служащей законному интересу.

(48) Контролеры, являющиеся частью группы предприятий или институтов, относящихся к центральному органу, могут иметь законный интерес, связанный с передачей персональных данных в рамках группы предприятий для внутренних административных целей, включая обработку персональных данных клиентов и работников. Общие принципы передачи персональных данных в рамках группы предприятий расположенному в третьей стране предприятию остаются в силе.

(49) Обработка персональных данных органами государственной власти, группой реагирования на компьютерные чрезвычайные происшествия (CERTs), группой 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 контролера данных в той мере, в какой она необходима и пропорциональна 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 сохраненных или переданных персональных данных, а также безопасность соответствующих услуг, переданных через указанные сети или системы. Указанный законный интерес может включать в себя, например, предотвращение несанкционированного доступа к сетям электронных коммуникаций и распространения 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 указанном случае не требуется иное законное основание, отдельное от того, посредством которого был разрешен сбор персональных данных. Если обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий, предоставленных контролеру, законодательство Союза или государства-члена ЕС может определить и установить задачи и цели, для которых дальнейшая обработка считается соответствующей и законной. Дальнейшая обработка для целей архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях рассматривается в качестве соответствующей законной обработки. Законное основание, предусмотренное законодательством Союза или государства-члена ЕС для обработки персональных данных, может также предусматривать законное основание для дальнейшей обработки. Для того чтобы убедиться в том, соответствует ли цель дальнейшей обработки цели, для которой персональные данные были первоначально получены, контролер, после выполнения всех требований относительно законности первоначальной обработки, должен принять во внимание, inter alia, 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 контролером, относительно их дальнейшего использования; характер персональных данных; последствия запланированной дальнейшей обработки для субъектов данных, и наличие соответствующих гарантий первоначальной и запланированной дальнейшей обработки.

В случае если субъект данных дал свое согласие или если обработка основана на законодательстве Союза или государства-члена ЕС, которое в демократическом обществе является необходимой и пропорциональной мерой для защиты, в частности, важных целей общего интереса общества, необходимо разрешить контролеру дальнейшую обработку персональных данных независимо от сопоставимости целей. В любом случае необходимо гарантировать применение принципов, установленных в настоящем Регламенте и, в частности, информирование субъекта данных об указанных других целях и о его правах, в том числе праве на возражение. Указания контролера на возможные уголовно-наказуемые деяния или угрозы общественной безопасности и передача соответствующих 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 контролера. Однако указанная передача в рамках законного интереса контролера или дальнейшая обработка персональных данных должны быть запрещены, если обработка не соответствует законной, профессиональной или иной обязанности по соблюдению конфиденциальности.

(51) Персональные данные, которые по своей природе носят конфиденциальный характер в

отношении основных прав и свобод, нуждаются в особой защите, так как контекст их обработки может привести к существенному риску для основных прав и свобод. Указанные 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 Союз одобряет теории, 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 особых технических средств, позволяющих провести уникальную идентификацию или аутентичность физического лица. Указанные персональные данные не должны обрабатываться за исключением случаев, когда обработка разрешена в особых установленных в настоящем Регламенте случаях, с учетом того, что законодательство государств-членов ЕС может установить особые положения о защите данных, для того чтобы адаптировать применение положений настоящего Регламента в целях соблюдения законного обязательства или в целях выполнения задачи в интересах общества или при осуществлении должностных полномочий контролера. В дополнение к особым требованиям для указанной обработки должны применяться общие принципы и другие положения настоящего Регламента, в частности, относительно условий законной обработки. Необходимо прямо предусмотреть частичные отступления от общего запрета на обработку указанных особых категорий персональных данных, inter alia, если субъект данных дает прямое согласие или если имеются особые потребности, в частности, если обработка осуществляется в рамках законной деятельности определенных объединений или фондов, целью которых является разрешение на реализацию основных свобод.

(52) Также частичные отступления от запрета на обработку особых категорий персональных данных необходимо разрешить, если они предусмотрены в законодательстве Союза или государства-члена ЕС и имеются соответствующие гарантии для 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 законодательства, законодательства о социальной защите, включая пенсии, и в целях обеспечения безопасности, мониторинга здоровья и предупреждения заболеваний, предотвращения или контроля инфекционных заболеваний и других серьезных угроз здоровью. Указанные частичные отступления могут быть сделаны в целях здоровья, включая здоровье населения и управление медицинскими услугами, особенно для гарантии качества и экономической эффективности методов, используемых для урегулирования претензий в системе медицинского страхования, или в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. Частичное отступление также может быть сделано для обработки персональных данных, необходимой для обоснования, исполнения или оспаривания исковых требований, в рамках судебной процедуры или в рамках административной или внесудебной процедуры.

(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 частности, 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 и трансграничного медицинского обслуживания или в целях обеспечения безопасности, мониторинга здоровья и предупреждения заболеваний, или в целях архивирования в интересах общества, в целях научного или исторического исследования, или в статистических целях, на основании законодательства Союза или государства-члена ЕС, которое должно соответствовать цели общественного интереса, а также в отношении исследований, проводимых в области общественного здравоохранения в интересах общества. 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 определенных, связанных со здоровьем, целях лицами, которые несут законную обязанность о соблюдении профессиональной тайны. Законодательство Союза или государства-члена ЕС должно предусматривать особые и приемлемые меры для защиты основных прав и персональных данных физических лиц. Государства-члены ЕС могут сохранять или вносить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных, касающихся здоровья. Однако это не должно препятствовать свободному обращению персональных данных в Союзе, если указанные условия применяются в отношении трансграничной обработки указанных 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 особыми мерами для защиты прав и свобод физических лиц. В указанном контексте понятие "общественное здравоохранение" должно пониматься в значении Регламента (ЕС) 1338/2008 Европейского Парламента и Совета ЕС[12] 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, отнесенные к медицинскому обслуживанию, предоставление и универсальный доступ к медицинскому обслуживанию, а также соответствующие расходы и финансирование и причины смертности. Указанная обработка касающихся здоровья данных 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) Кроме того, обработка персональных данных официальными органами для достижения установленной конституционным правом или международным публичным правом цели официально признанных религиозных организаций осуществляется по причинам общественного интереса.

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

(57) Если персональные данные, обрабатываемые контролером, не позволяют ему идентифицировать физическое лицо, контролер данных не обязан получать дополнительную информацию для идентификации субъекта данных только в целях соблюдения положения настоящего Регламента. Однако контролер не должен отказываться принимать дополнительную информацию, предоставляемую субъектом данных в целях содействия осуществлению своих прав. Идентификация должна включать в себя цифровую идентификацию субъекта данных, например, посредством механизма аутентификации, например, тех же самых удостоверяющих документов, используемых субъектом данных для того, чтобы войти под своим логином в онлайновую службу, предоставляемую контролером данных.

(58) Принцип прозрачности требует, чтобы любая информация, предоставляемая общественности или субъекту данных, была лаконичной, легкодоступной и понятной, и чтобы использовался ясный и простой язык, и дополнительно, при необходимости, использовались визуальные элементы. Указанная 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. Исходя из того, что дети требуют особой защиты, любая информация и сообщения, если обработка адресована ребенку, должны быть составлены на ясном, простом и понятном ребенку языке.

(59) Необходимо предусмотреть условия для содействия осуществлению прав субъекта

данных согласно настоящему Регламенту, включая механизмы для запроса и, при необходимости, бесплатного получения, в частности, доступа к персональным данным, их исправления или удаления и осуществления права на возражение. Контролер также должен предусмотреть средства для электронного запроса, особенно, если персональные данные обрабатываются электронным способом. Контролер обязан незамедлительно и как минимум в течение одного месяца ответить на запросы субъекта данных и, если он не намерен удовлетворять просьбу, указать причины.

(60) Принципы справедливой и прозрачной обработки требуют, чтобы субъект данных был проинформирован о наличии процесса обработки и ее целях. Контролер должен предоставить субъекту данных всю дополнительную информацию, необходимую для обеспечения справедливой и прозрачной обработки, с учетом особых обстоятельств и условий, в которых обрабатываются данные. Кроме этого, субъект данных должен быть проинформирован о наличии профиля и его последствиях. 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 отчетливо видимой, понятной и четкой форме дать общее представление о запланированной 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 субъекту данных в момент сбора у него 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 контролер намерен обрабатывать персональные данные в целях, отличных от целей, для которых они собирались, он до начала обработки должен представить субъекту данных информацию относительно указанной другой цели и 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, обязанность по предоставлению информации может не налагаться, если субъект данных уже обладает информацией, если регистрация или раскрытие персональных данных установлено на законодательном уровне или если предоставление информации субъекту данных невозможно или влечет за собой несоизмеримые усилия. В частности, в том, что касается последнего обстоятельства, это может быть обработка, которая осуществляется в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. В этой связи необходимо принять во внимание количество субъектов данных, возраст данных и любые соответствующие гарантии.

(63) Субъект данных должен иметь право доступа к относящимся к нему собранным персональным данным; указанное право должно осуществляться беспрепятственно и с определенной периодичностью в целях получения информации об обработке и проверки ее законности. Сюда относится право субъектов данных на доступ к касающимся их здоровья данным, например, данным в их медицинских документах, содержащих следующую информацию: диагнозы, результаты обследований, наблюдения лечащих врачей и сведения о любом лечении или вмешательствах. Вследствие этого каждый субъект данных должен 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, логической схемы любой автоматизированной обработки персональных данных и последствий указанной обработки, если она как минимум основана на формировании профиля. При наличии соответствующей возможности контролер должен обеспечить удаленный доступ к защищенной системе, которая предоставит субъекту данных прямой доступ к его персональным данным. Указанное право не должно отрицательно влиять на права или свободы других лиц, включая

коммерческую тайну или результаты интеллектуальной деятельности и, в частности, авторское право на программное обеспечение. Однако указанные ограничения не должны вести к отказу на предоставление всей информации субъекту данных. Если контролер 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) Контролер должен использовать все приемлемые способы для того, чтобы проверить и подтвердить личность субъекта данных, который подает запрос на доступ, в частности, в рамках онлайновых служб и в случае онлайновых идентификаторов. Контролер не должен сохранять персональные данные только в целях реагирования на потенциальный запрос.

(65) Субъект данных должен иметь право на исправление относящихся к нему персональных данных, а также "право на забвение", если сохранение указанных данных нарушает положения настоящего Регламента или законодательства Союза или государства-члена ЕС, под действие которого подпадает контролер. В частности, субъект данных должен иметь право на удаление своих 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 аннулировал свое согласие или возражает против обработки относящихся к нему персональных данных или если обработка персональных данных не соответствует настоящему Регламенту. Указанное право имеет существенное значение в случае, когда субъект данных давал свое согласие, будучи ребенком, 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 указанное право, невзирая на тот факт, что он больше не является ребенком. Однако дальнейшее хранение персональных данных законно, если оно необходимо для осуществление права на свободу выражения мнения и информации, для соблюдения законной обязанности, для выполнения задачи в интересах общества или при осуществлении должностных полномочий контролера, по причинам общественного интереса в области общественного здравоохранения, в целях архивировании в интересах общества, в целях научного или исторического исследования или в статистических целях, или для обоснования, исполнения или оспаривания исковых требований.

(66) Для того чтобы усилить право на забвение в сети, право на удаление следует расширить таким образом, чтобы контролер, который опубликовал персональные данные, был обязан проинформировать контролеров, которые обрабатывают указанные персональные данные, и удалить все ссылки, копии или репликации указанных персональных данных. При этом указанный контролер должен принять соответствующие меры с учетом имеющихся технологических возможностей и доступных средств, включая технические средства, чтобы проинформировать о запросе субъекта данных контролеров, которые обрабатывают персональные данные.

(67) Методы для ограничения обработки персональных данных могут включать в себя, inter alia, временную передачу отобранных данных другой системе обработки, непредставление пользователям отобранных персональных данных или временное удаление опубликованных данных с интернет-сайта. В автоматизированных файловых системах ограничение обработки должно гарантироваться техническими средствами таким образом, чтобы персональные данные не подлежали дальнейшей обработке и не могли быть изменены. Факт того, что обработка персональных данных ограничена, должен быть четко указан в системе.

(68) Для усиления контроля над собственными данными в случае, если обработка персональных данных осуществляется при помощи автоматизированных средств, субъект данных может получить относящиеся к нему персональные данные, которые он предоставил контролеру, в структурированном, широко используемом, машиночитаемом и функционально совместимом формате, и передать их другому контролеру. Контролеры данных должны усовершенствовать функционально совместимые форматы, чтобы способствовать переносимости данных. Указанное 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 законном основании, не связанном с согласием или договором. По своему характеру указанное право не должно осуществляться в отношении контролеров, обрабатывающих персональные данные при исполнении своих общественных обязанностей. Вследствие этого, оно не должно применяться, если обработка персональных данных необходима для соблюдения законного обязательства, под действие которого подпадает контролер, или для выполнения задачи в интересах общества или при осуществлении должностных обязанностей контролера. Право субъекта данных на передачу или получение относящихся к нему персональных данных не должно порождать обязательство для контролеров принимать или сохранять технически совместимые системы обработки. Если персональные данные в рамках определенного ряда касаются более одного субъекта данных, право на получение персональных данных должно действовать без ущерба правам и свободам остальных субъектов данных в соответствии с настоящим Регламентом. При этом указанное право не должно наносить ущерб праву субъекта данных на удаление персональных данных и ограничение указанного права согласно настоящему Регламенту и, в частности, не должно подразумевать удаление персональных данных, касающихся субъекта данных, которые были предоставлены им для исполнения договора, в той степени и покуда персональные данные необходимы для исполнения указанного договора. Если это технически возможно, субъект данных должен иметь право на прямую передачу персональных данных от одного контролера другому.

(69) В случае если персональные данные могут обрабатываться на законном основании вследствие того, что обработка необходима для выполнения задачи в интересах общества или при осуществлении должностных полномочий контролера, или на основании законных интересов контролера или третьей стороны, тем не менее, субъект данных должен иметь право на возражение против обработки любых персональных данных, относящихся к определенной ситуации. Контролер должен доказать, что его законный интерес превалирует над интересами или основными правами и свободами субъекта данных.

(70) В случае если персональные данные обрабатываются в целях адресного маркетинга, субъект данных в любое время и на бесплатной основе должен иметь право на возражение против указанной, первоначальной или последующей, обработки, включая формирование профиля, в той степени, в какой обработка связана с указанным адресным маркетингом. Необходимо обратить внимание субъекта данных на указанное право; о нем необходимо сообщить в четкой форме, отдельно от любой другой информации.

(71) Субъект данных должен иметь право на то, чтобы не подпадать под действие решения, которое может включать в себя меру, для оценки относящихся к нему персональных аспектов, которое основано исключительно на автоматизированной обработке и которое порождает юридические последствия в отношении субъекта данных или аналогичным образом существенно влияет на него, например, автоматический отказ в заявке на получение кредита онлайн или онлайновый процесс отбора кадров без вмешательства оператора. Указанная обработка включает в себя "формирования профиля", состоящее из любой формы автоматизированной обработки персональных данных при оценке относящихся к физическому лицу персональных аспектов, в частности, для анализа или прогнозирования аспектов, касающихся производственных показателей указанного лица, экономической ситуации, здоровья, индивидуальных предпочтений, интересов, надежности, поведения, месторасположения или передвижения, если это порождает юридические последствия в отношении субъекта данных или аналогичным образом влияет на него. Однако процесс принятия решения, основанный на указанной обработке, включая формирование профиля, необходимо разрешить, если это допустимо законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер, в том числе в целях мониторинга и предупреждения мошенничества и незаконного сокрытия доходов в соответствии с регламентами, стандартами и рекомендациями институтов Союза или национальных органов надзора, а также для гарантии безопасность и надежности услуги, предоставляемой контролером, или если это необходимо для

заключения или исполнения договора между субъектом данных или контролером, или если субъект данных дал свое прямое согласие. В любом случае указанная обработка должна осуществляться в соответствии с надлежащими гарантиями, включающими в себя особое информирование субъекта данных и право на вмешательство оператора, на высказывание своей точки зрения, получение объяснения в отношении решения, принятого после оценки, а также на оспаривание такого решения. Указанная мера не должна касаться ребенка.

Для того чтобы гарантировать справедливую и прозрачную обработку в отношении субъекта данных, с учетом особых обстоятельств и контекста, в котором обрабатываются персональные данные, контролер должен использовать соответствующие математические и статистические методы для формирования профиля, имплементировать технические и организационные меры в целях гарантии того, что факторы, которые приводят к неточностям персональных данных, исправлены, а риски возникновения ошибок минимизированы, защитить персональные данные таким образом, чтобы принять во внимание 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 указанное воздействие. Автоматизированный процесс принятия решения и формирование профиля на основе особых категорий персональных данных должны осуществляться только при определенных условиях.

(72) Формирование профиля осуществляется в соответствии с положениями настоящего Регламента, регулирующими обработку персональных данных, например, законные основания для обработки или принципы защиты данных. В указанном контексте Европейский совет по защите данных ("Совет") должен иметь возможность издавать руководящие указания.

(73) В законодательстве Союза или государства-члена ЕС могут быть предусмотрены ограничения в отношении особых принципов и прав на получение информации, доступ к данным и исправление или уничтожение персональных данных, в отношении права на переносимость данных, права на возражение, в отношении решений, основанных на формировании профиля, а также в отношении сообщения субъекту данных об утечке персональных данных и в отношении определенных соответствующих обязанностей контролеров, при условии, что это необходимо и пропорционально в демократическом обществе для обеспечения общественной безопасности, в том числе для защиты жизни людей, особенно, вследствие природных и техногенных катастроф, 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 Союза или государства-члена ЕС, в частности, важного экономического или финансового интереса Союза или государства-члена ЕС; а также в отношении ведения общественных реестров по причинам общественного интереса, дальнейшей обработки архивированных персональных данных для предоставления особой информации, связанной с политическим поведением в бывших тоталитарных режимах, или защиты субъекта данных или прав и свобод других лиц, включая социальную защиту, общественное здравоохранение и гуманитарные цели. Указанные ограничения должны соответствовать требованиям, установленным в Хартии и в Европейской Конвенции о защите прав человека и основных свобод.

(74) Необходимо установить ответственность и обязательства контролера в отношении любой обработки персональных данных, осуществляемой контролером или от его имени. В частности контролер обязан имплементировать соответствующие и эффективные меры и иметь возможность продемонстрировать соответствие обработки настоящему Регламенту, включая эффективность мер. Указанные меры должны учитывать характер, сферу применения, контекст и цели обработки и риск для прав и свобод физических лиц.

(75) Риски для прав и свобод физических лиц, разной степени вероятности и серьезности,

могут возникать в результате обработки персональных данных, которая может привести к физическому, материальному или нематериальному ущербу, в частности: если обработка может привести к дискриминации, хищению 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 иному неблагоприятному экономическому или социальному положению; если 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 преступлениях или соответствующих мерах безопасности; если оцениваются персональные аспекты, в частности, для анализа или прогнозирования аспектов, касающихся производственных показателей, экономической ситуации, здоровья, индивидуальных предпочтений, интересов, надежности, поведения, месторасположения или передвижения, в целях создания или использования персональных профилей; если обрабатываются персональные данные социально незащищенных физических лиц, в частности, детей; или если обработка охватывает большое количество персональных данных и влияет на большое количество субъектов данных.

(76) Вероятность и серьезность риска для прав и свобод субъекта данных должны определяться исходя из характера, сферы применения, контекста и целей обработки. Риск должен оцениваться на основе объективной оценки, посредством которой будет установлено, влечет ли обработка данных риск или риск высокой степени.

(77) Руководства по имплементации соответствующих мер и по подтверждению соблюдения требований контролером или обрабатывающим данные лицом, особенно в отношении идентификации риска, связанного с обработкой, оценки относительно происхождения, характера, вероятности и серьезности, а также идентификации передового опыта по снижению риска, могут предоставляться, в частности, в форме утвержденных норм поведения, утвержденных сертификационных процедур, руководящих указаний Совета или указаний инспектора по защите персональных данных. Совет может также издать руководящие указания в отношении обработки, которая рассматривается в качестве обработки, которая не может привести к риску высокой степени для прав и свобод физических лиц, и указать, какие меры могут быть достаточными в указанных случаях для устранения указанного риска.

(78) Защита прав и свобод физических лиц при обработке персональных данных требует принятия соответствующих технических и организационных мер в целях гарантии того, что соблюдаются требования настоящего Регламента. Для того чтобы подтвердить соблюдение настоящего Регламента, контролер должен принять внутренние правила и имплементировать меры, которые, в частности, соответствуют принципам защиты данных по умолчанию и на основе продуманных действий. Указанные меры могут включать, inter alia, минимизацию обработки персональных данных, псевдонимизацию персональных данных в максимально короткие сроки, прозрачность в отношении функций и обработки персональных данных, которые позволят субъекту данных контролировать процесс обработки данных, а контролеру позволят создать и улучшить средства защиты. При разработке, проектировании, выборе и использовании приложений, услуг и товаров, которые основаны на обработке персональных данных или обрабатывают персональные данные для выполнения своих задач, производители товаров, услуг и приложений могут принять во внимание право на защиту данных при разработке и проектировании указанных товаров, услуг и приложений, и с учетом современного состояния техники убедиться в том, что контролеры и обрабатывающие данные лица в состоянии исполнять свои обязанности, связанные с защитой данных. Принципы защиты данных по умолчанию и на основе продуманных действий должны учитываться в контексте публичных торгов.

(79) Защита прав и свобод субъектов данных, а также ответственность и обязанность

контролеров и обрабатывающих данные лиц, также в отношении мониторинга со стороны надзорных органов и их мер, требует четкого распределения обязанностей согласно настоящему Регламенту, в том числе, если контролер определяет цели и средства обработки совместно с другими контролерами или если обработка осуществляется от имени контролера.

(80) Если контролер или обрабатывающее данные лицо, не учрежденные в Союзе, обрабатывают персональные данные находящихся в Союзе субъектов данных и если их деятельность по обработке связана с предложением товаров и услуг указанным субъектам данных в Союзе, вне зависимости от того, требуется ли оплата от субъекта данных, или связана с мониторингом их линии поведения постольку, поскольку оно имеет место в Союзе, контролер или обрабатывающее данные лицо должно назначить представителя за исключением случаев, когда обработка носит случайный характер, не включает в себя масштабную обработку специальных категорий персональных данных, или обработка персональных данных, связанных с уголовными приговорами и преступлениями, вероятно, не приведет к возникновению риска для прав и свобод физических лиц, с учетом характера, обстоятельств, сферы применения и целей обработки, или если контролер является органом или учреждением государственной власти. Представитель должен действовать от имени контролера или обрабатывающего данные лица и являться для любого надзорного органа контактным центром. Представитель должен быть назначен посредством письменного предписания контролера или обрабатывающего данные лица на выполнение деятельности от их имени относительно обязанностей согласно настоящему Регламенту. Назначение указанного представителя не влияет на ответственность или обязанности контролера или обрабатывающего данные лица согласно настоящему Регламенту. Указанный представитель должен выполнять свои задачи согласно предписанию, полученному от контролера или обрабатывающего данные лица, включая сотрудничество с компетентными надзорными органами в отношении любых мер, принятых в целях гарантии соблюдения настоящего Регламента. Назначенный представитель должен подвергаться правоохранительным процедурам в случае нарушений со стороны контролера или обрабатывающего данные лица.

(81) Для того чтобы гарантировать соблюдение требований настоящего Регламента в отношении обработки, осуществляемой обрабатывающим данные лицом от имени контролера, при возложении на указанное лицо обязанности по обработке данных контролер должен использовать обрабатывающих данные лиц, которые предусматривают соответствующие гарантии, в частности, в отношении экспертных знаний, надежности и ресурсов, для того чтобы имплементировать технические и организационные меры, которые будут отвечать требованиям настоящего Регламента, в том числе в отношении безопасности обработки. Соблюдение обрабатывающим данные лицом утвержденных норм поведения или утвержденного сертификационного механизма может использоваться в качестве элемента для подтверждения соблюдения обязанностей контролера. Осуществление обработки лицом, обрабатывающим данные, должно регулироваться договором или иным законодательным актом согласно законодательству Союза или государства-члена ЕС, привязывающим обрабатывающее данные лицо к контролеру, устанавливающим предмет и продолжительность обработки, характер и цели обработки, тип персональных данных и категории субъектов данных, с учетом определенных задач и обязанностей обрабатывающего данные лица в контексте обработки и риска для прав и свобод субъекта данных. Контролер и обрабатывающее данные лицо могут по выбору использовать индивидуальный договор или стандартные договорные условия, принятые или Европейской Комиссией, или надзорным органом в соответствии с механизмом сопоставимости, а затем утвержденные Европейской Комиссией. После завершения обработки от имени контролера обрабатывающее данные лицо должно по выбору контролера вернуть или удалить персональные данные, за исключением случаев, когда существует требование о хранении персональных данных в соответствии с законодательством Союза или государства-члена ЕС, под действие которого подпадает обрабатывающее данные лицо.

(82) Для того чтобы подтвердить соблюдение настоящего Регламента, контролер или обрабатывающее данные лицо должны вести учет обработки, осуществляемой под их

ответственностью. Каждый контролер и обрабатывающее данные лицо обязано сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учетные сведения в целях мониторинга процесса обработки.

(83) Для того чтобы обеспечить безопасность и предотвратить обработку в нарушение настоящего Регламента, контролер или обрабатывающее данные лицо должно оценить риски, присущие обработке, и имплементировать меры по снижению указанных рисков, например, криптографическую защиту. Указанные меры должны гарантировать соответствующий уровень защиты, в том числе конфиденциальности, с учетом уровня развития техники и расходов на имплементацию в отношении рисков и характера 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, сохраненным или иным образом обрабатываемым данным, которые могут привести к физическому, материальному или нематериальному ущербу.

(84) Для того чтобы улучшить соблюдение положений настоящего Регламента, если обработка может привести к риску высокой степени для прав и свобод физических лиц, контролер должен отвечать за выполнение оценки воздействия на защиту данных для того, чтобы определить, в частности, характер, специфику и серьезность указанного риска. Необходимо принять во внимание результат оценки при определении соответствующих мер, которые должны быть приняты для подтверждения того, что обработка персональных данных соответствует настоящему Регламенту. Если оценка воздействия на защиту данных указывает на то, что обработка влечет риск высокой степени, который контролер не может смягчить посредством соответствующих мер в отношении имеющихся технологий и расходов на имплементацию, до начала обработки необходимо проконсультироваться с надзорным органом.

(85) Утечка персональных данных, если она не была вовремя и соответствующим образом устранена, может привести к физическому, материальному или нематериальному ущербу для физических лиц, например, потере контроля над персональными данными или ограничению прав, дискриминации, хищению персональных данных или мошенничеству с данными, финансовым потерям, несанкционированному отказу от псевдонимизации, ущербу репутации, нарушению конфиденциальности персональных данных, защищенных обязанностью соблюдать профессиональную тайну, или любому другому неблагоприятному экономическому или социальному положению для соответствующего лица. Вследствие этого, как только контролеру станет известно об утечке персональных данных, он должен уведомить об этом надзорный орган незамедлительно и, при наличии возможности, не позднее 72 часов после того, как он узнал об утечке, за исключением случаев, когда контролер способен доказать, в соответствии с принципом предоставления отчетности, что утечка персональных данных не приведет к риску для прав и свобод физических лиц. Если указанное уведомление не может быть сделано в течение 72 часов, причины отсрочки необходимо указать в уведомлении, информация может быть предоставлена поэтапно без дальнейшего промедления.

(86) Контролер незамедлительно должен сообщить субъекту данных об утечке персональных данных, если указанная утечка может привести к возникновению риска высокой степени для прав и свобод физического лица, для того чтобы указанное лицо приняло необходимые меры предосторожности. В сообщении необходимо описать характер нарушения, а также дать рекомендации физическому лицу по снижению возможного негативного воздействия. Указанные сообщения субъектам данных должны быть сделаны как можно быстрее и в тесном сотрудничестве с надзорным органом в соответствии с руководящим указанием данного органа или иного соответствующего органа, например, правоохранительных органов. Например, чтобы снизить непосредственный риск ущерба, необходимо мгновенно уведомить субъекты данных, при этом, если необходимо имплементировать соответствующие меры против продолжения совершения утечки персональных данных, может потребоваться больше времени для общения.

(87) Необходимо удостовериться, все ли соответствующие технологические и организационные меры были имплементированы для того, чтобы незамедлительно установить факт утечки персональных данных и проинформировать об этом надзорный орган и субъект данных. Тот факт, что уведомление необходимо сделать незамедлительно, должен быть установлен с учетом, в частности, характера и серьезности утечки персональных данных, ее последствий и негативного воздействия на субъект данных. Указанное уведомление может привести к вмешательству надзорного органа в соответствии с его задачами и полномочиями, установленными в настоящем Регламенте.

(88) При установлении подробных правил относительно формата и процедур, применяемых к уведомлению об утечке персональных данных, необходимо должное внимание уделить обстоятельствам указанной утечки, в том числе тому, была ли обеспечена защита персональных данных посредством соответствующих технических мер, которые эффективным образом снижают вероятность мошенничества с персональными данными или иных форм противоправного использования данных. Кроме того, указанные правила и процедуры должны учитывать законные интересы правоохранительных органов, если раннее раскрытие данных 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. Вследствие этого указанные бессистемные общие обязанности в отношении уведомления должны быть отменены и заменены эффективными процедурами и механизмами, которые фокусируются на тех типах обработки данных, которые могут привести к возникновению риска высокой степени для прав и свобод физических лиц в соответствии с их характером, сферой применения, контекстом и целями. К указанным типам обработки могут относиться, в частности, те типы, которые включают в себя использование новых технологий, или которые сами являются новыми, и если контролер не проводил оценку воздействия на защиту данных или если они необходимы с учетом времени, которое прошло с момента первоначальной обработки.

(90) В указанных случаях оценка воздействия на защиту данных должна осуществляться контролером до обработки данных с тем, чтобы оценить особую вероятность и серьезность риска высокой степени, с учетом характера, сферы применения, контекста и целей обработки, а также источников риска. Указанная оценка воздействия должна включать в себя, в частности, меры, гарантии и механизмы, предусмотренные для устранения указанного риска, гарантии защиты персональных данных и подтверждения соблюдения настоящего Регламента.

(91) В частности, это должно применяться в отношении масштабной обработки, которая направлена на обработку значительного количества персональных данных на региональном, национальном и наднациональному уровне, и может повлиять на большое количество субъектов данных, и может привести к риску высокой степени, например, на основании их уязвимости, если в соответствии с достигнутым уровнем технологических знаний в большом количестве используются новые технологии, а также в отношении иных видов обработки, которые могут привести к риску высокой степени для прав и свобод субъектов данных, в частности, если указанная обработка затрудняет осуществление прав субъектами данных. Оценка воздействия на защиту данных должна быть проведена, если персональные данные обрабатываются в целях принятия решений в отношении определенных физических лиц в соответствии с систематической и всесторонней оценкой персональных аспектов в отношении физических лиц, основанных на формировании профиля указанных данных, или в соответствии с обработкой особых категорий персональных данных, биометрических данных или данных об уголовных приговорах и преступлениях или о соответствующих мерах безопасности. Оценка воздействия на защиту данных требуется для мониторинга открытых для общего доступа областей, особенно, если используются оптоэлектронные устройства, или для иных действий, если компетентный надзорный орган считает, что обработка может привести к риску высокой степени для прав и свобод субъектов данных, в

частности, вследствие того, что они препятствуют субъектам данных осуществлять право или использовать услугу или договор, или вследствие того, что они осуществляются систематически и в большом количестве. Обработка персональных данных не должна считаться масштабной, если она касается персональных данных пациентов или клиентов и осуществляется лечащим врачом, иным медицинским работником или юристом. В указанных случаях оценка воздействия на защиту данных не считается обязательной.

(92) При определенных обстоятельствах может быть приемлемо и целесообразно с экономической точки зрения не относить оценку воздействия на защиту данных к определенному проекту, например, если органы государственной власти или учреждения намерены установить общее применение или платформу для обработки информации или если несколько контролеров планируют ввести общее применение или условие обработки для промышленном сектора, или сегмента, или для широко применяемой горизонтальной деятельности.

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

(94) Если оценка воздействия на защиту данных указывает на то, что обработка, при отсутствии гарантий, мер безопасности и механизмов для снижения риска, может привести к высокой степени риска для прав и свобод физических лиц, и контролер считает, что риск не может быть снижен при помощи имеющихся технологических средств и расходов на имплементацию, до начала процесса обработки необходимо проконсультироваться с надзорным органом. Указанная высокая степень риска может возникнуть в результате определенных типов обработки, объема и периодичности обработки, и может также повлечь за собой ущерб или посягательство на права и свободы физического лица. Надзорный орган в установленный срок должен ответить на запрос о проведении консультации. Однако отсутствие ответа надзорного органа в указанный срок действует без ущерба любому вмешательству надзорного органа в соответствии с его задачами и полномочиями, установленными в настоящем Регламенте, включая полномочие на запрет процесса обработки. В рамках процесса консультации результат оценки воздействия на защиту данных, проведенной в отношении рассматриваемой обработки, может быть представлен надзорному органу, в частности, меры по снижению риска для прав и свобод физических лиц.

(95) Обрабатывающее данные лицо должно оказывать содействие контролеру, в соответствующем случае и по запросу, при обеспечении соблюдения обязанностей, возникающих из осуществления оценки воздействия на защиту данных и из предварительной консультации надзорного органа.

(96) Консультация надзорного органа также должна проводиться в ходе подготовки законодательной или регулятивной меры, которая предусматривает обработку персональных данных для обеспечения соответствия запланированной обработки настоящему Регламенту и, в частности, смягчения риска для субъекта данных.

(97) В случае если обработка осуществляется органом государственной власти, за исключением судов или независимых судебных органов, действующих в рамках своей судейской дееспособности, если в частном секторе обработка осуществляется контролером, целевая деятельность которого состоит в обработке, требующей регулярного и систематического мониторинга субъектов данных, или если целевая деятельность контролера или обрабатывающего данные лица состоит в масштабной обработке специальных категорий персональных данных и данных, связанных с уголовными судимостями и преступлениями, лицо, обладающее экспертными знаниями в области законодательства и практики о защите персональных данных, должно содействовать контролеру или обрабатывающему данные лицу при мониторинге внутреннего соблюдения настоящего Регламента. В частном секторе целевая деятельность контролера относится к его основной деятельности и не относится к обработке персональных данных в качестве вспомогательного вида деятельности. Необходимый уровень экспертных знаний должен

определяться, в частности, в соответствии с проведенной обработкой данных и требуемой защитой для персональных данных, обработанных контролером или обрабатывающим данные лицом. Инспекторы по защите персональных данных, вне зависимости от того, являются ли они работниками контролера, должны быть в состоянии независимо исполнять свои обязанности и выполнять свои задачи.

(98) Объединения или иные органы, представляющие определенные категории контролеров или обрабатывающих данные лиц, могут в рамках настоящего Регламента разработать нормы поведения для того, чтобы способствовать эффективному применению настоящего Регламента, при этом необходимо учитывать характеристики обработки, осуществляемой в определенных секторах, и специфические потребности микропредприятий, малых и средних предприятий. В частности, указанные нормы поведения могут точно определять обязательства контролеров и обрабатывающих данные лиц, с учетом риска для прав и свобод физических лиц в результате обработки.

(99) При разработке нормы поведения, при изменении или расширении указанной нормы объединения и иные органы, представляющие определенные категории контролеров или обрабатывающих данные лиц, должны проконсультироваться с соответствующими участниками, и при наличии возможности с субъектами данных, 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 данных в третьи страны и международные организации, а также из третьих стран и международных организаций необходимы для расширения внешней торговли и международного сотрудничества. Увеличение объемов указанных потоков привело к новым вызовам и требованиям, связанным с защитой персональных данных. Однако если персональные данные передаются из Союза контролерам, обрабатывающим данные лицам или иным получателям в третьих странах или международным организациям, уровень защиты физических лиц, гарантированный в Союзе настоящим Регламентом, не должен быть ослаблен, в том числе в случаях передачи персональных данных из третьей страны или международной организации контролерам, обрабатывающим данные лицам в той же самой или другой третьей стране или международной организации. В любом случае, передача данных третьим странам и международным организациям может осуществляться только при полном соблюдении положения настоящего Регламента. Передача может осуществляться только, если в соответствии с другими положениями настоящего Регламента, контролер или обрабатывающее данные лицо соблюдает условия, установленные в положениях настоящего Регламента относительно передачи персональных данных третьим странам или международным организациям.

(102) Настоящий Регламент действует без ущерба международным соглашениям между Союзом и третьими странами в отношении передачи персональных данных, включая соответствующие гарантии для субъектов данных. Государства-члены ЕС могут заключить международные соглашения, касающиеся передачи персональных данных третьим странам и международным организациям, поскольку указанные соглашения не влияют на настоящий Регламент или на иные положения законодательства Союза и включают в себя соответствующий уровень защиты основных прав субъектов данных.

(103) Европейская Комиссия может принять действительное для всего Союза решение о том, что третья страна, территория или определенный сектор в третьей стране или международная организация гарантирует соответствующий уровень защиты данных, таким образом обеспечивается юридическая определенность и единообразие на территории Союза в отношении третьей страны или международной организации, которая гарантирует указанный уровень защиты. В указанных случаях передача персональных данных третьей стране или международной организации может осуществляться без получения дальнейшего разрешения. Европейская Комиссия может также

отменить указанное решение и сообщить об этом, с указанием причин, третьей стране или международной организации.

(104) В соответствии с основополагающими ценностями Союза, к которым, в частности, относится защита прав человека, Европейская Комиссия при оценке третьей страны или территории или определенного сектора в третьей стране должна принять во внимание то, каким образом третья страна соблюдает принципы правового государства, обеспечивает доступность правосудия, а также соблюдает нормы и стандарты международного права в области прав человека, основного и секторального законодательства, включая законодательство относительно общественной безопасности, обороны и внутренней безопасности, а также общественный порядок и уголовное законодательство. При принятии решения о соответствии в отношении территории или определенного сектора в третьей стране следует учитывать четкие и объективные критерии, например, определенный вид обработки и область применения правовых стандартов и действующего в третьей стране законодательства. Третья страна должна предоставить гарантии, обеспечивающие соответствующий уровень защиты, эквивалентный уровню, гарантированному в Союзе, в особенности, если персональные данные обрабатываются в одном или нескольких особых секторах. В частности, третья страна должна гарантировать эффективный и независимый мониторинг защиты данных и должна предусмотреть механизмы сотрудничества с органами государств-членов ЕС по защите данных, субъектам данных должны быть предоставлены обеспеченные законодательством эффективные права и 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 имплементацию указанных 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 контролировать исполнение решений об уровне защиты в третьей стране, территории или определенном секторе в третьей стране или в международной организации, а также контролировать исполнение решений, принятых на основе Статьи 25(6) или Статьи 26(4) Директивы 95/46/ЕС. В своих решениях о соответствии 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 контроля и осуществления периодических проверок Европейская Комиссия должна учитывать мнения и замечания Европейского Парламента и Совета ЕС, а также всех других соответствующих органов и источников. Европейская Комиссия в приемлемый срок должна оценить исполнение указанных решений и направить отчет со всеми соответствующими выводами Комитету в значении Регламента (ЕС) 182/2011 Европейского Парламента и Совета ЕС[13] в установленном согласно настоящему Регламенту порядке, а также Европейскому Парламенту и Совету ЕС.

(107) Европейская Комиссия может признать, что третья страна, территория или определенный 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 приемлемыми гарантиями, включая юридически обязывающие корпоративные правила, и частичные отступления от определенных ситуаций. В указанном случае следует предусмотреть консультации между Европейской Комиссией и указанными 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 соответствии контролер или обрабатывающее данные лицо должно принять меры для восполнения недостатка в защите данных в третьей стране посредством соответствующих гарантий для субъекта данных. Указанные соответствующие гарантии могут включать в себя использование юридически обязывающих корпоративных правил, установленных Европейской Комиссией стандартных условий по защите данных, установленных надзорным органом стандартных условий по защите данных или договорных условий, разрешенных надзорным органом. Указанные гарантии должны обеспечить соблюдение требований по защите данных и прав субъектов данных, связанных с обработкой в Союзе, включая наличие обеспеченных прав субъекта данных и доступность эффективных средств правовой защиты, в том числе права на получение эффективной административной и судебной помощи и требование компенсации в Союзе или в третьей стране. Они должны относиться, в частности, к соблюдению общих принципов в отношении обработки персональных данных, принципов запланированной защиты данных или защиты данных по умолчанию. Передача данных может также осуществляться органами государственной власти или учреждениями совместно с органами государственной власти или учреждениями в третьей стране или с международными организациями с соответствующими обязанностями или задачами, в том числе на основе положений, которые должны быть внесены в административные соглашения, например, протокол о взаимопонимании, с учетом обеспеченных законодательством и эффективных прав для субъектов данных. Разрешение компетентного надзорного органа должно быть получено, если гарантии предусмотрены в административных соглашениях, не имеющих обязательную юридическую силу.

(109) Возможность контролера или обрабатывающего данные лица использовать стандартные условия для защиты данных, утвержденные Европейской Комиссией или надзорным органом, не должна препятствовать контролерам или обрабатывающим данные лицам включать стандартные условия для защиты данных в расширенный договор, например, договор между обрабатывающим данные лицом и иным лицом по обработке данных, а также добавлять иные условия или дополнительные гарантии, при условии, что они прямо или косвенно не противоречат стандартным договорным условиям, утвержденным Европейской Комиссией или надзорным органом, или не причиняют вред основным правам и свободам субъектов данных. Контролеры или обрабатывающие данные лица могут предусматривать дополнительные гарантии посредством договорных обязательств, которые дополняют стандартные условия защиты.

(110) Группа предприятий или группа компаний, участвующих в совместной экономической деятельности, должна иметь возможность использовать утвержденные обязательные корпоративные правила для международной передачи своих данных из Союза организациям в рамках той же группы предприятий или группы компаний, участвующих в совместной экономической деятельности, при условии, что указанные корпоративные правила включают в себя все существенные принципы и защищенные законодательством права для обеспечения соответствующих гарантий передачи или категорий передачи персональных данных.

(111) При определенных условиях необходимо предусмотреть возможность передачи данных, если субъект данных дал свое 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. Также необходимо предусмотреть возможность передачи данных, если это требуется по важным причинам общественного интереса согласно законодательству Союза или государства-члена ЕС или если передача осуществляется из установленного законодательством реестра и предназначена для ознакомления общественности или лиц, имеющих законный интерес. В последнем случае указанная передача не должна затрагивать все персональные данные или категории данных, содержащиеся в реестре, и, если реестр предназначен

для ознакомления лиц, имеющих законный интерес, передача должна осуществляться только по запросу указанных лиц или, если они являются получателями, необходимо полностью учитывать интересы и основные права субъекта данных.

(112) Указанные частичные отступления, в частности, должны применяться в отношении передачи данных, необходимых по важным 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 общественное здравоохранение, например, в случае прослеживания контакта 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 свое согласие. При отсутствии решения о соответствии законодательство Союза или государства-члена ЕС может по важным причинам общественного интереса прямо ограничить передачу особых категорий данных третьей стране или международной организации. Государства-члены ЕС должны уведомить об указанных положениях Европейскую Комиссию. Любая передача международной гуманитарной организации персональных данных субъекта данных, который физически или юридически не в состоянии дать свое согласие, в целях выполнения задачи, возложенной Женевской Конвенцией, или в целях соблюдения международного гуманитарного права, применяемого в период вооруженных конфликтов, может рассматриваться в качестве необходимой исходя из важных 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 соблюдения законных интересов контролера, если указанные интересы не превалируют над интересами или правами и свободами субъекта данных и если контролер проверил все обстоятельства, связанные с передачей данных. Контролер должен уделить особое внимание характеру персональных данных, цели и продолжительности запланированной обработки, а также ситуации в стране происхождения, третьей стране или стране конечного адресата, а также должен предусмотреть приемлемые гарантии для защиты основных прав и свобод физических лиц при обработке персональных данных. Указанная передача возможна в оставшихся случаях только, когда не применяются иные основания для передачи данных. В целях научного или исторического исследования или в статистических целях следует принять во внимание правомерные ожидания общества относительно расширения знаний. Контролер должен проинформировать надзорный орган и субъекта данных о передаче данных.

(114) В любом случае, если Европейская Комиссия не приняла решения относительно соответствующего уровня защиты данных в третьей стране, контролер или обрабатывающее данные лицо должно использовать решения, посредством которых субъектам данных предоставляются осуществимые и эффективные права в отношении обработки их персональных данных в Союзе после передачи указанных данных с тем, чтобы они могли и дальше пользоваться основными правами и гарантиями.

(115) Некоторые третьи страны принимают законодательные, регламентарные и другие правовые акты, которые предназначены для непосредственного регулирования связанной с обработкой деятельности физических и юридических лиц, которые подпадают под юрисдикцию государств-членов ЕС. Это может включать в себя приговоры судов или трибуналов или решения административных органов в третьих странах, которые требуют от контролера или обрабатывающего данные лица передачи или раскрытия персональных данных и которые не основаны на действующем международном соглашении, например, договоре о взаимной правовой помощи, между запрашивающей третьей страной и Союзом или государством-членом ЕС. Экстерриториальное применение указанных законодательных, регламентарных и иных правовых

актов может нарушать международное право и может препятствовать защите физических лиц, гарантированной в Союзе настоящим Регламентом. Передача данных должна быть разрешена только, если соблюдаются условия настоящего Регламента в отношении передачи данных третьим странам. Это, inter alia, может являться случаем, когда разглашение необходимо по причине важного общественного интереса, который признан законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер.

(116) Если персональные данные перемещаются за пределы Союза, это может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в частности, защитить себя от незаконного 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 их государства-члена ЕС. Их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или корректирующими полномочиями, противоречивыми правовыми режимами и практическими препятствиями, например, ограничением на ресурсы. 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 ЕС, уполномоченных на полностью независимое выполнение своих задач и осуществление своих полномочий, является существенным компонентом защиты физических лиц при обработке персональных данных. Государства-члены ЕС должны иметь возможность учреждать более одного надзорного органа, если это соответствует их конституционной, организационной и административной структуре.

(118) Независимость надзорных органов не означает, что они не могут подлежать контролю или мониторингу в отношении своих финансовых расходов или судебному надзору.

(119) В случае если государство-член ЕС учреждает несколько надзорных органов, он должен на законодательном уровне установить механизмы для обеспечения эффективного участия указанных надзорных органов в рамках механизма сопоставимости. Указанное государство-член ЕС должно, в частности, назначить надзорный орган, который будет функционировать в качестве единственного контактного центра для эффективного участия указанных органов в механизме и для обеспечения быстрого и бесперебойного сотрудничества 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 задач, связанных с взаимной помощью и сотрудничеством с другими надзорными органами на территории Союза. Каждый надзорный орган должен иметь отдельный, публичный, годовой бюджет, который может являться частью общего государственного или национального бюджета.

(121) На законодательном уровне в каждом государстве-члене ЕС необходимо установить общие условия для члена или членов надзорного органа; они должны, в частности, предусматривать, что указанные члены назначаются посредством прозрачной процедуры или парламентом, правительством или главой государства члена ЕС на основе предложения правительства, члена правительства, парламента или палаты парламента или независимым надзорным органом, уполномоченный согласно законодательству государства-члена ЕС. Для того чтобы гарантировать независимость 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 возмездной или безвозмездной деятельности. Надзорный орган должен обладать своим собственным персоналом, который выбран надзорным органом или независимым органом, учрежденным в соответствии с законодательством государства-члена ЕС, и который находится в подчинении члена или членов надзорного органа.

(122) Каждый надзорный орган должен быть компетентным на территории своего собственного государства-члена ЕС и осуществлять полномочия и выполнять задачи, возложенные на него в соответствии с настоящим Регламентом. В частности, это относится к обработке в рамках деятельности учреждения контролера или обрабатывающего данные лица на территории его государства-члена ЕС, к обработке персональных данных органами государственной власти или частными организациями, действующими в общественных интересах, к обработке, затрагивающей субъекты данных на его территории, или обработке контролером или обрабатывающим данные лицом, не учрежденным в Союзе, если целью являются субъекты данных, проживающие на его территории. Это также включает в себя обработку жалоб, поданных субъектом данных, проведение расследований о применении настоящего Регламента, а также содействие информированности общественности о рисках, нормах, гарантиях и правах в отношении обработки персональных данных.

(123) Надзорные органы должны контролировать применение положений настоящего Регламента и способствовать его согласованному применению на территории Союза для защиты физических лиц при обработке их персональных данных и для содействия свободному обращению персональных данных на внутреннем рынке. Для указанной цели надзорные органы должны сотрудничать друг с другом и с Европейской Комиссией, при этом соглашения между государствами-членами ЕС о предоставлении взаимной помощи или о таком сотрудничестве могут не заключаться.

(124) В случае если обработка персональных данных осуществляется в рамках деятельности учреждения контролера или обрабатывающего данные лица в Союза и контролер или обрабатывающее данные лицо учреждены в нескольких государствах-членах ЕС, или если обработка, осуществляемая в рамках деятельности единственного учреждения контролера или обрабатывающего данные лица в Союзе, существенно влияет или может существенно повлиять на субъекты данных в нескольких государствах-членах ЕС, надзорный орган в отношении основного учреждения контролера или обрабатывающего данные лица или в отношении единственного учреждения контролера или обрабатывающего данные лица должен выступать в роли главного органа. Он должен сотрудничать с другими соответствующими органами вследствие того, что учреждение контролера или обрабатывающего данные лица находится на территории их государства-члена ЕС, что на субъекты данных, проживающих на их территории, оказывается существенное воздействие, или что им была подана жалоба. Также если субъект данных, не проживающий в указанном государстве-члене ЕС, подал жалобу, надзорный орган, в который была подана жалоба, должен также являться соответствующим надзорным органом. В рамках своих задач по изданию руководящих указаний по любому вопросу, затрагивающему применение настоящего Регламента, Совет должен иметь возможность издавать указания, в частности, в отношении критериев, которые должны быть приняты во внимание, для того чтобы удостовериться, влияет ли обработка на субъекты данных в нескольких государствах-членах ЕС, а также относительно того, что представляет собой существенное и мотивированное возражение.

(125) Главный орган должен быть вправе принимать юридически обязательные решения в отношении мер, посредством которых осуществляются полномочия, предоставленные ему в соответствии с настоящим Регламентом. В качестве главного органа надзорный орган должен содействовать привлечению надзорных органов к участию в процессе принятия решения, а также их координированию. Если принимается решение относительно полного или частичного отклонения жалобы субъекта данных, указанное решение должно быть принято надзорным органом, в который была подана жалоба.

(126) Решение должно быть согласовано совместно главным надзорным органом и соответствующими надзорными органами и должно быть адресовано основному или единственному учреждению контролера или обрабатывающего данные лица и иметь обязательную силу для контролера и обрабатывающего данные лица. Контролер или обрабатывающее данные лицо должно принять необходимые меры для обеспечения соблюдения настоящего Регламента и для имплементации решения, о котором главный надзорный орган уведомил основное учреждение контролера или обрабатывающего данные лицо в отношении обработки в Союзе.

(127) Каждый надзорный орган, не выступающий в роли главного надзорного органа, должен иметь право на рассмотрение местных случаев, если контролер или обрабатывающее данные лицо учреждено в нескольких государствах-членах ЕС, но предмет особой обработки касается только обработки, осуществляемой в одном государстве-члене ЕС, и только субъектов данных в указанном государстве-члене ЕС, например, если предмет рассмотрения касается обработки персональных данных работников при выполнении особых должностных обязанностей государства-члена ЕС. В указанных случаях надзорный орган незамедлительно должен проинформировать главный надзорный орган об указанном обстоятельстве. После получения соответствующей информации главный надзорный орган должен решить, будет ли он рассматривать дело в соответствии с положением о сотрудничестве между главным надзорным органом и другими соответствующими органами ("механизм сотрудничества и сопоставимости") или надзорный орган, который его проинформировал, должен рассмотреть дело на местном уровне. При решении вопроса относительно рассмотрения дела главный надзорный орган должен принять во внимание, находится ли учреждение контролера или обрабатывающего данные лица в государстве-члене ЕС надзорного органа, который его проинформировал, в целях гарантии эффективного исполнения решения в отношении контролера или обрабатывающего данные лица. Если главный надзорный орган решает рассматривать дело, проинформировавший его надзорный орган должен иметь возможность представить проект решения, который главный надзорный орган должен принять во внимание при подготовке своего проекта решения в рамках механизма сотрудничества и сопоставимости.

(128) Положения о главном надзорной органе и о механизме сотрудничества и сопоставимости не должны применяться, если обработка осуществляется органами государственной власти или частными организациями в области общественного интереса. В указанных случаях единственным надзорным органом, компетентным осуществлять полномочия, предоставленные ему в соответствии с настоящим Регламентом, должен являться надзорный орган государства-члена ЕС, в котором учрежден орган государственной власти или частная организация.

(129) Для того чтобы обеспечить согласованный мониторинг и исполнение настоящего Регламента в Союзе, надзорный орган в каждом государстве-члене ЕС должен иметь одинаковые задачи и осуществлять эффективные полномочия, в том числе следственные и корректирующие полномочия, полномочия санкций, разрешительные и консультативные полномочия, в частности, в случаях жалоб физических лиц, и без ущерба полномочиям органов уголовного преследования согласно законодательству государства-члена ЕС довести до сведения судебных органов факт нарушения настоящего Регламента и участвовать в судебном процессе. Указанные полномочия также должны включать в себя полномочие по установлению временного или окончательного ограничения на обработку, в том числе запрета. Государства-члены ЕС могут определить иные задачи, связанные с защитой персональных данных согласно настоящему Регламенту. Полномочия надзорных органов должны осуществляться беспристрастно, справедливо и в разумный срок в соответствии с процессуальными гарантиями, установленными в законодательстве Союза или государства-члена ЕС. В частности, каждая мера должна быть соответствующей, необходимой и пропорциональной с учетом гарантии соблюдения настоящего Регламента, принимая во внимание обстоятельства каждого отдельного дела, должна соблюдать право каждого лица быть выслушанным до принятия определенной меры, которая может отрицательно повлиять на него, и не должна допускать излишних расходов и чрезмерных затруднений для соответствующего лица. Следственные полномочия в отношении доступа к помещениям должны осуществляться в

соответствии со специальными требованиями в процессуальном законодательстве государства-члена ЕС, например, требованием о получении предварительного судебного разрешения. Каждая юридически обязательная мера надзорного органа должна быть оформлена в письменной форме, должна быть четкой и недвусмысленной, указывать надзорный орган, который принял меру, дату принятия меры, подпись главы или уполномоченного им члена надзорного органа, причины принятия меры и отсылку к праву на эффективное средство правовой защиты. Это не должно исключать дополнительных требований в соответствии с процессуальным законодательством государства-члена ЕС. Принятие юридически обязательного решения подразумевает, что оно может послужить основанием судебному пересмотру в государстве-члене ЕС надзорного органа, который принял решение.

(130) В случае если надзорный орган, в который была подана жалоба, не является главным надзорным органом, главный надзорный орган должен тесно сотрудничать с надзорным органом, в который была подана жалоба, в соответствии с положениями о сотрудничестве и сопоставимости, установленными в настоящем Регламенте. В указанных случаях главный надзорный орган при принятии мер, которые должны породить юридические последствия, включая наложение административных штрафов, должен учесть мнение надзорного органа, которому была подана жалоба и который должен оставаться компетентным при осуществлении расследования на территории его собственного государства-члена ЕС совместно с компетентным надзорным органом.

(131) В случае если другой надзорный орган должен выступать в качестве главного надзорного органа в отношении обработки контролера или обрабатывающего данные лица, но конкретный предмет жалобы или возможное нарушение касается только обработки контролера или обрабатывающего данные лица в государстве-члене ЕС, в котором жалоба была подана или было обнаружено возможное нарушение, и обстоятельство дела существенно не влияет или не должно влиять на субъекты данных в других государствах-членах ЕС, надзорный орган, в который подается жалоба или который установил или иным образом был проинформирован о ситуациях, которые влекут за собой возможные нарушения настоящего Регламента, должен прилагать усилия для мирного разрешения споров с контролером и, если это окажется безрезультатным, должен использовать все свои полномочия. Это должно включать в себя следующее: особую обработку на территории государства-члена ЕС надзорного органа или в отношении субъектов данных на территории указанного государства-члена ЕС; обработку в рамках предложения товаров или услуг, предназначенных для субъектов данных на территории государства-члена ЕС надзорного органа; или обработку, которая должна быть оценена с учетом соответствующих правовых обязательств согласно законодательству государства-члена ЕС.

(132) Мероприятия надзорного органа, направленные на повышение осведомленности населения, должны включать в себя специальные меры в отношении контролеров и обрабатывающих данные лиц, включая микропредприятия, малые и средние предприятия, а также физических лиц, в частности, в сфере образования.

(133) Надзорные органы должны поддерживать друг друга 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 определенного срока.

(135) В целях обеспечения согласованного применения настоящего Регламента на территории Союза необходимо установить механизм сопоставимости для сотрудничества между надзорными органами. Указанный механизм, в частности, должен применяться, если надзорный орган намерен принять меру для порождения юридических последствий в отношении процесса обработки, который

существенно влияет на определенное количество субъектов данных в нескольких государствах-членах ЕС. Он также должен применяться, если соответствующий надзорный орган или Европейская Комиссия запрашивают рассмотрение указанного вопроса в рамках механизма сопоставимости. Указанный механизм должен действовать без ущерба любым мерам, которые Европейская Комиссия может принять при осуществлении своих полномочий согласно Договорам.

(136) При применении механизма сопоставимости Совет в течение определенного промежутка времени должен дать заключение, если так решает большинство его членов или если так запросил любой соответствующий надзорный орган или Европейская Комиссия. Совет должен также обладать полномочием на принятие юридически обязательных решений, если существуют разногласия между надзорными органами. Для указанной цели в четко определенных случаях он большинством в две трети голосов своих членов должен принять юридически обязательные решения, если между надзорными органами, в частности, в рамках механизма сотрудничества между главным надзорным органом и соответствующими надзорными органами, имеются противоречия по существу дела, в частности, по вопросу о нарушении настоящего Регламента.

(137) Может существовать острая необходимость для защиты прав и свобод субъектов данных, в частности, если имеется риск того, что осуществление права субъекта данных может быть затруднено. Вследствие этого надзорный орган должен иметь возможность принять должным образом обоснованные временные меры на своей территории с определенным сроком действия, который не должен превышать трех месяцев.

(138) Применение указанного механизма в случаях, когда оно обязательно, должно являться условием законности меры надзорного органа, которая порождает юридические последствия. В других случаях трансграничной обоснованности должен применяться механизм сотрудничества между главным надзорным органом и соответствующими надзорными органами; соответствующие надзорные органы могут на двусторонней или многосторонней основе предоставлять взаимную помощь и осуществлять совместные действия без использования механизма сопоставимости.

(139) В целях содействия согласованному применению настоящего Регламента Совет должен быть учрежден в качестве независимого органа Союза. 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, учрежденную Директивой 95/46/ЕС. Он должен включать в себя главу надзорного органа каждого государства-члена ЕС и Европейского инспектора по защите персональных данных или их представителей. Европейская Комиссия должна принимать участие в деятельности Совета без права голоса, Европейский инспектор по защите данных должен обладать специальным правом голоса. Совет должен способствовать согласованному применению настоящего Регламента в Союзе, 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 Союзе. Совет должен действовать независимо при выполнении своих задач.

(140) Совету оказывает содействие секретариат, который обеспечивается Европейским инспектором по защите персональных данных. Персонал Европейского инспектора по защите персональных данных, который участвует в осуществлении задач, возложенных на Совет настоящим Регламентом, должен выполнять свои задачи только на основании указаний Президиума Совета, он также должен представлять ему отчеты.

(141) Каждый субъект данных обладает правом на подачу жалобы в один надзорный орган, в частности, в государстве-члене ЕС места своего проживания, и правом на эффективное средство судебной защиты в соответствии со Статьей 47 Хартии, если субъект данных считает, что его права согласно настоящему Регламенту нарушены, или если надзорный орган не принимает меры в отношении жалобы, полностью или частично отклоняет жалобу или отказывает в ее удовлетворении или не действует, если такая мера необходима для защиты прав субъекта данных. На основании жалобы следует провести расследование в соответствии с судебным пересмотром в той мере, в какой это необходимо в особом 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 случае если субъект данных считает, что его права согласно настоящему Регламенту нарушены, он вправе передать некоммерческому органу, организации или объединению, которые были основаны в соответствии с законодательством государства-члена ЕС, имеют уставные задачи в сфере общественного интереса, а также осуществляют деятельность в области защиты персональных данных, право подавать в надзорный орган жалобу от его имени, осуществлять права на судебную защиту от имени субъектов данных или в случаях, предусмотренных законодательством государства-члена ЕС, осуществлять право на получение компенсации от его имени субъектов данных. Государство-член ЕС может предусмотреть, что любой такой орган, организация или объединение, независимо от поручения субъекта данных, имеет право подавать в указанном государстве-члене ЕС жалобу и право на эффективное средство судебной защиты, если он считает, что права субъектов данных были нарушены в результате обработки данных, которая нарушает настоящий Регламент. Указанному 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 на возбуждение судебного процесса об аннулировании решений Совета согласно условиям, предусмотренным в Статье 263 TFEU. В качестве адресатов таких решений соответствующие надзорные органы, которые хотят их оспорить, должны предъявить иск в течение двух месяцев с момента получения уведомления об указанных решениях в соответствии со Статьей 263 TFEU. Если решения Совета касаются непосредственно и персонально контролера, обрабатывающего данные лица или заявителя, указанные лица могут возбудить судебный процесс об аннулировании указанных решений в течение двух месяцев после их опубликования на интернет-сайте Совета в соответствии со Статьей 263 TFEU. Без ущерба указанному праву согласно Статье 263 TFEU каждое физическое или юридическое лицо должно иметь право на эффективное средство защиты в компетентном национальном суде в отношении решения надзорного органа, которое порождает юридические последствия в отношении указанного лица. Указанное решение касается, в частности, осуществления следственных, корректирующих и разрешительных полномочий надзорного органа или отклонения жалобы или отказа в ее удовлетворении. Однако право на эффективное средство судебной защиты не включает в себя принятые надзорным органом меры, которые не являются юридически обязательными, например, его заключения или рекомендации. Судебное производство в отношении надзорного органа должно быть возбуждено в судах государства-члена ЕС, в котором учрежден надзорный орган, и должно осуществляться в соответствии с процессуальным законодательством указанного государства-члена ЕС. Указанные суды должны осуществлять юрисдикцию, которая должна включать в себя полномочия на изучение всех вопросов факта и права, относящихся к рассматриваемому ими спору.

Если надзорный орган отклоняет жалобу или отказывает в ее удовлетворении, заявитель может возбудить производство в судах того же самого государства-члена ЕС. В контексте судебной защиты прав в отношении применения настоящего Регламента национальные суды, которые считают, что для вынесения судебного решения им необходимо решение по указанному вопросу, могут или в случае, предусмотренном в Статье 267 TFEU, должны запросить Европейский суд о вынесении предварительного постановления о толковании законодательства Союза, в том числе настоящего Регламента. Также, если решение надзорного органа, имплементирующее решение Совета, оспаривается в национальном суде и действительность решения Совета является спорной, указанный национальный суд не обладает полномочием признавать решение Совета недействительным, но должен передать вопрос о действительности Европейскому суду в соответствии со Статьей 267 TFEU в толковании Европейского суда, если он считает решение

недействительным. Однако национальный суд может не передавать вопрос о действительности решения Совета по запросу физического или юридического лица, которое имело возможность возбудить производство об аннулировании указанного решения, в частности, если указанное решение напрямую и персонально касалось его, но не сделало этого в срок, указанный в Статье 263 TFEU.

(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 контролером или обрабатывающим данные лицом, или тех же оснований для иска, возбуждено в компетентном суде в другом государстве-члене ЕС, он должен связаться с указанным судом для того, чтобы подтвердить существование указанного соответствующего производства. Если соответствующее производство рассматривается в суде другого государства-члена ЕС, любой суд, рассматривающий дело позже, может приостановить производство по делу или по заявлению одной из сторон может отказаться от юрисдикции в пользу суда, который начал рассмотрение дела, если указанный суд уполномочен рассматривать указанные дела и его законодательство разрешает объединение соответствующих производств. Производства считаются смежными, если они настолько тесно взаимосвязаны, что целесообразно рассмотреть их вместе, для того чтобы избежать риска принятия противоречащих друг другу приговоров в результате отдельных производств.

(145) В случае производства в отношении контролера или обрабатывающего данные лица истец может возбудить дело в судах государств-членов ЕС, в которых находится учреждение контролера или обрабатывающего данные лица или в которых проживает субъект данных, за исключением случаев, когда контролер является органом государственной власти государства-члена ЕС, действующим при осуществлении своих официальных полномочий.

(146) Контролер или обрабатывающее данные лицо должно компенсировать любой ущерб, который лицо может понести в результате обработки, нарушающей настоящий Регламент. Контролер или обрабатывающее данные лицо освобождается от ответственности, если оно докажет, что оно никоим образом не несет ответственность за ущерб. Понятие ущерба должно широко толковаться в свете прецедентной практики суда таким образом, чтобы полностью соответствовать целям настоящего Регламента. Это положение действует без ущерба любым искам о возмещении ущерба в результате нарушения других норм законодательства Союза или государства-члена ЕС. Обработка, которая нарушает настоящий Регламент, также включает в себя обработку, которая нарушает делегированные акты и имплементационные акты, принятые в соответствии с настоящим Регламентом и с законодательством государства-члена ЕС для уточнения положений настоящего Регламента. Субъекты данных должны получить полную и эффективную компенсацию за понесенный ими ущерб. В случае если контролеры или обрабатывающие данные лица участвуют в одной и той же обработке данных, каждый контролер или обрабатывающее данные лицо должно нести ответственность за ущерб в целом. Однако если они в соответствии с законодательством государства-члена ЕС привлекаются к одному и тому же судебному процессу, компенсация может быть соразмерно распределена согласно ответственности каждого контролера или обрабатывающего данные лица за ущерб, причиненный обработкой, при условии гарантии полной и эффективной компенсации для понесшего ущерб субъекта данных. Любой контролер или обрабатывающее данные лицо, которое заплатило полную компенсацию, может впоследствии обратиться в суд с регрессным требованием относительно других контролеров или обрабатывающих данные лиц, участвовавших в одной и той же обработке.

(147) В случае если в настоящем Регламенте содержаться особые нормы о юрисдикции, в частности, относительно процедуры о судебной защите прав, в том числе о получении компенсации от контролера или обрабатывающего данные лица, общие нормы о юрисдикции, например положения Регламента (ЕС) 1215/2012 Европейского Парламента и Совета ЕС[14], должны действовать без ущерба применению указанных особых норм.

(148) В интересах последовательного осуществления положений 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 принять во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения причиненного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролера или обрабатывающего данные лица, соблюдение нормы поведения, а также любые другие 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 законодательства Союза и Хартии, включая эффективную судебную защиту и должную правовую процедуру.

(149) Государства-члены ЕС могут установить нормы об уголовном наказании за нарушение настоящего Регламента, включая нарушения национальных положений, принятых согласно и в рамках настоящего Регламента. Указанные уголовные наказания могут также предусматривать лишение преимуществ, полученных вследствие нарушения настоящего Регламента. Однако наложение уголовных наказаний за нарушения указанных национальных положений и наложение административных штрафов не должны вести к нарушению принципа ne bis in idem в толковании Суда.

(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 верхнее ограничение и критерии для установления соответствующих административных штрафов, которые должны определяться компетентным надзорным органом в каждом отдельном случае, принимая во внимание все соответствующие обстоятельства специфической ситуации, с учетом, в частности, характера, тяжести и продолжительности нарушения и его последствий, а также мер, принятых для обеспечения соблюдения обязанностей согласно настоящему Регламенту и для предотвращения или смягчения последствий нарушения. В случае если административные штрафы налагаются на предприятие, для указанных целей оно должно являться предприятием в значении Статей 101 и 102 TFEU. Если административные штрафы налагаются на физических лиц, в отношении которых речь не идет о предприятии, надзорный орган при определении соответствующего размера штрафа должен принять во внимание общий уровень дохода в государстве-члене ЕС, а также экономическую ситуацию физического лица. Для содействия согласованному применению административных штрафов также может использоваться механизм сопоставимости. Государства-члены ЕС могут определить, подлежат ли надзорные органы наложению административных штрафов и если да, то в какой мере. Наложение административного штрафа или выдача предупреждения не влияет на применение иных полномочий надзорных органов или других санкций в рамках настоящего Регламента.

(151) Правовая система Дании и Эстонии не допускает административные штрафы, предусмотренные в настоящем Регламенте. Нормы об административных штрафах могут применяться таким образом, что в Дании штраф налагается компетентными национальными судами в качестве уголовного наказания, в Эстонии штраф налагается надзорным органом в рамках процедуры административного правонарушения, при условии, что применение норм в указанных государствах-членах ЕС имеет воздействие, эквивалентное воздействию 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, пропорциональными и оказывать сдерживающее воздействие.

(152) В случае если настоящий Регламент не гармонизирует административные наказания или если это необходимо в других случаях, например, в случае серьезных нарушений настоящего Регламента, государства-члены ЕС должны имплементировать систему, которая предусматривает эффективные, пропорциональные и оказывающие сдерживающее воздействие санкции. Характер указанных санкций, уголовный или административный, должен определяться в соответствии с законодательством государства-члена ЕС.

(153) В законодательстве государств-членов ЕС должны быть согласованы нормы, регулирующие свободу выражения мнений и свободу информации, включая свободу журналистского, научного, художественного и/или литературного самовыражения, с правом на защиту персональных данных согласно настоящему Регламенту. Обработка персональных данных только в журналистских целях или в целях научного, художественного или литературного самовыражения подлежит применению частичного отступления или исключения из определенных положений настоящего Регламента, если это необходимо для того, чтобы согласовать право на защиту персональных данных со свободой выражения мнений и информации согласно Статье 11 Хартии. Это положение должно применяться, в частности, в отношении обработки персональных данных в аудиовизуальной области, а также в новостных и печатных архивах. Вследствие этого, государства-члены ЕС должны принять законодательные меры, регулирующие исключения и отступления, необходимые для целей гармоничного сочетания указанных основных прав. Государства-члены ЕС должны принять указанные отступления и исключения в отношении общих принципов, прав субъектов данных, контролера и обрабатывающего данные лица, передачи персональных данных третьим странам или международным организациям, независимых надзорных органов, сотрудничества и сопоставимости, и особых ситуаций обработки данных. Если указанные отступления или исключения отличаются от одного государства-члена ЕС к другому, должно применяться законодательство государства-члена ЕС, под действие которого подпадает контролер. Для того чтобы принять во внимание важность права на свободу выражения мнения в каждом демократическом обществе, необходимо разъяснить понятия, относящиеся к указанной свободе, например, понятие "журналистика".

(154) Настоящий Регламент учитывает 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 правительственных учреждений, должны быть опубликованы указанными органами или учреждениями, если раскрытие информации предусмотрено законодательством Союза или государства-члена ЕС, под действие которого подпадает орган государственной власти или правительственное учреждение. Указанное законодательство должно согласовывать доступ общественности к официальным документам и вторичное использование информации публичного сектора 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 указанном контексте все органы или другие учреждения, подпадающие под действие законодательства государства-члена ЕС о доступе общественности к документам. Директива 2003/98/ЕС Европейского Парламента и Совета ЕС[15] не затрагивает и никоим образом не влияет на уровень защиты физических лиц в отношении обработки персональных данных в рамках положений законодательства Союза или государства-члена ЕС, а также, в частности, не изменяет обязанности и права, установленные в настоящем Регламенте. В частности, указанная Директива не применяется в отношении документов, доступ к которым исключен 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, вторичное использование которых предусмотрено законодательством, несовместимым с законодательством относительно защиты персональных данных при обработке персональных данных.

(155) В законодательстве государства-члена ЕС или коллективных договорах, в том числе в "договорах о производстве работ", могут быть предусмотрены специальные положения об обработке персональных данных работников при выполнении должностных обязанностей, в частности, условия, согласно которым персональные данные могут обрабатываться на основе согласия работника, в целях приема 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 в целях архивирования в интересах общества, в целях научного или исторического исследования, а также в статистических целях должна подлежать применению соответствующих гарантий для прав и свобод субъекта данных согласно настоящему Регламенту. Указанные гарантии должны обеспечить наличие технических и организационных мер, для того чтобы, в частности, гарантировать принцип минимизации данных. Дальнейшая обработка персональных данных в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях должна осуществляться, если контролер оценил технические возможности для достижения указанных целей посредством обработки данных, при которой невозможно провести идентификацию субъектов данных, при условии, что имеются соответствующие гарантии (например, псевдонимизация данных). Государства-члены ЕС должны предусмотреть соответствующие гарантии для обработки персональных данных в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. Государства-члены ЕС вправе на специальных условиях и согласно соответствующим гарантиям для субъектов данных предусмотреть спецификации и частичные отступления относительно требований к информации, а также относительно прав на исправление, уничтожение, на забвение, ограничение обработки, на переносимость данных, на возражение, если персональные данные обрабатываются в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях. 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 соответствовать другим законодательным актам, например, о клинических испытаниях.

(157) Путем объединения информации из реестров исследователи могут получать новые сведения большой ценности в отношении распространенных медицинских состояний таких, как сердечно-сосудистые заболевания, рак и депрессивный синдром. Посредством использования реестров могут быть получены улучшенные результаты исследований, так как они основываются на большей части населения. В рамках общественных наук исследование на основе реестров дает исследователям возможность получить существенные знания о долговременном соотношении ряда социальных условий, например, безработицы и образования, с другими условиями жизни. Результаты исследований, полученные посредством реестров, обеспечивают твердые и достоверные знания, которые могут являться основанием для разработки и имплементации политических мер, основанных на знаниях, а также могут улучшить качество жизни ряда лиц и повысить эффективность общественных услуг. Для облегчения научных исследований персональные данные могут обрабатываться в целях научного исследования согласно соответствующим условиям и гарантиям, предусмотренным в законодательстве Союза или государства-члена ЕС.

(158) Настоящий Регламент также применяется в отношении обработки персональных данных в целях архивирования; необходимо учесть, что настоящий Регламент не применяется в отношении умерших лиц. Органы государственной власти, правительственные учреждения или

частные организации, которые ведут учет общественного интереса, согласно законодательству Союза или государства-члена ЕС должны быть юридически обязаны получать, сохранять, оценивать, классифицировать, описывать, сообщать, содействовать, распространять учетные сведения непреходящей ценности в интересах общества, а также предоставлять к ним доступ. Государства-члены ЕС также вправе предусмотреть дальнейшую обработку персональных данных в целях архивирования, например, в отношении представления специальной информации, относящейся к политическому поведению 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 целях настоящего Регламента обработка персональных данных для целей научного исследования должна трактоваться более широко, включая, например, развитие технологий и презентацию, фундаментальные исследования, прикладные исследования и исследования, финансируемые за счет частных средств. В дополнение к этому также необходимо принять во внимание цель Союза согласно Статье 179(1) TFEU о создании Европейского исследовательского пространства. Цели научного исследования также должны включать в себя исследования, проводимые в интересах общества в сфере общественного здравоохранения. Для того чтобы соответствовать особенностям обработки персональных данных в целях научных исследований, необходимо применять специальные условия, в частности, в отношении публикации или иного раскрытия персональных данных в контексте целей научного исследования. Если результат научного исследования, в частности, в сфере здравоохранения обосновывает принятие дальнейших мер в интересах субъекта данных, общие положения настоящего Регламента должны применяться в отношении указанных мер.

(160) Настоящий Регламент также применяется в отношении обработки персональных данных в целях исторического исследования. Сюда относится 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 ЕС[16].

(162) Настоящий Регламент применяется в отношении обработки персональных данных в статистических целях. Законодательство Союза или государства-члена ЕС в рамках настоящего Регламента должно определить статистическое содержание, 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" понимается любая деятельность по сбору и обработке персональных данных, необходимых для статистического изучения или для подготовки статистических результатов. Указанные статистические результаты могут быть в дальнейшем использованы в других 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 определенному физическому лицу.

(163) Конфиденциальная информация, которую национальные статистические органы и статистические органы Союза собирают для подготовки официальной европейской и официальной национальной статистики, должна находиться под защитой. Европейские статистические данные должны разрабатываться, подготавливаться и распространяться в соответствии со статистическими принципами, установленными в Статье 338(2) TFEU; при этом национальные статистические данные также должны соответствовать законодательству государства-члена ЕС. Регламент (ЕС) 223/2009 Европейского Парламента и Совета ЕС[17] предусматривает дополнительные спецификации относительно статистической конфиденциальности европейской статистики.

(164) В том, что касается полномочий надзорных органов в отношении получения от

контролера или обрабатывающего данные лица доступа к персональным данным и доступа к их помещениям, государства-члены ЕС могут на законодательном уровне, в рамках настоящего Регламента принять особые нормы для обеспечения обязанностей по соблюдению профессиональной или иной эквивалентной тайны, в той мере, в какой это необходимо для согласования права на защиту персональных данных с обязанностью соблюдать профессиональную тайну. Это положение действует без ущерба существующим обязанностям государства-члена по принятию норм относительно соблюдения профессиональной тайны, если этого требует законодательство Союза.

(165) В соответствии со Статьей 17 TFEU настоящий Регламент соблюдает и не ухудшает статус церквей и религиозных организаций или общин в государствах-членах ЕС, согласно существующему конституционному праву.

(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 обращения персональных данных в Союзе, полномочие по принятию актов в соответствии со Статьей 290 TFEU должно быть делегировано Европейской Комиссии. В частности, делегированные акты должны приниматься в отношении критериев и требований для сертификационных 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 составлении делегированных актов Европейская Комиссия должна гарантировать одновременную, своевременную и соответствующую передачу релевантных документов Европейскому Парламенту и Совету ЕС.

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

(168) Процедура проверки должна использоваться для принятия имплементационных актов относительно стандартных договорных условий между контролерами и обрабатывающими данные лицами, а также между обрабатывающими данные лицами; норм поведения; технических стандартов и механизмов для сертификации; соответствующего уровня защиты, предусмотренного третьей страной, территорией или определенным сектором в указанной третьей стране или международной организацией; стандартных условий защиты; формата и процедур для обмена электронной информацией между контролерами, обрабатывающими данные лицами и надзорными органами в отношении юридически обязывающих корпоративных правил; взаимной помощи; и соглашений об обмене электронной информацией между надзорными органами, а также между надзорными органами и Советом.

(169) Европейская Комиссия должна незамедлительно принять имплементационные акты в случае, если имеется доказательство относительно того, что третья страна, территория или определенный сектор в указанной третьей стране или международная организация не гарантирует соответствующий уровень защиты, и если это необходимо по причинам безотлагательной срочности.

(170) Так как цель настоящего Регламента, а именно обеспечение эквивалентного уровня защиты физических лиц и свободного обращения персональных данных на территории Союза, не может быть в достаточной степени достигнута государствами-членами ЕС, но может быть эффективнее достигнута на уровне Союза, в силу своего масштаба и воздействия, Союз может принять меры в соответствии с принципом субсидиарности, указанным в Статье 5 Договора о Европейском Союзе (TEU). В соответствии с принципом пропорциональности, указанным в данной Статье, настоящий Регламент не выходит за пределы того, что необходимо для достижения

указанной 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 контролер 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 персональных данных, и 7 марта 2012 г. он дал свое заключение[18].

(173) Настоящий Регламент должен применяться в отношении всех вопросов, связанных с защитой основных прав и свобод при обработке персональных данных, которые не подпадают под обязательства, установленные в Директиве 2002/58/ЕС Европейского Парламента и Совета ЕС[19] и преследующих одну и ту же цель, включая обязанности контролера 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:

Глава I
Общие положения

Статья 1
Предмет и цели

1. Настоящий Регламент устанавливает правила в отношении защиты физических лиц при обработке персональных данных и правила в отношении свободного обращения персональных данных.

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

3. Свободное обращение персональных данных в Союзе не должно быть ни ограничено, ни запрещено по причинам, связанным с защитой физических лиц при обработке персональных данных.

Статья 2
Фактическая сфера применения

1. Настоящий Регламент применяется в отношении обработки персональных данных полностью либо частично при помощи автоматизированных средств, а также в отношении обработки персональных данных иными способами, которые являются частью файловой системы или которые имеют целью стать частью файловой системы.

2. Настоящий Регламент не применяется в отношении обработки персональных данных:

(a) в процессе деятельности, которая не подпадает под действие законодательства Союза;

(b) государствами-членами ЕС при осуществлении деятельности, которая подпадает под

действие Главы 2 Раздела V TEU;

(c) физическим лицом в процессе осуществления исключительно личной или бытовой деятельности;

(d) компетентными органами в целях предупреждения, расследования, выявления уголовных преступлений, или привлечения к ответственности, или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности.

3. В том, что касается обработки персональных данных институтами, органами, учреждениями и агентствами Союза, применяется Регламент (ЕС) 45/2001. Регламент (ЕС) 45/2001 и другие законодательные акты Союза в области обработки персональных данных должны быть изменены в соответствии с принципами и правилами настоящего Регламента согласно Статье 98.

4. Настоящий Регламент действует без ущерба применению Директивы 2000/31/ЕС, в частности, нормы об ответственности поставщиков посреднических услуг в Статьях 12-15 указанной Директивы.

Статья 3
Территориальное действие

1. Настоящий Регламент применяется в отношении обработки персональных данных в контексте деятельности учреждения контролера или обрабатывающего данные лица в Союзе, вне зависимости от того, проводится обработка в Союзе или нет.

2. Настоящий Регламент применяется в отношении обработки персональных данных субъектов данных, находящихся в Союзе, контролером или обрабатывающим данные лицом, не учрежденными в Союзе, если обработка данных касается:

(a) предоставления товаров и услуг субъектам данных в Союзе вне зависимости от того, требуется ли оплата от указанного субъекта данных, или

(b) мониторинга их деятельности при условии, что деятельность осуществляется на территории Союза.

3. Настоящий Регламент применяется в отношении обработки персональных данных контролером, не учрежденным в Союзе, но учрежденным в месте, где законодательство государства-члена ЕС применяется в соответствии с международным публичным правом.

Статья 4
Определения

Для целей настоящего Регламента:

(1) под термином **"персональные данные"** понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу ("субъект данных"); идентифицируемое лицо - это лицо, которое может быть идентифицировано, прямо или косвенно, в частности, посредством таких идентификаторов как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн или через один или несколько признаков, характерных для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного физического лица;

(2) под термином **"обработка"** понимается любая операция или набор операций, осуществляемых с персональными данными, с применением автоматизированных средств или без таковых, например сбор, запись, организация, структурирование, хранение, модификация и изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространение или предоставление иным способом, упорядочение или комбинирование, ограничение, стирание или разрушение;

(3) под термином **"ограничение обработки"** понимается маркировка сохраненных персональных данных в целях ограничения их обработки в будущем;

(4) под термином **"формирование профиля"** понимается любая форма автоматизированной обработки персональных данных, состоящая из использования персональных данных в целях оценки определенных индивидуальных аспектов, касающихся физического лица, в частности, для анализа или определения аспектов, относящихся к производственным показателям указанного лица, экономической ситуации, здоровью, индивидуальным предпочтениям, интересам, надежности, поведению, месторасположению или передвижению;

(5) под термином **"псевдонимизация"** понимается обработка персональных данных таким образом, что персональные данные не могут быть больше отнесены к определенному субъекту данных без использования дополнительной информации, при условии, что дополнительная информация хранится отдельно и подлежит применению технических и организационных мер, гарантирующих, что персональные данные не отнесены к идентифицированному или идентифицируемому физическому лицу;

(6) под термином **"файловая система"** понимается любой структурированный набор персональных данных, доступных в соответствии с определенными критериями, вне зависимости от того используется ли при этом централизованный, децентрализованный, функциональный или географический принцип;

(7) под термином **"контролер"** понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; если цели и способы указанной обработки определены законодательством Союза или законодательством государства-члена ЕС, контролер или определенные критерии для его назначения могут быть предусмотрены законодательством Союза или государства-члена ЕС;

(8) под термином **"обрабатывающее данные лицо"** понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который обрабатывает персональные данные от имени контролера;

(9) под термином **"получатель"** понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, которому раскрываются персональные данные, вне зависимости от того, является ли он третьим лицом или нет. Однако органы государственной власти, которые могут получать персональные данные в рамках частного запроса в соответствии с законодательством Союза или государства-члена ЕС, не должны рассматриваться в качестве получателей; обработка данных указанными органами государственной власти должна соответствовать применимым нормам о защите данных согласно целям обработки;

(10) под термином **"третья сторона"** понимается физическое или юридическое лицо, органы государственной власти, агентство или орган, отличный от субъекта данных, контролера, обрабатывающего данные лица или лиц, которые уполномочены проводить обработку персональных данных под непосредственным руководством контролера или обрабатывающего данные лица;

(11) под термином **"согласие субъекта данных"** понимается любое свободно данное, конкретное, содержательное и определенное указание о своей воле, посредством которого субъект персональных данных оповещает о своем согласии на обработку относящихся к нему персональных данных;

(12) под термином **"утечка персональных данных"** понимается нарушение безопасности, ведущее к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к переданным, сохраненным или иным образом обработанным персональным данным;

(13) под термином **"генетические данные"** понимаются персональные данные, касающиеся унаследованных или приобретенных генетических характеристик физического лица, которые предоставляют уникальную информацию о физиологии или здоровье указанного физического лица

и которые являются результатом, в частности, анализа биологического образца соответствующего физического лица;

(14) под термином **"биометрические данные"** понимаются персональные данные, возникающие в результате особой технической обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица, например, изображение лица человека или дактилоскопические данные;

(15) под термином **"данные в отношении здоровья"** понимаются персональные данные, касающиеся физического или психического здоровья физического лица, в том числе предоставление медицинских услуг, которые раскрывают информацию о состоянии его/ее здоровья;

(16) под термином **"основное учреждение"** понимается:

(a) в отношении контролера с учреждениями в нескольких государствах-членах ЕС, месторасположение его центральной администрации в Союзе, кроме случаев, когда решения о целях и способах обработки персональных данных принимаются в другом учреждении контролера в Союзе, и последнее учреждение обладает правом на имплементацию указанных решений, в этом случае учреждение, принимающее такие решения, должно рассматриваться в качестве основного учреждения;

(b) в отношении лица, обрабатывающего данные, с учреждениями в нескольких государствах-членах ЕС, месторасположение его центральной администрации в Союзе, или, если лицо, обрабатывающее данные, не имеет центральной администрации в Союзе, учреждение указанного лица в Союзе, где производится основная обработка в контексте деятельности учреждения лица, обрабатывающего данные, в той степени, в какой указанное лицо ограничено специальными обязательствами в соответствии с настоящим Регламентом;

(17) под термином **"представитель"** понимается физическое или юридическое лицо, учрежденное в Союзе, которое в письменной форме назначается контролером или лицом, обрабатывающим данные, в соответствии со Статьей 27 и представляет контролера или лицо, обрабатывающее данные, с учетом их соответствующих обязательств согласно настоящему Регламенту;

(18) под термином **"компания"** понимается физическое или юридическое лицо, участвующее в экономической деятельности, вне зависимости от организационно-правовой формы, в том числе товарищества или объединения, регулярно участвующие в экономической деятельности;

(19) под термином **"группа предприятий"** понимается контролирующее предприятие и подконтрольные ему предприятия;

(20) под термином **"юридически обязывающие корпоративные правила"** понимаются меры по обеспечению защиты персональных данных, которые обязаны соблюдать контролер или обрабатывающее данные лицо, учрежденные на территории государства-члена ЕС, относительно передачи или совокупности передач персональных данных контролеру или обрабатывающему данные лицу в одной или нескольких третьих странах в рамках группы предприятий или группы компаний, участвующих в совместной экономической деятельности;

(21) под термином **"надзорный орган"** понимается независимый орган государственной власти, который учрежден государством-членом ЕС согласно Статье 51;

(22) под термином **"соответствующий надзорный орган"** понимается надзорный орган, который занимается обработкой персональных данных, так как:

(a) контролер или обрабатывающее данные лицо учреждено на территории государства-члена ЕС указанного надзорного органа;

(b) обработка данных в значительной степени оказывает воздействие или может оказывать воздействие на субъекты данных, находящихся в государстве-члене ЕС указанного надзорного органа; или

(c) в указанный надзорный орган подана жалоба;

(23) под термином **"трансграничная обработка"** понимается:

(a) обработка персональных данных, которая осуществляется в контексте деятельности учреждений в нескольких государствах-членах ЕС контролера или осуществляющего обработку лица в Союзе, если контролер или лицо, осуществляющее обработку, учреждены в нескольких государствах-членах ЕС;

(b) обработка персональных данных, которая осуществляется в контексте деятельности единичного учреждения контролера или лица, осуществляющего обработку, в союзе, но которая существенно влияет или может существенно влиять на субъекты данных в нескольких государствах-членах ЕС.

(24) под термином **"существенное и мотивированное возражение"** понимается возражение против проекта решения относительно того, имеется ли нарушение настоящего Регламента или соответствует ли намеченная деятельность контролера или обрабатывающего данные лица настоящему Регламенту, что четко демонстрирует важность рисков, возникших в результате проекта решения в отношении основных прав и свобод субъектов данных и при необходимости свободного потока персональных данных на территории Союза;

(25) под термином **"услуга информационного общества"** понимается услуга, в значении определения, указанного в пункте (b) Статьи 1(1) Директивы (ЕС) 2015/1535 Европейского Парламента и Совета ЕС[20];

(26) под термином **"международная организация"** понимается организация и ее подведомственные органы, регулируемые международным публичным правом, или любой другой орган, установленный соглашением между двумя или более странами или установленный на основе такого соглашения.

Глава II
Принципы

Статья 5
Принципы, связанные с обработкой персональных данных

1. Персональные данные должны:

(a) обрабатываться законно, беспристрастно и прозрачным образом в отношении субъекта данных ("законность, беспристрастность и прозрачность");

(b) собираться для определенных, явных и законных целей и в дальнейшем не должны обрабатываться несовместим с этими целями способом; дальнейшая обработка для достижения целей общественного интереса, а также целей научного или исторического исследования или статистических целей не должна в соответствии со Статьей 89(1) рассматриваться в качестве несовместимой с первоначальными целями ("целевое ограничение")"

(c) быть адекватными, соответствующими и должны ограничиваться тем, что необходимо относительно целей, для которых они обрабатываются ("минимизация данных");

(d) быть точными и, при необходимости, актуальными; необходимо принимать обоснованные меры для того, чтобы гарантировать своевременное удаление или исправление неточных данных с учетом целей, для которых они обрабатываются ("точность");

(e) храниться в форме, которая позволяет идентифицировать субъектов данных, в течение срока, необходимого для целей, относительно которых обрабатываются персональные данные; персональные данные могут храниться в течение более длительного срока, если они будут обрабатываться исключительно в целях общественного интереса, а также в целях научного или исторического исследования или в статистических целях в соответствии со Статьей 89(1), с учетом имплементации соответствующих технических и организационных мер, требуемых настоящим Регламентом для защиты прав и свобод субъекта данных ("ограничение по хранению");

(f) обрабатываться способом, гарантирующим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки и от случайной потери, разрушения или уничтожения данных, с использованием соответствующих технических и организационных мер ("целостность и конфиденциальность");

2. Контролер несет ответственность за соблюдение требований параграфа 1, он должен быть в состоянии продемонстрировать это ("ответственность").

Статья 6
Законность обработки

1. Обработка должна быть законной, только если и поскольку применяется одно из следующих условий:

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

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

(c) обработка необходима для соблюдения юридической обязанности, объектом которой является контролер;

(d) обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица;

(e) защита необходима для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером;

(f) обработка необходима для целей обеспечения законных интересов контролера или третьей стороны, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты персональных данных, в частности, если субъектом данных является ребенок.

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

2. Государства-члены ЕС могут сохранить или предусмотреть более конкретные положения для применения норм настоящего Регламента в отношении обработки для выполнения пунктов (c) и (e) параграфа 1 посредством определения более точных специальных требований для обработки и других мер для того, чтобы гарантировать законную и справедливую обработку, в том числе для иных особых ситуаций обработки, предусмотренных в Главе IX.

3. Основание для обработки, указанной в пункте (c) и (e) параграфа 1, должно устанавливаться:

(a) законодательством Союза; или

(b) законодательством государства-члена ЕС, под действие которого подпадает контролер.

Цель обработки должна определяться в рамках указанного юридического основания или, в том, что касается обработки, указанной в пункте (e) параграфа 1, должна быть необходимой для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером. Указанное юридическое основание может содержать конкретные положения для применения норм настоящего Регламента, inter alia: общие условия, регулирующие законность обработки контролером; типы данных, подлежащих обработке; соответствующие субъекты данных; субъекты, которым могут быть раскрыты данные, и цели, для которых персональные данных раскрываются; целевое ограничение; сроки хранения; и процедуры и процесс обработки данных, в том числе меры, гарантирующие законную и справедливую обработку, как например, для иных особых ситуаций обработки, предусмотренных в Главе IX. Законодательство Союза или государства-члена ЕС должно соответствовать цели государственных интересов и быть пропорциональным в отношении законной цели.

4. Если обработка для цели, отличной от цели, для которой были получены персональные данные, не основывается на согласии субъекта данных или на законодательстве Союза или государства-члена ЕС, которое представляет собой необходимую и пропорциональную меру в демократическом обществе для защиты целей, указанных в Статье 23(1), контролер в целях проверки того, соответствует ли обработка, проводимая для иных целей, цели, для которой первоначально собирались персональные данные, должен принять во внимание, inter alia:

(a) любую связь между целями, для которых были получены персональные данные, и целями предполагаемой последующей обработки;

(b) обстановку, в которой собирались персональные данные, в частности, отношения между субъектами данных и контролером;

(c) характер персональных данных, в частности, производится ли обработка особых категорий данных, согласно Статье 9, или производится ли обработка персональных данных, связанных с судимостями и преступлениями, согласно Статье 10;

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

(e) существование средств по обеспечению безопасности, которые могут включать в себя криптографическое закрытие или псевдонимизацию.

Статья 7
Условия для согласия

1. Если обработка основывается на согласии, контролер должен иметь возможность доказать, что субъект данных согласился на обработку своих персональных данных.

2. Если согласие субъекта данных дается в виде письменного заявления, которое также касается других обстоятельств, запрос о предоставлении согласия должен быть представлен в понятной и легкодоступной форме на ясном и доступном языке в том виде, который четко отличал бы его от других обстоятельств. Любая часть такого заявления, которая представляет собой нарушение настоящего Регламента, не является обязательной для исполнения.

3. Субъект данных должен иметь право в любое время отозвать свое согласие. Отзыв согласия не должен влиять на законность обработки, основанной на согласии до его отзыва. 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 проведении оценки относительно того, было ли согласие дано по доброй воле, основное внимание необходимо уделить тому, inter alia, зависит ли выполнение договора, включая предоставление услуги, от согласия на обработку персональных данных, которые не являются необходимыми для выполнения указанного договора.

Статья 8
Условия, применимые к согласию ребенка, в отношении услуг информационного общества

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

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

2. Контролер с учетом имеющихся технологических возможностей должен принять разумные

меры для того, чтобы в указанных случаях подтвердить, что согласие было дано лицом, обладающим родительской ответственностью в отношении ребенка, или было дано с его одобрения.

3. Параграф 1 не должен влиять на общее договорное право государств-членов ЕС, например, на нормы о действительности, вступлении в силу или правовых последствиях договора в отношении ребенка.

Статья 9
Обработка особых категорий персональных данных

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

2. Параграф 1 не применяется в случае, если:

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

(b) обработка необходима в целях исполнения обязательств и особых прав контролера или субъекта данных в сфере трудового законодательства, права социального обеспечения и социальной защиты постольку, поскольку это допускается законодательством Союза или государства-члена ЕС или коллективным договором согласно законодательству государства-члена ЕС, предусматривающему соответствующие средства защиты основных прав и интересов субъекта данных;

(c) обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица, если субъект данных физически или юридически неспособен дать свое согласие;

(d) обработка осуществляется фондом, объединением или 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 относится к персональным данным, которые субъект данных явно сделал общедоступными;

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

(g) обработка необходима по причинам особого общественного интереса на основании законодательства Союза или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных;

(h) обработка необходима в целях превентивной или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи или лечения или для управления системами и услугами здравоохранения и социального обеспечения на основании законодательства Союза или государства-члена ЕС или на основании договора с работником здравоохранения и в соответствии с условиями и гарантиями, указанными в параграфе 3.

(i) обработка необходима по причинам общественного интереса в области 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 законодательства Союза или государства-члена ЕС, которое предусматривает приемлемые и конкретные меры для защиты прав и свобод субъекта данных, в частности, профессиональной тайны;

(j) обработка необходима для целей архивизации информации в интересах государства, для научных, исторических или статистических целей в соответствии со Статьей 89(1), основанных на законодательстве Союза или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности 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, если указанные данные обрабатываются специалистом или под его ответственность и указанный специалист обязан соблюдать профессиональную тайну согласно законодательству Союза или государства-члена ЕС или согласно нормам, установленным национальными компетентными органами, или если обработка осуществляется иным лицом, которое обязано соблюдать конфиденциальность согласно законодательству Союза или государства-члена ЕС или согласно правилам, установленным национальными компетентными органами.

4. Государства-члены ЕС могут сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных о здоровье.

Статья 10
Обработка персональных данных, касающихся уголовных приговоров и преступлений

Обработка персональных данных, касающихся уголовных приговоров и преступлений или соответствующих мер по обеспечению безопасности на основании Статьи 6(1), должна осуществляться только под контролем официального органа или, если обработка разрешена законодательством Союза или государства-члена ЕС, которое предусматривает соответствующие гарантии правам и свободам субъектов данных. Полный реестр уголовных приговоров должен вестись только под контролем официального органа.

Статья 11
Обработка, не требующая идентификации соответствующего лица

1. Если цели, для которых контролер обрабатывает персональные данные, не требуют идентификации субъекта данных контролером, контролер не обязан сохранять, получать или обрабатывать дополнительную информацию для установления личности субъекта данных только лишь в целях соблюдения настоящего Регламента.

2. Если в случаях, указанных в параграфе 1 настоящей Статьи, контролер может подтвердить, что он не в состоянии установить личность субъекта данных, он должен проинформировать об этом субъекта данных, при наличии соответствующей возможности. В указанных случаях Статьи 15 - 20 не применяются, кроме случаев, когда субъект данных для осуществления своих прав согласно указанным Статьям, предоставляет дополнительную информацию, которая обеспечивает его/ее идентификацию.

Глава III
Права субъекта данных

Раздел 1
Прозрачность и условия

Статья 12
Прозрачная информация, связь и условия для осуществления прав субъектов данных

1. Контролер должен принять соответствующие меры для предоставления субъекту данных любой информации, указанной в Статьях 13 и 14, и любых сведений согласно Статьям 15-22 и Статьей 34, которые касаются обработки, в сжатой, прозрачной, понятной и легкодоступной форме на понятном и простом языке, в частности в отношении любой информации, адресованной ребенку. Информация должна предоставляться в письменной форме или при помощи иных средств, в том числе, при необходимости, при помощи электронных средств связи. По просьбе субъекта данных информация может быть предоставлена в устной форме, при условии, что личность субъекта данных установлена иным способом.

2. Контролер должен содействовать осуществлению прав субъекта данных согласно Статьям 15 - 22. В случаях, указанных в Статье 11(2), контролер может отказаться действовать по запросу субъекта данных в целях осуществления его/ее прав согласно Статьям 15 - 22 только тогда, когда он подтверждает, что он не в состоянии установить личность субъекта данных.

3. Контролер должен незамедлительно предоставить субъекту данных информацию о мерах, принятых в рамках запроса согласно Статьям 15 - 22, и в любом случае в течение одного месяца после получения запроса. Указанный срок может быть продлен еще на два месяца, при необходимости, с учетом сложности и количества запросов. Контролер должен проинформировать субъекта данных о любом таком продлении в течение одного месяца после получения запроса, с указанием причин превышения срока. Если субъект данных подает запрос посредством электронной формы, информация должна быть предоставлена по возможности электронным способом, если субъект данных не запрашивает иной способ передачи информации.

4. Если контролер не принимает меры по запросу субъекта данных, он должен незамедлительно или не позднее одного месяца после получения запроса проинформировать субъекта данных о причинах непринятия мер, а также о возможности подачи жалобы надзорному органу и о возможности судебной защиты прав.

5. Информация согласно Статьям 13 и 14, а также любые сведения и принятые меры согласно Статьям 15 - 22 и Статье 34 должны предоставляться бесплатно. Если запросы субъекта данных являются явно необоснованными или носят чрезмерный характер в частности вследствие многочисленных повторов, контролер может:

(a) взимать приемлемую плату с учетом административных расходов на предоставление информации или сведений или принятие запрашиваемых мер; или

(b) отказаться действовать в соответствии с запросом.

Контролер должен нести бремя доказывания явной необоснованности запроса или его чрезмерного характера.

6. Без ущерба действию Статьи 11, если контролер имеет достаточные основания для сомнения относительно идентификации личности физического лица, подающего запрос согласно Статьям 15 - 21, он может затребовать предоставление дополнительной информации, необходимой для подтверждения личности субъекта данных.

7. Информация, которая должна быть предоставлена субъектам данных согласно Статьям 13 и 14, может предоставляться в сочетании со стандартизированными графическими обозначениями для того, чтобы в отчетливо видимой, понятной и разборчивой форме дать общее представление о предполагаемой обработке. Если графические изображения представлены в электронной форме, они должны быть пригодными для машинного считывания.

8. Европейская Комиссия должна иметь возможность принимать делегированные акты в

соответствии со Статьей 92 в целях определения информации, которая должны быть представлена посредством графических обозначений, и определения процедур для предоставления стандартизированных графических обозначений.

Раздел 2
Информация и доступ к персональным данным

Статья 13
Информация, которая должна предоставляться в случае получения персональных данных от субъекта данных

1. Если относящиеся к субъекту данных персональные данные предоставляются субъектом данных, контролер в момент получения персональных данных должен предоставить субъекту данных следующую информацию:

(a) идентификационную информацию и контактные данные контролера и, при необходимости, его представителя;

(b) контактные данные инспектора по защите персональных данных, в соответствующих случаях;

(c) цели обработки, для которых предназначаются персональные данные, а также юридическое основание для обработки;

(d) в случае если обработка основывается на пункте (f) Статьи 6(1), законные интересы, преследуемые контролером или третьей стороной;

(e) получатели или категории получателей персональных данных, при наличии;

(f) в соответствующих случаях, намерение контролера передать персональные данные третьей стране или международной организации, а также наличие или отсутствие решения Европейской Комиссии о соразмерности, или в случае передачи согласно Статье 46 или 47 или согласно второму подпараграфу Статьи 49(1) - ссылка на соответствующие и надлежащие гарантии и способы, посредством которых может быть получена их копия, или где они могут быть предоставлены.

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

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

(b) существование права требования от контролера доступа к соответствующим персональным данным и их исправления или удаления или ограничения обработки или возражение против обработки, а также права на переносимость данных;

(c) в случае если обработка основывается на пункте (a) Статьи 6(1) или на пункте (a) Статьи 9(2), существование права на отзыв своего согласия, без воздействия на законность обработки, основанной на согласии до его отзыва;

(d) право подачи жалобы в надзорный орган;

(e) является ли предоставление персональных данных требованием, предусмотренным законодательством или договором, или требованием, которое необходимо для заключения договора, а также обязан ли субъект данных предоставлять персональные данные и возможные последствия непредставления указанных данных;

(f) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно Статье 22(1) и (4) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях

обработки для субъекта данных.

3. Если контролер собирается в дальнейшем обрабатывать персональные данные в целях, отличных от целей, для которых персональные данные были получения, до начала указанной обработки он должен предоставить субъекту данных информацию относительно иной цели, а также любую дополнительную информацию, указанную в параграфе 2.

4. Параграфы 1, 2 и 3 не должны применяться, поскольку и если субъект данных уже располагает соответствующей информацией.

Статья 14
Информация, которая должна предоставляться при получении персональных данных не от субъекта данных

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

(a) идентификационную информацию и контактные данные контролера и, при необходимости, его представителя;

(b) контактные данные инспектора по защите персональных данных, в соответствующих случаях;

(c) цели обработки, для которых предназначаются персональные данные, а также юридическое основание для обработки;

(d) категории соответствующих персональных данных;

(e) получатели или категории получателей персональных данных, при наличии;

(f) в соответствующих случаях, намерение контролера передать персональные данные получателю в третьей стране или международной организации, а также наличие или отсутствие решения Европейской Комиссии о соразмерности, или в случае передачи согласно Статье 46 или 47 или согласно второму подпараграфу Статьи 49(1) - ссылка на соответствующие и надлежащие гарантии и способы получения их копии или того, где они могут быть предоставлены.

2. В дополнение к информации, указанной в параграфе 1, контролер 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 для определения указанного срока;

(b) в случае если обработка основывается на пункте (f) Статьи 6(1), законные интересы, преследуемые контролером или третьей стороной;

(c) существование права требования от контролера доступа к соответствующим персональным данным и их исправления или удаления или ограничения обработки или возражение против обработки, а также права на переносимость данных;

(d) в случае если обработка основывается на пункте (a) Статьи 6(1) или на пункте (a) Статьи 9(2), существование права на отзыв своего согласия, без воздействия на законность обработки, основанной на согласии до его отзыва;

(e) право подачи жалобы в надзорный орган;

(f) из каких источников происходят персональные данные и, при необходимости, взяты ли они из общедоступных источников;

(g) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно Статье 22(1) и (4) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях указанной обработки для субъекта данных.

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

(a) в приемлемый срок после получения персональных данных, но как минимум в течение

одного месяца, с учетом особых условий обработки персональных данных;

(b) если персональные данные должны использоваться для общения с субъектом данных, как минимум во время первого обращения к указанному субъекту данных; или

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

4. Если контролер намерен в дальнейшем обрабатывать персональные данные в целях, отличных от целей, для которых они были получены, перед последующей обработкой он должен предоставить субъекту данных информацию об указанных иных целях, а также любую существенную дополнительную информацию, указанную в параграфе 2.

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

(a) субъект данных уже располагает информацией;

(b) предоставление указанной информации оказывается невозможным или требует непропорционального усилия, в частности, для обработки в целях архивирования в интересах общества, в целях научных или исторических исследований или в статистических целях, с учетом условий и гарантий, указанных в Статье 89(1), или постольку, поскольку обязанность, указанная в параграфе 1 настоящей Статьи, может сделать невозможным или негативно отразиться на достижении целей указанной обработки. В указанных случаях контролер должен принять соответствующие меры для защиты прав, свобод и законных интересов субъекта данных, включая доведение информации до всеобщего сведения;

(c) получение или раскрытие информации прямо установлено законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер и которое обеспечивает соответствующие меры для защиты законных интересов субъекта данных; или

(d) если персональные данные не должны разглашаться в соответствии с обязательством о соблюдении профессиональной тайны согласно законодательству Союза или государства-члена ЕС, включая установленные законодательством обязательства о сохранении профессиональной тайны.

Статья 15
Право субъекта данных на доступ к данным

1. Субъект данных имеет право запрашивать у контролера подтверждение относительно того, обрабатываются ли относящиеся к нему персональные данные, и если дело обстоит именно так, он имеет право на доступ к персональным данным и следующей информации:

(a) цели обработки;

(b) категории обрабатываемых персональных данных;

(c) получатели или категории получателей, которым были или будут раскрыты персональные данные, в частности, получатели в третьих странах или международные организации;

(d) по мере возможности, предусмотренный срок, в течение которого будут храниться персональные данные, или, при отсутствии соответствующей возможности, критерии, используемые для определения указанного периода;

(e) существование права требования от контролера исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки;

(f) право подачи жалобы в надзорный орган;

(g) в случае если персональные данные получены не от субъекта данных, любая доступная информация об их источнике;

(h) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно Статье 22(1) и (4) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях указанной обработки для субъекта данных.

2. В случае если персональные данные передаются третьей стране или международной организации, субъект данных вправе получить информацию о соответствующих гарантиях согласно Статье 46 относительно передачи данных.

3. Контролер должен обеспечить наличие копии обрабатываемых персональных данных. За любые иные копии, запрашиваемые субъектом данных, контролер может взимать приемлемую плату на основании административных расходов. Если субъект данных подает запрос электронным способом, информация должна предоставляться в принятой электронной форме, если субъект данных не запрашивает иное.

4. Право на получение копии, указанной в параграфе 3, не должно отрицательно влиять на права и свободы других лиц.

Раздел 3
Внесение исправлений и удаление информации

Статья 16
Право на внесение исправлений

Субъект данных вправе потребовать от контролера незамедлительного изменения относящихся к нему неточных персональных данных. Принимая во внимание цели обработки, субъект данных имеет право на внесение дополнений в персональные данные, в том числе посредством предоставления дополнительного заявления.

Статья 17
Право на удаление ("право на забвение")

1. Субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные, если применяется одно из следующих оснований:

(a) персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях;

(b) субъект данных отзывает свое согласие, на основании которого согласно пункту (a) Статьи 6(1) или пункту (a) Статьи 9(2) проводилась обработка, и если отсутствует иное юридическое основание для обработки;

(c) субъект данных возражает против обработки согласно Статье 21(1), и отсутствуют имеющую преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки согласно Статье 21(2);

(d) персональные данные обрабатывались незаконно;

(e) персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер;

(f) персональные данные собирались в отношении предоставления услуг информационного общества согласно Статье 8(1).

2. Если контролер обнародовал персональные данные и он согласно параграфу 1 обязан удалить персональные данные, он с учетом имеющихся технологических возможностей и расходов на имплементацию должен принять необходимые меры, в том числе технические меры, чтобы проинформировать контролеров, которые обрабатывают персональные данные, о том, что субъект данных затребовал от них удаление любых ссылок, копий или точных повторений указанных персональных данных.

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

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

(b) в целях соблюдения юридической обязанности, которая требует проведение обработки согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер, или для выполнения задачи, осуществляемой в интересах общества, или при осуществлении официальных полномочий, возложенных на контролера;

(c) по причинам государственного интереса в области общественного здравоохранения в соответствии с пунктами (h) и (i) Статьи 9(2), а также Статьи 9(3);

(d) в целях архивирования в интересах общества, в целях научных или исторических исследований или в статистических целях, указанных в Статье 89(1), постольку, поскольку право, указанное в параграфе 1, может сделать невозможным или негативно отразиться на достижении целей указанной обработки; или

(e) для обоснования, исполнения или ведения защиты по судебным искам.

Статья 18
Право на ограничение обработки

1. Субъект данных вправе потребовать от контролера ограничить обработку, если применяется одно из следующих условий:

(a) точность персональных данных оспаривается субъектом данных, в течение срока, необходимого контролеру для подтверждения точности персональных данных;

(b) обработка является незаконной, и субъект данных возражает против удаления персональных данных, вместо этого он требует ограничить их использование;

(c) контролеру больше не требуются персональные данные для целей обработки, но они требуются субъекту данных для обоснования, исполнения или ведения защиты по судебным искам;

(d) субъект данных возражал против обработки согласно Статье 21(1) до установления факта относительно того, превалируют ли законные основания контролера над законными основаниями субъекта данных.

2. Если обработка была ограничена согласно параграфу 1, указанные персональные данные, за исключением хранения, должны обрабатываться только с согласия субъекта данных, или для обоснования, исполнения или ведения защиты по судебным искам, или для защиты прав другого физического или юридического лица, или по причинам важного общественного интереса Союза или государства-члена ЕС.

3. Субъект данных, который добился ограничения обработки согласно параграфу 1, должен быть проинформирован контролером прежде, чем ограничение будет снято.

Статья 19
Обязанность уведомления относительно изменения или уничтожения персональных данных или ограничения обработки

Контролер должен сообщить о любом изменении или уничтожении персональных данных или ограничении обработки, осуществляемой 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 требует несоразмерного усилия. Контролер должен проинформировать субъекта данных об указанных получателях, если субъект данных этого требует.

Статья 20
Право на переносимость данных

1. Субъект данных имеет право получить относящиеся к нему персональные данные, которые он предоставил контролеру, в структурированном, универсальном и машиночитаемом формате; он имеет право передать указанные данные другому контролеру беспрепятственно со стороны контролера, которому были предоставлены персональные данные, если:

(a) обработка основывается на согласии в соответствии с пунктом (a) Статьи 6(1), или пунктом (a) Статьи 9(2), или пунктом (b) Статьи 6(1); и

(b) обработка осуществляется при помощи автоматизированных средств.

2. При осуществлении своего права на переносимость данных согласно параграфу 1 субъект данных должен иметь право на передачу персональных данных непосредственно от одного контролера другому, если это технически осуществимо.

3. Осуществление права, указанного в параграфе 1 настоящей Статьи, должно действовать без ущерба Статье 17. Указанное право не должно применяться для обработки, необходимой для выполнения задачи, осуществляемой в рамках общественного интереса или при исполнении официальных полномочий, возложенных на контролера.

4. Право, указанное в параграфе 1, не должно отрицательно влиять на права и свободы других лиц.

Раздел 4
Право на возражение и автоматизированный процесс принятия решения в конкретном случае

Статья 21
Право на возражение

1. Субъект данных на основаниях, вытекающих из его конкретной ситуации, имеет право на возражение против обработки относящихся к нему персональных данных на основе пункта (e) или (f) Статьи 6(1), включая формирование профиля, основанного на указанных положениях. Контролер не должен больше обрабатывать персональные данные, кроме случаев, когда он может подтвердить наличие веских законных оснований для обработки, которые превалируют над интересами, правами и свободами субъекта данных, или обработка необходима для обоснования, исполнения или ведения защиты по судебным искам.

2. Если персональные данные обрабатываются для целей прямого маркетинга, субъект данных должен иметь право на возражение против обработки относящихся к нему персональных данных для целей указанного маркетинга, включая формирование профиля в той мере, в какой это связано с прямым маркетингом.

3. В случае если субъект данных возражает против обработки в целях прямого маркетинга, персональные данные больше не должны обрабатываться для указанных целей.

4. Как минимум при первом общении с субъектом данных до его сведения необходимо довести информацию о наличии права, указанного в параграфах 1 и 2, указанная информация должна быть представлена четко и отдельно от любой другой информации.

5. В связи с использованием услуг информационного общества и безотносительно Директивы 2002/58/ЕС субъект данных может осуществлять свое право на возражение при помощи автоматизированных средств с использованием технических спецификаций.

6. В случае если персональные данные обрабатываются в целях научного или исторического исследования согласно Статье 89(1), субъект данных на основании связанной с ним конкретной ситуации должен иметь право на возражение против обработки относящихся к нему персональных данных, за исключением случаев, когда обработка необходима для выполнения задачи, осуществляемой по причинам общественного интереса.

Статья 22
Автоматизированный процесс принятия решения в конкретном случае, в том числе формирование профиля

1. Субъект данных должен иметь право не подпадать под действие решения, основанного исключительно на автоматической обработке, включая формирование профиля, которое порождает юридические последствия в отношении него или нее или существенно воздействует на него или на нее.

2. Параграф 1 не должен применяться, если решение:

(a) необходимо для заключения или исполнения договора между субъектом данных и контролером данных;

(b) допускается законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер и которое также устанавливает приемлемые меры защиты прав, свобод и законных интересов субъекта данных; или

(c) основывается на прямом согласии субъекта данных.

3. В случаях, указанных в пунктах (a) и (c) параграфа 2, контролер данных должен имплементировать приемлемые меры защиты прав, свобод и законных интересов субъекта данных, как минимум права требования принятия решительных мер со стороны контролера, права на выражение своей точки зрения и на оспаривание решения.

4. Решения, указанные в параграфе 2, не должны основываться на особых категориях персональных данных, указанных в Статье 9(1), кроме случаев, когда применяется пункт (a) или (g) Статьи 9(2) и имеются приемлемые меры защиты прав, свобод и законных интересов субъекта данных.

Раздел 5
Ограничения

Статья 23
Ограничения

1. Законодательство Союза или государства-члена ЕС, под действие которого подпадает контролер или лицо, обрабатывающее данные, может посредством законодательных мер ограничить объем и содержание обязательств и прав, предусмотренных в Статьях 12 - 22 и в Статье 34, а также в Статье 5 постольку, поскольку его положения соответствуют правам и обязанностям, предусмотренным в Статьях 12 - 22, если указанное ограничение соответствует сущности основных прав и свобод и является необходимой и пропорциональной мерой в демократическом обществе для обеспечения:

(a) национальной безопасности;

(b) обороны;

(c) общественной безопасности;

(d) предотвращения, расследования, раскрытия и обвинения по уголовным преступлениям или исполнения уголовных наказаний, включая защиту и предупреждение угроз общественной безопасности;

(e) иных важных целей общественного интереса Союза или государства-члена ЕС, в частности важных экономических или финансовых интересов Союза или государства-члена ЕС, включая денежные, бюджетные и налоговые вопросы, общественное здравоохранение и общественную безопасность;

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

(g) предотвращения, расследования, раскрытия и уголовного преследования в отношении нарушения этики для регулируемых профессий;

(h) функции мониторинга, инспекционной и регулятивной функции, связанной, даже случайно, с осуществлением официальных полномочий в случаях, указанных в пунктах (a) - (e) и (g);

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

(j) исполнения решения по гражданско-правовым искам.

2. В частности, любые законодательные меры, указанные в параграфе 1, должны содержать особые положения в отношении как минимум:

(a) целей обработки или категорий обработки;

(b) категорий персональных данных;

(c) объема и содержания введенных ограничений;

(d) гарантий против неправомерного использования, или несанкционированного доступа, или несанкционированной передачи;

(e) спецификации контролера или категорий контролеров;

(f) сроков хранения и существующих гарантий с учетом характера, объема и целей обработки или категорий обработки;

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

(h) права субъекта данных получить информацию об ограничении, кроме случаев, когда это может нанести ущерб цели ограничения.

Глава IV
Контролер и лицо, обрабатывающее данные

Раздел 1
Общие обязательства

Статья 24
Ответственность контролера

1. Принимая во внимание характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и опасности для прав и свобод физических лиц, контролер должен имплементировать соответствующие технические и организационные меры, гарантирующие и подтверждающие, что обработка осуществляется в соответствии с настоящим Регламентом. Указанные меры должны своевременно пересматриваться и уточняться, при необходимости.

2. Если это соизмеримо с обработкой данных, меры, указанные в параграфе 1, должны включать в себя имплементацию соответствующих мер по обеспечению защиты данных контролером.

3. Следование утвержденным нормам поведения согласно Статье 40 или утвержденным сертификационным механизмам согласно Статье 42 может быть использовано в качестве элемента для подтверждения соблюдения обязанностей контролера.

Статья 25
Защита данных по умолчанию и на основе продуманных действий

1. Принимая во внимание состояние развития науки и техники, расходы на имплементацию, характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и

опасности для прав и свобод физических лиц в результате обработки, контролер должен как во время определения средств обработки, так и во время самой обработки имплементировать соответствующие технические и организационные меры, например, псевдонимизацию, которые предназначены для эффективной имплементации принципов защиты данных, например, минимизации данных, и для интегрирования необходимых гарантий в обработку в целях выполнения требований настоящего Регламента и защиты прав субъектов данных.

2. Контролер должен имплементировать соответствующие технические и организационные меры для обеспечения того, что по умолчанию обрабатываются только те персональные данные, которые необходимы для каждой конкретной цели обработки. Указанная обязанность применяется в отношении большого количества собранных персональных данных, объема их обработки, срока их хранения и возможности доступа к ним. В частности, указанные меры должны гарантировать, что по умолчанию доступ к персональным данным не будет предоставлен неопределенному количеству физических лиц без участия отдельного лица.

3. Утвержденный сертификационный механизм согласно Статье 42 может использоваться в качестве элемента для подтверждения соблюдения требований, установленных в параграфах 1 и 2 настоящей Статьи.

Статья 26
Контролеры, осуществляющие совместную обработку

1. В случае если два или более контролера совместно определяют цели и средства обработки, они должны считаться контролерами, осуществляющими совместную обработку. Они должны посредством соглашения и с соблюдением принципов прозрачности определить соответствующие обязанности для соблюдения обязательств согласно настоящему Регламенту, в частности, в отношении осуществления прав субъекта данных, а также определить соответствующие обязанности по предоставлению информации согласно Статьям 13 и 14, за исключением случаев, когда и поскольку соответствующие обязанности контролера определены законодательством Союза или государства-члена ЕС, под действие которого подпадают контролеры. В соглашении может быть указан контрольный пункт связи для субъектов данных.

2. Соглашение, указанное в параграфе 1, должно отражать соответствующие функции и отношения осуществляющих совместную обработку контролеров относительно субъектов данных. Существование соглашения должно быть доведено до сведения субъекта данных.

3. Независимо от условий соглашения, указанного в параграфе 1, субъект данных может осуществлять свои права в рамках настоящего Регламента в отношении каждого из контролеров и в противовес каждому из них.

Статья 27
Представители контролеров или обрабатывающих данные лиц, не учрежденных в Союзе

1. В случае если применяется Статья 3(2), контролер или лицо, обрабатывающее данные, должны в письменной форме назначить представителя в Союзе.

2. Обязанность, установленная в параграфе 1 настоящей Статьи, не применяется в отношении:

(a) обработки, которая носит случайный характер, не включает в себя масштабную обработку особых категорий данных в значении Статьи 9(1) или масштабную обработку персональных данных, связанных с судимостями и уголовными преступлениями в значении Статьи 10, и которая, с учетом характера, особенностей, объема и целей обработки, предположительно не приведет к риску для прав и свобод физических лиц; или

(b) органа государственной власти или правительственного учреждения.

3. Представитель должен быть учрежден в одном из государств-членов ЕС, в котором находятся субъекты данных, персональные данные которых обрабатываются в отношении предлагаемых им товаров и услуг или поведенческая активность которых находится под наблюдением.

4. Контролер или обрабатывающее данные лицо должны уполномочить представителя решать совместно с ними или вместо них все связанные с обработкой вопросы в целях обеспечения соблюдения настоящего Регламента, особенно для надзорных органов и субъектов данных.

5. Назначение представителя контролером или обрабатывающим данные лицом должно действовать без ущерба правовым мерам в отношении самого контролера или лица, обрабатывающего данные.

Статья 28
Лицо, обрабатывающее данные

1. В случае если обработка осуществляется от имени контролера, он должен работать только с теми обрабатывающими данные лицами, которые предоставят надлежащие гарантии того, что соответствующие технические и организационные меры будут проведены таким образом, что обработка будет соответствовать требованиям настоящего Регламента и гарантирует защиту прав субъекта данных.

2. Лицо, обрабатывающее данные, не должно привлекать к работе другое лицо, обрабатывающее данные, без предварительного особого или общего письменного разрешения контролера. В случае общего письменного разрешения лицо, обрабатывающее данные, должно проинформировать контролера о любых запланированных изменениях, касающихся привлечения или замены других лиц, обрабатывающих данные, тем самым давая контролеру возможность высказать возражение против таких изменений.

3. Обработка, осуществляемая лицом, обрабатывающим данные, должна регулироваться договором или иным юридическим актом в рамках законодательства Союза или государства-члена ЕС, который имеет обязательную силу для обрабатывающего данные лица относительно контролера и в котором указываются предмет и продолжительность обработки, характер и цель обработки, тип персональных данных и категории субъектов данных и обязанности и права контролера. Указанный договор или иной юридический акт должны в частности предусматривать, что обрабатывающее данные лицо:

(a) обрабатывает персональные данные только на основании документально подтвержденных указаний контролера, также в отношении передачи персональных данных третьей стране или международной организации, кроме случаев, когда этого требует законодательство Союза или государства-члена ЕС, под действие которого подпадает лицо, обрабатывающее данные; в таком случае лицо, обрабатывающее данные, должно проинформировать контролера об указанном законном требовании до начала обработки, за исключением случаев, когда указанное законодательство запрещает передачу указанной информации исходя из соображений общественного интереса;

(b) гарантирует, что лица, уполномоченные на обработку персональных данных, обязались соблюдать конфиденциальность или по законодательству обязаны соблюдать конфиденциальность;

(c) принимает все меры, необходимые согласно Статье 32;

(d) соблюдает условия, указанные в параграфах 2 и 4, для привлечения к работе иного лица, обрабатывающего данные;

(e) с учетом характера обработки, по мере возможности посредством соответствующих технических и организационных мер содействует контролеру в выполнении его обязанности реагировать на требования по осуществлению прав субъекта данных, установленных в Главе III;

(f) содействует контролеру при соблюдении обязанностей согласно Статьям 32 - 36, с учетом характер обработки и информации, доступной лицу, обрабатывающему данные;

(g) по выбору контролера удаляет или возвращает все персональные данные контролеру после предоставления услуг, связанных с обработкой, и удаляет существующие копии, кроме случаев, когда законодательством Союза или государства-члена ЕС требуется хранение персональных данных;

(h) предоставляет в распоряжение контролера всю информацию, необходимую для подтверждения соблюдения обязанностей, установленных в настоящей Статье, а также предусматривает возможность и содействует аудиторским проверкам, включая инспекционные проверки, проводимые контролером или аудитором, уполномоченным контролером.

С учетом пункта (h) первого подпараграфа, обрабатывающее данные лицо должно незамедлительно проинформировать контролера, если, по его мнению, указание нарушает настоящий Регламент или другие положения Союза или государства-члена ЕС по защите данных.

4. Если лицо, обрабатывающее данные, привлекает к работе другое лицо для выполнения определенной обработки данных от имени контролера, те же самые обязанности по защите данных, указанные в договоре или другом юридическом акте между контролером и лицом, обрабатывающем данные, согласно параграфу 3, должны возлагаться на указанное иное лицо, обрабатывающее данные, посредством договора или иного юридического акта в рамках законодательства Союза или государства-члена ЕС, при этом должны быть предоставлены достаточные гарантии для имплементации соответствующих технических и организационных мер с тем, чтобы обработка соответствовала требованиям настоящего Регламента. Если указанное другое лицо, обрабатывающее данные, не выполняет обязательства по защите данных, первое лицо, обрабатывающее данные, несет ответственность перед контролером за выполнение обязанностей указанного другого лица, обрабатывающего данные.

5. Следование лицом, обрабатывающим данные, утвержденным нормам поведения согласно Статье 40 или утвержденным сертификационным механизмам согласно Статье 42 может быть использовано в качестве элемента для подтверждения достаточных гарантий, указанных в параграфах 1 - 4 настоящей Статьи.

6. Без ущерба действию индивидуального договора между контролером и лицом, обрабатывающим данные, договор или другой юридический акт, указанный в параграфах 3 и 4 настоящей Статьи, может полностью или частично основываться на стандартных договорных условиях, указанных в параграфах 7 и 8 настоящей Статьи, в том числе, если они являются составной частью сертификата, выданного контролеру или лицу, обрабатывающему данные, согласно Статьям 42 и 43.

7. Европейская Комиссия может определить стандартные договорные условия для регулирования вопросов, указанных в параграфах 3 и 4 настоящей Статьи, в соответствии с процедурой проверки согласно Статье 93(2).

8. Надзорный орган может утвердить стандартные договорные условия для регулирования вопросов, указанных в параграфах 3 и 4 настоящей Статьи, в соответствии с механизмом сопоставимости, указанным в Статье 63.

9. Договор или иной юридический акт, указанный в параграфах 3 и 4, должен быть составлен в письменном виде, в том числе в электронной форме.

10. Без ущерба Статьям 82, 83 и 84 обрабатывающее данные лицо, которое с нарушением требований настоящего Регламента определяет цели и способы обработки, должно считаться контролером в отношении указанной обработки.

Статья 29
Обработка от имени контролера или обрабатывающего данные лица

Лицо, обрабатывающее данные, и любое лицо, действующее от имени контролера или обрабатывающего данные лица и имеющее доступ к персональным данным, должны обрабатывать указанные данные только по распоряжению контролера, за исключением случаев, предусмотренных законодательством Союза или государства-члена ЕС.

Статья 30
Учетные сведения об обработке данных

1. Каждый контролер и, в соответствующих случаях, представитель контролера должен вести учет всей деятельности, связанной с обработкой данных и подпадающей под его ответственностью. Учетные сведения должны содержать всю следующую информацию:

(a) фамилию и контактные сведения контролера и, в соответствующих случаях, контролера, осуществляющего обработку совместно с ним, представителя контролера и инспектора по защите персональных данных;

(b) цели обработки;

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

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

(e) в соответствующих случаях, передачи персональных данных третьей стране или международной организации, включая идентификационные данные указанной третий страны или международной организации, и в случае передачи, указанной во втором подпараграфе Статьи 49(1), документальное подтверждение надлежащих гарантий;

(f) при наличии возможности, предусмотренные сроки для уничтожения различных категорий данных;

(g) при наличии возможности, общее описание технических и организационных мер безопасности, указанных в Статье 32(1).

2. Каждое лицо, обрабатывающее данные, и, в соответствующих случаях, его представитель должны вести учет всех категорий обработки данных, осуществляемой от имени контролера; учетные сведения должны содержать следующее:

(a) фамилию и контактные сведения обрабатывающего данные лица или лиц и каждого контролера, от имени которого действует указанное лицо, и, в соответствующих случаях, представителя контролера или обрабатывающего данные лица, и инспектора по защите персональных данных;

(b) категории обработки, осуществляемой от имени контролера;

(c) в соответствующих случаях, передачи персональных данных третьей стране или международной организации, включая идентификационные данные указанной третий страны или международной организации, и в случае передачи, указанной во втором подпараграфе Статьи 49(1), документальное подтверждение надлежащих гарантий;

(d) при наличии возможности, общее описание технических и организационных мер безопасности, указанных в Статье 32(1).

3. Учетные сведения, указанные в параграфах 1 и 2, должны сохраняться в письменном виде, в том числе в электронной форме.

4. Контролер или лицо, обрабатывающее данные, и, в соответствующих случаях, их представитель должны предоставить учетные сведения в распоряжение надзорных органов по их требованию.

5. Обязанности, указанные в параграфах 1 и 2, не должны применяться в отношении предприятия или организации, на которых занято менее 250 человек, кроме случаев, когда осуществляемая ими обработка может повлечь за собой возникновение риска для прав и свобод субъектов данных, обработка не носит случайный характер или включает в себя специальные

категории данных, указанных в Статье 9(1), или персональные данные, связанные с судимостями и преступлениями согласно Статье 10.

Статья 31
Сотрудничество с надзорным органом

Контролер и обрабатывающее данные лицо, и, в соответствующих случаях, их представители, должны сотрудничать по требованию с надзорным органом при осуществлении своих задач.

Раздел 2
Безопасность персональных данных

Статья 32
Безопасность обработки

1. Принимая во внимание состояние развития науки и техники, расходы на имплементацию, характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и опасности для прав и свобод физических лиц, контролер и обрабатывающее данные лицо должны имплементировать соответствующие технические и организационные меры, чтобы гарантировать соразмерный риску уровень безопасности, включая inter alia следующее:

(a) псевдонимизацию и криптографическую защиту персональных данных;

(b) способность гарантировать постоянную конфиденциальность, целостность, доступность и устойчивость систем и услуг, связанных с обработкой;

(c) способность своевременно восстанавливать доступность и доступ к персональным данным в случае возникновения инцидента физического или технического свойства;

(d) процедуру регулярной проверки и оценки эффективности технических и организационных мер для обеспечения безопасности обработки.

2. При оценке соответствующего уровня безопасности необходимо учесть риски, связанные с процессом обработки, в частности со случайным или незаконным уничтожением, потерей, изменением, несанкционированным распространением или доступом к персональным данным, которые передаются, хранятся или иным образом обрабатываются.

3. Следование утвержденным нормам поведения согласно Статье 40 или утвержденному сертификационному механизму согласно Статье 42 может быть использовано в качестве элемента для подтверждения соблюдения требований, указанных в параграфе 1 настоящей Статьи.

4. Контролер и обрабатывающее данные лицо должно принять меры для того, чтобы гарантировать, что любое физическое лицо, действующее от имени контролера или обрабатывающего данные лица и имеющее доступ к персональным данным, должно обрабатывать указанные данные только по распоряжению контролера, за исключением случаев, предусмотренных законодательством Союза или государства-члена ЕС.

Статья 33
Уведомление надзорного органа об утечке персональных данных

1. В случае утечки персональных данных контролер незамедлительно и при наличии соответствующей возможности в течение 72 часов, после того как ему стало известно об утечке, должен уведомить об этом компетентный в соответствии со Статьей 55 надзорный орган, кроме

случаев, когда утечка персональных данных вероятно не приведет к риску для прав и свобод физических лиц. В случае если уведомление надзорного органа не было сделано в течение 72 часов, в нем необходимо указать причины задержки.

2. Лицо, обрабатывающее данные, должно уведомить контролера об утечке персональных данных сразу же, как только ему стало известно об этом.

3. Уведомление, указанное в параграфе 1, должно содержать в себе как минимум следующую информацию:

(a) описание характера утечки персональных данных, в том числе по возможности указание категорий и приблизительного количества субъектов данных и категории и приблизительного количество записей персональных данных;

(b) фамилию и контактные данные инспектора по защите персональных данных или иного координационного центра, в котором можно получить более подробную информацию;

(c) описание возможных последствий утечки персональных данных;

(d) описание принятых или планируемых контролером мер для устранения нарушения, в том числе, в соответствующих случаях, мер по смягчению его возможного отрицательного воздействия.

4. В случае если и постольку, поскольку в то же самое время предоставление информации не возможно, она может быть предоставлена поэтапно без дальнейшего промедления.

5. Контролер должен документировать любые утечки персональных данных, в том числе все относящиеся к утечке персональных данных факты, ее последствия и принятые корректирующие меры. Указанная документация должна обеспечить возможность проверки надзорным органом соблюдения настоящей Статьи.

Статья 34
Информирование субъекта данных об утечке персональных данных

1. В случае если утечка персональных данных может привести к высокой степени риска для прав и свобод физических лиц, контролер должен незамедлительно уведомить субъекта данных об утечке персональных данных.

2. Уведомление субъекта данных, указанное в параграфе 1 настоящей Статьи, должно описывать ясным и простым языком характер утечки персональных данных и содержать как минимум информацию и меры, указанные в пунктах (b), (c) и (d) Статьи 33(3).

3. Уведомление субъекта данных, указанное в параграфе 1, не требуется, если соблюдается любое из следующих условий:

(a) контролер имплементировал соответствующие технические и организационные меры защиты, и указанные меры применялись в отношении затронутых утечкой персональных данных, в особенности те меры, посредством которых персональные данные будут непонятны всем лицам, не обладающим доступом к ним, например, криптографическая защита;

(b) контролер принял дополнительные меры, которые гарантируют, что не возникнет высокая степень риска для прав и свобод субъектов данных согласно параграфу 1;

(c) оно требует несоразмерного усилия. В указанном случае, вместо этого делается сообщение для информирования общественности или принимается аналогичная мера, посредством которой информируются субъекты данных.

4. Если контролер еще не проинформировал субъекта данных об утечке персональных данных, надзорный орган, изучив вероятность возникновения высокой степени риска вследствие утечки персональных данных, может потребовать от контролера проинформировать субъекта данных или может принять решение о том, что соблюдается одно из условий, указанных в параграфе 3.

Раздел 3

Оценка воздействия на защиту данных и предварительная консультация

Статья 35
Оценка воздействия на защиту данных

1. В случае если тип обработки данных, особенно при использовании новых технологий и с учетом характера, объема, особенностей и целей обработки, может привести к высокой степени риска для прав и свобод физических лиц, контролер перед обработкой осуществляет оценку воздействия предусмотренного процесса обработки данных на защиту персональных данных. Отдельная оценка может быть проведена в отношении совокупности аналогичных процессов обработки данных с аналогичной высокой степенью риска.

2. При проведении оценки воздействия на защиту данных контролер должен обратиться за советом к инспектору по защите персональных данных, если он был назначен.

3. Оценка воздействия на защиту данных, указанная в параграфе 1, требуется, в частности, в случае:

(a) систематической и масштабной оценки личностных аспектов физических лиц, которая основывается на автоматизированной обработке, включая формирование профиля, и которая служит основой для решений, порождающих юридические последствия в отношении физического лица или аналогичным образом существенно влияющих на физическое лицо;

(b) масштабной обработки особых категорий данных, указанных в Статье 9(1), или персональных данных, относящихся к уголовным приговорам и преступлениям согласно Статье 10; или

(c) систематического обширного мониторинга открытой для общего доступа области.

4. Надзорный орган должен создать и опубликовать перечень процессов обработки данных, относительно которых должна осуществляться оценка воздействия на защиту данных согласно параграфу 1. Надзорный орган должен передать данные перечни Совету, указанному в Статье 68.

5. Надзорный орган может также создать и опубликовать перечень видов обработки данных, для которых не требуется оценка воздействия на защиту данных. Надзорный орган должен передать указанные перечни Совету.

6. До утверждения перечней, указанных в параграфах 4 и 5, компетентный надзорный орган должен применить механизм сопоставимости, указанный в Статье 63, если указанные перечни охватывают обработку данных, связанных с предложением товаров и услуг субъектам данных или с мониторингом их поведенческой активности в нескольких государствах-членах ЕС или могущих существенно повлиять на свободное обращение персональных данных на территории Союза.

7. Оценка должна содержать как минимум следующее:

(a) систематическое описание предусмотренных процессов обработки данных и целей обработки, в том числе, в соответствующих случаях, законного интереса контролера;

(b) оценку необходимости и пропорциональности обработки данных относительно целей;

(c) оценку рисков для прав и свобод субъектов данных, указанных в параграфе 1; и

(d) меры, предусмотренные для устранения рисков, включая гарантии, меры безопасности и механизмы для обеспечения защиты персональных данных и подтверждения соблюдения настоящего Регламента с учетом прав и законных интересов субъектов данных и других заинтересованных лиц.

8. Соблюдение утвержденных норм поведения согласно Статье 40 соответствующими контролерами или лицами, обрабатывающими данные, следует учитывать при оценке воздействия обработки данных, проведенной указанными контролерами или лицами, обрабатывающими данные, в частности в целях оценки воздействия на защиту данных.

9. В соответствующих случаях контролер должен узнать мнение субъектов данных или их представителей относительно запланированной обработки, без ущерба защите коммерческих или

общественных интересов или безопасности обработки данных.

10. В случае если обработка согласно пункту (c) или (e) Статьи 6(1) имеет правовое основание в законодательстве Союза или государства-члена ЕС, под действие которого подпадает контролер, если указанное законодательство регулирует определенный процесс обработки данных или совокупность процессов обработки и если оценка воздействия на защиту данных уже проводилась в рамках общей оценки воздействия в отношении утверждения указанного правового основания, параграфы 1 - 7 не должны применяться кроме случаев, когда государства-члены ЕС считают необходимым провести указанную оценку до обработки данных.

11. При необходимости контролер должен провести проверку для того, чтобы оценить, выполняется ли обработка в соответствии с оценкой воздействия на защиту данных, как минимум, когда имеется изменение относительно риска, связанного с обработкой данных.

Статья 36
Предварительная консультация

1. Контролер должен проконсультироваться с надзорным органом до начала обработки, если оценка воздействия на защиту данных согласно Статье 35 указывает на то, что обработка может привести к возникновению высокой степени риска при отсутствии мер, принятых контролером для снижения риска.

2. Если надзорный орган считает, что запланированная обработка согласно параграфу 1 может нарушить положения настоящего Регламента, в частности, если контролер в недостаточной степени идентифицировал или снизил риск, надзорный орган в течение не более восьми недель с момента получения запроса о проведении консультации должен предоставить контролеру и в соответствующих случаях лицу, обрабатывающему данные, письменные рекомендации и может осуществлять полномочия, указанные в Статье 58. Указанный срок может быть увеличен на шесть недель с учетом сложности запланированной обработки. Надзорный орган должен проинформировать контролера и в соответствующих случаях лицо, обрабатывающее данные, об указанном увеличении срока в течение месяца после получения запроса о проведении консультации и указать причины отсрочки. Указанные сроки могут быть приостановлены до тех пор, пока надзорный орган не получит информацию, запрашиваемую в целях консультации.

3. В случае консультации согласно параграфу 1 контролер должен предоставить надзорному органу следующую информацию:

(a) в соответствующих случаях, сведения об обязанностях контролера, контролеров, совместно осуществляющих обработку, и участвующих в обработке лиц, обрабатывающих данные, в частности при обработке в рамках группы предприятий;

(b) цели и способы запланированной обработки;

(c) меры и гарантии для защиты прав и свобод субъектов данных согласно настоящему Регламенту;

(d) в соответствующих случаях, контактные данные инспектора по защите персональных данных;

(e) оценку воздействия на защиту данных согласно Статье 35; и

(f) любую другую информацию, требуемую надзорным органом.

4. Государства-члены ЕС должны проконсультироваться с надзорным органом при подготовке предложения по законодательной мере, которая должна быть принята национальным парламентом, или при подготовке регулятивной меры, основанной на такой законодательной мере, относящейся к обработке.

5. Безотносительно параграфа 1 законодательство государства-члена ЕС может обязать контролеров проконсультироваться с надзорным органом, а также получить от него предварительное разрешение при обработке для выполнения задачи в интересах общества, в том

числе при обработке в целях социальной защиты и общественного здравоохранения.

Раздел 4
Инспектор по защите персональных данных

Статья 37
Назначение инспектора по защите персональных данных

1. Контролер и обрабатывающее данные лицо должны назначить инспектора по защите персональных данных в случае, если:

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

(b) основная деятельность контролера или обрабатывающего данные лица заключается в обработке данных, которая в силу своего характера, объема и/или целей, требует масштабного, регулярного и систематического мониторинга субъектов данных; или

(c) основная деятельность контролера или обрабатывающего данные лица заключается в масштабной обработке особых категорий данных согласно Статье 6 и персональных данных, связанных с уголовными приговорами и преступлениями согласно Статье 10.

2. Группа предприятий может утвердить единого инспектора по защите персональных данных, при условии, что инспектор по защите персональных данных может быть легкодоступен от каждого учреждения.

3. В случае если контролер или обрабатывающее данные лицо является органом государственной власти или правительственным учреждением, единый инспектор по защите персональных данных может быть назначен для нескольких таких органов или учреждений, с учетом их организационной структуры и размера.

4. В случаях, отличных от указанных в параграфе 1, контролер, или обрабатывающее данные лицо, или объединения и иные органы, представляющие категории контролеров или обрабатывающих данные лиц, могут или, если этого требует законодательство Союза или государства-члена ЕС, должны назначить инспектора по защите персональных данных. Инспектор по защите персональных данных может действовать от лица указанных объединений и иных органов, представляющих контролеров или обрабатывающих данные лиц.

5. Инспектор по защите персональных данных должен назначаться на основе профессиональных качеств и, в частности, на основе экспертного знания законодательства и практики в области защиты данных, а также на основе способности выполнять задачи, указанные в Статье 39.

6. Инспектор по защите персональных данных может являться сотрудником контролера или обрабатывающего данные лица, или он может выполнять задачи на основе договора об оказании услуг.

7. Контролер или обрабатывающее данные лицо должно опубликовать контактные данные инспектора по защите персональных данных и сообщить их надзорному органу.

Статья 38
Положение инспектора по защите персональных данных

1. Контролер и обрабатывающее данные лицо должны гарантировать, что инспектор по защите персональных данных принимает своевременное и надлежащее участие в решении всех вопросов, связанных с защитой персональных данных.

2. Контролер и обрабатывающее данные лицо должны оказывать поддержку инспектору по

защите персональных данных при выполнении задач, указанных в Статье 39, посредством предоставления ресурсов, необходимых для осуществления указанных задач, и доступа к персональным данным и процессу обработки, а также ресурсов, необходимых для сохранения его/ее экспертных знаний.

3. Контролер и обрабатывающее данные лицо должны гарантировать, что инспектор по защите персональных данных не получает иных указаний относительно выполнения указанных задач. Инспектор по защите персональных данных не должен быть отстранен или оштрафован контролером или обрабатывающим данные лицом за выполнение своих задач. Инспектор по защите персональных данных должен напрямую отчитываться перед руководством высшего уровня контролера или лица, обрабатывающего данные.

4. Субъекты данных могут обращаться к инспектору по защите персональных данных относительно всех вопросов, связанных с обработкой их персональных данных и с осуществлением их прав согласно настоящему Регламенту.

5. Инспектор по защите персональных данных обязан в соответствии с законодательством Союза или государства-члена ЕС соблюдать тайну или конфиденциальность при осуществлении своих задач.

6. Инспектор по защите персональных данных может выполнять иные задачи и обязанности. Контролер или обрабатывающее данные лицо должны гарантировать, что любые такие задачи и обязанности не влекут за собой конфликт интересов.

Статья 39
Задачи инспектора по защите персональных данных

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

(a) информировать и давать советы контролеру или обрабатывающему данные лицу и сотрудникам, которые осуществляют обработку, относительно их обязанностей согласно настоящему Регламенту, а также согласно иным положениям Союза или государства-члена ЕС о защите данных;

(b) контролировать соблюдение настоящего Регламента, иных положений Союза или государства-члена ЕС о защите данных, а также методов контролера или обрабатывающего данные лица для защиты персональных данных, включая распределение обязанностей, повышение уровня информированности и обучение персонала, занятого в обработке данных, и соответствующие аудиторские проверки.

(c) осуществлять консультирование, при необходимости, относительно оценки воздействия на защиту данных и контролировать ее выполнение согласно Статье 35;

(d) сотрудничать с надзорным органом;

(e) действовать в качестве координационного центра для надзорного органа по вопросам, связанным с обработкой, включая предварительную консультацию согласно Статье 36, и консультировать, в соответствующих случаях, относительно иных вопросов.

2. Инспектор по защите персональных данных при выполнении своих задач должен принимать во внимание риск, связанный с процессом обработки данных, с учетом характера, объема, особенностей и целей обработки.

Раздел 5
Нормы поведения и сертификация

Статья 40

Нормы поведения

1. Государства-члены ЕС, надзорные органы, Совет и Европейская Комиссия должны содействовать разработке норм поведения, предназначенных для надлежащего применения настоящего Регламента, с учетом специфических особенностей различных секторов обработки и специфических потребностей микропредприятий, малых и средних предприятий.

2. Объединения и другие организации, представляющие категории контролеров или обрабатывающих данные лиц, могут разработать нормы поведения, внести в них изменения или расширить их в целях определения применения настоящего Регламента, с учетом следующего:

(a) справедливой и прозрачной обработки;

(b) законных интересов контролеров в определенных контекстах;

(c) сбора персональных данных;

(d) псевдонимизации персональных данных;

(e) информации, предоставляемой общественности и субъектам данных;

(f) осуществления прав субъектов данных;

(g) информирования и защиты детей, а также способа, посредством которого должно быть получено согласие лиц, обладающих родительской ответственностью в отношении ребенка;

(h) мер и процедур, указанных в Статьях 24 и 25, а также мер для обеспечения безопасности обработки согласно Статье 32;

(i) уведомления надзорных органов об утечке персональных данных и информирования об указанных утечках персональных данных субъектов данных;

(j) передачи персональных данных третьим странам или национальным организациям; или

(k) внесудебных процедур и иных процедур разрешения спорных вопросов между контролерами и субъектами данных в отношении обработки, без ущерба правам субъектов данных согласно Статьям 77 и 79.

3. В дополнение к соблюдению контролерами или обрабатывающими данные лицами, подпадающими под действие настоящего Регламента, нормы поведения, утвержденные в соответствии с параграфом 5 настоящей Статьи и обладающие общей действительностью согласно параграфу 9 настоящей Статьи, могут соблюдаться контролерами или обрабатывающими данные лицами, которые не подпадают под действие настоящего Регламента согласно Статье 3, для того чтобы предоставить соответствующие гарантии в рамках передачи персональных данных третьим странам или международным организациям в соответствии с пунктом (e) Статьи 46(2). Указанные контролеры или обрабатывающие данные лица должны посредством договора или иных документов, имеющих юридическую силу, взять на себя осуществимые обязательства по применению соответствующих гарантий, в том числе с учетом прав субъектов данных.

4. Норма поведения, указанная в параграфе 2 настоящей Статьи, должна содержать механизмы, которые позволят органу, указанному в Статье 41(1), осуществлять обязательный мониторинг соблюдения положений контролерами или обрабатывающими данные лицами, которые обязаны соблюдать нормы поведения, без ущерба задачам и полномочиям надзорных органов, компетентных в соответствии со Статьей 55 или 56.

5. Объединения и другие органы, указанные в параграфе 2 настоящей Статьи, которые намерены разработать норму поведения, внести изменение или расширить существующую норму, должны представить проект нормы, ее изменения или расширения надзорному органу, который является компетентным в соответствии со Статьей 55. Надзорный орган должен дать свое заключение относительно того, соответствует ли проект нормы, изменения или расширения настоящему Регламенту, и должен утвердить проект нормы, изменения или расширения, если он считает, что он предусматривает соответствующие гарантии.

6. Если проект нормы, ее изменения или расширения утвержден в соответствии с параграфом 5 и если соответствующая норма поведения не относится к обработке данных в нескольких государствах-членах ЕС, надзорный орган должен зарегистрировать и опубликовать норму.

7. В случае если проект нормы поведения относится к обработке данных в нескольких государствах-членах ЕС, надзорный орган, компетентный согласно Статье 55, до утверждения проекта нормы, ее изменения или расширения, должен передать его в соответствии с процедурой, указанной в Статье 63, Совету, который должен дать заключение относительно того, соответствует ли проект нормы, ее изменения или расширения настоящему Регламенту или в случае, указанном в параграфе 3 настоящей Статьи, предусматривает ли он соответствующие гарантии.

8. В случае если заключение, указанное в параграфе 7, подтверждает, что проект нормы, ее изменения или расширения соответствует настоящему Регламенту или в случае, указанном в параграфе 3, предусматривает соответствующие гарантии, Совет должен представить свое заключение Европейской Комиссии.

9. Европейская Комиссия посредством имплементационных актов может принять решение о том, что переданные ей в соответствии с параграфом 8 настоящей Статьи утвержденные нормы поведения, их изменение или расширение обладают общей действительностью на территории Союза. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

10. Европейская Комиссия должна гарантировать распространение информации об утвержденных нормах, общая действительность которых была признана в соответствии с параграфом 9.

11. Совет должен внести все утвержденные нормы поведения, их изменения или расширения в реестр и посредством соответствующих мер довести их до всеобщего сведения.

Статья 41
Мониторинг утвержденных норм поведения

1. Без ущерба задачам и полномочиям компетентного надзорного органа согласно Статьям 57 и 58 мониторинг соблюдения нормы поведения согласно Статье 40 может осуществляться органом, обладающим соответствующим уровнем компетентности в отношении предмета нормы и уполномоченным для указанной цели компетентным надзорным органом.

2. Орган, указанный в параграфе 1, может быть уполномочен на мониторинг соблюдения нормы поведения, если он:

(a) подтвердил компетентному надзорному органу свою независимость и компетентность в отношении предмета нормы;

(b) установил процедуру, которая позволит ему оценить, могут ли контролеры и обрабатывающие данные лица применять норму, а также проконтролировать соблюдение нормы контролерами и обрабатывающими данные лицами и проводить периодическую проверку ее применения;

(c) установил процедуры и структуры, для того чтобы рассматривать жалобы на нарушения нормы или на способы, при помощи которых норма была имплементирована или имплементируется контролером или обрабатывающим данные лицом, а также для того чтобы сделать указанные процедуры и структуры прозрачными для субъектов данных и общественности; и

(d) подтвердил компетентному надзорному органу, что его задачи и обязанности не приведут к конфликту интересов.

3. Компетентный надзорный орган должен передать проект критерий утверждения органа, указанного в параграфе 1 настоящей Статьи, Совету согласно механизму сопоставимости, указанному в Статье 63.

4. Без ущерба задачам и полномочиям компетентного надзорного органа и положениям Главы VIII орган, указанный в параграфе 1 настоящей Статьи, должен с учетом соответствующих гарантий принять надлежащие меры в случае нарушения нормы контролером или обрабатывающим данные лицом, включая временное или окончательное отстранение контролера или обрабатывающего

данные лица от нормы. Он должен проинформировать компетентный надзорный орган об указанных мерах и причинах их принятия.

5. Компетентный надзорный орган должен отозвать утверждение органа, указанного в параграфе 1, если условия его утверждения больше не соблюдаются или если меры, принятые указанным органом, нарушают положения настоящего Регламента.

6. Настоящая Статья не применяется в отношении обработки, осуществляемой компетентными органами государственной власти и правительственными учреждениями.

Статья 42
Сертификация

1. Государства-члены ЕС, надзорные органы, Совет и Европейская Комиссия должны содействовать, особенно на уровне Союза, внедрению сертификационных механизмов защиты данных, а также печатей и маркировочных знаков для защиты данных в целях подтверждения соблюдения настоящего Регламента при обработке, осуществляемой контролерами и лицами, обрабатывающими данные. Необходимо учитывать определенные потребности микропредприятий, малых и средних предприятий.

2. В дополнение к соблюдению контролерами или обрабатывающими данные лицами, подпадающими под действие настоящего Регламента, сертификационные механизмы защиты данных, печати или маркировочные знаки, утвержденные в соответствии с параграфом 5 настоящей Статьи, могут быть установлены в целях подтверждения наличия соответствующих гарантий, предоставляемых контролерами или обрабатывающими данные лицами, которые не подпадают под действие настоящего Регламента согласно Статье 3, в рамках передачи персональных данных третьим странам или международным организациям в соответствии с пунктом (f) Статьи 46(2). Указанные контролеры или обрабатывающие данные лица должны посредством договора или иных документов, имеющих юридическую силу, взять на себя осуществимые обязательства по применению соответствующих гарантий, в том числе с учетом прав субъектов данных.

3. Сертификация должна быть добровольной и доступной посредством прозрачного процесса.

4. Сертификация согласно настоящей Статье не уменьшает ответственность контролера или обрабатывающего данные лица за соблюдение настоящего Регламента и действует без ущерба задачам и полномочиям надзорного органа, компетентного в соответствии со Статьей 55 или 56.

5. Сертификация согласно настоящей Статье должна осуществляться сертификационными органами, указанными в Статье 43, или компетентным надзорным органом на основе критериев, утвержденных указанным компетентным надзорным органом согласно Статье 58(3) или Советом согласно Статье 63. Если критерии утверждаются Советом, это может привести к общей сертификации, к европейской печати о защите данных.

6. Контролер или обрабатывающее данные лицо, которое подвергает осуществляемую им обработку сертификационному механизму, должно предоставить сертификационному органу, указанному в Статье 43, или в соответствующих случаях компетентному надзорному органу всю информацию, необходимую для проведения сертификационной процедуры, и обеспечить доступ к обработке данных.

7. Сертификация должна предоставляться контролеру или обрабатывающему данные лицу на срок не более трех лет, указанный срок может быть продлен на тех же самых условиях в том случае, если продолжают соблюдаться соответствующие требования. Сертификация должна быть отменена сертификационными органами, указанными в Статье 43, или компетентным надзорным органом, если требования для сертификации больше не соблюдаются.

8. Совет должен внести все сертификационные механизмы, печати и маркировочные знаки о защите данных в реестр и посредством соответствующих мер довести их до всеобщего сведения.

Статья 43
Сертификационные органы

1. Без ущерба задачам и полномочиям компетентного надзорного органа согласно Статьям 57 и 58 сертификационные органы, обладающие соответствующим уровнем компетентности в отношении защиты данных, должны после информирования надзорного органа в целях содействия ему в осуществлении его полномочий согласно пункту (h) Статьи 58(2), при необходимости, предоставить и продлить сертификацию. Государства-члены ЕС должны гарантировать, что указанные сертификационные органы утверждены:

(a) надзорным органом, компетентным согласно Статье 55 или 56; и/или

(b) национальной сертификационной организацией, определенной в соответствии с Регламентом (ЕС) 765/2008 Европейского Парламента и Совета ЕС[21], в соответствии с EN-ISO/IEC 17065/2012 и с дополнительными требованиями, установленными надзорным органом, компетентным согласно Статье 55 или 56.

2. Сертификационные органы, указанные в параграфе 1, должны быть аккредитованы в соответствии с указанным параграфом только, если они:

(a) подтвердили компетентному надзорному органу свою независимость и компетентность в отношении предмета сертификации;

(b) приняли на себя обязательство соблюдать критерии, указанные в Статье 42(5) и утвержденные надзорным органом, компетентным согласно Статье 55 или 56, или Советом согласно Статье 63;

(c) установили процедуры для выдачи, периодической проверки и отмены сертификации защиты данных, печатей и маркировочных знаков о защите данных;

(d) установили процедуры и структуры, для того чтобы рассматривать жалобы на нарушения сертификации или на способы, при помощи которых сертификация была имплементирована или имплементируется контролером или обрабатывающим данные лицом, а также для того чтобы сделать указанные процедуры и структуры прозрачными для субъектов данных и общественности; и

(e) подтвердили компетентному надзорному органу, что его задачи и обязанности не приведут к конфликту интересов.

3. Аккредитация сертификационных органов, указанных в параграфах 1 и 2 настоящей Статьи, должна осуществляться на основе критериев, утвержденных надзорным органом, компетентным согласно Статье 55 или 56, или Советом согласно Статье 63. В случае аккредитации согласно пункту (b) параграфа 1 настоящей Статьи, указанные требования должны дополнять требования, предусмотренные Регламентом (ЕС) 765/2008 и техническими нормами, которые описывают методы и процедуры сертификационных органов.

4. Сертификационные органы, указанные в параграфе 1, должны отвечать за надлежащую оценку, которая лежит в основе сертификации или отмены такой сертификации, без ущерба ответственности контролера или обрабатывающего данные лица за соблюдение настоящего Регламента. Аккредитация выдается на срок не более пяти лет и указанный срок может быть продлен на тех же самых условия в случае, если сертификационный орган соблюдает требования, установленные в настоящей Статье.

5. Сертификационные органы, указанные в параграфе 1, должны сообщить компетентному надзорному органу причины предоставления или отмены требуемой сертификации.

6. Требования, указанные в параграфе 3 настоящей Статьи, и критерии, указанные в Статье 42(5), должны быть опубликованы надзорным органом в легкодоступной форме. Надзорные органы должны также передать указанные требования и критерии Совету. Совет должен внести все сертификационные механизмы и печати о защите данных в реестр и посредством соответствующих мер довести их до всеобщего сведения.

7. Без ущерба действию Главы VIII компетентный надзорный орган или национальная сертификационная организация должны отменить аккредитацию сертификационного органа

согласно параграфу 1 настоящей Статьи, если условия аккредитации больше не соблюдаются или если принятые сертификационным органом меры нарушают положения настоящего Регламента.

8. Европейская Комиссия вправе принять делегированные акты в соответствии со Статьей 92 в целях установления требований, которые необходимо учесть для сертификационных механизмов защиты данных, указанных в Статье 42(1).

9. Европейская Комиссия может принять имплементационные акты, устанавливающие технические стандарты для сертификационных механизмов, печатей и маркировочных знаков о защите данных, а также механизмы для содействия и признания указанных сертификационных механизмов, печатей и маркировочных знаков. Указанные имплементационные акты должны быть приняты 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, которые уже обрабатываются или которые должны будут быть обработаны после передачи третьей стране или международной организации, должна осуществляться только, если контролер или обрабатывающее данные лицо соблюдают условия, установленные в настоящей Главе, а также иные положения настоящего Регламента, включая передачу персональных данных из третьей страны или международной организации в другую третью страну или другую международную организацию. Все положения настоящей Главы должны применяться для обеспечения того, что уровень защиты физических лиц, гарантированный настоящим Регламентом, остается неизменным.

Статья 45
Передача на основании решения о соответствии

1. Передача персональных данных третьей стране или международной организации может осуществляться, если Европейская Комиссия приняла решение о том, что третья страна, территория, или один или несколько специфических секторов в указанной третьей стране, или соответствующая международная организация гарантируют надлежащий уровень защиты. Указанная передача не требует специального разрешения.

2. При оценке соответствия уровня защиты Европейская Комиссия должна, в частности, принять во внимание следующие элементы:

(a) верховенство законодательства, уважение прав и основных свобод человека, соответствующее законодательство, как общего характера, так и отраслевое, в том числе в отношении общественной безопасности, обороны, внутренней безопасности и уголовного права и доступа органов государственной власти к персональным данным, а также имплементацию указанного законодательства, норм о защите данных, профессиональных правил и мер безопасности, включая правила передачи персональных данных другой третьей стране или международной организации, которые соблюдаются в указанной третьей стране или международной организации, прецедентное право, а также эффективные и защищенные права субъектов данных и эффективные административные и правовые средства защиты для субъектов данных, персональные данные которых передаются;

(b) существование и эффективное функционирование одного или нескольких независимых надзорных органов в третьей стране или органов, в ведении которых находится международная

организация, обладающих компетенцией в отношении обеспечения и реализации соблюдения норм о защите данных, включая соответствующие правоприменительные полномочия, а также в отношения содействия и консультирования субъектов данных при осуществлении ими своих прав и сотрудничества с надзорными органами государств-членов ЕС; и

(c) международные обязательства, которые взяли на себя третья страна или международная организация, или иные обязанности, вытекающие из юридически обязательных конвенций или нормативных документов, а также из участия в многосторонних или региональных системах, в частности, в отношении защиты персональных данных.

3. Европейская Комиссия, после оценки соответствия уровня защиты, может посредством имплементационного акта принять решение о том, что третья страна, территория, или один или несколько определенных секторов в указанной третьей стране, или соответствующая международная организация гарантирует соответствующий уровень защиты в значении параграфа 2 настоящей Статьи. Имплементационный акт должен предусматривать механизм периодической проверки, как минимум каждые четыре года, которая должна учесть все соответствующие изменения в третьей стране или международной организации. Имплементационный акт должен устанавливать территориальное или секторальное применение и, при необходимости, определять надзорный орган или органы, указанные в пункте (b) параграфа 2 настоящей Статьи. Имплементационный акт должен быть принят в соответствии с процедурой проверки, указанной в Статье 93(2).

4. Европейская Комиссия на постоянной основе должна контролировать изменения в третьих странах и международных организациях, которые могут повлиять на выполнение решений, принятых согласно параграфу 3 настоящей Статьи, и решений, принятых на основе Статьи 25(6) Директивы 95/46/ЕС.

5. Европейская Комиссия при обнаружении соответствующей информации, в частности, в результате проверки, указанной в параграфе 3 настоящей Статьи, о том, что третья страна, территория, или один или несколько определенных секторов в указанной третьей стране, или соответствующая международная организация более не гарантирует в той мере, в какой это необходимо, соответствующий уровень защиты в значении параграфа 2 настоящей Статьи, должна отменить, внести изменение или приостановить действие решения, указанного в параграфе 3 настоящей Статьи, посредством имплементационных актов без эффекта обратной силы. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2). Исходя из соображений крайней необходимости, Европейская Комиссия должна незамедлительно принять имплементационные акты в соответствии с процедурой, указанной в Статье 93(3).

6. Европейская Комиссия должна начать консультации с третьей страной или международной организацией с тем, чтобы исправить ситуацию, которая привела к решению, принятому согласно параграфу 5.

7. Решение согласно параграфу 5 настоящей Статьи действует без ущерба передаче персональных данных третьей стране, территории, одному или нескольким специфическим секторам в указанной третьей стране или соответствующей международной организации согласно Статьям 46 - 49.

8. Европейская Комиссия должна опубликовать в Официальном Журнале Европейского Союза и на своем интернет-сайте перечень третьих стран, территорий и специфических секторов в третьей стране и международных организаций, в отношении которых она приняла решение о том, что они гарантируют или больше не гарантируют соответствующий уровень защиты.

9. Решения, принятые Европейской Комиссией на основании Статьи 25(6) Директивы 95/46/ЕС, остаются в силе до тех пор, пока они не будут изменены, заменены или отменены Решением Европейской Комиссии, принятым в соответствии с параграфом 3 или 5 настоящей Статьи.

Статья 46
Передача при условии соблюдения соответствующих гарантий

1. В случае отсутствия решения согласно Статье 45(3) контролер или обрабатывающее данные лицо могут передать персональные данные третьей стране или международной организации только, если контролер или обрабатывающее данные лицо предусмотрели соответствующие гарантии и если субъекты данных обладают юридически защищенными правами и эффективными средствами правовой защиты.

2. Соответствующие гарантии, указанные в параграфе 1, могут быть предоставлены без особого разрешения надзорного органа посредством:

(a) имеющего обязательную юридическую силу документа между органами государственной власти или правительственными учреждениями;

(b) юридически обязывающих корпоративных правил в соответствии со Статьей 47;

(c) стандартных условий о защите данных, принятых Европейской Комиссией в соответствии с процедурой проверки, указанной в Статье 93(2);

(d) стандартных условий о защите данных, принятых надзорным органом и утвержденных Европейской Комиссией согласно процедуре проверки, указанной в Статье 93(2);

(e) утвержденной нормы поведения согласно Статье 40 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных; или

(f) утвержденного сертификационного механизма согласно Статье 42 совместно с юридически обязывающими и защищенными обязательствами контролера или обрабатывающего данные лица в третьей стране по применению соответствующих гарантий, в том числе в отношении прав субъектов данных.

3. При условии наличия разрешения компетентного надзорного органа соответствующие гарантии, указанные в параграфе 1, могут быть также предоставлены, в частности, посредством:

(a) статей договора, согласованных между контролером или обрабатывающим данные лицом и контролером, обрабатывающим данные лицом или получателем персональных данных в третьей стране или международной организации; или

(b) положений, которые должны быть внесены в административные договоренности между органами государственной власти или правительственными учреждениями и которые включают в себя защищенные и действующие права субъектов данных.

4. Надзорный орган должен применять механизм сопоставимости согласно Статье 63 в случаях, указанных в параграфе 3 настоящей Статьи.

5. Разрешения, выданные государством-членом ЕС или надзорным органом на основании Статьи 26(2) Директивы 95/46/ЕС, остаются в силе до тех пор, пока они не будут при необходимости изменены, заменены или отменены указанным надзорным органом. Решения, принятые Европейской Комиссией на основании Статьи 26(4) Директивы 95/46/ЕС, остаются в силе до тех пор, пока они не будут при необходимости изменены, заменены или отменены Решением Европейской Комиссии, принятым в соответствии с параграфом 2 настоящей Статьи.

Статья 47
Юридически обязывающие корпоративные правила

1. Компетентный надзорный орган в соответствии с механизмом сопоставимости, указанным в Статье 63, должен утвердить юридически обязывающие корпоративные правила при условии, что они:

(a) являются юридически обязательными и применяются в отношении каждого члена группы

предприятий или группы компаний, занятых в совместной экономической деятельности, в том числе их сотрудников, а также обеспечиваются указанными лицами;

(b) прямо предоставляют юридически защищенные права субъектам данных в отношении обработки их персональных данных;

(c) соблюдают требования, установленные в параграфе 2.

2. Юридически обязывающие корпоративные правила, указанные в параграфе 1, должны определять как минимум следующее:

(a) структуру и контактные данные группы предприятий или группы компаний, занятых в совместной экономической деятельности, а также контактные данные каждого из ее членов;

(b) передачу данных или ряд таких передач, включая категории персональных данных, тип обработки и ее цели, тип субъектов данных и идентификационную информацию относительно соответствующей третьей страны или стран;

(c) свой юридически обязательный характер, как внутренне, так и внешне;

(d) применение общих принципов защиты данных, в частности, целевое ограничение, минимизация данных, ограниченные сроки хранения, качество данных, защита данных, запланированная и по умолчанию, законное основание для обработки, обработка специальных категорий персональных данных, меры для обеспечения безопасности данных, требования относительно передачи данных органам, не связанным юридически обязывающими корпоративными правилами;

(e) права субъектов данных в отношении обработки и способы осуществления указанных прав, включая право не подчиняться решениям, основанным исключительно на автоматизированной обработке, включая формирование профиля, в соответствии со Статьей 22, а также право на подачу жалобы компетентному надзорному органу и в компетентные суда государств-членов ЕС в соответствии со Статьей 79, и право на возмещение и, в соответствующем случае, компенсацию за нарушение юридически обязывающих корпоративных правил;

(f) ответственность, которую контролер или обрабатывающее данные лицо, учрежденные на территории государства-члена ЕС, берут на себя за любое нарушение юридически обязывающих корпоративных правил любым членом группы предприятий, не учрежденным в Союзе; контролер или обрабатывающее данные лицо полностью или частично освобождаются от указанной обязанности только тогда, когда они докажут, что указанный член не несет ответственность за событие, послужившее причиной ущерба;

(g) способ предоставления субъектам данных информации о юридически обязывающих корпоративных правилах, в частности, о положениях, указанных в пунктах (d), (e) и (f) настоящего параграфа, в дополнение к Статьям 13 и 14;

(h) задачи любого инспектора по защите персональных данных, назначенного в соответствии со Статьей 37, или любого иного физического или юридического лица, отвечающего за контроль соблюдения юридически обязывающих корпоративных правил в рамках группы предприятий или группы компаний, занятых в совместной экономической деятельности, а также мониторинг обучения и рассмотрения жалоб;

(i) процедуры рассмотрения жалоб;

(j) механизмы в группе предприятий или группе компаний, занятых в совместной экономической деятельности, которые гарантирую проверку и подтверждение соблюдения юридически обязывающих корпоративных правил. Указанные механизмы должны включать в себя аудиторские проверки защиты данных и методы обеспечения корректирующих мер для защиты прав субъектов данных. Результаты указанной проверки должны быть представлены физическому или юридическому лицу, указанному в пункте (h), и совету, который осуществляет контроль предприятия в группе предприятий или группе компаний, занятых в совместной экономической деятельности, указанные результаты должны быть доступны компетентному надзорному органу по его запросу;

(k) механизмы для сообщения и учета изменений в правилах, а также механизмы

информирования об указанных изменениях надзорного органа;

(l) механизм сотрудничества с надзорным органом в целях обеспечения соблюдения предписаний любым членом группы предприятий или группы компаний, задействованных в совместной экономической деятельности, в частности, посредством предоставления надзорному органу результатов проверок мер, указанных в пункте (j);

(m) механизм предоставления отчетов компетентному надзорному органу относительно любых законных требований, под действие которых подпадает член группы предприятий или группы компаний, задействованных в совместной экономической деятельности, в третьей стране, и которые могут оказать существенное негативное воздействие на гарантии, предоставленные юридически обязывающими корпоративными правилами; и

(n) соответствующее обучение защите данных для персонала, имеющего постоянный доступ к персональным данным.

3. Европейская Комиссия может установить формат и процедуры для обмена информацией относительно юридически обязывающих корпоративных правил в значении настоящей Статьи между контролерами, обрабатывающими данные лицами и надзорными органами. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

Статья 48
Передача или раскрытие данных, не разрешенное законодательством Союза

Любое решение суда или трибунала и любое решение административного органа третьей страны, требующее от контролера или обрабатывающего данные лица передать или раскрыть персональные данные, может быть признано или может подлежать исполнению, если оно основано на действующем международном соглашении, например, на договоре о взаимной юридической помощи между запрашивающей третьей страной и Союзом или государством-членом ЕС, без ущерба иным основаниям для передачи согласно настоящей Главе.

Статья 49
Частичное отступление для определенных случаев

1. В случае отсутствия решения о соответствии согласно Статье 45(3) или соответствующих гарантий согласно Статье 46, включая юридически обязывающие корпоративные правила, передача или ряд передач персональных данных третьей стране или международной организации должна осуществляться только при соблюдении одного из следующих условий:

(a) субъект данных дал прямое согласие на соответствующую передачу данных после того, как он был проинформирован о возможных рисках указанной передачи данных вследствие отсутствия решения о соответствии и надлежащих гарантий;

(b) передача необходима для выполнения договора между субъектом данных и контролером или для имплементации преддоговорных мер, принятых по запросу субъекта данных;

(c) передача необходима для заключения договора или для исполнения договора, заключенного в интересах субъекта данных между контролером и другим физическим или юридическим лицом;

(d) передача необходима по причинам общественного интереса;

(e) передача необходима для обоснования, осуществления или оспаривания судебного иска;

(f) передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных физически или юридически не может дать свое согласие;

(g) передача осуществляется из реестра, целью которого согласно законодательству Союза

или государства-члена ЕС является предоставление информации общественности и который открыт для ознакомления широкой общественности или любому лицу, которое может доказать наличие законного интереса, но только в той мере, в какой соблюдаются условия, установленные законодательством Союза или государства-члена ЕС, для ознакомления в отдельном случае.

В случае если передача не может основываться на положении Статьи 45 или 46, в том числе на положениях о юридически обязывающих корпоративных правилах, и если не применяются частичные отступления для определенных случаев согласно первому подпараграфу настоящего параграфа, передача данных третьей стране или международной организации может осуществляться только, если передача не носит повторяющийся характер, касается ограниченного количества субъектов данных, необходима в целях защиты законных интересов контролера, при условии, что интересы или права и свободы субъекта данных не превалируют над ними, и контролер оценил все обстоятельства, связанные с передачей данных, и на основании указанной оценки предусмотрел надлежащие гарантии относительно защиты персональных данных. Контролер должен проинформировать о передаче надзорный орган. В дополнение к предоставлению информации, указанной в Статьях 13 и 14, контролер должен проинформировать субъекта данных о передаче данных и о своих законных интересах.

2. Передача согласно пункту (g) первого подпараграфа параграфа 1 не должна включать в себя все персональные данные или все категории персональных данных, содержащихся в реестре. Если целью реестра является ознакомление лиц, имеющих законный интерес, передача должна осуществляться только по запросу указанных лиц или если указанные лица являются получателями данных.

3. Пункты (a), (b) и (c) первого подпараграфа параграфа 1, а также второй подпараграф параграфа 1 не должны применяться в отношении деятельности, осуществляемой органами государственной власти при выполнении ими своих полномочий.

4. Общественный интерес в значении пункта (d) первого подпараграфа параграфа 1 должен быть признан в законодательстве Союза или в законодательстве государства-члена ЕС, под действие которого подпадает контролер.

5. В случае отсутствия решения о соответствии в законодательстве Союза или государства-члена ЕС может быть по причинам общественного интереса предусмотрено ограничение передачи определенных категорий персональных данных третьей стране или международной организации. Государства-члены ЕС должны уведомить об указанных положениях Европейскую Комиссию.

6. Контролер или обрабатывающее данные лицо должно зафиксировать в учетных сведениях, указанных в Статье 30, оценку и надлежащие гарантии, указанные во втором подпараграфе параграфа 1 настоящей Статьи.

Статья 50
Международное сотрудничество для защиты персональных данных

В том, что касается третьих стран и международных организаций, Европейская Комиссия и надзорные органы должны принять соответствующие меры:

(a) для совершенствования механизмов международного сотрудничества в целях содействия эффективной реализации законодательства о защите персональных данных;

(b) для оказания международного взаимного содействия при реализации законодательства о защите персональных данных, в том числе посредством уведомления, передачи жалоб на рассмотрение, помощи в расследовании и обмена информацией, при наличии соответствующих гарантий для защиты персональных данных и других основных прав и свобод;

(c) для привлечения соответствующих заинтересованных лиц к участию в обсуждениях и деятельности, направленной на содействие международному сотрудничеству при реализации

законодательства о защите персональных данных;

(d) для содействия обмену и документальному оформлению законодательства и установившейся практики в области защиты персональных данных, включая судебные конфликты с третьими странами.

Глава VI
Независимые надзорные органы

Раздел 1
Независимый статус

Статья 51
Надзорный орган

1. Каждое государство-член ЕС должно предусмотреть один или несколько независимых органов государственной власти, ответственных за мониторинг применения настоящего Регламента, для защиты основных прав и свобод физических лиц при обработке данных и для содействия свободному движению персональных данных в Союзе ("надзорный орган").

2. Каждый надзорный орган должен способствовать согласованному применению настоящего Регламента на территории всего Союза. Для указанной цели надзорные органы должны сотрудничать друг с другом и с Европейской Комиссией в соответствии с Главой VII.

3. В случае если в государстве-члене ЕС учреждено более одного надзорного органа, указанное государство-член ЕС должно определить надзорный орган, который должен будет представлять указанные органы в Совете, и установить механизм обеспечения соблюдения другими органами правил, связанных с механизмом сопоставимости согласно Статье 63.

4. Каждое государство-член ЕС не позднее 25 мая 2018 г. должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно принимает согласно настоящей Главе, а также незамедлительно о любых последующих изменениях указанных положений.

Статья 52
Независимость

1. Каждый надзорный орган должен быть полностью независим при выполнении своих задач и осуществлении своих полномочий в соответствии с настоящим Регламентом.

2. Член или члены каждого надзорного органа при выполнении своих задач и осуществлении своих полномочий в соответствии с настоящим Регламентом не должны подвергаться прямому или косвенному воздействию внешних факторов, а также не должны ни стремиться получить, ни получать указания от кого бы то ни было.

3. Член или члены каждого надзорного органа должны воздерживаться от любых действий, несовместимых с их обязанностями, и в течение срока действия полномочий не должны участвовать в любой другой несовместимой с их полномочиями оплачиваемой или неоплачиваемой деятельности.

4. Каждое государство-член ЕС должно гарантировать, что каждый надзорный орган обеспечен кадровыми, техническими или финансовыми ресурсами, помещениями и инфраструктурой, необходимой ему для эффективного выполнения задач и осуществления полномочий, в том числе в рамках взаимной помощи, сотрудничества и участия в Совете.

5. Каждое государство-член ЕС должно гарантировать, что каждый надзорный орган

выбирает и располагает собственным персоналом, который находится в непосредственном подчинении члена или членов соответствующего надзорного органа.

6. Каждое государство-член ЕС должно гарантировать, что каждый надзорный орган подлежит финансовому контролю, который не влияет на его независимость, и что он имеет отдельные, государственные, годовые бюджетные сметы, которые могут являться частью всего государственного или национального бюджета.

Статья 53
Общие условия для членов надзорного органа

1. Государства-члены ЕС должны гарантировать, что каждый член их надзорных органов утверждается посредством прозрачной процедуры:

- парламентом;
- правительством;
- главой государства; или
- независимым органом, на который возлагаются обязанности по назначению согласно законодательству государства-члена ЕС.

2. Каждый член должен обладать необходимыми для выполнения своих обязанностей и осуществления своих полномочий квалификациями, опытом и навыками, в частности, в области защиты персональных данных.

3. Обязанности члена должны заканчиваться с истечением срока действия его полномочий, с увольнением или обязательным выходом на пенсию в соответствии с законодательством государства-члена ЕС.

4. Член должен быть освобожден от должности только в случае серьезного нарушения дисциплины или если он больше не соблюдает условия, необходимые для выполнения обязанностей.

Статья 54
Правила учреждения надзорного органа

1. Каждое государство-член ЕС законодательно должно предусмотреть следующее:

(a) учреждение каждого надзорного органа;

(b) необходимые квалификации и условия для назначения члена каждого надзорного органа;

(c) правила и процедуры для назначения члена или членов каждого надзорного органа;

(d) срок полномочий члена или членов каждого надзорного органа не менее четырех лет; это не относится к первому назначению после 24 мая 2016 г., срок которого для части членов может быть меньше, если для защиты независимости надзорного органа необходима процедура дифференцированного назначения;

(e) вопрос о том, могут ли, и если да, как часто, член или члены каждого надзорного органа назначаться на новый срок;

(f) условия, регулирующие обязательства члена или членов и персонала каждого надзорного органа, запреты на несовместимые с указанными обязательствами действия, профессиональную деятельность и выплаты в течение и по окончании срока полномочий, а также правила, регулирующие прекращение службы.

2. Член или члены и персонал каждого надзорного органа в соответствии с законодательством Союза или государства-члена ЕС должны, как в течение, так и по окончании срока их полномочий, соблюдать профессиональную тайну относительно любой конфиденциальной информации, которая стала известна им в ходе выполнения задач или осуществления полномочий. В течение срока их полномочий указанная обязанность по соблюдению профессиональной тайны должна, в частности,

применяться в отношении нарушений настоящего Регламента, о которых сообщили физические лица.

Раздел 2
Компетенция, задачи и полномочия

Статья 55
Компетенция

1. Каждый надзорный орган отвечает за выполнение поставленных задач и осуществление предоставленных ему полномочий в соответствии с настоящим Регламентом на территории его собственного государства-члена ЕС.

2. Если обработка осуществляется органами государственной власти или частными организациями, действующими на основе пункта (c) или (e) Статьи 6(1), ответственным является надзорный орган соответствующего государства-члена ЕС. В указанном случае Статья 56 не применяется.

3. Надзорные органы не должны отвечать за контроль над обработкой данных, осуществляемой судами в рамках их судебных функций.

Статья 56
Компетенция главного надзорного органа

1. Без ущерба действию Статьи 55 надзорный орган центрального учреждения или единственного учреждения контролера или обрабатывающего данные лица должен выступать в качестве компетентного главного надзорного органа для трансграничной обработки, осуществляемой указанным контролером или обрабатывающим данные лицом в соответствии с процедурой, предусмотренной в Статье 60.

2. Путем частичного отступления от параграфа 1 каждый надзорный орган должен отвечать за рассмотрение поданных ему жалоб или возможных нарушений настоящего Регламента, если предмет относится только к учреждению в его государстве-члене ЕС или существенно влияет на субъекты данных только в его государстве-члене ЕС.

3. В случаях, указанных в параграфе 2 настоящей Статьи, надзорный орган должен незамедлительно проинформировать главный надзорный орган об указанном обстоятельстве. В течение трех недель после получения соответствующей информации главный надзорный орган должен принять решение о рассмотрении указанного дела в соответствии с процедурой, предусмотренной в Статье 60, принимая во внимание тот факт, находится ли учреждение контролера или обрабатывающего данные лица в государстве-члене ЕС, надзорный орган которого проинформировал его.

4. В случае если главный надзорный орган принимает решение о рассмотрении дела, должна применяться процедура согласно Статье 60. Надзорный орган, который проинформировал главный надзорный орган, может предоставить ему проект решения. Главный надзорный орган должен уделить внимание указанному проекту при подготовке проекта решения, указанного в Статье 60(3).

5. Если главный надзорный орган принимает решение не рассматривать дело, надзорный орган, который проинформировал главный надзорный орган, должен рассмотреть его согласно Статьям 61 и 62.

6. Главный надзорный орган должен являться единственным посредником контролера или обрабатывающего данные лица по вопросам, связанным с трансграничной обработкой, осуществляемой указанным контролером или обрабатывающим данные лицом.

Статья 57
Задачи

1. Без ущерба другим задачам, установленным в настоящем Регламенте, каждый надзорный орган на своей территории должен:

(a) контролировать и обеспечивать применение настоящего Регламента;

(b) содействовать информированности общества и пониманию рисков, норм, гарантий и прав в отношении обработки. Особое внимание необходимо уделять деятельности, касающейся детей;

(c) консультировать в соответствии с законодательством государства-члена ЕС, национальный парламент, правительство и другие институты и органы о законодательных и административных мерах, связанных с защитой прав и свобод физических лиц при обработке их данных;

(d) содействовать информированности контролеров и обрабатывающих данные лиц относительно их обязанностей согласно настоящему Регламенту;

(e) по запросу предоставить информацию любому субъекту данных относительно осуществления его прав согласно настоящему Регламенту и, в соответствующих случаях, сотрудничать в связи с этим с надзорными органами других государств-членов ЕС;

(f) рассматривать жалобы, поданные субъектом данных или органом, организацией или объединением в соответствии со Статьей 80, расследовать, в соответствующих случаях, предмет жалобы и в приемлемый срок проинформировать заявителя о ходе и результатах расследования, в частности, если необходимо дальнейшее расследование или сотрудничество с другим надзорным органом;

(g) сотрудничать с другими надзорными органами, включая обмен информацией и предоставление взаимной помощи, с тем, чтобы гарантировать согласованное применение и исполнение настоящего Регламента;

(h) проводить расследования относительно применения настоящего Регламента, в том числе на основании информации, предоставленной другим надзорным органом или органом государственной власти;

(i) контролировать соответствующие изменения, если они влияют на защиту персональных данных, в частности, разработку информационных и коммуникационных технологий и деловых практик;

(j) принимать стандартные договорные условия, указанные в Статье 28(8) и в пункте (d) Статьи 46(2);

(k) составить и вести список в отношении требования об оценке воздействия на защиту данных согласно Статье 35(4);

(l) консультировать относительно обработки данных, указанной в Статье 36(2);

(m) способствовать разработке норм поведения согласно Статье 40(1), давать заключение и утверждать указанные нормы поведения, которые обеспечивают соответствующие гарантии согласно Статье 40(5);

(n) способствовать установлению сертификационных механизмов защиты данных, а также печатей и маркировочных знаков для защиты данных согласно Статье 42(1) и утверждать критерии сертификации согласно Статье 42(5);

(o) в соответствующих случаях, проводить периодическую проверку выданных в соответствии со Статьей 42(7) сертификаций;

(p) составить и опубликовать критерии аккредитации органа по контролю за соблюдением норм поведения согласно Статье 41 и критерии аккредитации сертификационного органа согласно Статье 43;

(q) провести аккредитацию органа по контролю за соблюдением норм поведения согласно

Статье 41 и аккредитацию сертификационного органа согласно Статье 43;

(r) утвердить условия договора и положения, указанные в Статье 46(3);

(s) утвердить юридически обязывающие корпоративные правила согласно Статье 47;

(t) содействовать деятельность Совета;

(u) вести внутренний учет нарушений настоящего Регламента и мер, принятых в соответствии со Статьей 58(2); и

(v) выполнять иные задачи, связанные с защитой персональных данных.

2. Каждый надзорный орган должен облегчить подачу жалоб, указанных в пункте (f) параграфа 1, посредством таких мер, как предоставление формы для подачи жалобы, которая может заполняться электронным образом, не исключая других способов взаимодействия.

3. Выполнение задач каждого надзорного органа осуществляется на бесплатной основе для субъекта данных и, в соответствующих случаях, для инспектора по защите персональных данных.

4. В случае если запросы явно не обоснованы или чрезмерны, в частности, вследствие их повторяющегося характера, надзорный орган может взимать приемлемую плату на основе административных расходов или отказаться действовать на основании запроса. Надзорный орган должен нести бремя доказывания необоснованного или чрезмерного характера запроса.

Статья 58
Полномочия

1. Каждый надзорный орган должен располагать следующими следственными полномочиями:

(a) поручать контролеру и обрабатывающему данные лицу и, в соответствующих случаях, их представителю предоставить любую информацию, необходимую ему для выполнения его задач;

(b) проводить расследования в форме аудиторских проверок защиты данных;

(c) проводить проверку сертификаций, предоставленных согласно Статье 42(7);

(d) уведомить контролера или обрабатывающее данные лицо о предполагаемом нарушении настоящего Регламента;

(e) от контролера или обрабатывающего данные лица получить доступ ко всем персональным данным и всей информации, необходимой ему для выполнения его задач;

(f) получить доступ к любым помещениям контролера или обрабатывающего данные лица, включая оборудование и средства для обработки данных, в соответствии с процессуальным законодательством Союза или государства-члена ЕС.

2. Каждый надзорный орган должен располагать следующими корректирующими полномочиями:

(a) выдавать предупреждения контролеру или обрабатывающему данные лицу о том, что запланированная обработка данных может нарушать положения настоящего Регламента;

(b) делать предупреждения контролеру или обрабатывающему данные лицу, если обработка данных нарушила положения настоящего Регламента;

(c) требовать от контролера или обрабатывающего данные лица соблюдать запросы субъекта данных относительно осуществления его прав согласно настоящему Регламенту;

(d) потребовать от контролера или обрабатывающего данные лица привести процесс обработки данных в соответствие положениям настоящего Регламента, при необходимости, в установленном порядке и в установленный срок;

(e) потребовать от контролера сообщить субъекту данных об утечке персональных данных;

(f) наложить временное или окончательное ограничение на обработку данных, включая запрет;

(g) потребовать исправить или уничтожить персональные данные или ограничить обработку согласно Статьям 16, 17 и 18, а также уведомить об указанных мерах получателей, которым были

раскрыты персональные данные согласно Статье 17(2) и Статье 19;

(h) отменить сертификацию, или потребовать от сертификационного органа отменить сертификацию, предоставленную согласно Статьям 42 и 43, или потребовать от сертификационного органа не предоставлять сертификацию, если не соблюдаются требования для сертификации;

(i) наложить административный штраф в соответствии со Статьей 83 в дополнение к или вместо мер, указанных в настоящем параграфе, в зависимости от обстоятельств каждого отдельного случая;

(j) потребовать приостановить передачу данных получателю в третьей стране или международной организации.

3. Каждый надзорный орган должен располагать следующими разрешительными и консультативными полномочиями:

(a) консультировать контролера в соответствии с процедурой предварительной консультации, указанной в Статье 36;

(b) по собственной инициативе или по запросу выдавать национальному парламенту, правительству государства-члена ЕС или в соответствии с законодательством государства-члена ЕС другим институтам или органам, а также общественности заключения по любому вопросу, связанному с защитой персональных данных;

(c) разрешать обработку, указанную в Статье 36(5), если в соответствии с законодательством государства-члена ЕС требуется указанное предварительное разрешение;

(d) выдавать заключение и утверждать проект норм поведения согласно Статье 40(5);

(e) аккредитовывать сертификационные органы согласно Статье 43;

(f) выдавать сертификации и утверждать критерии сертификации в соответствии со Статьей 42(5);

(g) принимать стандартные условия по защите данных, указанные в Статье 28(8) и в пункте (d) Статьи 46(2);

(h) утверждать договорные условия, указанные в пункте (a) Статьи 46(3);

(i) разрешать административные договоренности, указанные в пункте (b) Статьи 46(3);

(j) утверждать юридически обязывающие корпоративные правила согласно Статье 47.

4. Полномочия, предоставленные надзорному органу согласно настоящей Статье, осуществляются при условии наличия соответствующих гарантий, включая эффективные средства судебной защиты и должную процедуру, установленную в законодательстве Союза или государства-члена ЕС в соответствии с Хартией.

5. Каждое государство-член ЕС должно законодательно предусмотреть, что его надзорный орган вправе довести до сведения органов судебной власти факт нарушения настоящего Регламента и, в соответствующих случаях, вправе начать или иным образом участвовать в судебном процессе в целях обеспечения исполнения положений настоящего Регламента.

6. Каждое государство-член ЕС может законодательно предусмотреть, что его надзорный орган должен обладать полномочиями, дополнительными к полномочиям, указанным в параграфах 1, 2 и 3. Выполнение указанных полномочий не влияет на эффективное осуществление Главы VII.

Статья 59
Отчеты о проделанной работе

Каждый надзорный орган подготавливает ежегодный отчет о проделанной работе, который может включать в себя перечень типов выявленных нарушений и принятых мер в соответствии со Статьей 58(2). Указанные отчеты должны передаваться национальному парламенту, правительству и другим органам, определенным законодательством государства-члена ЕС. Они должны быть доведены до сведения общественности, Европейской Комиссии и Совета.

Глава VII
Сотрудничество и сопоставимость

Раздел 1
Сотрудничество

Статья 60
Сотрудничество между главным надзорным органом и другими соответствующими надзорными органами

1. В стремлении достичь консенсуса главный надзорный орган должен сотрудничать с другими надзорными органами в соответствии с настоящей Статьей. Главный надзорный орган и соответствующие надзорные органы должны обмениваться друг с другом всей существенной информацией.

2. Главный надзорный орган всегда может запросить соответствующие другие надзорные органы о предоставлении взаимной помощи согласно Статье 61 и может проводить совместные действия согласно Статье 62, в частности, для осуществления расследований или мониторинга имплементации меры относительно контролера или обрабатывающего данные лица, учрежденных в другом государстве-члене ЕС.

3. Главный надзорный орган должен незамедлительно передать соответствующую информацию по делу другим надзорным органам. Он без промедления должен представить проект решения другим надзорным органам для их заключения и принять во внимание их мнение.

4. В случае если один из соответствующих надзорных органов в течение четырех недель после проведения консультации в соответствии с параграфом 3 настоящей Статьи высказывает существенное и мотивированное возражение против проекта решения, главный надзорный орган, если он не согласен с существенным и мотивированным возражением или считает, что возражение не существенно и не мотивировано, должен инициировать в отношении данного вопроса механизм сопоставимости, указанный в Статье 63.

5. В случае если главный надзорный орган соглашается с существенным и мотивированным возражением, он должен передать другим надзорным органам доработанный проект решения для их заключения. Указанный доработанный проект решения должен подлежать применению процедуры, указанной в параграфе 4, в течение двух недель.

6. Если ни один из других надзорных органов не возражает против проекта решения, который был представлен главным надзорным органом в течение срока, указанного в параграфах 4 и 5, главный надзорный орган и соответствующие надзорные органы считаются согласными с указанным проектом решения и должны быть им связаны.

7. Главный надзорный орган должен принять решение и уведомить о нем основное учреждение или единственное учреждение контролера или обрабатывающего данные лица, в соответствующих случаях, и проинформировать другие надзорные органы и Совет об указанном решении, включая краткое изложение фактов и оснований. Надзорный орган, которому была подана жалоба, должен проинформировать заявителя о решении.

8. Путем частичного отступления от параграфа 7, если жалоба отклонена или признана несостоятельной, надзорный орган, которому она была подана, должен утвердить решение и уведомить о нем заявителя и проинформировать контролера.

9. В случае если главный надзорный орган и соответствующие надзорные органы отклоняют или признают несостоятельной только часть жалобы и действуют в соответствии с другой ее частью, по каждой части дела необходимо принять отдельное решение. Главный надзорный орган должен вынести решение по части, касающейся действий в отношении контролера, должен уведомить о нем

основное учреждение или единственное учреждение контролера или обрабатывающего данные лица на территории своего государства-члена ЕС, а также должен проинформировать о нем заявителя; при этом надзорный орган заявителя должен вынести решение по части, касающейся отклонения жалобы или признания ее несостоятельной, и должен уведомить об этом заявителя и проинформировать контролера или обрабатывающее данные лицо.

10. После уведомления о решении главного надзорного органа согласно параграфам 7 и 9 контролер или обрабатывающее данные лицо должно принять необходимые меры, чтобы гарантировать соблюдение решения в отношении обработки данных во всех его учреждениях в Союзе. Контролер или обрабатывающее данные лицо должно уведомить о мерах, принятых в целях соблюдения решения, главный надзорный орган, который должен проинформировать другие соответствующие надзорные органы.

11. Если в исключительных обстоятельствах соответствующий надзорный орган имеет основания полагать, что существует острая необходимость действовать в целях защиты интересов субъектов данных, должна применяться неотложная процедура, указанная в Статье 66.

12. Главный надзорный орган и другие надзорные органы должны предоставлять друг другу информацию, необходимую согласно настоящей Статье, электронным способом, с использованием стандартизованного формата.

Статья 61
Взаимная помощь

1. Надзорные органы должны предоставлять друг другу соответствующую информацию и оказывать взаимную помощь в целях единообразной имплементации и применения настоящего Регламента; они должны принимать меры для эффективного сотрудничества друг с другом. Взаимная помощь, в частности, распространяется на информационные запросы и меры надзора, например, на запросы относительно предварительных консультаций и разрешений, а также относительно проведения проверок и расследований.

2. Каждый надзорный орган должен принять все соответствующие меры, чтобы незамедлительно и не позднее одного месяца после получения запроса дать на него ответ другому надзорному органу. Указанные меры могут включать в себя, в частности, передачу соответствующей информации о проведении расследования.

3. Запросы об оказании помощи должны содержать в себе всю необходимую информацию, включая цели и причины запроса. Переданная информация должна использоваться исключительно для цели, указанной в запросе.

4. Запрашиваемый надзорный орган должен отклонить запрос только в случае, если:

(a) он не обладает компетенцией относительно предмета запроса или относительно мер, которые он согласно запросу должен выполнить; или

(b) выполнение запроса может нарушить положения настоящего Регламента или законодательства Союза или государства-члена ЕС, под действие которого подпадает надзорный орган, получивший запрос.

5. Запрашиваемый надзорный орган должен проинформировать запрашивающий надзорный орган о результатах или, в соответствующих случаях, о ходе выполнения мер, принятых в ответ на запрос. Запрашиваемый надзорный орган должен предоставить причины отказа в выполнении запроса в соответствии с параграфом 4.

6. Запрашиваемый надзорный орган должен предоставлять информацию, требуемую другими надзорными органами, как правило, электронным способом, с использованием стандартизованного формата.

7. Запрашиваемый надзорный орган не должен взимать плату за действия, предпринятые им в соответствии с запросом о взаимной помощи. Надзорные органы могут согласовать правила по

возмещению друг другу в исключительных случаях особых затрат, возникших в результате предоставления взаимной помощи.

8. В случае если надзорный орган не предоставляет информацию, указанную в параграфе 5 настоящей Статьи, в течение месяца после получения запроса от другого надзорного органа, запрашивающий надзорный орган может принять временную меру на территории своего государства-члена ЕС в соответствии со Статьей 55(1). В указанном случае острая необходимость действия согласно Статье 66(1) требует срочного обязывающего решения Совета согласно Статье 66(2).

9. Европейская Комиссия посредством имплементационных актов может определить формат и процедуры взаимной помощи, указанной в настоящей Статье, а также формы электронного обмена информацией между надзорными органами и между надзорными органами и Советом, в частности, установить стандартизованный формат, указанный в параграфе 6 настоящей Статьи. Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки, указанной в Статье 93(2).

Статья 62
Совместные действия надзорных органов

1. Надзорные органы должны в соответствующих случаях проводить совместные действия, включая совместные расследования и совместные принудительные меры, в которых участвуют члены и персонал надзорных органов других государств-членов ЕС.

2. Если учреждения контролера или обрабатывающего данные лица находятся в нескольких государствах-членах ЕС или если обработка данных может существенно повлиять на значительное количество субъектов данных более чем в одном государстве-члене ЕС, надзорный орган каждого из указанных государств-членов ЕС вправе участвовать в совместных действиях. Надзорный орган, компетентный согласно Статье 56(1) или (4), должен пригласить надзорный орган каждого из указанных государств-членов ЕС принять участие в совместных действиях и должен незамедлительно дать ответ на запрос надзорного органа об участии.

3. Надзорный орган в соответствии с законодательством государства-члена ЕС и с разрешения оказывающего поддержку надзорного органа может наделить полномочиями, в том числе следственными полномочиями, участвующих в совместных действиях членов или персонал оказывающего поддержку надзорного органа, или постольку, поскольку это допустимо согласно законодательству государства-члена ЕС основного надзорного органа, может позволить членам или персоналу оказывающего поддержку надзорного органа осуществлять их следственные полномочия в соответствии с законодательством государства-члена ЕС оказывающего поддержку надзорного органа. Указанные следственные полномочия могут осуществляться только под руководством и в присутствии членов или персонала основного надзорного органа. Члены или персонал оказывающего поддержку надзорного органа подпадают под действие законодательства государства-члена ЕС основного надзорного органа.

4. Если в соответствии с параграфом 1 персонал оказывающего поддержку надзорного органа осуществляет свою деятельность в другом государстве-члене ЕС, государство-член ЕС основного надзорного органа должно взять на себя ответственность за их действия, в том числе финансовые обязательства за любой ущерб, причиненный в результате их деятельности, в соответствии с законодательством государства-члена ЕС, на территории которого они осуществляют свою деятельность.

5. Государство-член ЕС, на территории которого был причинен ущерб, должно устранить причиненный ущерб согласно условиям, применимым в отношении ущерба, причиненного его собственным персоналом. Государство-член ЕС оказывающего поддержку надзорного органа, персонал которого причинил ущерб любому лицу на территории другого государства-члена ЕС,

должно возместить указанному другому государству-члену ЕС в полном размере любую сумму, которую оно заплатило лицам, управомоченным от их имени.

6. Без ущерба осуществлению прав по отношению к третьим сторонам и за исключением параграфа 5 каждое государство-член ЕС в случае, предусмотренном в параграфе 1, должно отказаться от запрашиваемого возмещения от другого государства-члена ЕС относительно ущерба, указанного в параграфе 4.

7. В случае если совместные действия запланированы и надзорный орган в течение одного месяца не выполняет обязательство, установленное во втором предложении параграфа 2 настоящей Статьи, другие надзорные органы могут утвердить временную меру на территории своего государства-члена ЕС в соответствии со Статьей 55. В указанном случае острая необходимость действия согласно Статье 66(1) требует заключения или срочного обязывающего решения Совета согласно Статье 66(2).

Раздел 2
Сопоставимость

Статья 63
Механизм сопоставимости

В целях содействия единообразному применению настоящего Регламента в Союзе надзорные органы должны сотрудничать друг с другом и в соответствующих случаях с Европейской Комиссией в рамках указанного в настоящем Разделе механизма сопоставимости.

Статья 64
Заключение Совета

1. Совет должен дать свое заключение, если компетентный надзорный орган намерен утвердить одну из нижеследующих мер. В этой связи компетентный надзорный орган должен передать Совету проект решения, если он:

(a) направлен на утверждение перечня процессов обработки данных в соответствии с требованием об оценке воздействия на защиту данных согласно Статье 35(4);

(b) касается обстоятельства согласно Статье 40(7), а также вопроса относительно того, соответствует ли проект нормы поведения или ее изменение или расширение настоящему Регламенту;

(c) направлен на утверждение критериев для аккредитации органа согласно Статье 41(3) или сертификационного органа согласно Статье 43(3);

(d) направлен на определение стандартных условий защиты данных, указанных в пункте(d) Статьи 46(2) и в Статье 28(8);

(e) направлен на утверждение договорных условий согласно пункту (a) Статьи 46(3); или

(f) направлен на утверждение юридически обязывающих корпоративных правил в значении Статьи 47.

2. Любой надзорный орган, президиум Совета или Европейская Комиссия могут потребовать, чтобы любое дело общего применения или оказывающее воздействие в нескольких государствах-членах ЕС было изучено Советом в целях получения заключения, в частности, если компетентный надзорный орган не выполняет обязательства по оказанию взаимной помощи в соответствии со Статьей 61 или в отношении совместных действий в соответствии со Статьей 62.

3. В случаях, указанных в параграфах 1 и 2, Совет должен дать заключение по представленному ему на рассмотрение делу при условии, что он уже не дал своего заключения по

тому же самому делу. Указанное заключение должно быть принято в течение восьми недель простым большинством голосов членов Совета. Указанный срок может быть продлен еще на шесть недель с учетом сложности предмета рассмотрения. В отношении указанного в параграфе 1 проекта решения, направленного членам Совета в соответствии с параграфом 5, предполагается, что член, который не высказывает возражений в приемлемый срок, установленный Президиумом, согласен с проектом решения.

4. Надзорные органы и Европейская Комиссия незамедлительно должны передать Совету электронным способом, с использованием стандартизированного формата любую соответствующую информацию, в том числе в соответствующих случаях краткое изложение фактов, проект решения, основания для принятия необходимой меры, а также мнения других соответствующих надзорных органов.

5. Президиум Совета незамедлительно должен электронным способом проинформировать:

(a) членов Совета и Европейскую Комиссию о любой направленной ему соответствующей информации с использованием стандартизированного формата. Секретариат Совета при необходимости должен обеспечить перевод соответствующей информации; и

(b) надзорный орган, указанный в соответствующих случаях в параграфах 1 и 2, и Европейскую Комиссию о своем заключении и опубликовать его.

6. Компетентный надзорный орган не должен принимать проект решения, указанный в параграфе 1, в течение срока, указанного в параграфе 3.

7. Надзорный орган, указанный в параграфе 1, должен принять во внимание заключение Совета и в течение двух недель после получения заключения электронным способом, с использованием стандартизированного формата сообщить Президиуму Совета о том, оставит ли он проект решения без изменений или внесет в него изменения; в соответствующих случаях он должен передать измененный проект решения.

8. В случае если соответствующий надзорный орган в течение срока, указанного в параграфе 7 настоящей Статьи, информирует Президиум Совета о том, что он не намерен частично или полностью следовать заключению Совета, и указывает соответствующие причины, должна применяться Статья 65(1).

Статья 65
Решение Советом спорных вопросов

1. Для того чтобы в отдельных случаях гарантировать правильное и единообразное применение настоящего Регламента, Совет должен принять обязательное для исполнения решение в следующих случаях:

(a) если в случае, указанном в Статье 60(4), соответствующий надзорный орган высказал соответствующее и обоснованное возражение против проекта решения главного органа или главный орган отклонил указанное возражение по причине его несоответствия или необоснованности. Обязательное для исполнения решение должно касаться всех обстоятельств, которые являются предметом соответствующего и обоснованного возражения, в частности, вопросов относительно наличия нарушения настоящего Регламента;

(b) если имеются противоречивые точки зрения относительно того, какой из соответствующих надзорных органов отвечает за основное учреждение;

(c) если компетентный надзорный орган не требует заключения Совета в случаях, указанных в Статье 64(1), или не следует заключению Совета, предоставленному согласно Статье 64. В указанном случае любой соответствующий надзорный орган или Европейская Комиссия могут передать дело Совету.

2. Решение, указанное в параграфе 1, должно быть принято в течение одного месяца после передачи предмета дела на рассмотрение большинством в две трети голосов членов Совета.

Указанный срок может быть продлен еще на один месяц исходя из сложности предмета рассмотрения. Решение, указанное в параграфе 1, должно быть мотивированным и направлено в главный надзорный орган и всем соответствующим надзорным органам; оно должно быть обязательным для их исполнения.

3. Если Совет не смог принять решение в течение срока, указанного в параграфе 1, он должен принять свое решение в течение двух недель после истечения второго месяца, указанного в параграфе 2, простым большинством голосов членов Совета. При равенстве голосов членов Совета правом решающего голоса при принятии решения обладает его Президиум.

4. Соответствующие надзорные органы не должны принимать решение по существу вопроса, направленного в Совет согласно параграфу 1, в течение сроков, указанных в параграфах 2 и 3.

5. Президиум Совета должен незамедлительно уведомить о решении, указанном в параграфе 1, соответствующие надзорные органы. Он должен проинформировать о нем Европейскую Комиссию. Решение должно быть опубликовано на интернет-сайте Совета сразу после того, как надзорный орган уведомит об окончательном решении, указанном в параграфе 6.

6. Главный надзорный орган или, в соответствующих случаях, надзорный орган, которому была подана жалоба, должен принять свое окончательное решение на основании решения, указанного в параграфе 1 настоящей Статьи, незамедлительно и не позднее одного месяца, после того как Совет уведомил о своем решении. Главный надзорный орган или, в соответствующих случаях, надзорный орган, которому была подана жалоба, должен проинформировать Совет о дате, когда контролер или обрабатывающее данные лицо и субъект данных будут уведомлены о его окончательном решении. Окончательное решение надзорных органов должно быть принято согласно Статье 60(7), (8) и (9). Окончательное решение должно соотноситься с решением, указанным в параграфе 1 настоящей Статьи, и должно устанавливать, что решение, указанное в данном параграфе, будет опубликовано на интернет-сайте Совета в соответствии с параграфом 5 настоящей Статьи. К окончательному решению должно прилагаться решение, указанное в параграфе 1 настоящей Статьи.

Статья 66
Неотложная процедура

1. В исключительных обстоятельствах, если соответствующий надзорный орган считает, что существует острая необходимость в защите прав и свобод субъектов данных, он может, путем частичного отступления от механизма сопоставимости, указанного в Статьях 63, 64 и 65, или от процедуры, указанной в Статье 60, незамедлительно принять временные меры, порождающие юридические последствия на его собственной территории, с определенным сроком действия, который не должен превышать трех месяцев. Надзорный орган незамедлительно должен сообщить об указанных мерах и причинах для их принятия другим соответствующим надзорным органам, Совету и Европейской Комиссии.

2. В случае если надзорный орган принял меру согласно параграфу 1 и считает, что необходимо срочно принять окончательные меры, он может запросить неотложного заключения Совета или срочного обязательного решения Совета и указать причины запроса такого заключения или решения.

3. Любой надзорный орган может запросить Совет предоставить неотложное заключение или, в соответствующем случае, срочное обязательное решение, если компетентный надзорный орган не принял соответствующую меру, несмотря на то, что имелась острая необходимость в защите прав и свобод субъектов данных, и указать причины для запроса такого заключения или решения, в том числе в отношении указанной острой необходимости.

4. Путем частичного отступления от Статьи 64(3) и от Статьи 65(2) неотложное заключение или срочное обязательное решение согласно параграфам 2 и 3 настоящей Статьи должно быть

принято в течение двух недель простым большинством голосов членов Совета.

Статья 67
Обмен информацией

Европейская Комиссия может принимать имплементационные акты общего действия для того, чтобы определить порядок электронного обмена информацией между надзорными органами, а также между надзорными органами и Советом, в частности, стандартизированный формат, указанный в Статье 64.

Указанные имплементационные акты должны быть приняты в соответствии с процедурой проверки согласно Статье 93(2).

Раздел 3
Европейский совет по защите данных

Статья 68
Европейский совет по защите данных

1. Европейский совет по защите данных ("Совет") настоящим учреждается в качестве органа Союза и обладает правоспособностью.

2. Совет представлен его Президиумом.

3. В состав Совета входят глава одного надзорного органа каждого государства-члена ЕС и Европейский инспектор по защите персональных данных или их представители.

4. В случае если в государстве-члене ЕС более одного надзорного органа отвечают за мониторинг применения положений настоящего Регламента, в соответствии с законодательством указанного государства-члена ЕС должен быть назначен совместный представитель.

5. Европейская Комиссия вправе 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, указанных в Статье 65, Европейский инспектор по защите персональных данных имеет право голоса только в отношении решений, которые касаются принципов и правил, применяемых к институтам, органам, ведомствам и агентствам Союза, и которые по существу соответствуют принципам и правилам настоящего Регламента.

Статья 69
Независимость

1. Совет должен действовать независимо при выполнении своих задач и осуществлении своих полномочий согласно Статьям 70 и 71.

2. Без ущерба требованиям Европейской Комиссии, указанным в пункте (b) Статьи 70(1) и в Статье 70(2), Совет при выполнении своих задач и осуществлении своих полномочий не должен ни стремиться получить, ни получать указания от кого бы то ни было.

Статья 70
Задачи Совета

1. Совет должен гарантировать единообразное применение настоящего Регламента. В этой связи Совет должен по собственной инициативе или, в соответствующих случаях, по требованию Европейской Комиссии, в частности:

(a) контролировать и гарантировать правильное применение настоящего Регламента в случаях, предусмотренных в Статьях 64 и 65, без ущерба задачам национальных надзорных органов;

(b) консультировать Европейскую Комиссию по любому вопросу, связанному с защитой персональных данных в Союзе, включая любые предполагаемые изменения настоящего Регламента;

(c) консультировать Европейскую Комиссию относительно формата и процедур обмена информацией между контролерами, обрабатывающими данные лицами и надзорными органами в отношении юридически обязывающих корпоративных правил;

(d) издавать руководящие указания, рекомендации и стандарты передовой практики относительно процедур удаления ссылок на персональные данные, копий или реплик указанных данных с общедоступных служб связи согласно Статье 17(2);

(e) по собственной инициативе, по запросу одного из своих членов или по требованию Европейской Комиссии рассматривать любые вопросы, связанные с применением настоящего Регламента, и издавать руководящие указания, рекомендации и стандарты передовой практики в целях содействия единообразному применению настоящего Регламента;

(f) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа для дальнейшего определения критериев и условий для решений, основанных на формировании профиля, согласно Статье 22(2);

(g) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа для установления утечек персональных данных и определения неоправданной задержки в значении Статьи 33(1) и (2), а также в отношении особых обстоятельств, при которых контролер или обрабатывающее данные лицо должны уведомить об утечке персональных данных;

(h) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа относительно обстоятельств, при которых утечка персональных данных может привести к высокой степени риска для прав и свобод физических лиц согласно Статье 34(1);

(i) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа в целях дальнейшего определения критериев и требований для передачи персональных данных, основанной на юридически обязывающих корпоративных правилах контролера или обрабатывающего данные лица, а также на необходимых требованиях, гарантирующих защиту персональных данных субъектов данных согласно Статье 47;

(j) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа в целях дальнейшего определения критериев и требований относительно передачи персональных данных на основании Статьи 49(1);

(k) разрабатывать руководящие указания для надзорных органов относительно применения мер, указанных в Статье 58(1), (2) и (3), и установить административные штрафы согласно Статье 83;

(l) проверять практическое применение руководящих указаний, рекомендаций и стандартов передовой практики согласно пунктам (e) и (f);

(m) издавать руководящие указания, рекомендации и стандарты передовой практики в соответствии с пунктом (e) настоящего параграфа в отношении установления общих процедур для сообщений физических лиц о нарушениях настоящего Регламента согласно Статье 54(2);

(n) содействовать разработке норм поведения и установлению сертификационных механизмов защиты данных, печатей и маркировочных знаков для защиты данных согласно Статьям 40 и 42;

(o) осуществлять аккредитацию сертификационных органов и их регулярную проверку согласно Статье 43, а также вести открытый реестр аккредитованных органов согласно Статье 43(6) и аккредитованных контролеров и обрабатывающих данные лиц, учрежденных в третьих странах

согласно Статье 42(7);

(p) определить требования, указанные в Статье 43(3), в целях аккредитации сертификационных органов согласно Статье 42;

(q) представить Европейской Комиссии заключение относительно сертификационных требований, указанных в Статье 43(8);

(r) представить Европейской Комиссии заключение относительно графических обозначений, указанных в Статье 12(7);

(s) представить Европейской Комиссии заключение относительно оценки соответствия уровня защиты в третьей стране или в международной организации, включая оценку вопроса относительно того, что третья страна, территория, или один или несколько специфических секторов в указанной третьей стране, или международная организация больше не гарантирует соответствующий уровень безопасности. В этой связи Европейская Комиссия должна представить Совету всю необходимую документацию, в том числе переписку с правительством третьей страны, в отношении указанной третьей страны, территории или специфического сектора, или с международной организацией.

(t) выдавать заключения относительно проектов решений надзорных органов согласно механизму сопоставимости, указанному в Статье 64(1), относительно вопросов, переданных на рассмотрение согласно Статье 64(2), а также принимать обязательные для исполнения решения согласно Статье 65, в том числе в случаях, указанных в Статье 66;

(u) содействовать сотрудничеству, а также эффективному двустороннему и многостороннему обмену информацией и стандартами передовой практики между надзорными органами;

(v) содействовать общим программам обучения и 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 и практики по защите данных с органами по надзору за соблюдением законодательства о защите персональных данных по всему миру;

(x) выдавать заключения относительно норм поведения, разработанных на уровне Союза, согласно Статье 40(9); и

(y) вести общедоступный электронный реестр решений, принятых надзорными органами и судами по вопросам, обработанным в рамках механизма сопоставимости.

2. В случае если Европейской Комиссии требуется консультация Совета, она может указать предельно допустимый срок, с учетом срочности обстоятельства дела.

3. Совет должен передать свои заключения, руководящие указания, рекомендации и стандарты передовой практики Европейской Комиссии и комитету, указанному в Статье 93, а также опубликовать их.

4. В соответствующих случаях Совет должен проконсультировать заинтересованные стороны и дать им возможность в приемлемый срок сделать свои замечания. Без ущерба Статьи 76 Совет должен довести результаты консультации до всеобщего сведения.

Статья 71
Представление отчетов

1. Совет должен составить ежегодный отчет относительно защиты физических лиц при обработке данных в Союзе и, в соответствующих случаях, в третьих странах и международных организациях. Отчет должен быть обнародован и передан Европейскому Парламенту, Совету ЕС и Европейской Комиссии.

2. Ежегодный отчет должен включать в себя проверку практического применения руководящих указаний, рекомендаций и стандартов передовой практики, указанных в пункте (l)

Статьи 70(1), а также обязательных для исполнения решений, указанных в Статье 65.

Статья 72
Процедура

1. Если иное не установлено в настоящем Регламенте, Совет должен принимать решения простым большинством голосов своих членов.

2. Совет принимает свои правила процедуры большинством в две трети голосов своих членов и устанавливает свой собственный режим работы.

Статья 73
Президиум

1. Совет из числа своих членов простым большинством голосов должен выбрать председателя и двух заместителей председателя.

2. Срок полномочий председателя и двух его заместителей должен составлять пять лет; допускается их однократное переизбрание.

Статья 74
Задачи Президиума

1. Президиум должен выполнять следующие задачи:

(a) созывать совещания Совета и подготавливать их повестку дня;

(b) уведомить о решениях, принятых Советом согласно Статье 65, главный надзорный орган и соответствующие надзорные органы;

(c) гарантировать своевременное выполнение задач Совета, в частности, в отношении механизма сопоставимости согласно Статье 63.

2. Совет должен установить распределение задач между председателем и двумя его заместителями в правилах процедуры.

Статья 75
Секретариат

1. Совет должен располагать секретариатом, который обеспечивается Европейским инспектором по защите персональных данных.

2. Секретариат должен выполнять задачи только на основании указаний Президиума Совета.

3. Персонал Европейского инспектора по защите персональных данных, который участвует в осуществлении задач, возложенных на Совет настоящим Регламентом, подпадает под действие других обязанностей по представлению отчетов в качестве персонала, участвующего в выполнении задач, возложенных на Европейского инспектора по защите персональных данных.

4. В соответствующих случаях Совет и Европейский инспектор по защите персональных данных должны составить и опубликовать Протокол о взаимопонимании, имплементирующий настоящую Статью, определяющий условия их сотрудничества и применимый к персоналу Европейского инспектора по защите персональных данных, участвующему в осуществлении задач, возложенных на Совет настоящим Регламентом.

5. Секретариат должен предоставить Совету аналитическую, административную и логистическую поддержку.

6. Секретариат несет ответственность, в частности:
(a) за повседневную деятельность Совета;
(b) за общение между членами Совета, его Президиумом и Европейской Комиссией;
(c) за общение с другими институтами и общественностью;
(d) за использование электронных средств для внутренней и внешней связи;
(e) за перевод существенной информации;
(f) за подготовку и анализ результатов заседаний Совета;
(g) за подготовку, составление и публикацию заключений, решений об урегулировании спорных вопросов между надзорными органами и других документов, принятых Советом.

Статья 76
Конфиденциальность

1. Обсуждения Совета согласно его правилам процедуры должны носить конфиденциальный характер, если Совет сочтет это необходимым.
2. Доступ к документам, представленным на рассмотрение членам Совета, экспертам и представителям третьих сторон, должен регулироваться Регламентом (ЕС) 1049/2001 Европейского Парламента и Совета ЕС[22].

Глава VIII
Правовые средства защиты, ответственность и санкции

Статья 77
Право на подачу жалобы в надзорный орган

1. Без ущерба любому другому административному или судебному средству защиты каждый субъект данных должен обладать правом подачи жалобы в надзорный орган, в частности, в государстве-члене ЕС места его проживания, места работы или места предполагаемого нарушения, если субъект данных считает, что обработка относящихся к нему персональных данных нарушает настоящий Регламент.
2. Надзорный орган, в который была подана жалоба, должен проинформировать заявителя о ходе и результатах рассмотрения жалобы, в том числе о возможности судебной защиты согласно Статье 78.

Статья 78
Право на эффективное средство судебной защиты в отношении надзорного органа

1. Без ущерба любым другим административным или несудебным средствам защиты каждое физическое или юридическое лицо должно иметь право на эффективное средство судебной защиты в отношении касающегося его юридически обязательного решения надзорного органа.
2. Без ущерба любым другим административным или несудебным средствам защиты каждый субъект данных имеет право на эффективное средство судебной защиты, если надзорный орган, компетентный согласно Статьям 55 и 56, не рассматривает жалобу или не информирует субъекта данных в течение трех месяцев о ходе или результатах рассмотрения жалобы, поданной согласно Статье 77.
3. Производство в отношении надзорного органа должно быть передано в суд государства-члена ЕС, в котором учрежден надзорный орган.

4. Если производство инициировано в отношении решения надзорного органа, которому предшествовало заключение или решение Совета в рамках механизма сопоставимости, надзорный орган должен направить указанное заключение или решение в суд.

Статья 79
Право на эффективное средство судебной защиты в отношении контролера или обрабатывающего данные лица

1. Без ущерба любым другим применимым административным или несудебным средствам защиты, в том числе праву на подачу жалобы в надзорный орган согласно Статье 77, каждый субъект данных должен иметь право на эффективное средство судебной защиты, если он считает, что его права согласно настоящему Регламенту были нарушены в результате обработки его персональных данных с нарушением требований настоящего Регламента.

2. Производство в отношении контролера или обрабатывающего данные лица должно быть передано в суд государства-члена ЕС, в котором находится учреждение контролера или обрабатывающего данные лица. Другая возможность предусматривает, что указанное производство может быть передано в суд государства-члена ЕС, в котором постоянно проживает субъект данных, за исключением случаев, когда контролер или обрабатывающее данные лицо является органом государственной власти государства-члена ЕС, действующим при осуществлении общественных полномочий.

Статья 80
Представительство субъектов данных

1. Субъект данных вправе передать некоммерческому органу, организации или объединению, которые были основаны в соответствии с законодательством государства-члена ЕС, имеют уставные задачи в сфере общественного интереса, а также осуществляют деятельность в области защиты прав и свобод субъектов данных в отношении защиты их персональных данных, право подавать жалобу от его имени, осуществлять права, указанные в Статьях 77, 78 и 79, от его имени и осуществлять право на получение компенсации согласно Статье 82 от его имени в случаях, предусмотренных законодательством государства-члена ЕС.

2. Государства-члены ЕС могут предусмотреть, что любой орган, организация или объединение, указанные в параграфе 1 настоящей Статьи, независимо от поручения субъекта данных, имеет право подавать в указанном государстве-члене ЕС жалобу в надзорный орган, компетентный в соответствии со Статьей 77, и осуществлять права, указанные в Статьях 78 и 79, если он считает, что права субъектов данных согласно настоящему Регламенту были нарушены в результате обработки данных.

Статья 81
Приостановление производства по делу

1. В случае если суд соответствующей инстанции государства-члена ЕС обладает информацией относительно производства, касающегося того же самого предмета в отношении обработки тем же самым контролером или обрабатывающим данные лицом и находящегося на рассмотрении в суде другого государства-члена ЕС, он должен связаться с указанным судом в другом государстве-члене ЕС, для того чтобы подтвердить наличие указанного производства.

2. В случае, если производство, касающееся того же самого предмета в отношении обработки тем же самым контролером или обрабатывающим данные лицом находится на рассмотрении в суде

другого государства-члена ЕС, любой суд соответствующей инстанции, рассматривающий дело позже, может приостановить его производство.

3. В случае если дело находится в производстве суда первой инстанции, любой суд, рассматривающий дело позже, может также по заявлению одной из сторон отказаться от юрисдикции, если суд, рассматривающий дело первым, уполномочен рассматривать указанные дела и его законодательство 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, должно иметь право на получение компенсации от контролера или обрабатывающего данные лица за понесенный ущерб.

2. Любой контролер, участвующий в обработке, несет ответственность за ущерб, причиненный не соответствующей настоящему Регламенту обработкой. Обрабатывающее данные лицо несет ответственность за ущерб, причиненный обработкой, только если она не соответствовала обязательствам обрабатывающего данные лица согласно настоящему Регламенту или если оно действовало, выходя за рамки законных инструкций контролера, или вопреки им.

3. Контролер или обрабатывающее данные лицо освобождается от ответственности согласно параграфу 2, если он докажет, что он никоим образом не несет ответственность за событие, которое явилось причиной причинения ущерба.

4. Если более одного контролера или обрабатывающего данные лица, или и контролер и обрабатывающее данные лицо участвуют в одной и той же обработке данных и если они согласно параграфам 2 и 3 несут ответственность за любой ущерб, причиненный обработкой, каждый контролер или каждое обрабатывающее данные лицо несет ответственность за весь ущерб, для того чтобы гарантировать эффективную компенсацию субъекту данных.

5. Если контролер или обрабатывающее данные лицо полностью компенсировало в соответствии с параграфом 4 причиненный ущерб, указанный контролер или обрабатывающее данные лицо вправе требовать от других контролеров или обрабатывающих данные лиц, участвовавших в той же самой обработке, возврата части компенсации, соответствующей их части ответственности за ущерб в соответствии с условиями параграфа 2.

6. Судебное производство в отношении осуществления права на получение компенсации должно быть передано в суд, компетентный согласно законодательству государства-члена ЕС, указанному в Статье 79(2).

Статья 83
Общие условия для наложения административных штрафов

1. Каждый надзорный орган должен гарантировать, что наложение административных штрафов согласно настоящей Статье в отношении нарушений положений настоящего Регламента, указанных в параграфах 4, 5 и 6, в каждом отдельном случае должно быть эффективным, пропорциональным и должно оказывать сдерживающее воздействие.

2. В зависимости от обстоятельств каждого отдельного случая административные штрафы должны налагаться в дополнение к мерам или вместо мер, указанных в пунктах (a) - (h) и (j) Статьи 58(2). При решении вопроса относительно наложения административного штрафа и о его размере в каждом отдельном случае необходимо учитывать следующее:

(a) характер, тяжесть и продолжительность нарушения, принимая во внимание характер, объем и цели обработки, а также количество субъектов данных, интересы которых были затронуты

указанной обработкой, и размер причиненного им ущерба;

(b) преднамеренный или неосторожный характер нарушения;

(c) любые меры, принятые контролером или обрабатывающим данные лицом, для смягчения ущерба, причиненного субъектам данных;

(d) степень ответственности контролера или обрабатывающего данные лица, принимая во внимание технические и организационные меры, имплементированные согласно Статьям 25 и 32;

(e) любые существенные нарушения, ранее совершенные контролером или обрабатывающим данные лицом;

(f) степень сотрудничества с надзорным органом для устранения нарушения и смягчения возможных негативных последствий;

(g) категории персональных данных, затронутых нарушением;

(h) способ, посредством которого надзорному органу стало известно о нарушении, в частности, уведомили ли контролер или обрабатывающее данные лицо о нарушении, и если да, то в какой степени;

(i) в случае если ранее были предписаны указанные в Статье 58(2) меры в отношении контролера или обрабатывающего данные лица относительно того же самого предмета рассмотрения, соблюдение указанных мер;

(j) соблюдение утвержденных норм поведения согласно Статье 40 или утвержденных сертификационных механизмов согласно Статье 42; и

(k) любые другие отягчающие или смягчающие обстоятельства в деле, например, полученную материальную выгоду или предотвращенные убытки, прямо или косвенно возникшие в результате нарушения.

3. Если контролер или обрабатывающее данные лицо нарушают положения настоящего Регламента намеренно или по неосторожности в рамках одного и того же процесса обработки или в рамках взаимосвязанных процессов обработки, общий размер административного штрафа не должен превышать размер, установленный для самого тяжкого нарушения.

4. За нарушения следующих положений в соответствии с параграфом 2 должны налагаться административные штрафы в размере не более 10 000 000 Евро или в случае предприятия, в размере не более 2% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) обязанностей контролера и обрабатывающего данные лица согласно Статьям 8, 11, 25 - 39 и 42 и 43;

(b) обязанностей сертификационного органа согласно Статьям 42 и 43;

(c) обязанностей контролирующего органа согласно Статье 41(4).

5. За нарушения следующих положений в соответствии с параграфом 2 должны налагаться административные штрафы в размере не более 20 000 000 Евро или в случае предприятия, в размере не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) основных принципов обработки, в том числе условий для согласия в соответствии со Статьями 5, 6, 7 и 9;

(b) прав субъектов данных согласно Статьям 12 - 22;

(c) передачи персональных данных получателю в третьей стране или международной организации согласно Статьям 44 - 49;

(d) любых обязанностей согласно законодательству государства-члена ЕС, принятому в рамках Главы IX;

(e) несоблюдения требования или временного или окончательного ограничения на обработку или приостановление передачи данных надзорным органом согласно Статье 58(2) или отказ в предоставлении доступа в нарушение Статьи 58(1).

6. За невыполнение требования надзорного органа согласно Статье 58(2) должны в соответствии с параграфом 2 налагаться административные штрафы в размере не более 20 000 000

Евро или, в случае предприятия, в размере не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

7. Без ущерба корректирующим полномочиям надзорных органов согласно Статье 58(2) каждое государство-член ЕС может установить правила относительно того, могут ли и в какой степени административные штрафы налагаться на органы государственной власти и другие государственные органы, учрежденные в указанном государстве-члене ЕС.

8. На осуществление надзорным органом своих полномочий согласно настоящей Статье распространяются соответствующие процессуальные гарантии в соответствии с законодательством Союза и государства-члена ЕС, включая эффективные средства судебной защиты и надлежащую правовую процедуру.

9. В случае если правовая система государства-члена ЕС не предусматривает административные штрафы, настоящая Статья может применяться таким образом, что наложение штрафа инициируется компетентным надзорным органом, а штраф накладывается компетентными национальными судами, при этом гарантируется, что указанные средства правовой защиты являются эффективными и имеют воздействие, эквивалентное воздействию административных штрафов, налагаемых надзорными органами. В любом случае, налагаемые штрафы должны быть эффективными, пропорциональными и должны оказывать сдерживающее воздействие. Указанные государства-члены ЕС должны уведомить Европейскую Комиссию о положениях своего законодательства, которые они принимают согласно настоящему параграфу, до 25 мая 2018 г. и незамедлительно о любых последующих законодательных актах, о поправках или любых изменениях, затрагивающих указанные положения.

Статья 84
Санкции

1. Государства-члены ЕС могут установить правила об иных санкциях, применимых к нарушениям настоящего Регламента, в частности, к нарушениям, которые не подпадают под административные штрафы согласно Статье 83, и принять все меры, необходимые для обеспечения их имплементации. Указанные санкции должны быть эффективными, пропорциональными и должны оказывать сдерживающее воздействие.

2. Каждое государство-член ЕС должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно принимает согласно параграфу 1, до 25 мая 2018 г. и незамедлительно о любых изменениях, затрагивающих указанные положения.

Глава IX
Положения в отношении особых ситуаций обработки

Статья 85
Обработка и свобода выражения мнений и информации

1. Государства-члены ЕС законодательно должны согласовать право на защиту персональных данных в соответствии с настоящим Регламентом с правом на свободу выражения мнений и информации, включая обработку в журналистских целях, а также в научных, художественных и литературных целях.

2. Для обработки, осуществляемой в журналистских, научных, художественных и литературных целях, государства-члены ЕС должны предусмотреть исключения и частичные отступления от Главы II (принципы), Главы III (права субъекта данных), Главы IV (контролер и обрабатывающее данные лицо), Главы V (передача персональных данных третьим странам и

международным организациям), Главы VI (независимые надзорные органы), Главы VII (сотрудничество и сопоставимость) и Главы IX (особые ситуации обработки данных), если они необходимы для того, чтобы согласовать право на защиту персональных данных со свободой выражения мнений и информации.

3. Каждое государство-член ЕС должно уведомить Европейскую Комиссию о положениях своего законодательства, которые оно приняло согласно параграфу 2, и незамедлительно о любых последующих законодательных актах, о поправках или любых изменениях, затрагивающих указанные положения.

Статья 86
Обработка и доступ общественности к официальным документам

Персональные данные в официальных документах, находящихся в органах государственной власти, или правительственных учреждениях, или частных организациях для осуществления задачи в рамках общественного интереса, могут быть раскрыты органом или учреждением в соответствии с законодательством Союза или государства-члена ЕС, под действие которого подпадает орган государственной власти или учреждение, для того чтобы согласовать доступ общественности к официальным документам с правом на защиту персональных данных согласно настоящему Регламенту.

Статья 87
Обработка национального идентификационного номера

Государства-члены ЕС могут определить особые условия для обработки национального идентификационного номера или любого другого идентификатора общего назначения. В указанном случае национальный идентификационный номер или любой другой идентификатор общего назначения должен использоваться только при обеспечении соответствующих гарантий для прав и свобод субъекта данных согласно настоящему Регламенту.

Статья 88
Обработка в контексте занятости

1. Государства-члены ЕС могут законодательно или посредством коллективных договоров предусмотреть более специфичные правила для того, чтобы гарантировать защиту прав и свобод в отношении обработки персональных данных работников при выполнении должностных обязанностей, в частности в целях приема 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, защиты собственности работодателя или клиента, а также в целях осуществления связанных с занятостью индивидуальных или коллективных прав и гарантий и в целях прекращения трудовых отношений.

2. Указанные правила должны включать в себя приемлемые и конкретные меры, для того чтобы гарантировать человеческое достоинство, законные интересы и основные права субъекта данных, особенно в отношении прозрачности обработки, передачи персональных данных в рамках группы предприятий или группы компаний, задействованных в совместной экономической деятельности, а также в отношении мониторинга систем на рабочем месте.

3. Каждое государство-член ЕС должно уведомить Европейскую Комиссию об указанных положениях своего законодательства, которые оно приняло согласно параграфу 1, до 25 мая 2018 г. и

незамедлительно о любых последующих изменениях, затрагивающих указанные положения.

Статья 89
Гарантии и частичные отступления в отношении обработки в целях архивирования в интересах общества, в целях научного или исторического исследования или в статистических целях

1. На обработку в целях архивирования в интересах общества, в научных целях, в целях исторического исследования или в статистических целях должны распространяться соответствующие гарантии в отношении прав и свобод субъекта данных согласно настоящему Регламенту. Указанные гарантии должны обеспечивать наличие технических и организационных мер, в частности, для соблюдения принципа минимизации данных. Указанные меры могут включать в себя псевдонимизацию при условии, что указанные цели могут быть достигнуты таким образом. Если указанные цели могут быть достигнуты при дальнейшей обработке, которая не допускает или больше не допускает идентификацию субъектов данных, указанные цели должны достигаться таким образом.

2. В случае если персональные данные обрабатываются в научных целях, в целях исторического исследования или в статистических целях, в законодательстве Союза или государства-члена ЕС могут быть предусмотрены частичные отступления от прав, указанных в Статьях 15, 16, 18 и 21, в соответствии с условиями и гарантиями, указанными в параграфе 1 настоящей Статьи, постольку, поскольку указанные права могут сделать невозможным или серьезно сказаться на достижении особых целей, и указанные частичные отступления необходимы для достижения указанных целей.

3. В случае если персональные данные обрабатываются в целях архивирования в интересах общества, в законодательстве Союза или государства-члена ЕС могут быть предусмотрены частичные отступления от прав, указанных в Статьях 15, 16, 18, 19, 20 и 21, в соответствии с условиями и гарантиями, указанными в параграфе 1 настоящей Статьи, постольку, поскольку указанные права могут сделать невозможным или серьезно сказаться на достижении особых целей, и указанные частичные отступления необходимы для достижения указанных целей.

4. В случае если обработка, указанная в параграфах 2 и 3, служит в одно и то же время для другой цели, частичные отступления должны применяться только в отношении обработки для целей, предусмотренных в указанных параграфах.

Статья 90
Обязанность неразглашения тайны

1. Государства-члены ЕС могут принять особые правила для утверждения полномочий надзорных органов в значении пунктов (e) и (f) Статьи 58(1) в отношении контролеров и обрабатывающих данные лиц, которые согласно законодательству Союза или государства-члена ЕС или согласно правилам, установленным национальными компетентными органами, обязаны соблюдать профессиональную тайну или имеют иные эквивалентные обязанности неразглашения тайны, если это необходимо и пропорционально для согласования права на защиту персональных данных с обязанностью неразглашения тайны. Указанные положения должны применяться только в отношении персональных данных, которые контролер или обрабатывающее данные лицо получили в результате деятельности, которая подпадает под указанную обязанность неразглашения тайны.

2. Каждое государство-член ЕС должно уведомить Европейскую Комиссию о положениях, принятых согласно параграфу 1, до 25 мая 2018 г. и незамедлительно о любых последующих изменениях, затрагивающих указанные положения.

Статья 91
Существующие положения о защите данных церквей и религиозных организаций

1. В случае если церкви и религиозные организации или общины в государстве-члене ЕС в момент вступления в силу настоящего Регламента применяют исчерпывающие правила в отношении защиты физических лиц при обработке их данных, указанные правила могут применяться в дальнейшем, при условии их соответствия настоящему Регламенту.

2. Церкви и религиозные организации, которые применяют исчерпывающие правила в соответствии с параграфом 1 настоящей Статьи, подлежат надзору со стороны независимого надзорного органа, который может иметь специфический характер, при условии, что он соблюдает условия, установленные в Главе VI настоящего Регламента.

Глава X
Делегированные акты и имплементационные акты

Статья 92
Осуществление делегирования

1. Полномочие на принятие делегированных актов предоставляется Европейской Комиссии согласно условиям, установленным в настоящей Статье.

2. Делегирование полномочий, указанных в Статье 12(8) и в Статье 43(8), предоставляется Европейской Комиссии на неопределенный срок, начиная с 24 мая 2016 г.

3. Делегирование полномочий, указанных в Статье 12(8) и в Статье 43(8), может быть отменено в любое время Европейским Парламентом или Советом ЕС. Решение об отмене прекращает делегирование полномочий, определенных в указанном решении. Оно вступает в силу на следующий день после публикации решения в Официальном Журнале Европейского Союза или в более поздний срок, определенный в решении. Оно не влияет на действительность делегированных актов, которые уже вступили в силу.

4. Сразу же после принятия делегированного акта Европейская Комиссия должна уведомить об этом Европейский Парламент и Совет ЕС.

5. Делегированный акт, принятый согласно Статье 12(8) и Статье 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 об указанном акте или если до истечения указанного срока Европейский Парламент и Совет ЕС проинформировали Европейскую Комиссию о том, что они не будут представлять возражения. Указанный срок должен быть продлен на три месяца по инициативе Европейского Парламента или Совета ЕС.

Статья 93
Процедура Комитета

1. Европейской Комиссии должен оказывать содействие Комитет. Указанный Комитет должен являться комитетом в значении Регламента (ЕС) 182/2011.

2. В случае если делается ссылка на настоящий параграф, применяется Статья 5 Регламента (ЕС) 182/2011.

3. В случае если делается ссылка на настоящий параграф, применяется Статья 8 Регламента (ЕС) 182/2011 совместно со Статьей 5 указанного Регламента.

Глава XI
Заключительные положения

Статья 94
Отмена Директивы 95/46/ЕС

1. Директива 95/46/ЕС отменяется 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 Статьей 29 Директивы 95/46/ЕС, должны рассматриваться как ссылки на Европейский совет по защите данных, учрежденный настоящим Регламентом.

Статья 95
Соотношение с Директивой 2002/58/ЕС

Настоящий Регламент не должен налагать дополнительные обязательства на физических и юридических лиц при обработке в сочетании с положением об общедоступных электронных услугах связи в сетях связи общего пользования в Союзе по вопросам, по которым у них есть специальные обязательства, установленные в Директиве 2002/58/ЕС и преследующие одну и ту же цель.

Статья 96
Соотношение с уже заключенными соглашениями

Международные соглашения, касающиеся передачи персональных данных третьим странам или международным организациям, которые государства-члены ЕС заключили до 24 мая 2016 г. и которые соответствуют законодательству Союза, применявшемуся до указанной даты, должны сохранять свою силу до тех пор, пока они не будут изменены, заменены 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 пересмотре настоящего Регламента в Европейский Парламент и Совет ЕС. Отчет должен быть опубликован.

2. В рамках оценки и пересмотра согласно параграфу 1 Европейская Комиссия должна проверить, в частности, применение и действие:

(a) Главы V о передаче персональных данных третьим странам или международным организациям, в особенности, с учетом решений, принятых согласно Статье 45(3) настоящего Регламента, и решений, принятых на основе Статьи 25(6) Решения 95/46/ЕС;

(b) Главы VII о сотрудничестве и сопоставимости.

3. Для цели параграфа 1 Европейская Комиссия может запрашивать информацию у государств-членов ЕС и надзорных органов.

4. При выполнении оценки и пересмотра согласно параграфам 1 и 2 Европейская Комиссия должна учесть позиции и выводы Европейского Парламента, Совета ЕС и других соответствующих органов или источников.

5. Европейская Комиссия, при необходимости, должна внести соответствующие предложения по изменению настоящего Регламента, в частности, с учетом развития информационных технологий и в свете прогресса в информационном обществе.

Статья 98
Пересмотр других правовых актов о защите данных

Европейская Комиссия, при необходимости, должна внести законодательные предложения по изменению других правовых актов о защите персональных данных, для того чтобы гарантировать единообразную и последовательную защиту физических лиц при обработке данных. В частности, это касается норм о защите физических лиц при обработке данных институтами, органами, службами и агентствами Союза, а также норм о свободном обращении указанных 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 ЕС.

Совершено в Брюсселе 27 апреля 2016 г.

От имени Европейского Парламента

Председатель
M. Schulz

От имени Совета ЕС
Председатель
J.A. Hennis-Plasschaert

---

[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) (Text with EEA relevance) Опубликован в Официальном Журнале (далее - ОЖ) N L 119, 04.05.2016, стр. 1 - 88.

[2] ОЖ N C 229, 31.07.2012, стр. 90.

[3] ОЖ N C 391, 18.12.2012, стр. 127.

[4] Позиция Европейского Парламента от 12 марта 2014 г. (еще не опубликована в ОЖ) и позиция Совета ЕС при первом чтении от 8 апреля 2016 г. (еще не опубликована в ОЖ). Позиция Европейского Парламента от 14 апреля 2016 г.

[5] Директива 95/46/ЕС Европейского Парламента и Совета ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (ОЖ N L 281, 23.11.1995, стр. 31).

[6] Рекомендация Европейской Комиссии от 6 мая 2003 г. относительно определения микропредприятий, малых и средних предприятий (C(2003) 1422) (ОЖ N L 124, 20.05.2003, стр. 36).

[7] Регламент (ЕС) 45/2001 Европейского Парламента и Совета ЕС от 18 декабря 2000 г. о защите физических лиц при обработке персональных данных, осуществляемой институтами и органами Сообщества и о свободном обращении таких данных (ОЖ N L 8, 12.01.2001, стр. 1).

[8] Директива (ЕС) 2016/680 Европейского Парламента и Совета ЕС от 27 апреля 2016 г о защите физических лиц

при обработке персональных данных компетентными органами в целях предупреждения, расследования, выявления уголовных преступлений или привлечения к ответственности, или приведения в исполнение уголовных наказаний, и о свободном движении таких данных и отмене Рамочного Решения 2008/977/ПВД Совета ЕС (см. стр. 89 настоящего ОЖ).

[9] 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) (ОЖ N L 178, 17.07.2000, стр. 1).

[10] Директива 2011/24/ЕС Европейского Парламента и Совета ЕС от 9 марта 2011 г. о правах пациентов в трансграничном медицинском обслуживании (ОЖ N L 88, 04.04.2011, стр. 45).

[11] Директива 93/13/ЕЭС Совета ЕС от 5 апреля 1993 г. о несправедливых условиях в договорах с потребителями (ОЖ N L 95, 21.04.1993, стр. 29).

[12] Регламент (ЕС) 1338/2008 Европейского Парламента и Совета ЕС от 16 декабря 2008 г. о статистике Сообщества в отношении общественного здравоохранения и безопасности на рабочих местах (ОЖ N L 354, 31.12.2008, стр. 70).

[13] Регламент (ЕС) 182/2011 Европейского Парламента и Совета ЕС от 16 февраля 2011 г., устанавливающий правила и общие принципы механизмов контроля со стороны государств-членов ЕС за осуществлением Европейской Комиссией имплементационных полномочий (ОЖ N L 55, 28.02.2011, стр. 13).

[14] 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 (ОЖ N L 351, 20.12.2012, стр. 1).

[15] Директива 2003/98/ЕС Европейского Парламента и Совета ЕС от 17 ноября 2003 г. о вторичном использовании информации публичного сектора (ОЖ N L 345, 31.12.2003, стр. 90).

[16] 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 (ОЖ N L 158, 27.05.2014, стр. 1).

[17] Регламент (ЕС) 223/2009 Европейского Парламента и Совета ЕС от 11 марта 2009 г. о Европейской статистике и об отмене Регламента (ЕС, Евратом) 1101/2008 Европейского Парламента и Совета ЕС о передаче данных при условии соблюдения их конфиденциальности Статистическому бюро Европейских Сообществ, Регламента (ЕС) 322/97 Совета ЕС о статистике Сообщества, а также Решения 89/382/ЕЭС Совета ЕС, Евратома об учреждении комитета по статистическим программам Европейских Сообществ (ОЖ N L 87, 31.03.2009, стр. 164).

[18] ОЖ N C 192, 30.06.2012, стр. 7.

[19] 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) (ОЖ N L 201, 31.07.2002, стр. 37).

[20] 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 (ОЖ N L 241, 17.09.2015, стр. 1).

[21] 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 (ОЖ N L 218, 13.08.2008, стр. 30).

[22] 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 (ОЖ N L 145, 31.05.2001, стр. 43).