

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)

▶Глава I. Общие положения

Статья 1. Предмет и цели

Статья 2. Фактическая сфера применения

Статья 3. Территориальное действие

Статья 4. Определения

▶Глава II. Принципы

Статья 5. Принципы, связанные с обработкой персональных данных

Статья 6. Законность обработки

Статья 7. Условия для согласия

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

Статья 9. Обработка особых категорий персональных данных

Статья 10. Обработка персональных данных, касающихся уголовных приговоров и преступлений

Статья 11. Обработка, не требующая идентификации соответствующего лица

▶Глава III. Права субъекта данных

▶Раздел 1. Прозрачность и условия

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

▶Раздел 2. Информация и доступ к персональным данным

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

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

Статья 15. Право субъекта данных на доступ к данным

▶Раздел 3. Внесение исправлений и удаление информации

Статья 16. Право на внесение исправлений

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

Статья 18. Право на ограничение обработки

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

Статья 20. Право на переносимость данных

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

Статья 21. Право на возражение

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

▶▶Раздел 5. Ограничения

Статья 23. Ограничения

▶▶Глава IV. Контролер и лицо, обрабатывающее данные

▶▶Раздел 1. Общие обязательства

Статья 24. Ответственность контролера

Статья 25. Защита данных по умолчанию и на основе продуманных действий

Статья 26. Контролеры, осуществляющие совместную обработку

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

Статья 28. Лицо, обрабатывающее данные

Статья 29. Обработка от имени контролера или обрабатывающего данные лица

Статья 30. Учетные сведения об обработке данных

Статья 31. Сотрудничество с надзорным органом

▶▶Раздел 2. Безопасность персональных данных

Статья 32. Безопасность обработки

Статья 33. Уведомление надзорного органа об утечке персональных данных

Статья 34. Информирование субъекта данных об утечке персональных данных

▶▶Раздел 3. Оценка воздействия на защиту данных и предварительная консультация

Статья 35. Оценка воздействия на защиту данных

Статья 36. Предварительная консультация

▶▶Раздел 4. Инспектор по защите персональных данных

Статья 37. Назначение инспектора по защите персональных данных

Статья 38. Положение инспектора по защите персональных данных

Статья 39. Задачи инспектора по защите персональных данных

▶▶Раздел 5. Нормы поведения и сертификация

Статья 40. Нормы поведения

Статья 41. Мониторинг утвержденных норм поведения

Статья 42. Сертификация

Статья 43. Сертификационные органы

▶▶Глава V. Передача персональных данных третьим странам или международным организациям

Статья 44. Общие принципы передачи

Статья 45. Передача на основании решения о соответствии

Статья 46. Передача при условии соблюдения соответствующих гарантий

Статья 47. Юридически обязывающие корпоративные правила

Статья 48. Передача или раскрытие данных, не разрешенное законодательством Союза

Статья 49. Частичное отступление для определенных случаев

Статья 50. Международное сотрудничество для защиты персональных данных

▶▶Глава VI. Независимые надзорные органы

▶▶Раздел 1. Независимый статус

Статья 51. Надзорный орган

Статья 52. Независимость

Статья 53. Общие условия для членов надзорного органа

Статья 54. Правила учреждения надзорного органа

▶▶Раздел 2. Компетенция, задачи и полномочия

Статья 55. Компетенция

Статья 56. Компетенция главного надзорного органа

Статья 57. Задачи

Статья 58. Полномочия

Статья 59. Отчеты о проделанной работе

▶▶Глава VII. Сотрудничество и сопоставимость

▶▶Раздел 1. Сотрудничество

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

Статья 61. Взаимная помощь

Статья 62. Совместные действия надзорных органов

▶▶Раздел 2. Сопоставимость

Статья 63. Механизм сопоставимости

Статья 64. Заключение Совета

Статья 65. Решение Советом спорных вопросов

Статья 66. Неотложная процедура

Статья 67. Обмен информацией

▶ Раздел 3. Европейский совет по защите данных

Статья 68. Европейский совет по защите данных

Статья 69. Независимость

Статья 70. Задачи Совета

Статья 71. Представление отчетов

Статья 72. Процедура

Статья 73. Президиум

Статья 74. Задачи Президиума

Статья 75. Секретариат

Статья 76. Конфиденциальность

▶ Глава VIII. Правовые средства защиты, ответственность и санкции

Статья 77. Право на подачу жалобы в надзорный орган

Статья 78. Право на эффективное средство судебной защиты в отношении надзорного органа

Статья 79. Право на эффективное средство судебной защиты в отношении контролера или обрабатывающего данные лица

Статья 80. Представительство субъектов данных

Статья 81. Приостановление производства по делу

Статья 82. Право на компенсацию и ответственность

Статья 83. Общие условия для наложения административных штрафов

Статья 84. Санкции

▶ Глава IX. Положения в отношении особых ситуаций обработки

Статья 85. Обработка и свобода выражения мнений и информации

Статья 86. Обработка и доступ общественности к официальным документам

Статья 87. Обработка национального идентификационного номера

Статья 88. Обработка в контексте занятости

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

Статья 90. Обязанность неразглашения тайны

Статья 91. Существующие положения о защите данных церквей и религиозных организаций

▶ Глава X. Делегированные акты и имплементационные акты

Статья 92. Осуществление делегирования

Статья 93. Процедура Комитета

▶ Глава XI. Заключительные положения

Статья 94. Отмена Директивы 95/46/ЕС

Статья 95. Соотношение с Директивой 2002/58/ЕС

Статья 96. Соотношение с уже заключенными соглашениями

Статья 97. Отчеты Европейской Комиссии

Статья 98. Пересмотр других правовых актов о защите данных

Статья 99. Вступление в силу и применение

(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 вопросам²,

На основании заключения Комитета регионов³,

Действуя в соответствии с обычной законодательной процедурой⁴,

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 ЕС⁵ 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) ТФЕУ 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 данных 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.

(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 ЕС7 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 ЕС8. 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, подпадает 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 судебской 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 ЕС9, 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 реальное 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 данным 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 ЕС10 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 личного 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 ЕС11 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 преваляют 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 ЕС12 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 онлайн-услугу, 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 онлайн-служб и в случае онлайн-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 осуществления 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 архивирования 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 онлайн-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 безопасности 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 находящиеся 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 наднациональном 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 обработке 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 судебской 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 ЕС¹³ 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 преобладают 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 Союзе 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 содержатся 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 ЕС14, 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 качестве 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 ЕС15 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 ЕС16.

(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 ЕС17 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 заключение¹⁸.

(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 ЕС¹⁹ 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:

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 С 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).

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)

Регламент адресован государствам-членам Европейского Союза. Российская Федерация членом ЕС не является.

Настоящий Регламент вступает в силу на двадцатый день после своего опубликования в Официальном Журнале Европейского Союза

Настоящий Регламент должен применяться с 25 мая 2018 г.