УТВЕРЖДАЮ
Генеральный директор ООО «Маткласс»
Пинчук Т.В.
ОГРН 1167746352916

Приказ № 178-1
от «16» мая 2017 г.

Генеральный директор

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

РЕДАКЦИЯ 1

2017 год

1. Общие положения

1.1. Настоящим Положением (далее также «Политика») определяется порядок обращения с персональными данными Клиентов или иных Контрагентов ООО «Маткласс», ОГРНИП 1167746352916 (далее – соответственно «Клиенты или иные Контрагенты» (либо «Клиент или иной Контрагент») и «Маткласс»).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Общества в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные при осуществлении коммерческой деятельности, в том числе, при проведении мастер-классов и осуществлении иных услуг и правоотношений.

1.3. Персональные данные Клиентов или иных Контрагентов – любая информация, относящаяся к конкретному Клиенту или иному Контрагенту (субъекту персональных данных) и необходимая Маткласс в связи с осуществлением Маткласс, указанной выше коммерческой деятельности.

1.4. Сведения о персональных данных Клиентов или иных Контрагентов относятся к числу конфиденциальных (составляющих охраняемую законом тайну Маткласс). Режим конфиденциальности в отношении персональных данных снимается:

в случае их обезличивания;

по истечении 75 лет срока их хранения;

в других случаях, предусмотренных федеральными законами.

2. Основные понятия. Состав персональных данных Клиентов или иных Контрагентов

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

обработка персональных данных Клиента и иного Контрагента – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

распространение персональных данных – действия, направленные на раскрытие персональных данных Клиентов или иных Контрагентов неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

предоставление персональных данных – действия, направленные на раскрытие персональных данных Клиентов или иных Контрагентов определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

блокирование персональных данных – временное прекращение обработки персональных данных Клиентов или иных Контрагентов (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных Клиентов или иных Контрагентов и (или) в результате которых уничтожаются материальные носители персональных данных (п. 8 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному Клиенту и иному Контрагенту (п. 9 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ);

информация – сведения (сообщения, данные) независимо от формы их представления;

документированная информация – зафиксированная на материальном носителе путем документирования

информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Информация, представляемая Клиентом и иным Контрагентом при инициации вышеуказанных правоотношений с Маткласс должна иметь документальную форму.

При заключении гражданско-правовых договоров, в том числе, на оказание услуг (например, по проведению мастер-класса и т.п.), включая случаи присоединения к Офертам Маткласс, Клиенты или иные Контрагенты предоставляют следующую свою информацию:

- фамилия, имя (в том числе, в качестве ИП, представителя ИП или юридического лица);
- ИНН, ОГРНИП (при наличии);
- контактный адрес;
- контактный e-mail;
- контактный номер телефона (для связи).

3. Обработка персональных данных

3.1. Источником информации обо всех персональных данных Клиента или иного Контрагента является непосредственно Клиент или иной Контрагент соответственно. Если персональные данные возможно получить только у третьей стороны, то Клиент или иной Контрагент должен быть заранее в письменной форме уведомлен об этом, и от него должно быть получено письменное согласие. Матклacс обязана сообщить Клиенту или иному Контрагенту о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа Клиента или иного Контрагента дать письменное согласие на их получение.

3.2. Матклacс не имеет права получать и обрабатывать персональные данные Клиента или иного Контрагент о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В соответствие со ст. 24 Конституции РФ МАТКЛАСС вправе получать и обрабатывать данные о частной жизни Клиента или иного Контрагента только с его письменного согласия.

3.3. Обработка персональных данных Клиентов или иных Контрагентов Матклacс возможна без согласия первых в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья Клиента или иного Контрагента, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия Клиента или иного Контрагента невозможно;
- по требованию полномочных государственных органов – в случаях, предусмотренных федеральным законом.

3.4. Матклacс вправе обрабатывать персональные данные Клиентов или иных Контрагентов только с их письменного согласия.

3.5. Письменное согласие Клиента или иного Контрагента на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Данным согласием Клиент (или иной Контрагент) также дает свое согласие на обработку и использование Матклacс предоставленной Клиентом (или иным Контрагентом) информации и (или) их персональных данных с целью осуществления по указанному Клиентом (или иным Контрагентом) контактному телефону и (или) контактному электронному адресу информационной рассылки (о Мероприятиях Матклacс) и/или рекламной рассылки об услугах Матклacс и/или партнера Матклacс

3.6. Согласие Клиента или иного Контрагента не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона,

устанавливающего цель обработки, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия Маткласс в качестве Контрагента указанных лиц;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов, если получение его согласия невозможно.

3.7. Клиент или иной Контрагент представляет в соответствующие подразделения (либо установленным контрагентам) Маткласс сведения о себе. Данные подразделения (либо установленные контрагенты) ИП Маткласс проверяют достоверность сведений. При изменении персональных данных Клиент или иной Контрагент письменно уведомляет Маткласс о таких изменениях в разумный срок, но не превышающий 14 календарных дней с момента появлений таких изменений.

3.8. В соответствии с законом в целях обеспечения прав и свобод человека и гражданина Маткласс и его законные, полномочные представители при обработке персональных данных Клиента или иного Контрагента должны выполнять следующие общие требования:

3.8.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов или иных правовых актов, содействия Клиентам или иным Контрагентам в удовлетворении их потребностей в получении соответствующих услуг, обеспечения личной безопасности Клиента или иного Контрагента, обеспечения сохранности имущества.

3.8.2. При определении объема и содержания обрабатываемых персональных данных Маткласс должна руководствоваться Конституцией РФ и иными федеральными законами.

3.8.3. При принятии решений, затрагивающих интересы Клиентов или иных Контрагентов, Маткласс не имеет права основываться на персональных данных, полученных о Клиентах или иных Контрагентах исключительно в результате их автоматизированной обработки или электронного получения.

3.8.4. Защита персональных данных Клиентов или иных Контрагентов от неправомерного их использования, утраты обеспечивается Маткласс за счет ее средств в порядке, установленном федеральным законом.

3.8.5. Клиенты или иные Контрагенты и их представители должны быть ознакомлены (с сохранением доказательств такого ознакомления) с документами Маткласс, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.8.6. Во всех случаях отказ Клиентов или иных Контрагентов от своих прав на сохранение и защиту тайны недействителен.

4. Передача персональных данных

4.1. При передаче персональных данных Клиента или иного Контрагента Маткласс. соблюдает следующие требования:

4.1.1. Не сообщать персональные данные Клиента или иного Контрагент третьей стороне без письменного согласия данного Клиента или иного Контрагента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Клиента или иного Контрагента, а также в случаях, установленных федеральным законом.

4.1.2. Не сообщать персональные данные Клиента или иного Контрагента в коммерческих целях без его письменного согласия. Обработка персональных данных Клиентов или иных Контрагентов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные Клиентов или иных Контрагентов, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные Клиентов или иных Контрагентов, обязаны соблюдать режим секретности (конфиденциальности). Федеральными законами могут быть установлены иные правила обмена персональными данным (в том числе, Клиентов или иных Контрагентов), чем те, что установлены настоящим Положением.

4.1.4. Осуществлять передачу персональных данных Клиентов или иных Контрагентов в пределах Маткласс в соответствии с настоящим Положением.

4.1.5. Разрешать доступ к персональным данным Клиентов или иных Контрагентов только специально

уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать информацию о состоянии здоровья Клиента или иного Контрагента, за исключением тех сведений, которые относятся к вопросу о реализации вышеуказанных правоотношений между Маткласс и соответствующим Клиентом или иным Контрагентом.

4.1.7. Передавать персональные данные Клиента или иного Контрагента его законным, полномочным представителям в порядке, установленном законом, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

4.2. Персональные данные Клиентов или иных Контрагентов обрабатываются и хранятся в бухгалтерии или у лица, осуществляющего данные функции по гражданско-правовому договору.

4.3. Персональные данные Клиентов или иных Контрагентов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

4.4. При получении персональных данных не от соответствующего Клиента или иного Контрагента (за исключением случаев, если персональные данные являются общедоступными) Маткласс до начала обработки таких персональных данных обязана предоставить Клиенту или иному Контрагенту следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральными законами права субъекта персональных данных.

5. Доступ к персональным данным Клиентов или иных Контрагентов

5.1. Право доступа к персональным данным Клиентов или иных Контрагентов имеют (при наличии таковых):

- Маткласс;
- работники отдела персонала Маткласс;
- работники бухгалтерии Маткласс;
- руководитель юридического отдела Маткласс;
- работники секретариата (информация о фактическом месте проживания и контакты Клиентов или иных Контрагентов);
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только тех Клиентов или иных Контрагентов, с которыми связана деятельность данного подразделения);
- сам Клиент или иной Контрагент, носитель данных.
- иные специально уполномоченные лица (при этом указанные лица должны иметь право получать только те персональные данные Клиента или иного Контрагента, которые необходимы для выполнения конкретных функций).

Перечень лиц, имеющих доступ к персональным данным Клиентов или иных Контрагентов, определяется приказом Маткласс.

5.2. Клиент или иной Контрагент Маткласс имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные.

5.2.2. Требовать от Маткласс уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Маткласс персональных данных.

5.2.3. Получать от Маткласс:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе, сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.4. Требовать извещения Маткласс всех лиц, которым ранее были сообщены неверные или неполные

персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Маткласс при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных Клиента или иного Контрагента разрешается исключительно в служебных целях с письменного разрешения начальника отдела бухгалтерии (или руководителя иного лица, осуществляющего функции бухгалтерии по гражданско-правовому договору.

5.4. Передача информации третьей стороне возможна только при письменном согласии Клиента или иного Контрагента.

6. Защита персональных данных

6.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Маткласс

6.4. Защита персональных данных Клиентов или иных Контрагентов от неправомерного их использования или утраты должна быть обеспечена Маткласс за счет ее средств, в порядке, установленном федеральным законом.

6.5. «Внутренняя защита» персональных данных.

6.5.1. Для обеспечения внутренней защиты персональных данных Клиентов или иных Контрагентов необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников (контрагентов, исполнителей, подрядчиков) Маткласс, функциональные обязанности (обязательства) которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками (контрагентами, исполнителями, подрядчиками) Маткласс;
- рациональное размещение рабочих мест работников Маткласс, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работниками (контрагентами, исполнителями, подрядчиками) Маткласс требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников Маткласс, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения Маткласс;
- воспитательная и разъяснительная работа с сотрудниками подразделения Маткласс по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.6. «Внешняя защита» персональных данных.

6.6.1. Для внешней защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и другое.

6.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Маткласс, посетители, и т.п. лица. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе бухгалтерии.

6.6.3. Для обеспечения внешней защиты персональных данных Клиентов или иных Контрагентов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- требования к защите информации при интервьюировании и собеседованиях.

6.7. По возможности персональные данные обезличиваются.

6.8. Кроме мер защиты персональных данных, установленных законодательством, Маткласс, Клиенты или иных Контрагенты и их представители могут вырабатывать совместные меры защиты персональных данных Клиентов или иных Контрагентов.

7. Ответственность за нарушение норм, регулирующих обработку персональных данных

7.1. Работники (контрагенты, исполнители, подрядчики)Маткласс, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами (в зависимости от статуса указанных лиц: то есть, в зависимости от того, являются ли они работниками либо иными указанными лицами).

7.2. Маткласс за нарушение порядка обращения с персональными данными несет административную ответственность согласно ст. 5.39 КоАП РФ, а также возмещает Клиенту или иному Контрагенту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом Клиенте или ином Контрагенте.

Приложение № 1 от 16.05.2017 г.
к Положению ООО «Матклacс
о защите персональных данных
от «16» мая 2017 г.

ООО «Матклacс» (далее – «Матклacс») приняла настоящее Приложение № 1 от 25.05.2018 г. к Положению Матклacс о защите персональных данных от «16» мая 2016 г. в связи с вступлением в силу 25.05.2018 года следующего документа - Регламент General Data Protection Regulation (GDPR) Европейского Союза О защите физических лиц относительно обработки персональных данных и о свободном перемещении таких данных (Общий Регламент по защите персональных данных), далее «Регламент».

Матклacс признает действие указанного Регламента, в частности, Матклacс признает следующие нормы Регламента, применительно к своей деятельности.

«Преамбула»

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

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

3. Исходя из того, что сама по себе доступность веб-сайта контролёра, обработчика или посредника в Евросоюзе, адреса электронной почты или иных контактных данных, либо использование языка, обычно используемого в третьей стране, в которой учреждён контролёр, являются недостаточными для установления подобных намерений, признаки, среди которых использование языка или валюты, обычно используемой в одном или нескольких государствах-членах, с возможностью заказывать товары и услуги на этом языке, либо упоминание потребителей или пользователей, которые находятся в Евросоюзе, могут делать очевидным то, что контролёр намерен предлагать товары или услуги субъектам данных в Евросоюзе (предложение 3 п. 23 Преамбулы).

4. Обработка персональных данных субъектов данных, находящихся в Евросоюзе, контролёром или обработчиком, которые не учреждены в Евросоюзе, также является предметом регулирования настоящего Регламента, когда это связано с мониторингом действий таких субъектов данных, постольку, поскольку их действия совершаются на территории Евросоюза (предложение первое п. 2.4 Преамбулы).

5. Принципы защиты данных должны применяться к любой информации, касающейся идентифицированного или идентифицируемого физического лица. Личные данные, подвергнутые псевдонимации, которые могут быть соотнесены с физическим лицом посредством использования дополнительной информации, следует рассматривать как информацию об идентифицируемом физическом лице. Для того, чтобы определить, идентифицируемо ли физическое лицо, следует учитывать все средства, которые могут быть достоверно с большей вероятностью быть использованы, к примеру – выявление, либо контролёром, либо иным лицом для того, чтобы идентифицировать физическое лицо прямо

или косвенно. Чтобы установить используются ли средства с достаточной степенью вероятности для идентификации физического лица, учитывать следует все объективные факторы, в том числе расходы и количество времени, необходимое для идентификации, принимая во внимание имеющиеся технологические возможности на момент обработки, а также развитие технологий. В силу этого принципы защиты данных не применяются к анонимной информации, т.е. к информации, не относящейся к идентификации физического лица или с помощью которой идентифицируется физическое лицо, или не относится к персональным данным, предоставленных анонимно (обезличено) таким способом, что субъект данных не идентифицируется или не поддаётся идентификации. Настоящий Регламент не распространяется по этой причине на обработку такой анонимной информации, в том числе для статистических или исследовательских целей (п. 26 Преамбулы).

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

7. Дети нуждаются в особой защите в отношении их персональных данных, поскольку они в меньшей степени осведомлены о рисках, последствиях и соответствующих средствах защиты, а также их правах в отношении обработки персональных данных. Такие особые меры защиты должны, в частности, применяться к использованию персональных данных детей в целях маркетинга или создания персонального или пользовательского профилей и сбора персональных данных, связанных с детьми при использовании услуг, предлагаемых непосредственно ребёнку. Согласие лиц, обладающих родительской ответственностью, не является необходимым в контексте превентивных мероприятий или консультационных услуг, предоставляемых непосредственно ребёнку (п. 38 Преамбулы).

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

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

данное добровольно, если у субъекта персональных данных нет действительного или свободного выбора или не в состоянии без ущерба отказаться или отозвать своё согласие (п. 42 Преамбулы).

10. Обработка персональных данных в целях, отличных от тех, для которых персональные данные первоначально собирались, должна быть разрешена только, если она соответствует целям, для которых персональные данные были изначально получены. В этом случае не требуется иное правовое основание, отдельное от того, посредством которого был разрешено осуществлять сбор персональных данных. Для того чтобы убедиться в том, соответствует ли цель дальнейшей обработки цели, для которой персональные данные были первоначально получены, Контролёр, после выполнения всех требований относительно законности первоначальной обработки, должен принять во внимание, в числе прочего, следующее: любую связь между указанными целями и целями запланированной дальнейшей обработки; контекст, в котором были получены персональные данные, в частности, разумные ожидания субъектов данных, основанные на отношении с контролёром, касающиеся их дальнейшего использования; характер персональных данных; последствия предполагаемой дальнейшей обработки для субъектов данных, и наличие соответствующих гарантий первоначальной и предполагаемой обработки (предложения 1. 2. 6 пункта 50 Преамбулы).

11. Такие персональные данные не должны обрабатываться за исключением случаев, когда обработка разрешена в конкретных случаях, предусмотренных настоящим Регламентом, принимая во внимание, что право государств-членов может установить конкретные положения о защите данных, чтобы адаптировать применение норм Регламента в отношении соблюдения правовых обязательств или выполнения задачи, осуществляемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контролёра (предложение 4 п. 51 Преамбулы).

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

13. Должны быть предусмотрены условия для содействия осуществления прав субъекта данных на основании настоящего Регламента, включая механизмы для запроса и, когда это применимо, бесплатно получать, в частности, доступ и исправление или удаление персональных данных и осуществление права на возражение (п. 59 Преамбулы).

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

15. Субъект данных должен иметь право доступа к относящимся к нему/к ней собранным персональным данным, это право должно осуществляться беспрепятственно и с определённой периодичностью в целях получения информации об обработке и проверки правомерности обработки. Это охватывает право субъектов данных на доступ к данным, касающихся их здоровья, например, данным в их медицинских документах, содержащих следующую информацию: диагнозы, результаты обследований, наблюдения лечащих врачей и сведения о любом лечении или вмешательствах. Каждый субъект данных должен, поэтому иметь право знать и получать сведения в отношении целей, для которых обрабатываются персональные данные, по возможности, в отношении срока, в течение которого обрабатываются данные, получателей персональных данных, алгоритма схемы любой автоматизированной обработки персональных данных и последствий такой обработки, если она как минимум основана на составлении профиля. При наличии соответствующей возможности контролёр должен обеспечить удалённый доступ к защищённой системе, которая даст субъекту данных прямой доступ к его/ее персональным данным. Указанное право не должно отрицательно влиять на права или свободы иных лиц, включая коммерческую тайну или результаты интеллектуальной деятельности и, в частности, авторское право на программное обеспечение. При этом такие ограничения не должны вести к отказу на предоставление всей информации субъекту данных. В том случае, когда контролёр обрабатывает большое количество информации, касающейся субъекта данных, он должен иметь возможность до передачи информации запросить субъекта данных уточнить информацию или вид обработки, к которому относится запрос (п. 61 Преамбулы).

16. Контролёр должен использовать все приемлемые способы для того, чтобы проверить и подтвердить личность субъекта данных, который запрашивает доступ, в частности, в рамках онлайновых служб и в случае

онлайновых идентификаторов. Контролёр не должен сохранять персональные данные только для реагирования на потенциальный запрос (п. 64 Преамбулы).

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

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

19. В автоматизированных системах учёта ограничение обработки в принципе должно обеспечиваться техническими средствами таким образом, чтобы персональные данные не подвергались дальнейшей обработке и не могли быть изменены. Тот факт, что обработка персональных данных ограничена, должен быть ясно указан в системе (учёта) (предложения 2 и 3 п. 67 Преамбулы).

20. Для усиления контроля над его/ее в случае, когда обработка персональных данных осуществляется при помощи автоматизированных средств, субъект данных может также получить персональные данные, относящиеся к нему/к ней, которые он/она предоставил контролёру, в структурированном, широко используемом, машиночитаемом и функционально совместимом формате, и передать их другому контролёру (предложение 1 п. 68 Преамбулы).

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

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

23. Субъект данных должен иметь право не подчиняться действию решения, которое может включать в себя меры по оценке личных аспектов, относящихся к нему/к ней, которая основана исключительно на автоматизированной обработке и которая порождает правовые последствия для него/неё или аналогичным образом существенно влияет на него/неё, например, автоматический отказ от онлайн-заявки на получение кредита или практики электронного найма персонала без какого-либо вмешательства человека. В любом случае такая обработка должна осуществляться в соответствии с надлежащими гарантиями, включающими конкретное информирование субъекта данных и право на вмешательства человека, чтобы выразить свою точку зрения, получить объяснение решения, принятого после такой оценки, а также оспорить это решение (предложения 1, 4 п. 70 Преамбулы).

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

25. Защита прав и свобод физических лиц в отношении обработки персональных данных требует принятия надлежащих технических и организационных мер для того, чтобы требования настоящего Регламента были выполнены.

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

26. Если контролёр или обработчик, не учреждённые в Евросоюзе, обрабатывают персональные данные находящихся в Евросоюзе субъектов данных и если их деятельность по обработке связана с предложением товаров и услуг этим субъектам данных в Евросоюзе, вне зависимости от того, требуется ли оплата от субъекта данных, либо связана с мониторингом их деятельности постольку, поскольку она осуществляется в Евросоюзе, контролёр или обработчик должны назначить представителя, за исключением случаев, когда обработка носит случайный характер, не включает в себя масштабную обработку конкретных категорий персональных данных, либо обработка персональных данных, связанных с уголовными приговорами и правонарушениями, едва ли обернётся рисками для прав и свобод физических лиц, с учётом характера, обстоятельств, сферы применения и целей обработки, или если контролёр является органом или учреждением государственной власти (предложение 1 п. 80 Преамбулы).

27. Для обеспечения соблюдения требований настоящего Регламента в отношении обработки, осуществляемой обработчиком от имени контролёра, в случаях, когда на обработчика возложена деятельность по обработке, контролёр должен использовать обработчика, предоставляющего соответствующие гарантии, в частности, в отношении экспертной осведомлённости, добросовестности и источников информации, для того чтобы применять технические и организационные меры, которые будут отвечать требованиям настоящего Регламента, в том числе в отношении безопасности обработки. Следование обработчика утверждённым кодексам поведения или утверждённым механизмам сертификации, может быть использовано в качестве показателя для подтверждения соблюдения обязанностей контролёра (предложение 1, 2 п. 81 Преамбулы).

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

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

30. В целях улучшения соблюдения положений настоящего Регламента, в случаях, когда возможными последствиями обработки данных являются риски высокой степени для прав и свобод физических лиц, контролёр должен нести ответственность за проведение оценки воздействия на защиту данных для того, чтобы определить, в частности, происхождение, характер, специфику и степень опасности такого риска. Результаты оценки должны приниматься во внимание при определении соответствующих мер, которые необходимо принять для подтверждения того, что обработка персональных данных соответствует настоящему Регламенту. В тех случаях, когда оценка воздействия на защиты данных указывает на то, что обработка данных связана с высоким риском, который контролёр не может смягчить с помощью соответствующих мер с точки зрения имеющихся технологий и затрат на реализацию, перед обработкой следует проконсультироваться с надзорным органом (п. 84 Преамбулы).

31. Поэтому, как только контролёру станет известно об утечке персональных данных, контролёр должен незамедлительно уведомить об утечке персональных данных надзорный орган, без неоправданной задержки и, когда это возможно, не позднее чем через 72 часа после того, как ему стало известно об этом, за исключением случаев, когда контролёр может доказать в соответствии с принципом подотчётности, что утечка персональных данных едва ли обернётся рисками для прав и свобод физических лиц. Если такое уведомление не может быть сделано в течение 72 часов, причины задержки должны быть указаны в уведомлении, а информация может предоставляться поэтапно без неоправданной дальнейшей задержки (предложения 2, 3 п. 85 Преамбулы).

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

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

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

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

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

37. Каждый субъект данных должен иметь право подать жалобу в один надзорный орган, в частности в государстве-члене его обычного места жительства, а также право на эффективные средства судебной защиты в соответствии со статьёй 47 Хартии Европейского Союза об основных правах, если субъект данных считает, что его/ее права на основании настоящего Регламента нарушены или когда надзорный орган не действует по жалобе, частично или полностью отклоняет жалобу или отказывает в ее удовлетворении, или не действует, когда такая мера необходима для защиты прав субъекта данных. Рассмотрение по жалобе должно проводиться при условии судебного пересмотра в той мере, в какой это уместно в конкретном случае. Надзорный орган в приемлемый срок должен проинформировать субъекта данных о ходе и результатах рассмотрения жалобы. Если дело требует дальнейшего расследования или сотрудничества с другим надзорным органом, субъекту данных должна быть представлена промежуточная информация. В целях содействия рассмотрению жалобы каждый надзорный орган должен принять такие меры, как предоставление формы жалобы, которая может быть заполнена электронным способом, не исключая других средств связи (п. 146 Преамбулы).

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

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

40. Контролёр или обработчик должны компенсировать любой ущерб, который лицо может понести в результате обработки, нарушающей настоящий Регламент. Контролёр или обработчик освобождается от ответственности, если он докажет, что он никоим образом не несёт ответственность за ущерб (предложения 1, 2 п. 146 Преамбулы).

41. Для того, чтобы усилить обязательность соблюдения норм настоящего Регламента, санкции, в том числе административные штрафы, должны налагаться за любое нарушение настоящего Регламента, в дополнение или вместо соответствующих мер, налагаемых надзорным органом согласно настоящему Регламенту. Однако следует принимать во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения нанесенного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролёра или обработчика, соблюдение кодексов поведения, а также любые иные отягчающие или смягчающие вину обстоятельства (предложения 1, 3 п. 148 Преамбулы).

4.2. любом случае налагаемые штрафы должны быть эффективными, соразмерными и оказывать сдерживающее воздействие (предложения 4 п. 151 Преамбулы).

ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1
Предмет и цели

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

2. Настоящий Регламент защищает основные права и свободы физических лиц, и, в частности, их право на защиту персональных данных (из п. 1, 2 статьи 1 Регламента).

Статья 2
Понятийно-терминологическая основа

Для целей настоящего Регламента:

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

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

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

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

«согласие» (*consent*) – субъекта данных означает любое свободно данное, конкретное, осознанное и однозначное идентифицируемое желание субъекта данных, посредством которого он/она путем заявления, либо ясным утвердительным действием, выражает согласие на обработку персональных данных, относящихся к нему/к ней (из пунктов 1, 2, 7, 8, 11 статьи 5 Регламента).

ГЛАВА II. ПРИНЦИПЫ

Статья 3

Принципы, связанные с обработкой персональных данных

1. Персональные данные должны:

(a) обрабатываться на законных основаниях, справедливым и открытым образом в отношении субъекта данных («правомерность, справедливость и открытость/траспаренность» – *lawfulness, fairness and transparency*);

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

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

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

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

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

2. Контролёр несет ответственность и должен быть способен подтвердить соблюдение требований параграф 1 статьи ст. 5 Регламента («подотчетность» – *accountability*) (из статьи ст. 5 Регламента)

Статья 4

Существенные условия относительно согласия

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

3. Субъект данных должен иметь право в любое время отозвать его/ее согласие. Отзыв согласия не должен влиять на правомерность обработки, основанной на согласии до его отзыва. Отзыв согласия не влияет на правомерность обработки, основанной на согласия до отзыва согласия. Прежде чем давать согласие, субъект данных должен быть проинформирован об этом. Процедура отзыва согласия должна быть такой же простой, как и процедура предоставления согласия (из статьи 7 Регламента).

Статья 5

Обработка особых категорий персональных данных

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

2. Параграф 1 не применяется, если применимо одно из положений, изложенных в п. 2 ст. 9 Регламента (из п.п. 1. 2 статьи 9 Регламента).

Статья 6

Обработка, не требующая идентификации

2. Когда, в случаях, предусмотренных в параграфе 1 ст. 11 Регламента, контролёр способен подтвердить, что он не в состоянии идентифицировать субъекта данных, контролёр должен соответственно проинформировать субъекта данных, при наличии соответствующей возможности. В таких случаях Статьи 15-20 Регламента не применяются, за тем исключением, когда субъект данных для осуществления его/ее прав, согласно указанным Статьям, предоставляет дополнительную информацию, которая обеспечивает его/ее идентификацию (из п. 2. ст. 11 Регламента).

ГЛАВА III.

ПРАВА СУБЪЕКТА ДАННЫХ

Раздел 1 ТРАСПАРЕНТНОСТЬ/ПРОЗРАЧНОСТЬ И МЕТОДЫ

Статья 7

Прозрачность информации, сообщения и методы осуществления прав субъектов данных

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

2. Контролёр должен предоставить информацию о действиях, предпринятых по запросу в соответствии со Статьям 15-22 Регламента, субъекту данных, без неоправданных задержек, и в любом случае в течение одного месяца после получения такого запроса. Этот срок может быть продлен еще на два месяца, при необходимости, принимая во внимание сложность и количество запросов.

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

4. Информация, предоставляемая в соответствии со Статьями 13 и 14 Регламента, а также любые сообщения и любые действия, предпринятые в соответствии со Статьями 15-22 и 34 Регламента предоставляются бесплатно. В случае,

если запросы от субъекта данных являются явно не обоснованными или чрезмерными, в частности, вследствие их повторяющегося характера, контролёр может либо:

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

(b) отказаться действовать в соответствии с этим запросом.

Контролёр несет бремя доказывания явной необоснованности запроса или чрезмерного характера этих запросов ((из ст. 12 Регламента).

Раздел 2

ИНФОРМАЦИЯ И ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Статья 8

Предоставляемая информация при сборе персональных данных от субъекта данных

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

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

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

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

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

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

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

2. В дополнение к информации, предусмотренной параграфом 1 ст. 13 Регламента, контролёр должен, в момент получения персональных данных, предоставить дополнительно субъекту данных следующую информацию, необходимую для обеспечения справедливой и прозрачной обработки:

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

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

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

(d) о праве подачи жалобы в надзорный орган;

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

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

3. В случае, если контролёр намерен в дальнейшем обрабатывать персональные данные в иных целях, чем те, для которых персональные данные были получены, этот контролёр должен, до начала такой дальнейшей обработки, предоставить субъекту данных информацию относительно этой иной цели, а также любую дополнительную информацию, согласно параграфу 2 ст. 13 Регламента.

4. Параграфы 1, 2 и 3 ст. 13 Регламента не применимы в случаях, если субъект данных уже располагает соответствующей информацией (из ст. 13 Регламента).

Статья 9

Предоставляемая информация при получении персональных данных не от субъекта данных

1. В случае если персональные данные получены не от субъекта данных, контролёр должен предоставить субъекту данных информацию в соответствие с пунктом 1 Регламента (из ст. 14 Регламента).

Статья 10

Право субъекта данных на доступ к данным

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

(a) о цели обработки;

(b) о соответствующих категориях обрабатываемых персональных данных;

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

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

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

(f) о праве подачи жалобы в надзорный орган;

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

(h) о применении автоматизированного способа принятия решения, в том числе, составление профиля, согласно Статье 22 (1) и (4) Регламента, а также, по крайней мере в этих случаях, достоверной информации об имеющем место алгоритме, также как о значимости и предполагаемых последствиях обработки для субъекта данных (из ст. 15 Регламента).

Раздел 3

ИСПРАВЛЕНИЕ И УДАЛЕНИЕ ДАННЫХ

Статья 11

Право на исправление данных

Субъект данных вправе потребовать от контролёра без неоправданной задержки исправления неточных персональных данных, касающихся его/ее. Принимая во внимание цели обработки, субъект данных должен иметь право дополнить неполные персональные данные, в том числе путем предоставления дополнительного заявления (из ст. 16 Регламента).

Статья 12

Право на удаление данных («право на забвение»)

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

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

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

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

(d) персональные данные были обработаны неправомерно;

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

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

2. В случае, если контролёр обнародовал персональные данные, а он обязан, согласно параграфу 1 ст. 13 Регламента, удалить эти персональные данные, контролёр, учитывая имеющиеся технологические возможности и расходы на исполнение, должен предпринять обоснованные меры, включая технические меры, чтобы проинформировать контролёров, обрабатывающих персональные данные, о том, что субъект данных затребовал от таких контролёров удаления любых ссылок на такие персональные данные, или их копирование или тиражирование.

3. Параграфы 1 и 2 ст. 17 Регламента не применяются в тех случаях, когда обработка необходима:

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

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

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

(d) для архивных целей в общественных интересах, научных или исторических исследовательских целях, либо для статистических целей в соответствии со статьей 89 (1) Регламента, постольку, поскольку право, предусмотренное в параграфе 1 ст. 17 Регламента, может сделать невозможным или отрицательно отразиться на достижении целей такой обработки; или

(e) для предъявления, исполнения или защиты правовых притязаний (из ст. 17 Регламента).

Статья 13

Право на ограничение обработки

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

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

позволяющего контроллеру проверить точность персональных данных;

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

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

(d) субъект данных возражал против обработки в соответствии со Статьей 21 (1) Регламента, ожидая удостоверения того, преобладают ли правовые основания контролёра таким правовым основаниям субъекта данных (ст. 18 Регламента).

Статья 14

Обязательства по уведомлению в отношении исправления

или удаления персональных данных или ограничении обработки

Контролёр должен сообщить о любом исправлении или удалении персональных данных, либо ограничении обработки, осуществляемых в соответствии со Статьей 16, Статьей 17 (1) и Статьей 18 Регламента, каждому получателю, которому были раскрыты персональные данные, кроме случаев, когда это оказывается невозможным или сопряжено с несоразмерными усилиями. Контролёр должен проинформировать субъекта данных об этих получателях, если субъект данных запрашивает его об этом (из ст. 19 Регламента).

Статья 15

Право на переносимость данных

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

(a) обработка основывается на согласии в соответствии с пунктом (a) Статьи 6 (1) или пунктом (a) статьи 9 (2) Регламента, либо по договору в соответствии с пунктом (б) Статьи 6 (1) Регламента; и

(в) обработка осуществляется с помощью автоматизированных средств.

2. При осуществлении его/ее права на переносимость данных в соответствии с параграфом 1 ст. 20 Регламента, субъект данных должен иметь право передавать персональные данные непосредственно от одного контролёра к другому, если это технически осуществимо (из ст. 20 Регламента).

Раздел 4

ПРАВО НА ВОЗРАЖЕНИЕ И АВТОМАТИЗИРОВАННОЕ ИНДИВИДУАЛЬНОЕ ПРИНЯТИЕ РЕШЕНИЯ

Статья 16

Право на возражение

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

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

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

4. Не позднее момента первого общения с субъектом данных, право, указанное в параграфах 1 и 2 статьи 21 Регламента, должно быть прямо доведено до сведения субъекта данных и должно быть представлено ясно и отдельно от любой иной информации (из статьи 21 Регламента).

Статья 17

Автоматизированное индивидуальное принятие решений, включая составление профиля

1. Субъект данных должен иметь право не подчиняться решению, основанному исключительно на автоматизированной обработке, включая составление профиля, которое порождает правовые последствия, касающиеся его/ее или аналогичным образом в значительной степени влияют на него/нее.

2. Параграф 1 статьи 22 Регламента не применяется в случаях, указанных в в п. 2 статьи 22 Регламента (из статьи 22 Регламента).

Раздел 5

ОГРАНИЧЕНИЯ

Статья 18

Ограничения

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

(a) национальной безопасности;(b) обороны;(c) общественной безопасности;(d) предотвращения, расследования, розыска преследования по

уголовным преступлениям или исполнения уголовных наказаний, в том числе защиты и предупреждения угроз общественной безопасности;

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

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

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

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

(i) защиты субъекта данных или прав и свобод иных лиц; (j) исполнения решений по гражданско-правовым искам (из статьи 23 Регламента).

ГЛАВА IV.

КОНТРОЛЁР И ОБРАБОТЧИК

Раздел 1

ОБЯЗАТЕЛЬСТВА ОБЩЕГО ХАРАКТЕРА

Статья 19

Ответственность контролёра

1. Принимая во внимание характер, сферу охвата, контекст и цели обработки, равно как и вероятность возникновения рисков и степень опасности для прав и свобод физических лиц, контролёр должен применять соответствующие технические и организационные меры, для того, чтобы обеспечить и быть способным подтвердить, что обработка осуществляется в соответствии с настоящим Регламентом. Такие меры должны пересматриваться и обновляться, в необходимых случаях (из ст. 24 Регламента).

Статья 20

Защита данных для определенных целей/случаев и по умолчанию

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

2. Контролёр должен осуществлять соответствующие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только персональные данные, которые необходимы для каждой конкретной цели их обработки. Такая обязанность распространяется на собранный массив персональных данных в части, касающейся их обработки, сроку их хранения, а также к доступу к ним. В частности, такие меры должны обеспечивать, что по умолчанию доступ к персональным данным не будет предоставлен неопределенному числу физических лиц без вмешательства этого индивидуума (из ст. 25 Регламента).

Статья 21

Представители контролёров или обработчиков, не учрежденных в Евросоюзе

1. В том случае, когда применяется Статья 3 (2) статьи 27 Регламента, контролёр или обработчик должны в форме письменного документа назначить представителя в Евросоюзе.

2. Обязательство, изложенное в параграфе 1 статьи 27 Регламента, не применяется: в отношении:

(a) к обработке, которая является единичной, не охватывает в больших масштабах обработку особых категорий

данных, согласно Статье 9 (1) статьи 27 Регламента, либо обработку персональных данных, связанных с уголовными приговорами и правонарушениями, согласно Статье 10 Регламента, а также к обработке персональных данных, которая едва ли обернется рисками для прав и свобод физических лиц, принимая во внимание характер, контекст, цели и задачи этой обработки; или

(b) в отношении органа государственной власти или учреждения.

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

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

5. Назначение представителя контролёром или обработчиком не должно наносить ущерба юридическим действиям, которые могут быть возбуждены против самого контролёра или обработчика (из статьи 27 Регламента).

Статья 22

Обработчик

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

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

(a) обрабатывает персональные данные только на основании документально подтвержденных распоряжений контролёра, в том числе в отношении передачи персональных данных третьей стране или международной организации, если только этого не требует право Евросоюза или право государств-члена, которое применяется к обработчику; в этом случае обработчик должен проинформировать контролёра об этих правовых требованиях до начала обработки, за исключением случаев, когда такое право запрещает подобное информирование по основаниям общественного интереса;

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

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

(d) соблюдает условия, указанные в параграфах 2 и 4 статьи 27 Регламента, по привлечению другого обработчика;

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

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

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

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

В части, относящейся к пункту (h) первого подпараграфа, обработчик должен незамедлительно информировать контролёра, в случае, если, по его мнению, распоряжения нарушают настоящий Регламент или иные положения по защите данных. Евросоюза или государства-члена (из ст. 28 Регламента).

Статья 23

Отчетные записи обработки данных

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

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

(b) цели обработки;

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

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

(e) о передаче персональных данных, когда это применимо, в третью страну или международную организацию, включая указание этой третьей страны или международной организации, а в случае передачи персональных данных согласно второму подпараграфу Статьи 49 (1) статьи 27 Регламента, документальное подтверждение надлежащего обеспечения защиты;

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

(g) общее описание технических и организационных мер безопасности, предусмотренных в Статье 32 (1) Регламента, когда это возможно (из ст. 30 Регламента).

Раздел 2

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 24

Безопасность обработки

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

(a) псевдонимизация и криптографическая защита персональных данных;

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

(c) средства своевременного восстановления доступности и доступа к персональным данным в случае

природного или технического инцидента;

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

2. При определении надлежащего уровня безопасности, в расчет должны приниматься в том числе риски, которые представляет собой сама обработка, в особенности риски от случайного или неправомерного уничтожения, потери, изменения, несанкционированного раскрытия или доступа к персональным данным переданным, сохраненным либо или иным образом обработанным (из статьи 23 Регламента).

Статья 25

Уведомление надзорного органа об утечке персональных данных

2. Обработчик должен уведомить контролёра без неоправданной задержки об утечке персональных данных как только ему стало известно об утечке персональных данных (из ст. 33 Регламента).

Статья 26

Сообщение субъекту данных об утечке персональных данных

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

2. Сообщение субъекту данных, предусмотренное параграфом 1 статьи 34 Регламента, должно излагать ясным и простым языком характер утечки персональных данных, а также содержать как минимум информацию и меры, предусмотренные в пунктах (b), (c) и (d) Статьи 33(3) Регламента.

3. Сообщение субъекту данных, предусмотренное параграфом 1 статьи 34 Регламента, не требуется, если выполнено любое из условий, указанных в п. 3 ст. 34 Регламента (из статьи 34 Регламента).

Раздел 3

ОЦЕНКА ВОЗДЕЙСТВИЯ НА ЗАЩИТУ ДАННЫХ И ПРЕДВАРИТЕЛЬНАЯ КОНСУЛЬТАЦИЯ

Статья 27

Оценка воздействия на защиту данных

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

7. Оценка должна содержать как минимум:

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

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

(c) оценку рисков в отношении прав и свобод субъектов данных, предусмотренных параграфом 1 ст. 35 Регламента; и

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

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

безопасности обработки данных.

11. В необходимых случаях контролёр должен провести анализ для того, чтобы оценить, осуществлена ли обработка в соответствии с оценкой воздействия на защиту данных, по крайней мере, когда существует изменение риска, представленного операциями обработки (из ст. 35 Регламента).

Статья 28

Предварительная консультация

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

3. При консультировании надзорным органом, в соответствии с параграфом 1 статьи 36 Регламента, контролёр должен предоставить надзорному органу:

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

(b) сведения о цели и способах предполагаемой обработки;

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

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

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

(f) любую иную информацию, по требованию надзорного органа (из статьи 36 Регламента).

Раздел 4

ИНСПЕКТОР ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 29

Назначение на должность инспектора по защите персональных данных

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

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

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

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

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

6. Инспектор по защите персональных данных может являться сотрудником контролёра или обработчика, или

осуществлять задачи на основании договора об оказании услуг.

7. Контролёр или обработчик должны опубликовать реквизиты инспектора по защите персональных данных и сообщить их надзорному органу (из статьи 37 Регламента).

Статья 30

Должность инспектора по защите персональных данных

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

2. Контролёр и обработчик должны оказывать содействие инспектору по защите персональных данных в осуществлении задач, предусмотренных в Статье 39 Регламента, посредством средств, необходимых для осуществления таких задач, а также предоставлением доступа к персональным данным и операциям обработки, и поддерживать его/ее экспертную осведомленность (из статьи 38 Регламента).

Статья 31

Задачи инспектора по защите персональных данных

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

(a) информировать и давать советы контролёру или обработчику, а также сотрудникам, которые осуществляют обработку, относительно их обязанностей по настоящему Регламенту и иным положениям о защите данных Евросоюза или государства-члена;

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

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

(d) сотрудничать с надзорным органом;

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

2. Инспектор по защите персональных данных при выполнении его/ее задач должен соответствующим образом учитывать риск, связанный с операциями обработки, принимая во внимание характер, объем, контекст и цели обработки (из статьи 39 Регламента).

ГЛАВА V.

ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ СТРАНАМ ИЛИ МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ

Статья 32

Общие принципы передачи

Любая передача персональных данных, подвергшихся обработке или предназначенные для обработки, после передачи третьей стране или международной организации, должна проводиться лишь в случаях, когда это допускается другими положениями настоящего Регламента, если условия, предусмотренные в этой Главе, соблюдаются контролёром или обработчиком, включая последующую передачу персональных данных из третьей страны или международной

организации в другую третью страну или в другую международную организацию. Все положения настоящей Главы должны применяться с целью обеспечения того, чтобы уровень защиты физических лиц, гарантированный настоящим Регламентом, не был подорван (из статьи 44 Регламента).

Статья 33

Передача при наличии надлежащих гарантий

1. При отсутствии решения в порядке Статьи 45(3) Регламента, контролёр или обработчик могут передать персональные данные третьей стране или международной организации только, если контролёр или обработчик предоставляют надлежащие гарантии, а также при условии, что имеющие законную силу права субъекта данных и действующие средства правовой защиты субъекта данных являются доступными (из статьи 46 Регламента).

ГЛАВА VIII.

СРЕДСТВА ПРАВОВОЙ ЗАЩИТЫ, ОТВЕТСТВЕННОСТЬ И САНКЦИИ

Статья 34

Право подавать жалобу в надзорный орган

1. Без ущерба любым иным административным или судебным средствам защиты, каждый субъект данных должен обладать правом подачи жалобы в надзорный орган, в том числе, в государстве-члене его/ее обычного места проживания, места работы или места предполагаемого нарушения, если субъект данных считает, что обработка относящихся к нему/ней персональных данных нарушает настоящий Регламент (из статьи 77 Регламента).

Статья 35

Право на эффективные средства судебной защиты против надзорного органа

1. Без ущерба любым иным административным или вне-судебным средствам защиты, каждое физическое или юридическое лицо должно иметь право на эффективные средства судебной защиты против юридически обязательного решения надзорного органа, касающихся их (из статьи 78 Регламента).

Статья 36

Право на эффективные средства судебной защиты в отношении контролёра или обработчика

1. Без ущерба любым иным административным или внесудебным средствам защиты, в том числе праву подачи жалобы в надзорный орган, согласно Статье 77 Регламента, каждый субъект данных должен иметь право на эффективные средства судебной защиты, если он/она считает, что его/ее права по настоящему Регламенту, были нарушены в результате обработки его/ее персональных данных в нарушение требований настоящего Регламента (из статьи 79 Регламента).

Статья 37

Право на компенсацию и ответственность

1. Любое лицо, которое понесло материальный или нематериальный ущерб в результате нарушения положений настоящего Регламента, обладает правом на получение компенсации от контролёра или обработчика за понесенный ущерб.

2. Любой контролёр, участвующий в обработке данных, должен нести ответственность за ущерб, вызванный обработкой данных, которая нарушает настоящий Регламент. Обработчик должен нести ответственность за ущерб, вызванный обработкой данных, только если он не выполнил обязательства по настоящему Регламенту, конкретно направленные на обработчиков, или когда он действовал вне пределов или в нарушение законных предписаний контролёра (из статьи 82 Регламента).

Статья 38

Общие условия наложения административных штрафов

1. Каждый надзорный орган должен обеспечить, чтобы наложение административных штрафов, в порядке настоящей Статьи в отношении нарушений положений настоящего Регламента, предусмотренных в параграфах 4, 5 и 6 статьи 83 Регламента, в каждом отдельном случае, было эффективным, соразмерным и имело сдерживающее воздействие.

2. Административные штрафы, в зависимости от обстоятельств каждого конкретного случая, должны налагаться в дополнение, либо вместо мер, предусмотренных пунктами (a)-(h) и (j) Статьи 58 (2) Регламента. При принятии решения по вопросу наложения административного штрафа и решения о размере административного штрафа, в каждом отдельном случае должно подлежать учету следующее:

(a) характер, тяжесть и продолжительность нарушения, принимая во внимание характер, объем и цели соответствующей обработки, также как и количество затронутых субъектов данных, а равно и размер ущерба, понесенного ими;

(b) умышленный или неосторожный характер нарушения; (c) любые меры, предпринятые контролёром или обработчиком, для

смягчения ущерба, полученного субъектами данных; (d) степень ответственности контролёра или обработчика, принимая во

внимание технические и организационные меры, осуществляемые ими в соответствии со Статьями 25 и 32 Регламента;

(e) любые соответствующие предыдущие нарушения контролёра или обработчика;

(f) степень сотрудничества с надзорным органом для того, чтобы устранить нарушения и смягчить возможные неблагоприятные последствия нарушений;

(g) категории персональных данных, затронутых нарушением;

(h) способ, посредством которого надзорному органу стало известно о нарушении, в том числе, уведомил ли контролёр или обработчик об этом нарушении, и если да, то в какой степени;

(i) соблюдение мер, предусмотренных Статьей 58 (2) Регламента, ранее было предписано против соответствующего контролёра или обработчика в отношение того же вопроса;

(j) соблюдение утвержденных кодексов поведения в соответствии со Статьей 40 Регламента, или утвержденных механизмов сертификации, в соответствии со Статьей 42 Регламента; и

(k) любые иные отягчающие или смягчающие факторы, применимые к обстоятельствам дела, например, полученные финансовые выгоды или избежание потерь, прямо или косвенно связанных с нарушением.

3. Если контролёр или обработчик умышленно или по неосторожности, по тем же самым или связанным с обработкой данных, нарушают несколько положения настоящего Регламента, общий размер административного штрафа не должен превышать размер, установленный для самого тяжкого нарушения.

4. Нарушения следующих положений должны, в соответствии с параграфом 2 статьи 83 Регламента, подпадать под административные штрафы в размере до 10 000 000 Евро, или применительно к хозяйствующему субъекту, в размере до 2% от «обще-странового» годового оборота хозяйствующего субъекта за весь предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) обязательства контролёра и обработчика в соответствии со Статьями 8, 11, 25-39 и 42 и 43 Регламента;

(b) обязательства органа сертификации в соответствии со Статьями 42 и 43 Регламента;

(c) обязательства органов, надзорного органа в соответствии со Статьей 41 (4) Регламента.

5. Нарушения следующих положений, в соответствии с параграфом 2 статьи 83 Регламента, должны подпадать под административные штрафы в размере до 20 000 000 Евро или применительно к хозяйствующему субъекту в размере до 4% от «обще-странового» годового оборота за весь предыдущий финансовый год, в зависимости от того, какая сумма больше:

(a) нарушение основных принципов обработки, в том числе условий, в отношении согласия, согласно Статьям 5, 6, 7 и 9 Регламента;

(b) прав субъектов данных, предусмотренных с Статьях 12-22 Регламента;

(c) передачи персональных данных получателю в третьей стране или международной организации, предусмотренной Статьями 44-49 Регламента;

(d) любых обязанностей в соответствии с правом государства-члена, принятому в рамках Главы IX Регламента;

(e) несоблюдения предписания, или временного или окончательного ограничения на обработку, или приостановление потоков данных надзорным органом в соответсвтии со Статьей 58 (2) Регламента, либо отказ в предоставлении доступа в нарушение Статьи 58 (1) Регламента.

6. Нарушения предписаний надзорного органа, в соответствии со Статьей 58 (2) статьи 83 Регламента, должны, в соответствии с параграфом 2 статьи 83 Регламента, подпадать под административные штрафы в размере не более 20 000 000 Евро или, применительно к хозяйствующему субъекту, в размере до 4% от «общестранового» годового оборота хозяйствующего субъекта за весь предыдущий финансовый год, в зависимости от того, какая сумма больше.

7. Без ущерба полномочиям надзорных органов по устранению недостатков, в соответствии со Статьей 58 (2) Регламента, каждое государство-член может установить правила относительно того, могут ли и в какой мере административные штрафы налагаться на органы государственной власти и учреждения, существующие в этом государстве-члене.

8. Осуществление надзорным органом своих полномочий в соответствии со Статьей 83 Регламента, должно подпадать под действие соответствующих процессуальных гарантий в соответствии с правом Евросоюза и правом государства-члена, включая эффективные средства судебной защиты и надлежащую правовую процедуру.

9. В случае, когда правовая система государства-члена не предусматривает административные штрафы, настоящая Статья может применяться таким образом, чтобы наложение штрафа инициировалось компетентным надзорным органом, а штраф налагался компетентными национальными судами, при этом гарантируя, что такие средства правовой защиты являются эффективными и обладают аналогичным эффектом как и административные штрафы, налагаемые надзорными органами. Во всяком случае, налагаемые штрафы должны быть эффективными, пропорциональными и должны оказывать сдерживающее воздействие. Такие государства-члены должны уведомить Европейскую Комиссию о положениях своего законодательства, которые они принимают в соответствии с соответствующим параграфом статьи 83 Регламента, до 25 мая 2018 г., а также незамедлительно уведомить о любых последующих изменениях законодательства или поправках, затрагивающих такие положения (из статьи 83 Регламента).