

ДИРЕКТИВА (ЕС) 2016/680 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА

27 апреля 2016

О защите физических лиц применительно к обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, и о свободном движении таких данных.

ЕВРОПЕЙСКИЙ ПАРЛАМЕНТ И СОВЕТ ЕВРОПЕЙСКОГО СОЮЗА,

Принимая во внимание договор о функционировании Европейского Союза, и в частности статье 16(2) этого закона,

Принимая во внимание предложение от Европейской Комиссии,

После передачи проекта законодательного акта национальным парламентам,

Принимая во внимание мнение Комитета регионов,

Действуя в соответствии с обычной законодательной процедурой,

В то время как:

- (1) Защите физических лиц в отношении обработки персональных данных) является фундаментальным правом. Статья 8(1) Хартии основных прав Европейского Союза (далее-Хартия) и статья 16(1) Договора о функционировании Европейского Союза предусматривает, что каждый имеет право на защиту персональных данных, касающихся его или ее.
- (2) Принципы и нормы о защите физических лиц в отношении обработки их) персональных данных, независимо от их гражданства или местожительства, уважения его основных прав и свобод, в частности право на защиту персональных данных. Эта Директива призвана способствовать достижению пространство свободы, безопасности и правосудия.
- (3) Стремительные технологические изменения и глобализация принесли) новые вызовы для защиты персональных данных. Масштаб сбора и передачи персональных данных значительно выросла. Технология позволяет обработку персональных данных в беспрецедентных масштабах в целях реализации мероприятий, таких как предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний.
- (4) Свободный поток персональных данных между компетентными органами в) целях предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности в рамках Союза и передача таких персональных данных третьим странам и международным организациям следует содействовать, обеспечивая при этом высокий уровень защиты персональных данных. Эти изменения требуют создания эффективной и

более однородной структуры по защите персональных данных в Союз, подкрепленный строгим соблюдением.

- (5) Директива 95/46/ЕС Европейского парламента и Совета распространяется на всю обработку персональных данных в государствах-членах в государственном и частном секторах. Однако, это не распространяется на обработку персональных данных в ходе осуществления деятельности, которая выходит за рамки законодательства сообщества, таких как деятельность в области судебного сотрудничества по уголовным делам и сотрудничества правоохранительных органов.
- (6) Рамочное Решение Совета 2008/977/ JHA применяется в области судебного сотрудничества по уголовным делам и сотрудничества правоохранительных органов. Сфера применения этого рамочного решения ограничивается обработку персональных данных, переданных или между государствами-членами.
- (7) Обеспечение последовательного и высокий уровень защиты личных данных физических лиц и облегчить обмен персональными данными между компетентными органами государств-членов имеет решающее значение для обеспечения эффективного судебного сотрудничества по уголовным делам и полицейского сотрудничества. В этой связи, уровень защищенности прав и свобод физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, должны быть эквивалентными во всех государствах-членах. Эффективную защиту личных данных по всему Союзу требует укрепления прав данных субъектов и обязательств тех, кто обрабатывает персональные данные, а также аналогичные полномочия для мониторинга и обеспечения соблюдения норм, касающихся защиты персональных данных в государствах-членах.
- (8) Статья 16(2) Договора ЕС мандаты Европейского парламента и Совета сформулируют правила о защите физических лиц с в отношении обработки персональных данных и правил, касающихся свободного перемещения персональных данных.
- (9) Исходя из этого, Регламент (EU) 2016/679 Европейского парламента и Совета ⁽⁵⁾ устанавливает общие правила для защиты физических лиц в отношении обработки личных данных и о свободном передвижении персональных данных в рамках Союза.
- (10) В Декларации «О защите персональных данных в области судебного сотрудничества по уголовным делам и полицейского сотрудничества», прилагаемых к заключительному акту межправительственной конференции, которая приняла Лиссабонский договор, конференция признала, что специальных правил о защите персональных данных и свободном передвижении персональных данных в области судебного

сотрудничества по уголовным делам и полицейского сотрудничества, основанного на статье 16 договора о функционировании Европейского Союза может оказаться необходимым в силу специфики характера этих полей.

- (11) Поэтому представляется целесообразным для тех полей, которые должны быть решены директива, которая устанавливает специальные правила о защите физических лиц применительно к обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, учете специфики этой деятельности. Такие компетентные органы могут включать в себя не только органы государственной власти, таких как судебные органы, полицию или другие правоохранительные органы, но и любые другие тела или органа, на который возложено государственное право участника на осуществление государственной власти и органами государственной власти для целей настоящей Директивы. Где такой орган или лицо, осуществляющее обработку персональных данных для иных целей, чем для целей настоящей Директивы, Регламента (ЕС) 2016/679 применяется. Поэтому регламентом (ЕС) 2016/679 применяется в случаях, когда орган или лица, собирающего персональные данные для других целей и дальнейшей обработки этих персональных данных в целях соблюдения юридической обязанности, которым он подчиняется. Например, для целей расследований, выявления или преследования преступных деяний финансовые институты сохраняют некоторые персональные данные, которые обрабатываются ими, и предоставлять эти персональные данные только для компетентных национальных органов в конкретных случаях и в соответствии с законодательством своего государства-члены. Орган или лицо, которое обрабатывает персональные данные по поручению таких органов в рамках настоящей Директивы, должны быть связаны договором или иным правовым актом и положениями, применимыми к обработчикам в соответствии с данной директивой, при одновременном применении Регламента (ЕС) 2016/679 остается неизменной для обработки персональных данных обработчика выходит за рамки этой Директивы.
- (12 Мероприятия, проводимые сотрудниками полиции или других) правоохранительных органов, ориентированы в основном на предотвращения, расследования, выявления или преследования преступных деяний, в том числе деятельность полиции без предварительного знания, если инцидент является уголовным преступлением или нет. Такая деятельность также может включать осуществление полномочий путем принятия принудительных мер, таких, как деятельность полиции на демонстрациях, крупных спортивных мероприятий и массовых беспорядков. Они также включают в себя

поддержание правопорядка в качестве задач, возложенных на полицию или другие правоохранительные органы в случае необходимости защиты от и предотвращения угроз общественной безопасности и фундаментальные интересы общества, охраняемые законом, которые могут привести к уголовному преступлению. Государства-члены могут уполномочить компетентные органы с выполнением других задач, которые не обязательно осуществлялись в целях предотвращения, расследования, выявления или преследования преступных деяний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, так что обработка персональных данных для этих целей, настолько, насколько это в рамках Союзного закона, подпадает под действие Регламента (ЕС) 2016/679.

- (13) Уголовное преступление по смыслу настоящей Директивы должна быть автономная концепция правовой Союз в трактовке суда Европейского Союза (суда справедливости).
- (14) Поскольку настоящая Директива не применяется к обработке персональных данных в ходе осуществления деятельности, которая выходит за рамки Союзного законодательства, деятельности, касающиеся национальной безопасности, деятельности учреждений или подразделений, занимающихся вопросами национальной безопасности и обработки персональных данных государствами-членами при осуществлении деятельности, которые подпадают под действие главы 2 раздела V Договора о Европейском Союзе (дес) не должны рассматриваться как виды деятельности, подпадающие под действие данной Директивы.
- (15) Для того, чтобы обеспечить такой же уровень защиты, для физических лиц через юридическую защиту своих прав по всему Союзу и не допустить расхождения затрудняют обмен персональными данными между компетентными органами, данная Директива должна предусматривать гармонизированные правила охраны и свободном передвижении персональных данных, обрабатываемых в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности. Сближении законов государств-членов не должно приводить к ослаблению защиты персональных данных они не дают, но должны, напротив, стремиться к обеспечению высокого уровня защиты в рамках Союза. Государства-члены не должны быть лишены возможности обеспечения более высокой гарантии, чем те, которые установлены в настоящей директиве по защите прав и свобод субъектов данных в отношении обработки персональных данных компетентными органами.
- (16) Настоящая Директива не затрагивает принцип публичного доступа к официальным документам. В соответствии с Регламентом (ЕС) 2016/679

персональные данные в официальных документах, проводимая органом государственной власти или общественный или частный орган для выполнения задач осуществляется в общественных интересах может быть передана этим органом или органом в соответствии с Союзом или государства-члена права, государственный орган или орган субъекта в целях согласования публичного доступа к официальным документам с право на защиту персональных данных.

- (17) Охрана, предоставляемая настоящей директивой, должны применяться к физическим лицам, независимо от их национальности или места жительства, в связи с обработкой их персональных данных.
- (18) Для того, чтобы предотвратить создание серьезный риск обхода защиты физических лиц должны быть технологически нейтральными и не должны зависеть от используемых методов. Защита физических лиц следует применять для обработки персональных данных с помощью автоматизированных средств, а также для обработки вручную, если персональные данные содержатся или должны содержаться в системе регистрации. Файлов или наборов файлов, а также их обложки, которая не структурирована в соответствии с конкретными критериями, не должны подпадать под сферу действия настоящей Директивы.
- (19) Регламентом (ЕС) № 45/2001 Европейского парламента и Совета ⁽⁶⁾ применяется к обработке персональных данных союзных институтов, органов, офисов и агентств. Регламентом (ЕС) № 45/2001 и других союзных нормативно-правовых актов, применимых к такой обработке персональных данных должны быть адаптированы к принципам и правилам, установленным в Регламенте (ЕС) 2016/679.
- (20) Эта Директива не препятствует государствам-членам с указанием технологических операций и процедур обработки в национальные правила об уголовной процедуры в отношении обработки персональных данных судов и других судебных органов, в частности, в отношении персональных данных, содержащихся в судебном решении или в записи в рамках уголовного судопроизводства.
- (21) Принципы защиты данных должны применяться к любой информации, касающейся идентифицированного или идентифицируемого физического лица. Чтобы определить, является ли физическое лицо идентифицируемым, следует учитывать все средства разумно может быть использовано, например, выделением, либо инспектор или иным лицом для идентификации физического лица, прямо или косвенно. Чтобы убедиться, означает, разумно вероятно, чтобы использоваться, чтобы идентифицировать физическое лицо, необходимо учитывать все объективные факторы, такие как стоимость и количество времени, необходимое для идентификации, с учетом доступных на тот момент технологий обработки и технологических разработок. Поэтому принципы защиты данных не должны применяться к анонимной информации, а

именно информация, не относящаяся к идентифицированному или идентифицируемому физическому лицу или личные данные обезличены, таким образом, что субъект данных более не поддается идентификации.

- (22) Органы государственной власти, к которой персональные данные раскрыты в соответствии с юридическим обязательством для осуществления своей официальной миссии, такие как налоговые и таможенные органы, финансовые органы дознания, независимыми административными органами или финансового рынка органов, ответственных за регулирование и надзор на рынке ценных бумаг не должны рассматриваться в качестве получателей, если они получают персональные данные, которые необходимы для проведения конкретного расследования в общих интересах, в соответствии с Союзом или государства-члена права. Запросы на раскрытие Отправлено органов государственной власти всегда должны быть в письменном виде, аргументированно и случайные и не должно касаться всей совокупности в системе подачи и привести к взаимосвязи системы подачи заявок. Обработка персональных данных те государственные органы должны соблюдать соответствующие правила по защите данных в соответствии с целями обработки.
- (23) Генетические данные должны быть определены как персональные данные, касающиеся наследственных или приобретенных генетических характеристик физического лица, которые дают уникальную информацию о физиологии и здоровье, что физическое лицо, и которые вытекают из анализа биологического образца от физического лица, в частности хромосомных, дезоксирибонуклеиновой кислоты (ДНК) или рибонуклеиновой кислоты (РНК) анализ, или анализ другого элемента включение эквивалентной информации, которое будет получено. Учитывая сложность и чувствительность генетической информации, существует большой риск неправильного использования и повторного использования для различных целей управления. Любая дискриминация, основанная на генетических особенностях, в принципе должно быть запрещено.
- (24) Персональные данные, касающиеся здоровья, должны включать все данные, относящиеся к состоянию здоровья субъекта данных, которые раскрывают информацию о прошлых, текущих или будущих физического или психического состояния здоровья субъекта данных. Это включает в себя информацию о физическое лицо, собранные в ходе регистрации, или обеспечение, медицинское обслуживание, как указано в Директивы 2011/24/ЕС Европейского парламента и Совета (7) для этого физическое лицо; число, символ или определенного физического лица, позволяющие однозначно идентифицировать физическое лицо, в медицинских целях; информация, полученная по результатам тестирования или обследования какой-либо части тела или телесной субстанции, в том числе и от генетических данных и биологических образцов; и никакой информации о, например, болезнь, инвалидность, риск заболевания, анамнеза,

клинического лечения или физиологическое или биомедицинских состояние данных субъекта независимо от его источника, например от врача или другого врача, больницу, медицинский прибор или приборку.

- (25) Всех государств-членов, входящих в Международную организацию уголовной полиции (Интерпол). Для выполнения своей миссии, Интерпол получает, хранит и распространяет персональные данные для оказания помощи компетентным органам в предотвращении и борьбе с международной преступностью. Поэтому необходимо укреплять сотрудничество между ЕС и Интерпол посредством поощрения эффективного обмена персональными данными при обеспечении уважения основных прав и свобод в отношении автоматизированной обработки данных личного характера. Где личные данные передаются из Союза в Интерпол, и в страны, которые делегировали членов Интерпола, эта Директива, в частности, Положения о международных поставках, должны применяться. Эта Директива должна применяться без ущерба конкретными Правилами, изложенными в общей позиции Совета 2005/69/ и решением Совета 2007/533/.
- (26) Любая обработка персональных данных должны быть законными, справедливыми и транспарентными в отношении указанных физических лиц, и обработаны только для определенных целей, установленных законом. Это само по себе не мешает правоохранительным органам проводить такие мероприятия, как негласные следственные действия или видеонаблюдения. Такая деятельность может быть сделано в целях предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, покуда они устанавливаются законом и является необходимой и соразмерной мерой в демократическом обществе, с должным учетом законных интересов физического лица. Принцип защиты данных добросовестной переработки является ясное понятие права на справедливое судебное разбирательство, закрепленное в статье 47 Хартия и в статье 6 Европейской конвенции о защите прав человека и основных свобод. Физические лица должны быть осведомлены о рисках, правила, гарантии и права в связи с обработкой их персональных данных и как воспользоваться своими правами в отношении обработки. В частности, конкретных целей, для которых персональные данные обрабатываются, должны быть явными и законными и определяется на момент сбора персональных данных. Персональные данные должны быть адекватными и уместными для целей, для которых они обрабатываются. Это следует, в частности, заверил, что собранные персональные данные не избыточны и не хранятся дольше, чем это необходимо для целей, для которых они обрабатываются. Персональные данные должны обрабатываться только в случае, если цель обработки не может разумно быть выполнены другими средствами. Для того, чтобы убедиться, что данные не хранятся дольше,

чем необходимо, сроки должны быть установлены регулятором для стирания или для периодического обзора. Государства-члены должны определить соответствующие гарантии для персональных данных, которые хранятся в течение более длительных периодов для архивирования в общественных интересах, научных, статистических или исторических использовании.

- (27 Для профилактики, расследования и судебного преследования уголовных преступлений, это необходимо для компетентных органов на обработку персональных данных, собранных в контексте предотвращения, расследования, обнаружения или преследования по конкретным уголовным преступлениям, вне данного контекста, для того чтобы развивать понимание преступной деятельности и связей между различными уголовными преступлениями обнаружены.
- (28 В целях поддержания безопасности в отношении обработки и предотвращения переработки в нарушение данной Директивы, личные данные должны быть обработаны таким образом, чтобы обеспечить требуемый уровень безопасности и конфиденциальности, включая предотвращение несанкционированного доступа или использование персональных данных, а также оборудовании, используемом для обработки, и что учитывает состояние техники и технологии, расходы на осуществление по отношению к рискам и характера обрабатываемых персональных данных должны быть защищены.
- (29 Персональные данные должны собираться для определенных, явных и законных целей в рамках этой Директивы и не должны быть обработаны для целей, несовместимых с целями предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности. Если персональные данные обрабатываются одним и тем же или другому инспектору с определенной целью в рамках данной Директивы, для которых она была собрана, такие обработки должны быть разрешены при условии, что такая обработка имеет право в соответствии с действующими правовыми нормами и является необходимым и соразмерным, что другой цели.
- (30 Принцип достоверности данных должны быть применены с учетом природы и назначения соответствующей обработки. В частности, в ходе судебного разбирательства, высказывания, содержащие персональные данные основаны на субъективном восприятии физических лиц и не всегда поддается проверке. Следовательно, требование точности, не должны принадлежать к точности изложения, а лишь к тому, что определенное заявление.
- (31 Это заложено на обработку персональных данных в области судебного сотрудничества по уголовным делам и полицейского сотрудничества, что

персональные данные, относящиеся к различным категориям субъектов персональных данных обрабатываются. Таким образом, четкое разграничение следует, где это уместно и насколько это возможно, между персональными данными различных категорий данных предметов, таких как: подозреваемых; лиц, осужденных за совершение уголовного преступления; потерпевшие и другие участники, такие как свидетели; лица, обладающие соответствующей информации или контактов, а также партнеров подозреваемых и осужденных преступников. Это не должно препятствовать применению право презумпции невиновности, гарантированного Хартияом и Европейским судом по правам человека, как трактуется в судебной практике суда ЕС и Европейского Суда по правам человека соответственно.

- (32) Компетентные органы должны гарантировать, что персональные данные, которые являются неточными, неполными или не в курсе не передаются или предоставляются. В целях обеспечения защиты физических лиц, точность, полноту или степень, в которой персональные данные являются актуальными и достоверность персональных данных, передаваемых или предоставляемых, компетентные органы должны, по мере возможности, добавить необходимую информацию, в все передачи персональных данных.
- (33) Где эта Директива относится к государственным законодательством-членов, правовую основу или законодательная мера, не обязательно требует законодательный акт, принятый парламентом, без ущерба для требований в соответствии конституционному порядку соответствующего государства-члена. Однако, такое положение закона-членами, правовая основа и законодательные меры должны быть ясными и четкими, и его применение предсказуемым для тех, кто ей подчиняется, как того требует прецедентное право суда ЕС и Европейского Суда по правам человека. Член государственного закона, регламентирующих обработку персональных данных в рамках настоящей Директивы, должны указать по крайней мере поставленных задач, обрабатываемых персональных данных, целей обработки и процедуры для сохранения целостности и конфиденциальности персональных данных и процедуры по их уничтожению, что обеспечивает достаточных гарантий против риска злоупотреблений и произвола.
- (34) При обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, должен охватывать любую операцию или набор операций, которые выполняются на персональных данных или персональных данных для этих целей, будь то с помощью автоматизированных средств или в противном случае, такие как сбор, запись, упорядочение, структурирование, хранение, адаптация или

изменение, извлечение, консультирование, использование, объединение или сочетание, ограничение обработки, стирания или разрушения. В частности, правила настоящей Директивы должны применяться на передачу персональных данных для целей настоящей Директивы получателю не соответствию с требованиями этой Директивы. Такой получатель должен представлять собой физическое или юридическое лицо, государственный орган, агентство или любой другой орган, к которому персональные данные законно переданы компетентным органом. Где личные данные были изначально собраны компетентным органом одной из целей данной Директивы, Регламента (ЕС) 2016/679 следует применять для обработки этих данных для целей, отличных от целей этой Директивы, где такая обработка является уполномоченным Союзом или государством-членом права. В частности, нормами постановления (ЕС) 2016/679 необходимо обратиться в передачу персональных данных для целей выходит за рамки этой Директивы. Для обработки персональных данных получателю, который не является компетентным органом или который не действует как таковой в понимании этой Директивы и какие персональные данные будут законно переданы компетентным органом, Регламент (ЕУ) 2016/679 должны применяться. При реализации настоящей Директивы, государства-члены должны также иметь возможность указать на применение правил Регламента (ЕС) 2016/679, в соответствии с условиями, изложенными в нем.

- (35) Для того, чтобы быть законным, обработку персональных данных в соответствии с настоящей директивой, должны быть необходимы для выполнения поставленной задачи осуществлялось в общественных интересах компетентным органом на основе Союза или государства-члена права в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности. Эти мероприятия должны охватывать защиту жизненно важных интересов субъекта персональных данных. Выполнение задач предотвращения, расследования, раскрытия и судебного преследования уголовных преступлений, институционально установленное законом компетентным органам позволяет им требовать или поручению физических лиц в соответствии с запросами. В таком случае согласия субъекта данных, как определено в Регламенте (ЕС) 2016/679, не должен служить основанием для обработки персональных данных компетентными органами. Где субъектом персональных данных является обязательным в соответствии с юридическая обязанность, субъект персональных данных не имеет подлинного и свободного выбора, так что реакция субъекта персональных данных не может рассматриваться как добровольно указанием его или ее желания. Это не должно препятствовать государствам-членам предоставлять, по закону, которые субъект персональных данных может согласиться на обработку своих персональных данных для целей настоящей Директивы, такие, как тесты

ДНК в рамках уголовных расследований или контроля его местоположения с электронными метками для исполнения уголовных наказаний.

- (36) Государства-члены должны предусмотреть, что там Союза или государства-члена, право, применимое к передаче компетентный орган предусматривает конкретные условия, применимые в конкретных условиях обработки персональных данных, таких как использование обработки кодов, передающий компетентный орган должен проинформировать получателя О персональных данных эти условия и соблюдать их. Такие условия могут, например, включать в себя запрет на передачу персональных данных далее к другим, или их использование в иных целях, чем те, для которых они были переданы получателю, или информирование субъекта данных, в случае ограничения права на информацию без предварительного согласия передающей компетентный орган. Эти обязательства также должны применяться к передачам передающий компетентный орган для получателей в третьих странах или международных организациях. Государства-члены должны гарантировать, что передающий компетентный орган не применять такие условия для получателей в других государствах-членах или учреждений и органов, созданных в соответствии с главами 4 и 5 раздела V ДФЕС другие, чем те, которые применяются к подобным передачи данных внутри государств-членов, что компетентный орган.
- (37) Личные данные, которые, по своей природе, особенно чувствительные в отношении основных прав и свобод заслуживают особой защиты в условиях их переработки могут создать значительную опасность для фундаментальных прав и свобод. Эти персональные данные должны включать личные данные, раскрывающие расовое или этническое происхождение, согласно которому использование термина "расовое происхождение" в этой директиве не предполагает принятия Союза теориями, пытающимися установить наличие отдельных человеческих рас. Такие персональные данные не должны обрабатываться, если обработка осуществляется при условии гарантии соблюдения прав и свобод субъекта персональных данных, предусмотренных законом, и допускается в случаях, предусмотренных законом; где не допущенного к такой закон, то обработка необходима для защиты жизненных интересов субъекта данных или другого лица; или обработка касается данных, которые явно обнародованы данные субъекта. Соответствующие гарантии для прав и свобод субъекта персональных данных может включать в себя возможность для сбора этих данных только в связи с другими данными на физическое лицо, то возможности для защиты данных, собранных надлежащим образом, строгие правила на доступ сотрудников компетентных органов для сведения и запрет на передачу этих данных. Обработка таких данных должна быть разрешена по закону, в котором субъект данных недвусмысленно согласился на обработку, что особенно

удобными для него или ее. Однако, согласие субъекта персональных данных не должна содержать в себе юридические основания для обработки таких чувствительных персональных данных компетентными органами.

- (38 Субъект персональных данных должен иметь право не быть объектом)
) принятия решения оценки личностных аспектов, связанных с ним или с ней, которая базируется исключительно на автоматизированной обработке и которая производит неблагоприятные юридические последствия в отношении, или существенно влияет на его или ее. В любом случае, такая обработка должна быть при соблюдении соответствующих мер предосторожности, в том числе предоставление информации субъекту данных и право на вмешательство человека, в частности, чтобы выразить свою точку зрения, получить объяснение решения, принятого после такой оценки или оспорить решение. Профилирования, что приводит к дискриминации в отношении физических лиц на основе персональных данных, которые по своей природе особо чувствительной по отношению к основным правам и свободам должны быть запрещены в соответствии с условиями, изложенными в статьях 21 и 52 Хартия.
- (39 Для того, чтобы позволить ему или ей для осуществления своих прав,)
) информацию на эту тему данные должны быть легко доступны, в том числе на сайте регулятора, и легко понять, используя ясный и простой язык. Такая информация должна быть адаптирована к потребностям уязвимых лиц, таких как дети.
- (40 Условия должны быть обеспечены для облегчения выполнения данных)
) субъекта права на основании положений, принятых во исполнение настоящей Директивы, включая механизмы запроса и, если необходимо, получить, бесплатно, в частности, доступ к данным и их исправления или уничтожения персональных данных и ограничение переработки. Инспектор должен быть обязан отвечать на запросы субъекта персональных данных без неоправданной задержки, если инспектор применяет ограничения для субъекта данных прав в соответствии с настоящей директивой. Кроме того, если запросы являются явно необоснованными или чрезмерными, например, когда данные подлежат необоснованно и repetitiously информационных запросов или данных субъекта с использованием своего права на получение информации, например, путем предоставления ложной или недостоверной информации при подаче запроса, инспектор должен быть в состоянии взимать разумную плату или отказываются работать с запросом.
- (41 Где регулятор требует предоставления дополнительной информации,)
) необходимой для подтверждения личности субъекта персональных данных, эта информация должна быть обработана только с этой конкретной целью и не должна храниться дольше, чем требуется для этой цели.

- (42 По крайней мере, следующие сведения должны быть предоставлены субъекту данных: идентификатор инспектора , наличие операции обработки, цели обработки, права на подачу жалобы и наличие права требовать от инспектора доступа и исправления или уничтожения персональных данных или ограничение обработки. Это может иметь место на сайте компетентного органа. Кроме того, в отдельных случаях и для того, чтобы обеспечить осуществление его прав, субъект данных должен быть проинформирован о правовых основах для обработки и сколько времени будут храниться данные, постольку, поскольку такая Дополнительная информация необходима, учитывая особые обстоятельства, в которых эти данные обрабатываются, чтобы гарантировать справедливую обработку в отношении субъекта данных.
- (43 Физическое лицо должно иметь право на доступ к данным, собранным в отношении его или ее, а воспользоваться этим правом легко и по разумной периодичностью, для того, чтобы быть в курсе и проверить законность обработки. Поэтому каждый субъект данных должен иметь право знать и получать сообщения о тех целях, для которых данные обрабатываются, срок, в течение которого данные обрабатываются и получателей данных, в том числе в третьих странах. Где таких сообщений содержали информацию о происхождении персональных данных, информация не должна раскрывать личность физических лиц, в частности конфиденциальных источников. Для этого права должны быть соблюдены, достаточно того, что субъект данных должен иметь полную сводку этих данных в понятной форме, то есть форме, которая позволяет, что сведения, подлежащие стали известны эти данные и убедитесь, что они точны и обрабатываются в соответствии с настоящей директивой, так что вполне возможно, ему или ей для осуществления прав, предоставленных ему или ей эту Директиву. Такое резюме может быть представлена в форме копии персональных данных, подвергающихся обработке.
- (44 Государства-члены должны иметь возможность принять законодательные меры, отсрочки, ограничения или опуская информацию до сведения субъектов или ограничить полностью или частично доступ к своим персональным данным, до такой степени, что и покуда такая мера является необходимой и соразмерной мерой в демократическом обществе, с должным учетом прав и законных интересов физического лица, чтобы не препятствовать должностным лицом или юридических запросов, проведения расследований или процедур, чтобы избежать ущерба для предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний, обеспечения государственной и общественной безопасности или национальной безопасности, или для защиты прав и свобод других лиц. Регулятор должен оценивать, по пути конкретного и индивидуального рассмотрения каждого случая, имеет ли право доступа должны быть частично или полностью ограничен.

- (45 Любой отказ или ограничение доступа в принципе должны быть изложены в письменной форме субъекта персональных данных и включают фактические и правовые мотивы, на которых основано решение.
- (46 Любое ограничение прав субъекта персональных данных должны соблюдать Хартия и с ЕКПЧ, как они интерпретируются в дело-закон суда юстиции и Европейского Суда по правам человека соответственно, и в частности относительно сущности этих прав и свобод.
- (47 Физическое лицо должно иметь право на неточных персональных данных, касающихся его или ее исправить, в частности, когда это касается фактов, а также право на удаление, когда обработка таких данных нарушает Директиву. Однако, право на исправление не должно затрагивать, например, содержанием показаний свидетеля. Физические лица также должны иметь право на ограничение обработки, где он или она оспаривает точность персональных данных и их точность или неточность не может быть установлено, или если персональные данные должны быть сохранены для целей доказательства. В частности, вместо того, чтобы стереть персональные данные, обработка должна быть ограничена, если в конкретном случае есть веские основания полагать, что уничтожение может повлиять на законные интересы субъекта персональных данных. В таком случае, данные с ограниченным доступом должна обрабатываться только для целей, которые мешали их стирания. Методы ограничения обработки персональных данных может включать, в частности, переместив некоторые данные в другую систему обработки, например, для архивирования, или некоторые данные недоступны. В автоматизированных системах подачи ограничение обработки в принципе должна быть обеспечена техническими средствами. Тот факт, что обработка персональных данных ограничивается, должны быть указаны в системе таким образом, что понятно, что обработка персональных данных, ограничен. Такие исправления или уничтожения персональных данных или ограничение обработки должны быть доведены до сведения адресатов, которым эти данные были раскрыты и в компетентные органы, из которых неточные данные получены. Инспекторы должны также воздержаться от дальнейшего распространения таких данных.
- (48 Где регулятор опровергает субъект данных его или ее право на информацию, доступ к данным или их изменении или уничтожении персональных данных или ограничение обработки, субъект персональных данных должен иметь право обращаться в Национальный надзорный орган проверить законность обработки. Субъект данных должен быть проинформирован об этом праве. Если надзорный орган действует от имени субъекта персональных данных, субъект данных должен быть проинформирован, контролирующим органом не менее, что все необходимые проверки или комментарии со стороны контролирующего органа имели место. Надзорный орган также должен сообщить субъекту данных право искать судебную защиту.

- (49) Где персональные данные обрабатываются в ходе расследования уголовного дела и судебного разбирательства по уголовным делам, государства-члены должны быть в состоянии предусмотреть, что осуществление права на получение информации, доступ к данным и их исправления или уничтожения персональных данных и ограничение переработки осуществляется в соответствии с национальными правилами о судебных разбирательствах.
- (50) Обязанность и ответственность регулятора за любые обработки персональных данных, осуществляемых контролером или от имени инспектора должны быть установлены. В частности, регулятор должен быть обязан осуществлять надлежащие и эффективные меры и должны быть способны продемонстрировать, что деятельность по обработке приведены в соответствие с настоящей директивой. Такие меры должны учитывать характер, масштаб, контекст и цели обработки и риск для прав и свобод физических лиц. Меры, принятые регулятором, должна включать в разработке и осуществлении конкретные гарантии в отношении обработки персональных данных физических лиц, уязвимых, таких как дети.
- (51) Риск для прав и свобод физических лиц, в разной степени вероятности и степени тяжести, могут возникнуть в результате обработки данных, которая может привести к физический, материальный или нематериальный ущерб, в частности: обработка может привести к дискриминации, кражи личных данных или мошенничества, финансовые потери, ущерб репутации, потерю конфиденциальности данных, защищенную профессиональной тайной, несанкционированное разворот псевдоцивилизационных или любым другим значительным экономическим или социальным неблагоприятием; где данные субъекты могут быть лишены своих прав и свобод и осуществления контроля за их персональных данных; если персональные данные обрабатываются, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, или членство в профсоюзах; где генетические данные или биометрические данные обрабатываются для того, чтобы однозначно идентифицировать человека или где данных, касающихся здоровья или данные, касающиеся половой жизни и сексуальной ориентации или судимости и преступления или связанные с ними меры безопасности обрабатываются; где личные аспекты оцениваются, в частности, анализа и прогнозирования аспектов, касающихся эффективности работы, экономической ситуации, состояния здоровья, личных предпочтений или интересов, надежность и поведения, местонахождения или движения, в целях создания или использования персональных данных; если персональные данные уязвимых физических лиц, в частности детей, обрабатываются; или где обработка включает в себя большое количество персональных данных и влияет на большое количество данных предметов.
- (52) Вероятности и серьезности риска должен определяться с учетом

-) характера, масштабов деятельности, контекста и целей обработки. Риск должен быть оценен на основе объективной оценки, в рамках которой установлено, являются ли данные-обработка операций сопряжено с высоким риском. Высокий риск-это конкретный риск ущерба для прав и свобод субъектов данных.
- (53 Защиты прав и свобод физических лиц в отношении обработки персональных данных требует принятия необходимых технических и организационных мер для обеспечения соблюдения требований настоящей Директивы. Осуществление таких мер не должна зависеть только от экономических соображений. Для того, чтобы иметь возможность продемонстрировать соответствие с настоящей директивой, регулятор должен принять внутренние политики и реализации мер, которые придерживаются, в частности, принципы защиты данных при разработке и защите данных по умолчанию. Когда инспектор осуществляет защиту оценке воздействия на информацию в соответствии с данной директивой, результаты должны быть учтены при разработке этих мер и процедур. Эти меры могли бы включать, среди прочего, применения псевдоцивилизационных, как можно раньше. Использование псевдоцивилизационных для целей настоящей Директивы может служить инструментом, который может способствовать, в частности, свободный поток персональных данных в зоны свободы, безопасности и правосудия.
- (54 Защиты прав и свобод субъектов данных, а также ответственности и обязательств инспекторов и обработчиков, а также в отношении мониторинга и меры надзорных органов, требуется четкое распределение обязанностей, изложенных в настоящей директиве, в том числе из-за которой инспектор определяет цели и средства обработки совместно с другими инспекторами или где обработка выполняется операция по имени инспектора .
- (55 Проведение обработки обработчиком должно регулироваться нормативно-правовым актом, в том числе договор, связывающий обработчик с инспектором и предусматривающий, в частности, что обработчик должен действовать только по инструкции от инспектора . Обработчик должен учитывать принцип защиты данных по конструкции и по умолчанию.
- (56 Для того, чтобы продемонстрировать соответствие с этой директивой, инспектор или обработчик должны вести учет по всем видам деятельности переработка под свою ответственность. Каждый инспектор и обработчик должен быть обязан сотрудничать с контролирующим органом и сделать эти записи доступными ему по запросу, так что они могут служить для контроля этих операций обработки. Инспектор или обработчик обработки персональных данных в автоматизированных системах обработки должны иметь эффективные методы демонстрации законности обработки, обеспечения самоконтроля и обеспечения целостности данных и безопасности данных, таких как журналы или другие формы записи.

- (57 Журналы должны храниться, по крайней мере, для операций в автоматизированных системах обработки данных, таких как сбор, изменения, консультации, раскрытие, включая передачу, комбинированной или стирания. Идентификация человека, который консультировался или раскрыты персональные данные должны быть зарегистрированы и от того, что определение должно быть по возможности установить обоснованность операций по переработке. Бревна должны быть использованы исключительно в целях проверки законности обработки, самоконтроля, для обеспечения целостности данных и данных безопасности и уголовного судопроизводства. Самоконтроль включает в себя также внутренние дисциплинарные разбирательства компетентных органов.
- (58 Защита данных оценка воздействия должна проводиться в инспектор, где операции обработки могут привести к высокий риск для прав и свобод субъектов данных в силу их характера, масштабов и целей, которые должны включать, в частности, мер, защитных мер и механизмов, призванных обеспечить защиту персональных данных и продемонстрировать соответствие с этой директивой. Оценка воздействия должна охватывать соответствующих систем и процессов обработки операции, а не отдельные случаи.
- (59 В целях обеспечения эффективной защиты прав и свобод субъектов данных, инспектор или обработчик должны проконсультироваться надзорного ведомства, в некоторых случаях, до обработки.
- (60 В целях сохранения безопасности и предотвращения обработки, что нарушает эту Директиву, инспектор или обработчик должен оценить риски, связанные с обработкой и следует принять меры по снижению этих рисков, таких как шифрование. Такие меры должны обеспечить надлежащий уровень безопасности, в том числе конфиденциальности и учитывать состояние техники, расходы на осуществление по отношению к риску и характера обрабатываемых персональных данных должны быть защищены. При оценке угроз безопасности данных, необходимо учитывать риски, которые представлены обработка данных, таких как случайного или незаконного уничтожения, потери, изменения или несанкционированного раскрытия или доступа к персональным данным, передаваемые, хранимые или иначе обработанных, которые могут, в частности, привести к физический, материальный или нематериальный ущерб. Инспектор и обработчик должен гарантировать, что обработка персональных данных не осуществляется неуполномоченными лицами.
- (61 Персональные данные нарушения могут, если их не решать своевременно и надлежащим образом, нанести физический, материальный или нематериальный ущерб для физических лиц, такие как потеря контроля над своими персональными данными или ограничение их прав, дискриминацию, кражи личных данных или мошенничества, финансовых потерь, несанкционированного разворота псевдоцивилизационных, ущерб

репутации, потеря конфиденциальности персональных данных, защищенную профессиональной тайной или любым другим значительным экономическим или социальным неблагоприятием физического лица заинтересованные. Поэтому, как только инспектор начинает осознавать, что персональные данные, утечка произошла, контролер должен сообщить персональные данные нарушения в контролирующий орган без неоправданных задержек и, насколько это возможно, не позднее 72 часов после ознакомления с ним, если инспектор способен продемонстрировать, в соответствии с принципом подотчетности, что персональные данные, нарушение вряд ли может привести к риск для прав и свобод физических лиц. Если такое уведомление не может быть достигнуто в течение 72 часов, причины задержки должны сопровождать уведомления и информация может быть предоставлена в фазах без излишних проволочек.

- (62) Физические лица должны быть информированным без неоправданных задержек, где персональные данные нарушения может повлечь за собой высокий риск для прав и свобод физических лиц, с тем чтобы позволить им принять необходимые меры предосторожности. Сообщение должно описывать характер личной кражи данных и включают в себя рекомендации по физическим лицом, заинтересованным в смягчении возможных неблагоприятных последствий. Сообщение для субъектов персональных данных должно быть сделано, как только представится возможным, в тесном сотрудничестве с надзорным органом, и соблюдения указаний или другие соответствующие органы. Например, нужно снизить непосредственный риск повреждения требуют оперативного общения субъектам данных, в то время как следовало принять надлежащие меры против продолжающихся или аналогичные данные нарушения могут быть обоснованы более времени для общения. Где избегая препятствий официальных или юридических запросов, проведения расследований или процедур, избегая ущерба для профилактики, выявления, расследования или судебного преследования уголовных преступлений или исполнения уголовных наказаний, защите общественной безопасности, защиты национальной безопасности или защиты прав и свобод других лиц не могут быть достигнуты путем отсрочки или ограничивающими передачу личных данных, нарушение естественного заинтересованного лица, такое общение может в исключительных случаях быть опущен.
- (63) Регулятор должен назначить лицо, которое будет оказывать помощь в мониторинге внутреннего соблюдения положений, принятых во исполнение настоящей Директивы, за исключением случаев, когда государство-член примет решение освободить суды и другие независимые судебные органы, действуя в своих судебных обязанностей. Этот человек может быть членом существующих сотрудников регулятора, который получил специальную подготовку в законе О защите данных и практики с целью приобретения экспертных знаний в этой области. Необходимый уровень экспертных знаний должно быть определено, в частности, по

обработке данных и защиты персональных данных, обрабатываемых инспектором. Его или ее задачи могут осуществляться на временной или постоянной основе. Сотрудники по защите данных могут быть назначены совместно несколько инспекторов, с учетом их организационной структуры и размера, например, в случае общих ресурсов в центральных подразделениях. Это лицо также может быть назначен на различные должности в структуре соответствующих инспекторов. Этот человек должен помочь инспектора и сотрудников по обработке персональных данных, информирование и консультирование их о соблюдении их соответствующих обязательств по защите данных. Таких офицеров по защите данных должны быть в состоянии выполнять свои обязанности и задачи в независимом порядке в соответствии с законодательством своего государства-члена.

- (64) Государства-члены должны гарантировать, что передача третьей страны или международной организации имеет место, только если это необходимо для предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, и что инспектор в третьей стране или международной организации, является орган, компетентный в значении настоящей Директивы. Передача должна осуществляться только компетентными органами в качестве инспекторов, кроме случаев, когда обработчики явно поручил передать от имени регуляторов. Такая передача может иметь место в тех случаях, когда комиссия постановила, что третье государство или международная организация не обеспечивает адекватный уровень защиты, где соответствующие гарантии были предоставлены, или если отступления в конкретных ситуациях применять. Где личные данные передаются от Союза инспекторы, обработчики или другим получателям на территории третьих стран или международных организаций, уровня защиты физических лиц, предусмотренных в Союзе настоящая Директива не должна быть подорвана, в том числе в случаях, когда передача персональных данных от третьей страной или международной организацией для инспекторов или обработчиков в той же или в другой третьей страны или международной организации.
- (65) Где осуществляется передача персональных данных от государств-членов с третьими странами или международными организациями, то такая передача должна, в принципе, иметь место только после того, как государство-член, из которого были получены данные дал свое разрешение на передачу. Интересы эффективного сотрудничества правоохранительных органов требуют, что если характер угрозы государственной безопасности государства-члена или третьей страны, или существенные интересы государства настолько близка, невозможно получить предварительное разрешение в хорошее время, компетентный орган должен иметь возможность передачи личных данных третьим странам или

международным организациям без такого предварительного разрешения. Государства-члены должны обеспечить, что любые конкретные условия, касающиеся передачи должны быть переданы третьим странам или международным организациям. Последующая передача персональных данных должна осуществляться с предварительного разрешения компетентного органа, который осуществил оригинальную передачу. При принятии решения по ходатайству для разрешения передачи, компетентный орган, который осуществил оригинальную передачу должны учитывать все соответствующие факторы, в том числе тяжести преступления, конкретных условий, и целей, для которых данные были изначально переданы, характера и условий исполнения уголовного наказания, и уровень защиты персональных данных в третью страну или международную организацию, какие персональные данные будут переданы дальше. Компетентный орган, который осуществил оригинальный передачи должны также быть в состоянии подвергнуть дальнейшей передачи в конкретных условиях. Такие специфические условия могут быть описаны, например, в обработке кодов.

- (66) Комиссия должна быть в состоянии решить, с эффектом на весь Союз, что некоторые третьи страны, территории, или одному или нескольким указанным секторам в рамках третьей страны, либо международная организация, предлагают адекватный уровень защиты данных, обеспечивая правовую определенность и единообразие в рамках Союза в отношении третьих стран или международных организаций, которые обеспечивают такого уровня защиты. В таких случаях, передача персональных данных для этих стран должны быть в состоянии происходить без необходимости получения специального разрешения, за исключением случаев, когда другое государство-член, из которого были получены эти данные должен дать свое разрешение на передачу.
- (67) В соответствии с основными ценностями, на которых основан Союз, в частности, защита прав человека, комиссия в своей оценке третьей страны или территории или определенной отрасли в третьей стране, учитывают как конкретной третьей стране, где уважается верховенство права, доступ к правосудию, а также международных норм и стандартов прав человека и его общего и отраслевого законодательства, включая законодательство в отношении общественной безопасности, обороны и национальной безопасности, а также общественного порядка и уголовного права. Принятие решения о достаточности применительно к территории или определенной отрасли в третьих странах следует учитывать четкие и объективные критерии, такие как конкретные виды деятельности, обработки и сферы применения соответствующих правовых норм и законодательства, действующего в третью страну. Третья страна должна предоставить гарантии обеспечения надлежащего уровня защиты, по существу, эквивалентную той, которая обеспечивается в рамках Союза, в

частности, когда данные обрабатываются в одном или нескольких конкретных секторах. В частности, третья страна должна обеспечить эффективный независимый контроль защиты данных и предусматривают механизмы сотрудничества с органами власти по защите данных государств-членов, и субъекты данных должны быть обеспечены эффективные и имеющие исковую силу прав и эффективной административной и судебной защиты.

- (68 Помимо международных обязательств третьей страной или) международной организацией, заключила комиссия также должна учитывать обязательства, вытекающие из третьей страны или международной организации участия в многосторонних или региональных систем, в частности в отношении защиты персональных данных, а также выполнения таких обязательств. В частности, присоединения третьей страны к Конвенции Совета Европы от 28 января 1981 г. о защите частных лиц в отношении автоматизированной обработки данных личного характера и дополнительный протокол к нему должны быть приняты во внимание. Комиссия должна консультироваться с Советом Европы по защите данных, установленных Регламентом (ЕС) 2016/679 ("Совета") при оценке уровня защиты в третьих странах и международных организациях. Комиссия должна также принимать во внимание любые соответствующие адекватности решения комиссии, принятые в соответствии со статьей 45 Регламента (ЕС) 2016/679.
- (69 Комиссия должна контролировать функционирование решений на уровень) защиты в третьей стране, территории или определенной отрасли в пределах третьей страны или международной организации. В своих решениях адекватность, комиссия должна обеспечить периодический обзор их функционирования. Что периодический обзор следует проводить на основе консультаций с третьей страной или международной организацией и должен учитывать все соответствующие изменения в третьей страной или международной организацией.
- (70 Комиссия должна также быть в состоянии признать, что третья страна,) территория или определенный сектор в третьей стране или международной организации, не обеспечивает адекватного уровня защиты данных. Следовательно, передача персональных данных третьим странам или международным организациям, должны быть запрещены, если требования этой Директивы, касающиеся переводов с учетом соответствующих гарантий и исключения для конкретных ситуаций выполнены. Необходимо предусмотреть процедуры для проведения консультаций между комиссией и такими третьими странами или международными организациями. Комиссия должна своевременно информировать третьей страны или международной организации причины и вступить в консультации с ним для того, чтобы исправить ситуацию.
- (71 Переводы не опирается на такую адекватность решения должно быть

) разрешено только там, где соответствующие гарантии были предоставлены в юридически обязательный документ, который гарантирует защиту персональных данных, или когда регулятор оценил все обстоятельства передачи данных и, на основе этой оценки, считает, что надлежащие гарантии в отношении защиты персональных данных существуют. Такие юридически обязывающие документы могут, например, быть юридически обязывающих двусторонних соглашений, которые были заключены государствами-членами и осуществляется в рамках их правовых систем и, которые могли бы быть реализованы по их данным предметам, соблюдение требования к защите данных и прав субъектов данных, в том числе право на получение эффективной административной или судебной защиты. Регулятор должен быть способен учитывать заключены соглашения о сотрудничестве между Европолем и Евроюстом и третьи страны, которые обеспечивают обмен персональными данными при проведении оценки всех обстоятельств, связанных с передачей данных. Инспектор должен быть в состоянии также принять во внимание тот факт, что передача персональных данных подлежат соблюдению конфиденциальности и принцип конкретности, гарантируя, что данные не будут обработаны для других целей, чем для целей передачи. Кроме того, регулятор должен учитывать, что персональные данные не будут использоваться для запроса, руки вниз или исполнения смертной казни или других форм жестокого и бесчеловечного обращения. Хотя эти условия могут рассматриваться в качестве надлежащих гарантий, позволяющей передавать данные, то регулятор должен быть способен потребовать дополнительных гарантий.

(72 Где нет адекватности решения или соответствующие гарантии существуют, или передача Категория трансферы могут осуществляться только в конкретных ситуациях, если это необходимо для защиты жизненных интересов субъекта данных или другого лица, или с целью обеспечения защиты законных интересов субъекта данных, если законодательство государства-члена, передача персональных данных не предусматривает; для предотвращения непосредственной и серьезной угрозы общественной безопасности государства-члена или третьей страны; в отдельном случае в целях предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний, в том числе по сохранению борьбы и профилактики угроз общественной безопасности, или в конкретном случае для установления, осуществления или защиты судебных исков. Те исключения должны толковаться ограничительно и не допускать частых, массовых и структурных передачи персональных данных или крупномасштабной передачи данных, но должна ограничиваться строго необходимыми данными. Такие переводы должны быть документально подтверждены и должны быть представлены контролирующему органу по запросу в целях контроля правомерности передачи.

- (73) Компетентными органами государств-членов применяются двусторонних или многосторонних международных соглашений, заключенных с третьими странами в сфере сотрудничества судебных органов по уголовным делам и полицейского сотрудничества, для обмена актуальной информацией, чтобы позволить им выполнять свои законно поставленные задачи. В принципе, это происходит через, или, по крайней мере, сотрудничество компетентных органов в третьих странах для целей настоящей Директивы, иногда даже в отсутствие двустороннего или многостороннего международного договора. Однако, в отдельных случаях регулярные процедуры, требующие связавшись такой орган третьей страны может оказаться неэффективным или неподходящим, в частности потому, что передача не может быть проведена своевременно, или потому, что орган третьей страны, не уважать верховенство права или международных норм и стандартов прав человека, так что компетентным органам государств-членов может принять решение о передаче персональных данных непосредственно получателям, установленным в этих третьих странах. Это может быть случай, когда есть острая необходимость передачи персональных данных, чтобы спасти жизнь человека, который находится в опасности стать жертвой уголовного преступления или в интересах предотвращения неминуемого совершения преступления, включая терроризм. Даже если такая передача между компетентными органами и получателями, установленных в третьих странах, должны иметь место только в отдельных случаях, данная Директива должна обеспечивать условия для регулирования таких случаев. Эти положения не должны рассматриваться как отступления от любых существующих двусторонних или многосторонних международных соглашений в сфере сотрудничества судебных органов по уголовным делам и полицейского сотрудничества. Эти правила должны применяться в дополнение к другим правилам настоящей Директивы, в частности, на правомерность обработки и главы V.
- (74) Где личные данные пересекают границы может положить на повышенный риск возможности физических лиц осуществлять свои права по защите данных, чтобы защитить себя от незаконного использования или разглашения этих данных. В то же время, надзорные органы могут обнаружить, что они не могут рассматривать жалобы и проводить расследования, связанные с деятельностью вне их границ. Их усилия для совместной работы в трансграничном контексте, также могут быть затруднены из-за недостаточной профилактической или лечебной полномочий и противоречащих друг другу правовых режимов. Поэтому, необходимо развивать более тесное сотрудничество между надзорными органами по защите данных, чтобы помочь им обмениваться информацией со своими зарубежными коллегами.
- (75) Создание в государствах-членах надзорных органов, которые способны выполнять свои функции в условиях полной независимости является

важным компонентом защиты физических лиц в отношении обработки их персональных данных. Надзорные органы должны следить за применением положений, принятых во исполнение настоящей Директивы и должны способствовать единообразному применению на всей территории Союза в целях защиты физических лиц в отношении обработки их персональных данных. В конце концов, надзорные органы должны сотрудничать друг с другом и с комиссией.

- (76) Государства-члены могут поручить надзорному органу уже)
устанавливается в соответствии с Положением (ЕС) 2016/679 ответственность за задачи, которые будут выполняться национальными надзорными органами должны быть созданы в соответствии с настоящей директивой.
- (77) Государства-члены должны установить более одного контролирующего)
органа, чтобы отразить их конституционные, организационные и административные структуры. Каждый контролирующий орган должен быть обеспечен финансовыми и людскими ресурсами, помещений и инфраструктуры, которые необходимы для эффективного выполнения своих задач, включая задачи, связанные с взаимной помощью и сотрудничества с другими надзорными органами по всему Союзу. Каждый контролирующий орган должен иметь отдельный публичный годового бюджета, который может быть частью общего государственного или национального бюджета.
- (78) Надзорные органы должны быть предметом независимого управления и)
механизмов контроля в отношении их финансовых расходов, при условии, что такое финансовый контроль не влияет на их независимость.
- (79) Общие условия для члена или членов контролирующего органа должны)
быть заложены член государственного права и, в частности, следует предусмотреть, чтобы эти члены должны быть назначены парламентом или правительством или главой государства, государства-члена на основе предложения правительства или членом правительства, или парламента или его палаты или независимого органа возложена на членов государственного права с назначением посредством прозрачной процедуры. В целях обеспечения независимости надзорного органа, член или члены, которые должны действовать добросовестно, должен воздерживаться от любых действий, несовместимых с их обязанностями и не должны, в течение срока их полномочий, участвовать в каких-либо несовместимых занятиях, будь то доходной или нет. В целях обеспечения независимости надзорного органа, персонал должен быть выбран наблюдательный орган, который может включать вмешательства независимого органа, на который возложена законом государства-члены.
- (80) Хотя эта Директива касается также деятельности национальных судов и)
других судебных органов, компетенцию контролирующих органов, не

должны затрагивать обработку персональных данных, где суды действуют в их судебных систем в целях обеспечения независимости судей при исполнении ими своих судебных функций. Что освобождение должно быть ограничено судебной деятельности в судах и не распространяется на другие виды деятельности, где судьи могут привлекаться в соответствии с законодательством своего государства-члена. Государства-члены должны также быть в состоянии обеспечить, что в компетенцию надзорного органа не распространяется на обработку персональных данных других независимых судебных органов, при исполнении своих судебных емкость, например в прокуратуру. В любом случае, в соответствии с правилами настоящей Директивы в судах и других независимых судебных органов всегда является предметом независимого надзора в соответствии со статьей 8(3) Хартия.

- (81) Каждый надзорный орган должен рассматривать жалобы, поданные любым данным объектом и должен расследовать это дело или направить его в компетентный надзорный орган. Расследование по жалобе должно проводиться, предметом судебной проверки, в том объеме, который уместен в конкретном случае. Надзорный орган должен сообщить субъекту информацию о ходе и результатах рассмотрения жалобы в течение разумного периода времени. Если дело требует дополнительного расследования или координации с другой надзорный орган, промежуточная информация должна быть предоставлена субъекту персональных данных.
- (82) В целях обеспечения эффективного, надежного и последовательного контроля за соблюдением и исполнением этой Директивы всему Союзу в соответствии с ДФЕС в интерпретации суда, надзорные органы должны иметь в каждом государстве-члене те же задачи и действенными полномочиями, в том числе следственных, исправительных и консультативными полномочиями, которые являются необходимыми средствами для выполнения своих задач. Однако их полномочия не должны мешать конкретным правил для уголовного преследования, включая расследование и судебное разбирательство уголовных преступлений, или независимость судебной власти. Без ущерба для полномочий органов прокуратуры в соответствии с законодательством штата члена, надзорные органы должны также иметь право принести нарушения этой Директивы до сведения судебной власти или к участию в судебном разбирательстве. Полномочия надзорных органов должно осуществляться в соответствии с надлежащими процессуальными гарантиями, заложенными Союза и государственного права, член, беспристрастно, справедливо и в разумные сроки. В частности, каждая мера должна быть соответствующей, необходимым и соразмерным в целях обеспечения соблюдения настоящей Директивы, принимая во внимание обстоятельства каждого конкретного случая, уважать право каждого человека быть выслушанным, прежде чем какие-либо отдельные меры,

которые могли бы отрицательно повлиять на лицо, и избегая лишних затрат и чрезмерных неудобств для лица. Следственные полномочия в отношении доступа в помещения должно осуществляться в соответствии с конкретными требованиями в области государственного права члены, такие, как необходимость получения предварительного судебного разрешения. Принятие юридически обязательного решения должны быть предметом судебного рассмотрения в государство-член наблюдательного органа, который принял решение.

- (83 Надзорные органы должны оказывать друг другу помощь при выполнении своих задач и оказывать взаимную помощь в целях обеспечения последовательного применения и соблюдения положений, принятых во исполнение настоящей Директивы.
- (84 Совет директоров должен способствовать последовательному применению настоящей Директивы всему Союзу, включая консультирование комиссии и содействие взаимодействию контролирующих органов на всей территории Союза.
- (85 Каждый субъект персональных данных должен иметь право подать жалобу в единого контролирующего органа и на эффективные средства правовой защиты в соответствии со статьей 47 Хартия в котором субъект персональных данных считает, что его или ее прав в соответствии с положениями, принятыми во исполнение этой Директивы были нарушены или когда надзорный орган не действовать на жалобу, частично или полностью отклоняет и отклоняет жалобу или не действовать там, где это необходимо для защиты прав субъекта данных. Расследование по жалобе должно проводиться, предметом судебной проверки, в том объеме, который уместен в конкретном случае. Компетентный надзорный орган должен сообщить субъекту информацию о ходе и результатах рассмотрения жалобы в течение разумного периода времени. Если дело требует дополнительного расследования или координации с другой надзорный орган, промежуточная информация должна быть предоставлена субъекту персональных данных. В целях содействия подаче жалоб, все надзорные органы должны принимать такие меры, как обеспечение подачи жалобы, форма которого также может быть заполнена в электронном виде, не исключая других средств связи.
- (86 Каждое физическое или юридическое лицо должен иметь право на эффективные средства правовой защиты в компетентном национальном суде решение контролирующего органа, который порождает юридические последствия в отношении этого лица. Такое решение касается, в частности, осуществление расследования, корректирующие и авторизации полномочия контролирующего органа или увольнение или отказ от жалобы. Однако это право не распространяется на другие меры контролирующих органов, которые не являются юридически обязательными, например, заключения или рекомендации, содержащиеся в

надзорном органе. Дело в отношении контролирующего органа должны быть привлечены в судах того государства, где создан наблюдательный орган и должна осуществляться в соответствии с законодательством своего государства-члены. Эти суды должны осуществлять полную юрисдикцию, которая должна включать компетенции рассматривать все вопросы факта и права, относящиеся к рассматриваемого спора.

- (87) Где субъект персональных данных считает, что его или ее прав в соответствии с настоящей директивой, были нарушены, он или она должны иметь право уполномочить орган, который направлен на защиту прав и интересов данных субъектов в отношении защиты их персональных данных и составлен в соответствии с государства-члена правом на подачу жалобы от своего имени в надзорный орган и в реализации права на судебную защиту. Право представительства субъектов данных должны быть без ущерба для государства-члена процессуального права, которые могут требовать обязательного представления субъектами данных адвокатом, как определено в директиве Совета 77/249/ЕЭС ⁽¹⁰⁾, прежде чем национальные суды.
- (88) Любое повреждение, которое Лицо может понести в результате обработки, которые нарушают положения принятых во исполнение настоящей Директивы, должны быть компенсированы регулятором или любой другой орган, компетентный в соответствии с законодательством штата члена. Понятие ущерба должны быть широко интерпретированы в свете прецедентного права суда в полной мере отражать целей настоящей Директивы. Это без ущерба для каких-либо претензий за ущерб, возникший из нарушения других правил в Союз или Государственный юридический члена. Когда речь идет о переработке, которые являются незаконными, что нарушает положения, принятые во исполнение этой Директивы он также охватывает обработке, что нарушает реализацию актов, принятых во исполнение настоящей Директивы. Субъекты данных должны получать полную и эффективную компенсацию за ущерб, который они понесли.
- (89) Штрафы должны быть наложены на любое физическое или юридическое лицо, как частным, так и публичным правом, которое нарушает эту Директиву. Государства-члены должны обеспечить, чтобы санкции были эффективными, соразмерными и сдерживающими, и принимали все меры для осуществления санкций.
- (90) В целях обеспечения единых условий для реализации настоящей Директивы, реализуя полномочия должны быть возложены на комиссию в отношении надлежащего уровня защиты, предоставляемой третьей страной, территорией или определенной отрасли в рамках третьей страны, либо международная организация, а формат и процедуры оказания взаимной помощи, а также порядок обмена информацией с помощью электронных средств между надзорными органами, а также между контролирующими органами и Советом. Эти полномочия должны

осуществляться в соответствии с Регламентом (ЕС) № 182/2011 Европейского парламента и Совета ⁽¹¹⁾.

- (91) Процедура экспертизы должна быть использована для принятия исполнительных актов на надлежащего уровня защиты, предоставляемой третьей страной, территорией или определенной отрасли в рамках третьей страны или международной организации, а также по формату и процедуры оказания взаимной помощи, а также порядок обмена информацией с помощью электронных средств между надзорными органами, а также между контролирующими органами и Советом, учитывая, что эти акты носят общий характер.
- (92) Комиссия должна принять немедленно применимые подзаконные акты, где, в должным образом обоснованных случаях, относящихся к третьей стране, территории или определенной отрасли в пределах третьей страны или международной организации, которые не обеспечивают надлежащего уровня защиты, императивные основания срочности этого требуют.
- (93) Поскольку цели настоящей Директивы, а именно в целях защиты основных прав и свобод физических лиц, и в частности их право на защиту персональных данных и обеспечения свободного обмена персональных данных компетентными органами в рамках Союза, не может быть в достаточной степени достигнута государствами-членами и могут, скорее, по причине масштабов или последствий действий, могут быть лучше реализованы на уровне Союза, Союз может принять меры в соответствии с принципом субсидиарности, предусмотренным в статье 5 дес. В соответствии с принципом пропорциональности, изложенным в этой статье, настоящая Директива не выходит за рамки необходимого для достижения этих целей
- (94) Конкретные положения нормативно-правовых актов Союза, принятый в области судебного сотрудничества по уголовным делам и полицейского сотрудничества, которое было принято до даты принятия настоящей Директивы, регламентирующие обработку персональных данных между государствами-членами или доступ уполномоченных органов государств-членов информационными системами, установленными в соответствии с договорами, должны оставаться неизменными, такие как, например, конкретные положения, касающиеся защиты персональных данных, применяемых в соответствии с решением Совета 2008/615/Джа ⁽¹²⁾ или статья 23 Конвенции о взаимной помощи в уголовных делах между государствами-членами Европейского Союза ⁽¹³⁾. Поскольку в статье 8 Хартияа и статье 16 договора о функционировании Европейского Союза требуют, что основополагающее право на защиту персональных данных может быть обеспечена последовательным образом по всему Союзу, комиссия должна оценить ситуацию в отношениях между этой Директивы и акты, принятые до даты принятия настоящей Директивы, регламентирующие обработку персональных данных между государствами-членами или доступ уполномоченных органов государств-

членов информационными системами, установленными в соответствии с договорами, для того, чтобы оценить необходимость согласования конкретных положений этой Директивы. Где это уместно, комиссия должна внести предложения, с тем чтобы обеспечить последовательное правовых норм, касающихся обработки персональных данных.

- (95 В целях обеспечения комплексной и последовательной защиты) персональных данных в рамках Союза, международных соглашений, заключенных государствами-членами до вступления в силу настоящей Директивы и в соответствии с соответствующими профсоюзными праве, применимом до этой даты должны оставаться в силе до момента их изменения, заменен или отозван.
- (96 Государствам-членам должно быть разрешено в срок не более двух лет с) даты вступления в силу настоящей Директивы, чтобы перенести ее. Уже обработка ведется на эту дату, должны быть приведены в соответствие с настоящей директивой в течение двух лет, после чего эта Директива вступит в силу. Однако, если такая обработка соответствует законам Союза, применяемыми до дня вступления в силу настоящей Директивы, требованиям настоящей Директивы, касающиеся предварительного согласования контролирующего органа не применять для обработки операции уже ведутся на эту дату, учитывая, что эти требования, по своему характеру, должны быть выполнены до начала обработки. Где государства-члены использовать дольше срок реализации истекает через семь лет после даты вступления в силу настоящей Директивы для встречи лесозаготовки обязательства для автоматизированной обработки систем, которые были созданы до этой даты, инспектор или обработчик должен иметь эффективные методы для демонстрации законности обработки данных, для обеспечения самоконтроля и для обеспечения целостности данных и безопасности данных, таких как журналы или другие формы записи.
- (97 Эта Директива применяется без ущерба для правил по борьбе с) сексуальными надругательствами и сексуальной эксплуатацией детей и детской порнографией, изложенным в директиве 2011/93/ЕС Европейского парламента и Совета ⁽¹⁴⁾.
- (98) Поэтому рамочное решение 2008/977/ПВД должны быть отменены.
- (99 В соответствии со статьей 6а протокол № 21 о позиции Соединенного) Королевства и Ирландии в отношении пространства свободы, безопасности и правосудия, изложенные в приложении к дес и ДФЕС, Великобритания и Ирландия не являются обязательными Правилами, изложенными в настоящей Директивы, которые касаются обработки персональных данных государств-членов при осуществлении деятельности которых подпадают под действие главы 4 и главы 5 раздела V части третьей договора о функционировании Европейского Союза Великобритания и Ирландия не являются обязательными правилами,

регулирующими форм сотрудничества судебных органов по уголовным делам и полицейского сотрудничества, которые требуют соответствия с положениями, закрепленными на основании статьи 16 договора о функционировании Европейского Союза.

- (100) В соответствии со статьями 2 и 2а протокол № 22 о позиции Дании, содержащийся в приложении к дес и ДФЕС, Дания не соблюдать правила, изложенные в этой директиве, или при их применении, которые касаются обработки персональных данных государств-членов при осуществлении деятельности которых подпадают под действие главы 4 и главы 5 раздела V части третьей договора о функционировании Европейского Союза. Учитывая, что данная Директива основывается на Шенгенскую норм в соответствии с разделом V части третьей договора о функционировании Европейского Союза, Дания, в соответствии со статьей 4 протокола, должен решить в течение шести месяцев после принятия настоящей Директивы, будет ли он его реализовать в своем национальном законодательстве.
- (101) Что касается Исландии и Норвегии, эта Директива представляет собой развитие положений шенгенских *достижений*, как это предусмотрено Соглашения, заключенного Советом Европейского Союза, Республикой Исландия и Королевством Норвегия об ассоциации этих двух государств с реализации, применения и развития шенгенских *достижений* ⁽¹⁵⁾.
- (102) Что касается Швейцарии, то эта Директива представляет собой развитие положений шенгенских *достижений*, как это предусмотрено в Соглашении между Европейским Союзом, Европейским сообществом и швейцарской Конфедерацией об ассоциации швейцарской Конфедерации в реализации, применения и развития шенгенских *достижений* ⁽¹⁶⁾.
- (103) Что касается Лихтенштейна, эта Директива представляет собой развитие положений шенгенских *достижений*, как это предусмотрено протокол между Европейским Союзом, Европейским сообществом, швейцарской Конфедерацией и княжеством Лихтенштейн о присоединении княжества Лихтенштейн к соглашению между Европейским Союзом, Европейским сообществом и швейцарской Конфедерацией о швейцарской Конфедерации, ассоциации с реализации, применения и развития шенгенских *достижений* ⁽¹⁷⁾.
- (104) Настоящая Директива уважает основные права и соблюдает принципы, признанные в Хартияе как записано в ДФЕС, в частности права на уважение частной и семейной жизни, право на защиту персональных данных, право на эффективную правовую защиту и на справедливое судебное разбирательство. Ограничения этих прав в соответствии со статьей 52(1) Хартияя, так как они необходимы для достижения целей, представляющих общий интерес, признанный Союз или необходимости защиты прав и свобод других лиц.
- (105) В соответствии с совместной политической декларацией от 28 сентября

-) 2011 года государствами-членами и комиссией в пояснительных документах, Государства-участники обязались сопровождать, в обоснованных случаях, уведомление об их мероприятиях транспонирования один или несколько документов, объясняющих взаимосвязь между компонентами директивы и соответствующими частями национальных мероприятий транспонирования. В связи с этой директивой, законодатель считает передачу таких документов, которые должны быть оправданы.
- (106 Европейского союза по защите данных руководителем были проведены консультации в соответствии со статьей 28(2) Регламента (ЕС) № 45/2001 и доставлен мнение 7 марта 2012.⁽¹⁸⁾)
- (107 Эта Директива не препятствует государствам-членам от реализации прав данных субъектов на информацию, доступ к данным и их исправления или уничтожения персональных данных и ограничение обработки в ходе производства по уголовному делу, и их возможных ограничений, к ним, в национальных правилах уголовного судопроизводства,

ПРИНЯЛИ НАСТОЯЩУЮ ДИРЕКТИВУ:

ГЛАВА I Общие положения

Статья 1 Предмет и задачи

1. Эта Директива устанавливает правила о защите физических лиц применительно к обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности.
2. В соответствии с настоящей директивой, государства-члены должны:
 - (а защищать основные права и свободы физических лиц, и в частности их) право на защиту персональных данных;
 - (б Обеспечить, чтобы обмен персональными данными компетентными) органами в Союзе, где такой обмен требуется по праву Союза или государств-членов, не ограничивается и не запрещается по причинам, связанным с защитой физических лиц в отношении обработки персональных данных.
3. Настоящая Директива не должна препятствовать государствам-членам предоставлять более высокие гарантии, чем те, которые установлены в настоящей Директиве для защиты прав и свобод субъекта данных в отношении обработки персональных данных компетентными органами.

Статья 2

Область

1. Настоящая Директива применяется к обработке персональных данных компетентными органами для целей, изложенных в статье 1(1).
2. Эта Директива относится к обработке персональных данных полностью или частично с помощью автоматизированных средств, а также для обработки других более автоматизированным способом персональных данных, которые являются частью системы подачи или предназначены для того, чтобы стать частью системы подачи.
3. Настоящая Директива не применяется к обработке персональных данных:
 - (а в ходе осуществления деятельности, которая выходит за рамки права Союза;
)
 - (б) Институтам, органам, ведомствам и учреждениям Союза.

Статья 3

Определения

Для целей настоящей Директивы:

- (1 "персональные данные" - означает любую информацию, относящуюся к
) идентифицированному или идентифицируемому физическому лицу («субъект данных»); Идентифицируемое физическое лицо - это лицо, которое может быть идентифицировано, прямо или косвенно, в частности, путем ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или на один или несколько факторов, специфичных для физического, Генетической, умственной, экономической, культурной или социальной идентичности этого физического лица;
- (2 'обработка' означает любую операцию или набор операций, выполняемых
) по персональным данным или наборам персональных данных независимо от того, осуществляется ли автоматизированными средствами, такими как сбор, запись, организация, структурирование, хранение, адаптация или изменение, поиск, консультации, использование, раскрытие Передача, распространение или иное предоставление, выравнивание или комбинация, ограничение, стирание или уничтожение;
- (3 'ограничение обработки' означает маркировку хранимых персональных
) данных с целью ограничения их переработки в будущем;
- (4 'профилирование' означает любую форму автоматизированной обработки
) персональных данных, состоящую из использования персональных данных для оценки некоторых личных аспектов, связанных с физическим лицом, в частности для анализа или прогнозирования аспектов, касающихся работы этого физического лица на работе, экономической ситуации, состояния здоровья, Личные предпочтения, интересы, надежность, поведение,

местоположение или движения;

- (5 «псевдонимизация» означает обработку персональных данных таким образом, что персональные данные больше не могут быть отнесены к конкретному субъекту данных без использования дополнительной информации при условии, что такая дополнительная информация хранится отдельно и подлежит техническим и организационным мерам Обеспечить, чтобы личные данные не были приписаны идентифицированному или идентифицируемому физическому лицу¹;
- (6 «система хранения документов» означает любой структурированный набор персональных данных, которые доступны в соответствии с конкретными критериями, будь то централизованными, децентрализованными или разбросанными на функциональной или географической основе;;
- (7 "компетентный орган" означает:
-)
- (а любой государственный орган, компетентный в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности; или
- (б любые другие органы или юридическим лицом, уполномоченным государством-членом права на осуществление государственной власти и органами государственной власти в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, в том числе профилактика и предупреждение угроз общественной безопасности;
- (8 'инспектор' означает компетентный орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; когда цели и средства такой обработки определяются правом Союза или государства-члена, инспектор, конкретные критерии его выдвижения могут быть предусмотрены правом Союза или государства-члена;
- (9 'обработчик' означает физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные по поручению инспектора;
- (10)«Получатель» означает физическое или юридическое лицо, государственный орган, агентство или иной орган, которому раскрываются персональные данные, независимо от того, является ли оно третьим лицом или нет. Однако государственные органы, которые могут получать персональные данные в рамках конкретного расследования в соответствии с

¹Псевдонимизация – замена имени или какого-либо другого идентификационного признака участников разговора на псевдоним. Информацию о связи между псевдонимом и реальной личностью можно хранить отдельно от сведений о вызовах во избежание доступа неуполномоченных лиц.

законодательством государства-члена, не рассматриваются как получатели; Обработка этих данных этими государственными органами осуществляется в соответствии с применимыми правилами защиты данных в соответствии с целями обработки;

(11) «Нарушение персональных данных» означает нарушение безопасности, ведущее к случайному или незаконному уничтожению, утрате, изменению, несанкционированному раскрытию или доступу к персональным данным, переданным, сохраненным или иным образом обработанным;

(12) «Генетические данные» означают персональные данные, относящиеся к наследуемым или приобретенным генетическим характеристикам физического лица, которые предоставляют уникальную информацию о физиологии или здоровье этого физического лица и которые, в частности, являются результатом анализа биологического образца из Физическое лицо;

(13) «Биометрические данные» означают персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица, которые позволяют или подтверждают уникальную идентификацию этого физического лица, такую как изображения лица или дактилоскопические данные;

(14) «Данные о здоровье» означают личные данные, связанные с физическим или психическим здоровьем физического лица, включая предоставление медицинских услуг, которые раскрывают информацию о его состоянии здоровья;

(15) «надзорный орган» означает независимый общественный орган, который создан государством-членом в соответствии со статьей 41;

(16) «Международная организация» означает организацию и подчиненные ей органы, регулируемые международным публичным правом, или любой другой орган, который создается на основе соглашения между двумя или более странами.

ГЛАВА II. Принципы

Статья 4

Принципы, касающиеся обработки персональных данных

1. Государства-члены должны предусмотреть персональных данных:

(а) обработаны законно и справедливо;

(б) собраны для определенных, явных и законных целей и не обработаны) способом, несовместимым с этими целями;

- (с адекватными, соответствующими и не избыточными по отношению к
) целям, для которых они обрабатываются;
- (д точный и там, где это необходимо, обновляются; все разумные меры
) должны быть предприняты, чтобы гарантировать, что персональные данные, которые являются неточными, с учетом целей, для которых они обрабатываются, будут удалены или исправлены без задержки;
- (е храниться в форме, позволяющей идентифицировать субъекты данных, не
) дольше, чем это необходимо для целей, для которых они обрабатываются;
- (Ф обработанные таким образом, чтобы обеспечить надлежащую сохранность
) персональных данных, включая защиту от несанкционированной или незаконной обработки и случайной потери, уничтожения или повреждения, используя соответствующие технические и организационные меры.
2. Обработка той же или другой инспектор для какой-либо из целей, изложенных в статье 1(1), для которых собираются персональные данные, не допускается, поскольку:
- (а инспектор уполномоченных на обработку персональных данных для такой
) цели в соответствии с Союз или Государственный закон-членов; и
- (б обработка является необходимым и соразмерным в том, что других целей в
) соответствии с Союза или государственного права члены.
3. Обработка той же или другой инспектор может включать архивацию в общественных интересах, научных, статистических или исторических пользование, для целей, изложенных в статье 1(1), с учетом соответствующих гарантий для прав и свобод субъектов данных.
4. Инспектор несет ответственность за, и быть в состоянии продемонстрировать соответствие с пунктами 1, 2 и 3.

Статья 5

Сроки хранения и проверки

Государства-члены должны предусмотреть соответствующие временные рамки для уничтожения персональных данных или для периодического анализа потребности в хранении персональных данных. Процедурные меры должны обеспечивать соблюдение этих сроков.

Статья 6

Разграничения между разными категориями субъекта данных

Государства-члены должны обеспечить, где это применимо, и насколько это возможно, инспектору проводить четкое разграничение между персональными данными разных категорий субъектов данных, такими как:

- (а лица, в отношении которого существуют серьезные основания полагать, что) они совершили или намереваются совершить уголовное преступление;
- (б) лицам, осужденным за уголовное преступление;
- (с жертвами уголовного преступления или лиц, в отношении которых) определенные факты порождают основания полагать, что он или она может стать жертвой уголовного преступления; и
- (д другими участниками уголовного преступления, такие как лиц, которые) могут быть вызваны для дачи показаний при проведении расследований в связи с уголовными преступлениями или последующего уголовного судопроизводства, лиц, которые могут предоставить информацию об уголовных преступлениях, или контакты или партнеры одного из лиц, указанных в пунктах (А) и (В).

Статья 7

Различие между личными данными и проверкой качества персональных данных

1. Государства-члены должны предоставлять персональные данные на основании фактов, которые следует отличать, насколько это возможно, от персональных данных, основанных на личных оценках.
2. Государства-члены должны предоставить компетентным органам принять все разумные меры, чтобы гарантировать, что персональные данные, которые являются неточными, неполными или не в курсе не передаются или предоставляются. С этой целью, каждый компетентный орган должен, насколько это возможно, проверить качество личных данных, прежде чем они передаются или предоставляются. Насколько это возможно, в передачи персональных данных, необходимой информации, позволяющей принимающего компетентного органа, чтобы оценить степень точности, полноты и достоверности персональных данных, и насколько они в курсе должны быть добавлены.
3. Если выяснится, что неверные персональные данные были переданы или персональные данные были незаконно переданы, получатель должен быть уведомлен незамедлительно. В таком случае персональные данные должны быть исправлены или стерты или обработки должны быть ограничены в соответствии со статьей 16.

Статья 8

Законность обработки

1. Государства-члены обеспечивают обработку для законности только в том случае, если обработка необходима для выполнения задачи, выполняемой компетентным органом для целей, указанных в Статье 1 (1), и что она основана на Союз или законодательство государства-члена.

2. Законодательство государств-членов, регулирующее обработку в рамках настоящей Директивы, должно определять, по крайней мере, цели обработки, персональные данные, подлежащие обработке, и цели обработки.

Статья 9

Специальные условия обработки

1. Личные данные, собранные компетентными органами для целей, указанных в Статье 1 (1), не обрабатываются для целей, отличных от целей, указанных в Статье 1 (1), если такая обработка не разрешена законодательством Союза или Государства-Члена. Если личные данные обрабатываются для таких других целей, правило (ЕС) 2016/679 применяется, если обработка не осуществляется в деятельности, которая выходит за рамки права Союза.

2. В тех случаях, когда компетентные органы наделяются правом государств-членов выполнением задач, отличных от задач, выполняемых для целей, указанных в Статье 1 (1), Регламент (ЕС) 2016/679 применяется к обработке для таких целей, в том числе для архивирования Целей в общественных интересах, научных или исторических целях исследования или статистических целях, если обработка не осуществляется в деятельности, которая выходит за рамки права Союза.

3. Государства-члены, если законодательство Союза или государств-членов, применимое к передающему компетентному органу, предоставляют конкретные условия для обработки, предусматривают, что передающий компетентный орган должен информировать получателя таких персональных данных об этих условиях и требованиях их соблюдения.

4. Государства-члены должны предоставлять передающему компетентному органу не применять условия в соответствии с пунктом 3 к получателям в других государствах-членах или к агентствам, ведомствам и органам, созданным в соответствии с главами 4 и 5 раздела V TFEU, за исключением тех, которые применимы к Аналогичные передачи данных в государстве-члене передающего компетентного органа.

Статья 10

Обработка специальных категорий персональных данных

Обработку персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, или членство в профсоюзах, и обработки генетических данных, биометрических данных для уникальной идентификации физического лица, данные, касающиеся здоровья или данные, касающиеся физического лица по половой жизни или сексуальной ориентации, допускается только в случае строгой необходимости, с учетом соответствующих гарантий для прав и свобод субъекта данных, и только:

(a) где уполномоченные Союза или законодательством штата-членов;

(б для защиты жизненно важных интересов субъекта данных или другого
) физического лица; или

(с где такая обработка относится к данным, которые явно обнародованы
) субъектом персональных данных.

Статья 11

Автоматизированное индивидуальное принятие решений

1. Государства-члены должны предусмотреть решение, основанное исключительно на автоматизированной обработке, включая профилирование, которое создает неблагоприятное юридическое действие в отношении субъекта данных или существенно влияет на него, должно быть запрещено, если это не разрешено правом Союза или государства-члена, Является предметом и который обеспечивает надлежащие гарантии прав и свобод субъекта данных, по крайней мере право на вмешательство человека со стороны инспектора.
2. Решения, упомянутые в пункте 1 настоящей статьи, не основаны на специальных категориях персональных данных, упомянутых в статье 10, если не приняты соответствующие меры для защиты прав и свобод субъекта данных и законных интересов.
3. Профилирование, приводящее к дискриминации в отношении физических лиц на основе специальных категорий персональных данных, указанных в статье 10, запрещается в соответствии с правом Союза.

ГЛАВА III. Права субъекта данных

Статья 12

Коммуникация и условия осуществления прав субъекта данных

1. Государства-члены должны предусмотреть, чтобы контролер предпринял разумные шаги для предоставления любой информации, указанной в Статье 13, и передал любое сообщение в отношении Статей 11, 14-18 и 31, относящееся к обработке субъекту данных в сжатой, понятной и Легко доступной форме, используя понятный и понятный язык. Информация должна быть предоставлена с помощью любых соответствующих средств, в том числе с помощью электронных средств. Как правило, диспетчер предоставляет информацию в той же форме, что и запрос.
2. Государства-члены должны предусмотреть, чтобы контролер содействовал осуществлению прав субъекта данных согласно статьям 11 и 14-18.
3. Государства-члены должны предусмотреть, чтобы контролер в письменной форме информировал субъекта данных о последующих действиях по его просьбе без неоправданной задержки.

4. Государства-члены обеспечивают информацию, предоставленную в соответствии со Статьей 13, и любое сообщение или действия, предпринятые в соответствии со Статьями 11, 14-18 и 31, которые должны предоставляться бесплатно. Если запросы от субъекта данных явно не обоснованы или чрезмерны, в частности из-за их повторяющегося характера, инспектор может либо:

(а) взимать разумную плату, с учетом административных расходов за предоставление информации и коммуникации и принятия решения; или

(б) отказываются действовать по запросу.

Инспектор несет бремя демонстрируя явно необоснованной или чрезмерной характер запроса.

5. Где инспекторе имеются разумные сомнения по поводу личности физического лица, сделав запрос, упомянутого в статье 14 или 16, инспектор может запросить предоставление дополнительной информации, необходимой для подтверждения личности субъекта персональных данных.

Статья 13

Информация доступная или предоставляемая субъекту данных

1. Государства-члены должны предусмотреть, чтобы инспектор предоставлял субъекту данных по крайней мере следующую информацию:

(а) личность и контактные данные инспектора ;

(б) контактные данные Уполномоченного по защите данных, где это применимо;

(с) цели обработки, для которых персональные данные предназначены;

(д) право подать жалобу в надзорный орган и контактные данные надзорного органа;

(е) наличие права требовать от регулятора доступа и исправления или уничтожения персональных данных и ограничение обработки персональных данных субъекта данных.

2. В дополнение к информации, указанной в пункте 1, государства-члены должны предусмотреть в законе для инспектора , чтобы дать субъекту данных, в конкретных случаях, следующим дополнительную информацию для осуществления своих прав:

(а) правовой основой для обработки;

(б) период, для которого личные данные будут храниться, или, если это невозможно, критерии, используемые для определения этого периода;

(с где это применимо, категории получателей персональных данных, в том) числе в третьих странах или международных организациях;

(д в случае необходимости, дополнительную информацию, в частности, где) личные данные собираются без ведома субъекта данных.

3. Государства-участники могут принимать законодательные меры, отсрочки, ограничения или опуская предоставление информации субъекту данных в соответствии с пунктом 2 в той мере, что и как, такая мера является необходимой и соразмерной мерой в демократическом обществе, с должным учетом прав и законных интересов физического лица, в целях:

(а не препятствовать должностным лицом или юридических запросов,) проведения расследований или процедур;

(б во избежание ущерба для профилактики, выявления, расследования или) судебного преследования уголовных преступлений или исполнения уголовных наказаний;

(с) защиты общественной безопасности;

(д) защита национальной безопасности;

(е) защиты прав и свобод других лиц.

4. Государства-участники могут принимать законодательные меры для того, чтобы определить категории обработка, которая может полностью или частично подпадает ни под один из пунктов, перечисленных в пункте 3.

Статья 14

Право доступа субъекта данных

В соответствии со Статьей 15, государства-члены должны обеспечивать право данных, подлежащих получению от инспектора подтверждения относительно того, обрабатываются ли личные данные о нем или нет, и, если это так, доступ к персональным данным И следующую информацию:

(а) цели и правовое основание для обработки;

(б) категории соответствующих персональных данных;

(с получатели или категории получателей, которым персональные данные) были раскрыты, в частности получателей в третьих странах или международных организациях;

(д там, где это возможно, предполагаемый срок, в течение которого будут) храниться персональные данные, или, если это невозможно, критерии, используемые для определения этого периода;

(е наличие права на запрос от инспектора изменении или уничтожении

-) персональных данных или ограничение обработки персональных данных субъекта;
- (Ф право подать жалобу в надзорный орган и контактные данные надзорного) органа;
- (г связи обрабатываемые персональные данные и информацию о своем) происхождении.

Статья 15

Ограничения на право доступа

1. Государства-члены могут принимать законодательные меры, ограничивающие, полностью или частично, право субъекта данных на доступ в той степени, в которой и до тех пор, пока такое частичное или полное ограничение является необходимой и пропорциональной мерой в демократическом обществе с должным учетом основополагающего Прав и законных интересов заинтересованного физического лица, чтобы:
 - (а не препятствовать должностным лицом или юридических запросов,) проведения расследований или процедур;
 - (б во избежание ущерба для профилактики, выявления, расследования или) судебного преследования уголовных преступлений или исполнения уголовных наказаний;
 - (с) защиты общественной безопасности;
 - (д) защита национальной безопасности;
 - (е) защиты прав и свобод других лиц.
2. Государства-участники могут принимать законодательные меры для того, чтобы определить категории обработка, которая может полностью или частично подпадают под пункты (А) и (е) пункта 1.
3. В случаях, упомянутых в параграфах 1 и 2, государства-члены должны предусмотреть, чтобы инспектор без промедления информировал субъекта данных о любом отказе или ограничении доступа, а также о причинах отказа или ограничения. Такая информация может быть опущена, если ее положение подрывает цель в соответствии с пунктом 1. Государства-члены должны предусмотреть, чтобы инспектор информировал субъекта данных о возможности подачи жалобы в надзорный орган или о поиске судебных средств правовой защиты.
4. Государства-члены должны предусмотреть, чтобы инспектор документировал фактические или юридические причины, на которых основано решение. Эта информация должна быть предоставлена надзорным органам.

Статья 16

Право на исправление или удаление персональных данных и ограничение переработки

1. Государства-члены должны предусмотреть право субъекта данных получать от инспектора без неоправданной задержки исправления неточных персональных данных, касающихся его или ее. С учетом целей обработки, государства-члены должны предусмотреть, что субъект данных имеет право завершить неполные персональные данные, в том числе путем предоставления дополнительного заявления.

2. Государства-члены должны требовать, регулятор, чтобы стереть персональные данные без неоправданной задержки и право субъекта данных получать от инспектора удаление личных данных, касающихся его или ее без промедления, где обработка нарушает нормы, принятые в соответствии со статьей 4, 8 или 10, или когда персональные данные должны быть удалены в целях соблюдения юридической обязанности, к которой инспектор зависит.

3. Вместо стирания, регулятор будет ограничивать обработки, где:

(а) точность персональных данных, оспариваемые субъектом персональных данных и их точность или неточность не может быть установлена; или

(б) персональные данные должны быть сохранены для целей доказательства.

Если обработка ограничивается в соответствии с пунктом (а) этого подпункта, инспектор должен информировать субъекта данных до отмены ограничения обработки.

4. Государства-члены должны предусмотреть инспектор информировать субъекта данных в письменной форме либо об отказе в изменении или уничтожении персональных данных или ограничение переработка и причин для отказа. Государства-участники могут принимать законодательные меры по ограничению, полностью или частично, обязательство предоставлять такую информацию при условии, что такое ограничение является необходимой и соразмерной мерой в демократическом обществе, с должным учетом прав и законных интересов физического лица, в целях:

(а) не препятствовать должностным лицам или юридическим запросам, проведения расследований или процедур;

(б) во избежание ущерба для профилактики, выявления, расследования или судебного преследования уголовных преступлений или исполнения уголовных наказаний;

(с) защиты общественной безопасности;

(д) защита национальной безопасности;

(е) защиты прав и свобод других лиц.

Государства-члены должны предусмотреть инспектор уведомлять субъекта персональных данных о возможности подачи жалобы в надзорный орган или ищет судебной защиты.

5. Государства-члены должны предусмотреть, чтобы инспектор сообщал об устранении неточных личных данных компетентному органу, из которого возникли неточные персональные данные.

6. Государства-члены должны, если личные данные были исправлены или удалены или обработка была ограничена в соответствии с пунктами 1, 2 и 3, предусматривают, что инспектор уведомляет получателей и что получатели должны исправлять или удалять персональные данные или ограничивать обработку под их личную ответственность.

Статья 17

Осуществление прав субъекта данных и проверка со стороны контролирующего органа

1. В случаях, упомянутых в Статье 13 (3), Статье 15 (3) и Статье 16 (4), государства-члены принимают меры, предусматривающие, что права субъекта данных могут также осуществляться через компетентный надзорный орган.

2. Государства-члены должны предусмотреть, чтобы контролер информировал субъекта данных о возможности осуществления своих прав через надзорный орган в соответствии с пунктом 1.

3. Если право, упомянутое в параграфе 1, осуществляется, надзорный орган должен информировать субъекта данных, по крайней мере, о том, что все необходимые проверки или рассмотрение органа надзора имели место. Контролирующий орган также информирует субъекта данных о своем праве искать средство судебной защиты.

Статья 18

Права субъекта данных при проведении уголовных расследований и разбирательств

Государства-члены могут предусматривать осуществление прав, предусмотренных в статьях 13, 14 и 16 должны быть проведены в соответствии с законом государства-члена, где персональные данные содержатся в судебном решении или запись или случае файл обрабатывается в ходе уголовного расследования и судебного разбирательства.

ГЛАВА IV. Инспектор и обработчик

Раздел 1 Общие обязательства

Статья 19

Обязанности инспектора

1. Государства-члены обеспечивают инспектора с учетом характера, сферы применения, контекста и целей обработки, а также рисков различной вероятности и серьезности прав и свобод физических лиц, осуществления соответствующих технических и организационных мер для обеспечить и продемонстрировать, что обработка выполняется в соответствии с настоящей Директивой. Эти меры должны, при необходимости, пересматриваться и обновляться.
2. В случае пропорциональности в отношении деятельности по переработке меры, упомянутые в пункте 1, должны включать в себя осуществление соответствующей политики защиты данных инспектором.

Статья 20

Защита данных в определенных целях и по умолчанию

1. Государства-члены должны предусмотреть для диспетчера с учетом уровня техники, стоимости осуществления и характера, сферы применения, контекста и целей обработки, а также рисков различной вероятности и серьезности прав и свобод Физические лица, создаваемые обработкой, как во время определения средств для обработки, так и во время самой обработки, для осуществления соответствующих технических и организационных мер, таких как псевдонимизация, которые предназначены для реализации принципов защиты данных, например Как минимизация данных, эффективным образом и интегрировать необходимые гарантии в обработку, чтобы соответствовать требованиям настоящей Директивы и защищать права субъектов данных.
2. Государства-члены должны предусматривать, чтобы контролер осуществлял надлежащие технические и организационные меры, гарантирующие, что по умолчанию обрабатываются только персональные данные, которые необходимы для каждой конкретной цели обработки. Это обязательство распространяется на объем собранных персональных данных, объем их обработки, период их хранения и их доступность. В частности, такие меры должны обеспечивать, чтобы по умолчанию персональные данные не становились доступными без вмешательства индивида неопределенному числу физических лиц.

Статья 21

Совместное инспектирование

1. Государства-члены, в которых два или более инспекторов роллеров совместно определить цели и средства обработки, обеспечивать их совместное инспекторов. Они, прозрачно, определения их соответствующих обязанностей по соблюдению условий настоящей Директивы, в частности, в отношении осуществления прав субъекта персональных данных и их обязанности по предоставлению информации, указанной в статье 13, посредством договоренности между ними, если и в той мере, соответствующие обязанности диспетчеров определяются Союза или государства-члена права на которые

инспекторы подлежат. Организация назначает координатора по данным предметам. Государства-члены могут определить, какие из совместных инспекторы могут действовать как единая точка контакта для субъекта данных, чтобы осуществлять свои права.

2. Независимо от условий соглашения, указанных в пункте 1, государства-члены могут предусмотреть данные субъекта для осуществления его или ее прав в соответствии с положениями, принятыми во исполнение этой Директивы в отношении и против каждого из инспекторов.

Статья 22

Обработчик

1. Государства-члены должны, если обработка производится от имени инспектора, предназначены для инспектор для использования только обработчиков предоставления достаточных гарантий для осуществления соответствующих технических и организационных мер таким образом, что обработка будет соответствовать требованиям данной Директивы, и обеспечивать защиту прав субъекта данных.

2. Государства-члены должны предусмотреть обработчик не заниматься другой обработчик без предварительного и письменного разрешения регулятора. В случае общего письменного разрешения, обработчик информирует инспектор о любых предполагаемых изменениях, касающихся дополнение или замена другими обработчиками, тем самым давая инспектору возможность возражать против таких изменений.

3. Государства-члены должны обеспечивать обработку обработчиком регулироваться договором или другим нормативно-правовым актом в рамках Союза или государства-члена права, что является обязательным для исполнения на обработчике с точки зрения инспектора , а также излагаются предмет и продолжительность обработки, характер и цели обработки, вида персональных данных и категории данных субъектов, а также обязанности и права инспектора . Этим договором или другим нормативно-правовым актом предусматривается, в частности, обработчик:

- (а) действует только по поручению инспектора ;
- (б гарантирует, что лиц, уполномоченных на обработку персональных данных) взяли на себя обязательство о конфиденциальности или в соответствующих нормативных обязательств о конфиденциальности;
- (с помогает инспектор с помощью любых надлежащих средств обеспечения) соблюдения положений, касающихся прав субъектов ПДН;
- (д при выборе инспектора , удаляет и возвращает все личные данные на) инспектор после окончания оказания услуги по обработке данных, а также удаление существующей копии, если Союз или государственное право члена требует хранения персональных данных;

(е делает доступными для инспектора все сведения, необходимые для
) подтверждения соответствия данной статье;

(Ф соответствует условиям, упомянутым в пунктах 2 и 3 для привлечения
) другой обработчик.

4. Договором или другим нормативно-правовым актом, указанным в пункте 3, должны быть в письменной форме, в том числе в электронном виде.

5. Если обработчик определяет, в нарушение этой Директивы, цели и средства обработки, что обработчик считается регулятора в отношении этого процесса.

Статья 23

Обработки под руководством инспектора или обработчика

Государства-члены должны обеспечивать обработчик и любое лицо, действующее по санкции инспектора или обработчика, которое имеет доступ к персональным данным, не обрабатывать эти данные, кроме как по указанию инспектора, если это не требуется по Союзу или государства-члена права.

Статья 24

Учет о деятельности обработки

1. Государства-члены предусматривают, что инспекторы должны вести учет всех категорий обрабатываемых видов деятельности, находящихся в их ведении. Эта запись должна содержать всю следующую информацию:

(а имя и контактные данные инспектора и, при необходимости, совместного
) управления и защиты данных сотрудника;

(б) целями обработки;

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

(д) описание категорий субъекта данных и категорий персональных данных;

(е) где это применимо, использование профилирования;

(Ф где это применимо, категории передач персональных данных в третью
) страну или международную организацию;

(г указанием организационно-правовой основой для операций по переработке,
) в том числе переводы, для которых персональные данные предназначены;

(ч где это возможно, предполагаемые сроки для стирания различных категорий
) персональных данных;

(я где это возможно, Общее описание технических и организационных мер) безопасности, указанных в статье 29(1).

2. Государства-члены должны обеспечить для каждого обработчика, чтобы вести учет всех видов деятельности, обработки, осуществляемой от имени инспектора , содержащий:

(а имя и контактные данные одного или нескольких обработчиков, каждый) инспектор, от имени которой действует обработчик и, где это применимо, защита данных сотрудника;

(б) категории обработки, осуществляемой от имени каждого инспектора ;

(с где это применимо, передача персональных данных в третью страну или) международную организацию, где явно указано в инспектор, включая определение того, что третьей страной или международной организацией;

(д где это возможно, Общее описание технических и организационных мер) безопасности, указанных в статье 29(1).

3. Записи, указанные в пунктах 1 и 2 должны быть в письменной форме, в том числе в электронной форме.

Инспектор и обработчик принимает эти данные доступны в контролирующий орган по запросу.

Статья 25

Ведение записей

1. Государства-члены должны обеспечить хранение журналов, по крайней мере, для следующих операций обработки в автоматизированных системах обработки: сбор, изменение, консультации, разглашение, включая переводы, объединение и стирание. Журналы консультаций и раскрытия информации позволяют установить обоснование, дату и время таких операций и, насколько это возможно, идентификацию лица, которое консультировалось или раскрывало личную информацию, а также личности получателей таких персональных данных ,

2. Журналы используются исключительно для проверки законности обработки, самоконтроля, обеспечения целостности и безопасности персональных данных, а также для уголовного судопроизводства.

3. Инспектор и обработчик должны предоставить журналы доступа контролирующему органу по запросу.

Статья 26

Сотрудничество с надзорным органом

Государства-члены должны предусмотреть инспектор и обработчик для сотрудничества, по запросу, с контролирующего органа в выполнении его задач по запросу.

Статья 27

Оценка воздействия защиты данных

1. Где Тип обработки, в частности, с использованием новых технологий, и принимая во внимание характер, объем, условия и цели обработки может повлечь за собой высокий риск для прав и свобод физических лиц, государства-члены должны обеспечить для инспектора выполнять до обработки, оценки влияния планируемых операций на защиту персональных данных.
2. Оценки, упомянутой в пункте 1, должны содержать, по крайней мере, Общее описание предполагаемых операций обработки, оценки рисков для прав и свобод субъектов данных, меры, предусмотренные для устранения этих рисков, гарантий, безопасности, меры и механизмы по обеспечению защиты персональных данных и для подтверждения соблюдения настоящей Директивы, принимая во внимание права и законные интересы данных субъектов и других заинтересованных лиц.

Статья 28

Предварительная консультация надзорного ведомства

1. Государства-члены должны предусмотреть инспектор или обработчик проконсультироваться контролирующего органа до обработки данных, которая станет частью новой системы подачи должны быть созданы, где:
 - (а защита оценка воздействия на данные, как это предусмотрено в статье 27) указано, что обработка может привести к высокому риску при отсутствии мер, принимаемых регулятором для снижения риска; или
 - (б Тип обработки, в частности, где с помощью новых технологий, механизмов) или процедур, предполагает высокий риск для прав и свобод субъектов данных.
2. Государства-члены должны предусматривать консультирование надзорного органа при подготовке предложения о законодательной мере, которая должна быть принята национальным парламентом, или о мерах регулирования, основанных на такой законодательной мере, которая касается обработки.
3. Государства-члены должны предусмотреть, что надзорный орган может составить список операций по обработке, которые подлежат предварительной консультации в соответствии с пунктом 1.
4. Государства-члены должны предусмотреть, чтобы контролер предоставил надзорному органу оценку воздействия на защиту данных в соответствии со Статьей 27 и, по запросу, с любой другой информацией, которая позволила бы надзорному органу оценить степень соответствия обработки и в В частности,

рисков для защиты персональных данных субъекта данных и соответствующих гарантий.

5. Государства-члены, если надзорный орган считает, что предполагаемая обработка, указанная в пункте 1 настоящей статьи, нарушит положения, принятые в соответствии с настоящей Директивой, в частности, если контролер недостаточно идентифицировал или смягчил риск, предоставить. Чтобы надзорный орган предоставил в течение периода до шести недель с момента получения запроса на консультацию письменную консультацию контролеру и, где это применимо, обработчику и мог использовать любую из своих полномочий, указанных в статье 47. Этот период может быть продлен на месяц с учетом сложности предполагаемой обработки. Контролирующий орган должен сообщить диспетчеру и, где применимо, обработчик любого такого продления в течение одного месяца с момента получения запроса на консультацию вместе с причинами задержки.

Раздел 2

Безопасности персональных данных

Статья 29

Безопасность обработки

1. Государства-члены должны предоставлять инспектору и обработчику с учетом уровня техники расходы на внедрение, а также характер, сферу применения, контекст и цели обработки, а также риск различной вероятности и серьезности для Прав и свобод физических лиц, осуществлять соответствующие технические и организационные меры для обеспечения уровня безопасности, соответствующего риску, в частности в отношении обработки специальных категорий персональных данных, упомянутых в статье 10.

2. В отношении автоматизированной обработки каждое государство-член должно предоставить инспектору или обработчику после оценки рисков меры, направленные на:

(а запретить несанкционированный доступ к обработке оборудования,
) используемого для переработки ('контроль доступа');

(б предотвратить несанкционированное чтение, копирование, модификация
) или удаление данных СМД (контроль данных СМД);

(с предотвращения несанкционированного ввода личных данных и
) несанкционированное проверка, изменение или удаление сохраненных персональных данных (далее-контроль за хранением');

(д предотвратить использование автоматизированных систем обработки
) неуполномоченными лицами с помощью оборудования связи данных (контроль пользователя);

(е обеспечить, чтобы лица, уполномоченного на использование

-) автоматизированной системы обработки имеют доступ только к тем персональным данным, которые охватываются авторизации доступа (контроль доступа данных);
- (Ф обеспечить это можно проверить и установить органах, в которых) персональные данные были или могут передаваться или предоставляться через оборудование передачи данных ('диспетчерской связи');
- (г обеспечить, чтобы впоследствии можно было проверить и установить,) какие личные данные введенные в автоматизированных системах обработки и когда и кем персональные данные входной сигнал (входной контроль);
- (ч предотвратить несанкционированное чтение, копирование, изменение или) удаление персональных данных при передаче персональных данных либо при транспортировке данных средств массовой информации (транспортный контроль);
- (я убедитесь, что установлены системы могут, в случае прерывания, быть) восстановлены ("восстановление");
- (Дж убедитесь, что функции системы проанализировать, что появление) неисправностей в функции, сообщает ("надежность") и хранить персональные данные не могут быть повреждены с помощью неисправной системы ("целостности").

Статья 30

Уведомление о нарушении персональных данных в контролирующей органу

1. Государства-члены должны, в случае, если персональные данные нарушения, предусматривают инспектор уведомить без промедления и, где это возможно, не позднее, чем за 72 часа после того, как стало известно о нем, личные данные и нарушения в контролирующей орган, кроме случаев, когда персональные данные нарушение вряд ли может привести к риск для прав и свобод физических лиц. Если уведомление в контролирующей орган не будет произведена в течение 72 часов, он сопровождается причины задержки.
2. Обработчик уведомляет инспектор без неоправданной задержки после того, как стало известно о личной кражи данных.
3. Уведомление, упомянутое в пункте 1, по крайней мере:
 - (а опишите характер персональных данных, нарушение, включая, где это) возможно, категории и примерное количество заинтересованных субъектов данных, а также категории и примерное количество записей с персональными данными лицами;
 - (б сообщить имя и контактные данные сотрудника по защите информации или) других контактных точки, где Дополнительная информация может быть

получена;

(с) опишите вероятные последствия личной кражи данных;

(д) опишите меры, принятые или предлагаемые инспектор для решения личной кражи данных, в том числе, в надлежащих случаях, меры по смягчению возможных негативных последствий.

4. Где, и как, это не возможно, чтобы предоставить информацию, в то же время, эта информация может быть предоставлена в фазах без излишнего промедления.

5. Государства-члены должны предусмотреть инспектор документировать любые нарушения персональных данных, упомянутых в пункте 1, включая факты, имеющие отношение к персональные данные нарушения, его последствий и принятых мер по их исправлению. Эта документация должна позволять контролирующему органу для подтверждения соответствия данной статьи.

6. Государства-члены обязуются в случае, когда персональные данные нарушения предусматривает персональные данные, которые были переданы или на инспектор другого государства-члена, представить на информации, упомянутой в пункте 3, должны быть доведены до сведения повелителя этого государства-члена без неоправданной задержки.

Статья 31

Сообщение о нарушении персональных данных к субъекту данных

1. Государства-члены обязуются в случае, когда персональные данные нарушения может повлечь за собой высокий риск для прав и свобод физических лиц, оказывающих инспектор запрашивать личные данные нарушения субъектом данных без неоправданной задержки.

2. В связи с данными субъекта, указанных в пункте 1 настоящей статьи, описать в ясной и простой язык природы персональных данных нарушение и должна содержать как минимум информацию и мер, упомянутых в пунктах (B), (C) и (D) статьи 30(3).

3. Сообщения к теме сведения, указанные в пункте 1 Не требуется, если любое из следующих условий:

(а) инспектор осуществляет соответствующие технические и организационные меры защиты, и эти меры были применены к персональным данным затронуты персональные данные нарушения, в частности те, которые отображают личные данные недоступными для любого человека, который не имеет права доступа к нему, такие как шифрование;

(б) инспектор принимает последующие меры, которые обеспечивают высокий риск для прав и свобод субъектов персональных данных, упомянутых в пункте 1, скорее всего, не оправдались;

(с это потребует несоизмерных усилий. В таком случае, там должна быть) публичной коммуникации или аналогичной мерой, посредством которой данные субъекты информированы в равной степени эффективно.

4. Если инспектор уже не сообщены персональные данные нарушения данным субъекта, контролирующего органа, рассмотрев вероятность того, что персональные данные нарушения в результате велик риск, вправе потребовать от него это сделать, или может решить, что какое-либо из условий, указанных в пункте 3 не встречал.

5. Сообщения к теме сведения, указанные в пункте 1 настоящей статьи, может быть отложить, ограничить или опустить в соответствии с условиями и по основаниям, указанным в статье 13(3).

Раздел 3

Сотрудник по защите данных

Статья 32

Назначение ответственного по защите данных

1. Государства-члены должны предусмотреть право инспектора назначать Уполномоченного по защите данных. Государства-члены могут освобождать суды и другие независимые судебные органы, когда они действуют в своем судебном качестве в связи с этим обязательством.

2. К уполномоченному по защите данных должна быть определена на основании его профессиональных качеств и, в частности, его или ее экспертные знания законодательства о защите данных и практика и способности для выполнения задач, упомянутых в статье 34.

3. Один сотрудник по защите данных может быть назначен для нескольких компетентных органов, с учетом их организационной структуры и размера.

4. Государства-члены должны предусмотреть инспектор опубликовать контактные данные Уполномоченного по защите данных и сообщать о них в контролирующий орган.

Статья 33

Должность Уполномоченного по защите данных

1. Государства-члены должны предусмотреть инспектор обеспечить участие сотрудника по вопросам защиты данных, надлежащим образом и своевременно, во всех вопросах, которые касаются защиты персональных данных.

2. Инспектор поддерживает уполномоченный по защите данных в выполнении задач, упомянутых в статье 34, предоставляя необходимые ресурсы для выполнения этих задач и доступ к персональным данным и операциям обработки, а также для поддержания его или ее экспертных знаний.

Статья 34

Задачи Уполномоченного по защите данных

Государства-члены должны предусмотреть инспектор поручить специалисту по защите данных, по крайней мере, следующие задачи:

- (а информировать и консультировать инспектор и работников, которые) осуществляют обработку своих обязательств в соответствии с настоящей директивой и другими Союза или государства-члена положениями закона О защите данных;
- (б следить за соблюдением этой Директивы, с другого Союза или государства-члена положениями закона О защите данных и с политикой регулятора в отношении защиты персональных данных, включая распределение обязанностей, повышение осведомленности и обучение персонала, участвующего в обработке операций и проверок;
- (с консультировать в котором просила что касается защиты оценка) воздействия на информацию и следить за его исполнением в соответствии со статьей 27;
- (д) сотрудничать с контролирующим органом;
- (е в качестве контактного пункта для контролирующего органа по вопросам,) касающимся переработки, включая проведение предварительных консультаций, упомянутых в статье 28, и проконсультироваться, где это уместно, в отношении любого другого вопроса.

ГЛАВА V. Передача персональных данных третьим странам или международным организациям

Статья 35

Общие принципы передачи персональных данных

1. Государства-члены должны обеспечить любые передачи компетентными органами персональных данных, которые подвергаются обработке или предназначенных для обработки после передачи в третьи страны или международной организации, в том числе для последующей передачи в другую третью страну, или международной организацией, при условии выполнения национальных положений, принятых в соответствии с остальными положениями настоящей Директивы, только когда условия, изложенные в настоящем разделе, будут выполнены, а именно:

- (а) передача необходима для целей, изложенных в статье 1(1);
- (б) персональные данные передаются диспетчеру в третьей страной или) международной организацией, которая является компетентным органом для целей, указанных в статье 1(1);

- (с когда персональные данные передаются или из другого государства-члена,
) государство-член дал предварительное разрешение на передачу в соответствии со своим национальным законодательством;
- (д комиссия приняла решение о достаточности в соответствии со статьей 36,
) или, в отсутствие такого решения, соответствующие гарантии были предоставлены или существуют в соответствии со статьей 37, либо, при отсутствии адекватности решения в соответствии со статьей 36 и соответствующих гарантий в соответствии со статьей 37, отступления для конкретных ситуаций применяется в соответствии со статьей 38; и
- (е в случае передачи в другую третью страну, или международной
) организации, компетентный орган, который осуществил оригинальную передачу или другой компетентный орган одного государства-члена уполномочивает передачи, после с должным учетом всех соответствующих факторов, включая серьезность преступления, цель, для которой персональные данные были изначально переведены и уровень защиты персональных данных в третью страну или международную организацию, какие персональные данные будут переданы дальше.

2. Государства-члены предусматривают переводы без предварительного разрешения другого государства-члена в соответствии с подпунктом (С) пункта 1 допускается, только если передача персональных данных необходима для предотвращения непосредственной и серьезной угрозы общественной безопасности государства-члена или третьей страны, или существенные интересы государства и разрешение не может быть получено своевременно. Орган, ответственный за предоставление предварительного разрешения должен быть проинформирован незамедлительно.

3. Все положения этой главы применяются в целях обеспечения того, чтобы уровень защиты физических лиц обеспечивается эта Директива не подорвали.

Статья 36

Передача данных на основе решения о достаточности

1. Государства-члены должны предусмотреть, что передача персональных данных в третьи страны или международной организации может иметь место, когда комиссия постановила, что третья страна, территория или одному или нескольким указанным секторам в рамках этой третьей страны или международной организации не обеспечивает адекватный уровень защиты. Такая передача не требует какого либо специального разрешения.

2. При оценке достаточности уровня защиты, комиссия должна, в частности, учитывать следующие элементы:

- (а верховенство права, уважение прав человека и основных свобод,
) соответствующих законодательных актов, как общих, так и отраслевых, в том числе касающихся общественной безопасности, обороны,

национальной безопасности и уголовного права и доступ государственных органов к персональным данным, а также осуществления такого законодательства, защита данных правил, правил профессиональной деятельности и меры безопасности, в том числе правила передачи персональных данных третьим странам или международным организациям, которые соблюдаются в этой стране или международной организации, судебная практика, а также эффективные и имеющие исковую силу права субъекта данных и эффективной административной и правовой помощи для субъектов данных, чьи персональные данные передаются;

(б существование и эффективное функционирование одного или более) независимых надзорных органов в третью страну, или в которой международная организация субъектом, в компетенцию которых входит обеспечение и обеспечение соблюдения правил защиты данных, в том числе обеспечение надлежащего исполнения полномочий, для оказания помощи и консультирования данных субъектов при осуществлении своих прав и сотрудничество с надзорными органами государств-членов; и

(с международных обязательств третьей заинтересованной стране или) международной организацией заключила, или другие обязательства, вытекающие из юридически обязательных конвенций или документов, а также от ее участия в многосторонних или региональных систем, в частности в отношении защиты персональных данных.

3. Комиссия, после оценки адекватности уровня защиты, может принять решение, посредством выполнения закона, что третья страна, территория или одному или нескольким указанным секторам в рамках третьей страны или международной организации обеспечивает достаточный уровень защиты по смыслу пункта 2 настоящей статьи. Закон об осуществлении Конвенции должна обеспечивать механизм для периодического пересмотра, по крайней мере, каждые четыре года, который должен учитывать все соответствующие события в третьей страной или международной организацией. Акт реализации должен указать свои территориальные и отраслевые приложения и, где это применимо, определить контролирующий орган или органы, о которых говорится в пункте (В) пункта 2 настоящей статьи. Закон об осуществлении Конвенции, должны приниматься в соответствии с процедурой рассмотрения, упомянутой в статье 58(2).

4. Комиссия будет на постоянной основе следить за развитием ситуации в третьих странах и международных организациях, которые могут повлиять на функционирование решений, принятых в соответствии с пунктом 3.

5. Комиссия, в которой имеющаяся информация свидетельствует, в частности, после проведения обзора, упомянутого в пункте 3 настоящей статьи, что третья страна, территория или одному или нескольким указанным секторам в рамках третьей страны, либо международная организация не обеспечивает достаточный уровень защиты по смыслу пункта 2 настоящей статьи, в объеме, необходимом, отменять, изменять или приостанавливать решения, указанного в пункте 3

настоящей статьи, путем осуществления действий, не ретро-активное воздействие. Исполнительные акты принимаются в соответствии с процедурой рассмотрения, упомянутой в статье 58(2).

На обоснованные императивные основания срочности, комиссия принимает немедленно применимые подзаконные акты в соответствии с процедурой, предусмотренной в статье 58(3).

6. Комиссия вступает в консультации с третьей страной или международной организацией с целью исправления ситуации, послужившие основанием для принятия решения в соответствии с пунктом 5.

7. Государства-члены должны предусмотреть решение в соответствии с пунктом 5 без ущерба для передачи персональных данных в третью страну, территорию или одному или нескольким указанным секторам в рамках этой третьей страны или международной организации в соответствии со статьями 37 и 38.

8. Комиссия должна опубликовать в *официальном журнале Европейского Союза* и на своем сайте список из третьих стран, территорий и конкретных секторов в третьей стране и международных организации, для которых он решил, что адекватный уровень защиты или не обеспечена.

Статья 37

Передача данных с учетом соответствующих гарантий

1. В отсутствие решения в соответствии со статьей 36(3), государства-члены должны предусмотреть, что передача персональных данных в третьи страны или международной организации может иметь место, когда:

(а) надлежащие гарантии в отношении защиты персональных данных, предусмотренных юридически обязательным документом; или

(б) регулятор оценил все обстоятельства, связанные с передачей персональных данных и приходит к выводу, что имеются соответствующие гарантии в отношении защиты персональных данных.

2. Контролер должен информировать контролирующий орган о категориях трансфертов в соответствии с пунктом (В) параграфа 1.

3. Когда перевод опирается на точку (В) пункта 1, такая передача должна быть документирована и документация должны быть предоставлены в контролирующий орган по требованию, в том числе дата и время передачи, сведениями о получении компетентным органом, основания для передачи персональных данных, переданных.

Статья 38

Исключения для конкретных ситуаций

1. При отсутствии адекватности решения в соответствии со статьей 36, или соответствующих гарантий в соответствии с положениями статьи 37, члены должны обеспечить, что перенос или категории передачи персональных данных

в третьи страны или международной организации может иметь место только при условии, что передачи необходимо:

(а в целях защиты жизненно важных интересов субъекта данных или другого лица;

(б для защиты законных интересов субъект персональных данных, если законодательство государства-члена, передача персональных данных не предусматривает;

(с для предотвращения непосредственной и серьезной угрозы общественной безопасности государства-члена или третьей страны;

(д) в отдельных случаях для целей, изложенных в статье 1(1); или

(е в конкретном случае для установления, осуществления или защиты правовых требований, касающихся целей, изложенных в статье 1(1).

2. Персональные данные не должны быть переданы, если передающий компетентный орган определяет, что основные права и свободы соответствующего субъекта данных переопределения общественный интерес в передаче, изложенных в пунктах (D) и (e) пункта 1.

3. Где перенос основан на пункте 1, такой перевод оформляется и документация должны быть предоставлены в контролирующий орган по требованию, в том числе дата и время передачи, сведениями о получении компетентным органом, основания для передачи персональных данных, переданных.

Статья 39

Передача персональных данных получателей, установленных в третьих странах

1. В отступление от пункта (б) статьи 35(1) и без ущерба для любого международного соглашения, указанного в пункте 2 настоящей статьи, Союза или государства законом может быть установлено компетентными органами, указанными в пункте (7)(а) статьи 3, в отдельных и конкретных случаях, на передачу персональных данных непосредственно получателям, установленных в третьих странах, только если другие положения настоящей Директивы не соблюдаются все следующие условия:

(а передачи строго необходимыми для выполнения задачи передачи компетентным органом, как это предусмотрено объединение или государственное право-членам для целей, изложенных в статье 1(1);

(б передачи компетентный орган определяет, что отсутствие основных прав и свобод соответствующего субъекта данных переопределения общественный интерес требует передачи в данном случае;

(с передающий компетентный орган считает, что передача в орган, компетентный для целей, указанных в статье 1(1) в третью страну

неэффективными или неподходящими, в частности потому, что перевод не может быть достигнуто в течение разумного периода времени,

(д органом, компетентным для целей, указанных в статье 1(1) в третью страну)
прошлого года без неоправданной задержки, если это является неэффективным или нецелесообразным;

(е передающий компетентный орган информирует получателя указанной цели)
или целей, для которых персональные данные используются только для обработки последнего при условии, что такая обработка необходима.

2. Международного соглашения, упомянутого в пункте 1, должны быть какие-либо двусторонние или многосторонние международные соглашения, действующие в отношении между государствами-членами и третьими странами в области судебного сотрудничества по уголовным делам и полицейского сотрудничества.

3. Перевод компетентный орган должен информировать контролирующий орган о передаче в соответствии с настоящей статьей.

4. Где перенос основан на пункте 1, такой перевод должны быть документально подтверждены.

Статья 40

Международное сотрудничество по защите персональных данных

В отношении третьих стран и международных организаций, комиссия и государства-члены принимают надлежащие меры для:

(а развивать механизмы международного сотрудничества в целях содействия)
эффективному исполнению законодательства по защите персональных данных;

(б оказание международной взаимной помощи в области соблюдения)
законодательства по защите персональных данных, в том числе посредством уведомления, направления жалоб, помощи в проведении расследований и обмен информацией, с учетом соответствующих гарантий по защите персональных данных и другие основные права и свободы;

(с вовлечение заинтересованных сторон в обсуждение и мероприятий,)
направленных на развитие международного сотрудничества в применении законодательства в области защиты персональных данных;

(д содействовать обмену и документацию законодательства о защите)
персональных данных и практике, в том числе о юрисдикционных конфликтов с третьими странами.

ГЛАВА VI

Независимые надзорные органы

Раздел 1

Независимый статус

Статья 41

Надзорный орган

1. Каждая страна-участница должна предусматривать один или несколько независимых государственных органов, которые отвечают за мониторинг применения настоящей Директивы, в целях защиты основных прав и свобод физических лиц в отношении обработки и облегчить свободный поток персональных данных в рамках Союза ('надзора').
2. Каждый надзорный орган должен способствовать последовательному применению настоящей Директивы по всему Союзу. Для этого надзорные органы должны сотрудничать друг с другом и с комиссией в соответствии с главой VII.
3. Государства-члены могут предусмотреть контролирующий орган, установленных в соответствии с Регламентом (ЕС) 2016/679 быть контролирующий орган указанные в настоящей директиве, и взять на себя ответственность за задачи контролирующий орган, который будет учрежден в соответствии с пунктом 1 настоящей статьи.
4. Где более одного контролирующий орган государства-члена, государство-член должно назначить контролирующий орган, который представляют эти органы в состав Совета, указанных в статье 51.

Статья 42

Независимость

1. Каждое государство-член должно обеспечить для каждого контролирующий орган действовать с полной независимостью при выполнении своих задач и осуществлении своих полномочий в соответствии с настоящей директивой.
2. Государства-члены должны обеспечить для члена или членов их надзорным органам в выполнении их задач и осуществление своих полномочий в соответствии с настоящей директивой, чтобы оставаться свободными от внешнего влияния, будь то прямые или косвенные, и что они не должны ни запрашивать или получать указания от кого-либо.
3. Члены надзорные органы государств-членов должны воздерживаться от любых действий, несовместимых с их обязанностями и не обязан в течение срока их полномочий, участвовать в каких-либо несовместимых занятий, будь то доходной или нет.
4. Каждая страна-участница должна гарантировать, что каждый контролирующий орган обеспечены кадровые, технические и финансовые ресурсы, помещение и инфраструктуру, необходимую для эффективного выполнения своих задач и осуществления им своих полномочий, в том числе тех, которые необходимо провести в рамках взаимной помощи, сотрудничества и участия в работе Совета.

5. Каждое государство-член должно гарантировать, что каждый надзорный орган выбирает и имеет свой собственный персонал, который подлежит исключительное направление члена или участника соответствующего контролирующего органа.

6. Каждое государство-член должно гарантировать, что каждый контролирующий орган субъекта финансового контроля, которая не влияет на его независимость и что она отдельная, государственных годовых бюджетов, которые могут быть частью общего государственного или национального бюджета.

Статья 43

Общие условия для членов надзорного органа

1. Государства-члены должны обеспечить для каждого члена их надзорные органы должны быть назначены посредством прозрачной процедуры:

- их парламентом;
- их правительство;
- их глава государства; или
- независимый орган, уполномоченное назначать в соответствии с законодательством штата члена.

2. Каждый участник должен иметь квалификацию, опыт и навыки, в частности в области защиты персональных данных, обязан выполнять свои обязанности и осуществлять свои полномочия.

3. Обязанности члена прекращаются в случае истечения срока полномочий, отставки или обязательного выхода на пенсию в соответствии с законодательством соответствующего государства-члена.

4. Член должен быть уволен только в случае серьезных проступков или если участник не выполняет условия, необходимые для исполнения должностных обязанностей.

Статья 44

Правила о создании наблюдательного органа

1. Каждое государство-участник предусмотреть в законе следующие:

- (а) создание каждого контролирующего органа;
- (б) требованиям и условиям допуска обязан быть назначен в качестве члена) каждого контролирующего органа;
- (с) правила и процедуры назначения члена или членов каждого) контролирующего органа;

(д срок полномочий члена или членов каждого контролирующего органа не
) менее четырех лет, за исключением первой встречи после 6 мая 2016, часть из которых может иметь место на более короткий срок, где это необходимо для защиты независимости надзорного органа посредством предварительной записи процедуры;

(е ли и, если да, то за сколько терминов члена или членов каждый
) контролирующий орган имеет право на переизбрание;

(Ф условия, определяющие обязательства члена или членов и сотрудников
) каждого контролирующего органа, запрета на действия, профессий и преимущества несовместимыми С В течение и после срока полномочий и нормы, регулирующие прекращение трудовых отношений.

2. Член или члены и сотрудники каждый контролирующий орган обязан, в соответствии с Союза или государства-члена права, распространяется обязанность сохранения профессиональной тайны как во время, так и после истечения срока их полномочий, в отношении любой конфиденциальной информации, которая доводится до их сведения в ходе исполнения своих обязанностей или осуществления своих полномочий. В течение срока их полномочий, что обязанность сохранения профессиональной тайны распространяются, в частности, отчетности по физическим лицам нарушения настоящей Директивы.

Раздел 2

Компетенции, задачи и полномочия

Статья 45

Компетенции

1. Каждое государство-член должно обеспечить для каждого контролирующего органа, чтобы быть компетентным для выполнения задач, возложенных на, и для осуществления полномочий, в соответствии с этой директивой на территории своего государства-члена.

2. Каждое государство-член должно обеспечить для каждого контролирующего органа, чтобы не быть компетентным для контроля операций по обработке судов, действуя в своих судебных обязанностях. Государства-члены могут предусмотреть их контролирующий орган не будет правомочен контролировать операции обработка прочих независимой судебной власти, действуя в их судебных систем.

Статья 46

Задачи

1. Каждое государство-член должно обеспечить, на своей территории, для каждого контролирующего органа:

(а контролировать и обеспечивать применение положений, принятых во

-) исполнение настоящей Директивы и принятых мер;
- (б содействовать повышению информированности общественности и) понимания рисков, правил, гарантий и прав в отношении переработки;
- (с посоветуйте, в соответствии с законом, члена национального парламента,) правительства и других учреждений и органов, о законодательных и административных мерах, касающихся защиты прав и свобод физических лиц в отношении обработки данных;
- (д способствовать осознанию инспекторы и обработчики свои обязательства в) соответствии с настоящей директивой;
- (е по запросу, предоставить информацию по любому вопросу сведения,) касающиеся осуществления их прав в соответствии с настоящей директивой и, в случае необходимости, сотрудничать с контролирующими органами в других государствах-членах с этой целью;
- (Ф рассмотрения жалоб, поданных в данных теме, или органа, организации) или ассоциации, в соответствии со статьей 55, и расследования, насколько это уместно, предмет жалобы и информирует заявителя о ходе и результатах расследования в течение разумного периода, в частности при дальнейшей проверке и согласованию с другого контролирующего органа;
- (г проверить законность оформления в соответствии со статьей 17, и сообщить) сведения, подлежащие в разумный срок о результатах проверки в соответствии с пунктом 3 этой статьи или из причин, почему проверка не проводилась;
- (ч сотрудничать с, в том числе путем обмена информацией и оказания) взаимной помощи других надзорных органов, с целью обеспечения согласованности применения и выполнения настоящей Директивы;
- (я проведение расследований о применении настоящей Директивы, в том) числе на основании информации, полученной от другого контролирующего органа или другого государственного органа;
- (Дж следить за соответствующими событиями, поскольку они оказывают) влияние на защиту персональных данных, в частности, развитие информационных и коммуникационных технологий;
- (к предоставляем консультации по операций по переработке, указанных в) статье 28; и
- (л) вклад в деятельность Совета.

2. Каждый контролирующий орган содействия подаче жалоб, упомянутых в подпункте (F) пункта 1, такие меры, как обеспечение подачи жалобы, форма которого также может быть заполнена в электронном виде, не исключая других средств связи.

3. Выполнение задачи каждый надзорный орган должен быть бесплатным для субъекта персональных данных и ответственного за защиту данных.

4. Если просьба является явно необоснованной или чрезмерной, в особенности потому, что он повторяющийся, контролирующий орган может взимать плату на основе своих административных расходов, или может отказаться действовать по запросу. Контролирующий орган несет бремя демонстрируя, что ходатайство является явно необоснованным или чрезмерным.

Статья 47

Полномочия

1. Каждое государство-участник предусмотреть в законе для каждого контролирующего органа, чтобы иметь эффективные механизмы расследования. Эти полномочия должны включать, как минимум, правом на получение от инспектора и обработчика доступ ко всем персональным данным, которые обрабатываются и получить всю информацию, необходимую для выполнения своих задач.

2. Каждое государство-участник обязуется предоставлять по закону для каждого контролирующего органа осуществлять эффективные корректирующие полномочия, такие как, например:

(а выдавать предупреждения на инспектор или обработчик, что операции) обработки могут нарушать положений, принятых во исполнение настоящей Директивы;

(б чтобы заказать инспектор или обработчик для приведения операций в) соответствие с Положением, принятым во исполнение настоящей Директивы, в случае необходимости, в установленном порядке и в пределах указанного срока, в частности, заказав их изменении или уничтожении персональных данных или ограничение обработки в соответствии со статьей 16;

(с о введении временного или окончательного ограничения, включая запрет на) обработку.

3. Каждая страна-участница должна предоставить в соответствии с законом для каждого контролирующего органа, чтобы иметь эффективные консультативные полномочия консультировать инспектора в соответствии с предварительной консультации процедурой, предусмотренной в статье 28, и на вопрос, по собственной инициативе или по запросу мнения своего национального парламента и его правительства, или же, в соответствии со своим национальным законодательством, для других учреждений и органов, а также общественности по любому вопросу, связанному с защитой персональных данных.

4. Осуществления полномочий, возложенных на контролирующий орган в соответствии с настоящей статьи, осуществляется с учетом соответствующих гарантий, включая эффективную судебную защиту и надлежащей правовой

процедуры, изложенные в Союз и государственного права членов в соответствии с Хартияом.

5. Каждая страна-участница должна предоставить в соответствии с законом для каждого контролирующего органа есть власть, чтобы принести нарушение положений, принятых во исполнение настоящей Директивы до сведения судебных органов, и, при необходимости, начинать или иным образом участвовать в судебном разбирательстве, в целях соблюдения положений, принятых во исполнение настоящей Директивы.

Статья 48

Отчетности нарушений

Государства-члены должны предоставить компетентным органам создать эффективные механизмы для стимулирования конфиденциального информирования о нарушениях настоящей Директивы.

Статья 49

Отчеты о деятельности

Каждый контролирующий орган обязан составлять ежегодный отчет о своей деятельности, который может включать в себя перечень видов нарушения уведомлен и видах наказаний. Эти доклады должны быть переданы в Национальный парламент, правительство и другие органы власти в соответствии с законом штата члена. Они должны быть доступны для общественности, комиссии и правления.

ГЛАВА VII

Сотрудничества

Статья 50

Взаимной помощи

1. Каждое государство-член должно обеспечить для их надзорных органов предоставлять друг другу соответствующую информацию и взаимной помощи с целью внедрения и применения настоящей Директивы в согласованном порядке, и принять меры для эффективного сотрудничества друг с другом. Взаимная помощь должна охватывать, в частности, информационные запросы и надзорные меры, такие как запросы на проведение консультаций, инспекций и расследований.

2. Каждое государство-член ЕС должно обеспечить для каждого контролирующего органа принять все надлежащие меры, необходимые для ответа на запрос другого контролирующего органа без неоправданной задержки и не позднее чем через один месяц после получения запроса. Такие меры могут включать, в частности, передавать соответствующую информацию о проведении расследования.

3. Просьба о помощи должна содержать всю необходимую информацию, включая цель и причины запроса. Обмен информацией должен использоваться только для цели, для которой он был запрошен.

4. Просил надзорный орган не вправе отказаться от выполнения запроса, если:

(а он не является компетентным по предмету запроса или для мероприятия)
) необходимо выполнить; или

(б соответствии с просьбой нарушает эту Директиву или Союза или)
) государства-члена, право которой контролирующий орган получения запроса субъекта.

5. Просил надзорный орган информирует запрашивающее контролирующего органа результатов или, в случае необходимости, в ходе мер, принятых для того, чтобы ответить на запрос. Запрашиваемые контролирующим органом должны быть указаны причины отказа в удовлетворении просьбы в соответствии с пунктом 4.

6. Просит надзорные органы, как правило, предоставить запрашиваемую информацию другими контролирующими органами с помощью электронных средств, используя стандартизированный Формат.

7. Просит надзорные органы не должны взимать плату за любые действия, предпринятые им во исполнение просьбы об оказании правовой помощи. Надзорные органы могут договориться о правилах, чтобы освободить друг друга для конкретных расходов, связанных с оказанием взаимной помощи в чрезвычайных обстоятельствах.

8. Комиссия, возможно, путем принятия исполнительных актов, указать формат и процедуры оказания взаимной помощи, указанных в настоящей статье, а также порядок обмена информацией с помощью электронных средств между надзорными органами, а также между контролирующими органами и Советом. Исполнительные акты принимаются в соответствии с процедурой рассмотрения, упомянутой в статье 58(2).

Статья 51

Задачи Совета

1. Совет, учрежденный Регламентом (ЕС) 2016/679 должен выполнять следующие задачи по отношению к обработке в рамках настоящей Директивы:

(а консультировать комиссию по любым вопросам, связанным с защитой)
) персональных данных в Союз, в том числе по любой предлагаемой поправке настоящей Директивы;

(б проверьте, по собственной инициативе, по требованию одного из его членов)
) или по требованию комиссии, любой вопрос, касающиеся применения настоящей Директивы и руководящие указания, рекомендации и передовую практику в целях содействия последовательному применению настоящей Директивы;

- (с разработать руководящие принципы для органов надзора о применении мер,
) упомянутых в статье 47(1) и (3);
- (д проблема руководящих принципов, рекомендаций и лучшей практики в
) соответствии с пунктом (В) настоящего подпункта для установления
личных данных нарушений и определения неоправданной задержки,
упомянутой в статье 30(1) и (2) и для особых обстоятельств, в которых
инспектор или обработчик должен сообщать персональные данные
нарушения;
- (е проблема руководящих принципов, рекомендаций и лучшей практики в
) соответствии с пунктом (В) настоящего подпункта, а в обстоятельства, при
которых персональные данные нарушение может повлечь за собой высокий
риск для прав и свобод физических лиц, упомянутых в статье 31(1);
- (Ф рассмотреть практическое применение руководящих принципов,
) рекомендаций и лучшей практики, указанных в пунктах (В) и (С);
- (г предоставить комиссии свое мнение для оценки адекватности уровня
) защиты в третьей стране, территории или одному или нескольким
указанным секторам в рамках третьей страны или международной
организации, в том числе для оценки целесообразности такой третьей
стране, территории, указанном секторе или международной организации не
обеспечивает адекватного уровня защиты;
- (ч поощрения сотрудничества и эффективного двустороннего и
) многостороннего обмена информацией и передовой практикой между
надзорными органами;
- (я развивать общие учебные программы и содействовать обмену персоналом
) между надзорными органами и, при необходимости, с надзорными
органами третьих стран или в международных организациях;
- (Дж содействовать обмену знаниями и документации о закон О защите данных
) и практики с контролирующими защиты данных власти во всем мире.

В отношении пункта (г) первого подпункта, комиссия должна представить комиссии все необходимые документы, включая переписку с правительством третьей страны, с территории или определенной отрасли в пределах этой третьей страны или международной организации.

2. Где комиссия просит провести консультации с Советом, это может указывать на ограничение по времени, принимая во внимание актуальность данного вопроса.

3. Комиссия направляет свои мнения, руководящих принципов, рекомендаций и лучшей практики в комиссии и Комитета, упомянутого в статье 58(1) и сделать их достоянием общественности.

4. Комиссия информирует Совет О мерах, принятых после заключения, руководящих принципов, рекомендаций и лучшей практики, выпущенными Советом.

ГЛАВА VIII

Средства правовой защиты, ответственность и санкции

Статья 52

Право подать жалобу в надзорный орган

1. Без ущерба для каких-либо других административных или судебных средств правовой защиты, государства-члены должны обеспечить для каждого субъекта данных, чтобы иметь право подать жалобу в единый надзорный орган, если субъект персональных данных считает, что обработка персональных данных, касающихся его или ее нарушением положений, принятых во исполнение настоящей Директивы.
2. Государства-члены должны предусмотреть контролирующий органа, с которым данная жалоба была подана направить его в компетентный надзорный орган, без необоснованного промедления, если жалоба не подана в надзорный орган, компетентный в соответствии со статьей 45(1). Субъект данных должен быть проинформирован о передаче.
3. Государства-члены должны предусмотреть контролирующий органа, с которым данная жалоба была подана в целях оказания дополнительной помощи по просьбе субъекта данных.
4. Субъект данных должен быть проинформирован компетентными надзорного органа о ходе и результатах рассмотрения жалобы, в том числе возможности судебной защиты в соответствии со статьей 53.

Статья 53

Право на эффективные средства правовой защиты в отношении надзорного органа

1. Без ущерба для каких-либо других административных или несудебным средствам правовой защиты, государства-члены должны предусмотреть право физического или юридического лица на эффективные средства правовой защиты против юридически обязательного решения контролирующий органа в отношении них.
2. Без ущерба для каких-либо других административных или несудебным средствам правовой защиты, каждый субъект персональных данных имеет право на эффективные средства правовой защиты, когда надзорный орган, который обладает компетенцией в соответствии со статьей 45(1) не обращаться с жалобой или не информировать субъекта данных в течение трех месяцев, о ходе или результатах рассмотрения жалобы, поданной в соответствии со статьей 52.
3. Государства-члены должны предусмотреть преследование в отношении надзорного органа в судах государства-члена, где создан наблюдательный орган.

Статья 54

Право на эффективные средства правовой защиты от инспектор или обработчик

Без ущерба для каких-либо административные или несудебным средствам правовой защиты, включая право подать жалобу в контролирующий орган в соответствии со статьей 52, государства-члены должны предусмотреть право субъекта данных на эффективные средства правовой защиты, где он или она считает, что его или ее прав, закрепленных в положениях, принятых во исполнение настоящей Директивы, которое было нарушено в результате обработки его персональных данных в соответствии с этими положениями.

Статья 55

Представительства субъектов данных

Государства-члены должны, в соответствии с государства-процессуального закона, предусматривающих данные темы имеют право на мандат не-для-некоммерческая организация, организации или ассоциации, который был надлежащим образом в соответствии с государства-члена права, Хартияные цели которых в интересах общества и активно работает в области защиты данных прав и свобод применительно к защите личных данных, чтобы подать жалобу от его или ее имени и для осуществления прав, указанных в статьях 52, 53 и 54 от его или ее имени.

Статья 56

Право на компенсацию

Государства-члены должны обеспечить любое лицо, которому причинен материальный или нематериальный ущерб в результате незаконной обработки операции или любые действия, нарушающие национальные положения, принятые во исполнение этой Директивы, чтобы иметь право на получение компенсации за ущерб, понесенный от инспектора или любой другой орган, компетентный в соответствии с законом государства-члена.

Статья 57

Штрафы

Государства-члены обязаны принять Правила о штрафах, применимых к нарушениям положений, принятых во исполнение настоящей Директивы, и принимают все необходимые меры для обеспечения их осуществления. Предусмотренные санкции должны быть эффективными, соразмерными и сдерживающими.

ГЛАВА IX

Реализация актов

Статья 58

Процедуры комитета

1. Комиссия будет оказывать помощь Комитету, учрежденному согласно статье 93 Регламента (ЕС) 2016/679. Этот комитет должен быть учрежден комитет в значении Регламента (ЕС) № 182/2011.
2. Если делается ссылка на этот параграф, статьи 5 Регламента (ЕС) № 182/2011 применяются.
3. Если делается ссылка на этот пункт статьи 8 Регламента (ЕС) № 182/2011, в сочетании со статьей 5 Конвенции, применяются.

ГЛАВА X

Заключительные положения

Статья 59

Отменить рамочное решение 2008/977/ПВД

1. Рамочное решение 2008/977/ПВД отменяется с вступлением в силу с 6 мая 2018 года.
2. Ссылки на отмененные решения, указанного в пункте 1 не должно толковаться как ссылки на настоящую Директиву.

Статья 60

Правовой Союз действует уже в силу

Конкретные Положения о защите персональных данных в законодательных актах ЕС, которые вступили в силу или до 6 мая 2016 года в области судебного сотрудничества по уголовным делам и полицейского сотрудничества, который регулирует переработки между государствами-членами и доступ уполномоченных органов государств-членов информационными системами, установленными в соответствии с договорами в рамках сферы применения настоящей Директивы, остаются в силе.

Статья 61

Взаимосвязи с ранее заключенными международными соглашениями в области судебного сотрудничества по уголовным делам и полицейского сотрудничества

Международных соглашений, касающихся передачи персональных данных третьим странам или международным организациям, которые были заключены с государствами-членами до 6 мая 2016 года и которые соответствуют Союзу правом в качестве применимых до этой даты, остаются в силе до момента их изменения, заменен или отозван.

Статья 62

Отчеты комиссии

1. К 6 мая 2022 года, а каждые четыре года после этого комиссия должна представить доклад о результатах обзора и оценки данной Директивы для Европейского парламента и Совета. Отчеты должны быть обнародованы.
2. В контексте оценки и комментарии, упомянутые в пункте 1, комиссия рассматривает, в частности, применения и функционирования Глава V о передаче персональных данных третьим странам или международным организациям, в частности в отношении решений, принятых в соответствии со статьей 36(3) и статья 39.
3. Для целей пунктов 1 и 2, комиссия может запросить информацию от государств-членов и надзорных органов.
4. При проведении оценки и комментарии, упомянутые в пунктах 1 и 2, комиссия должна учитывать позиции и выводов Европейского парламента, Совета и других соответствующих органов или источники.
5. Комиссия, при необходимости, внести соответствующие предложения с целью внесения поправок в настоящую Директиву, в частности с учетом достижений в области информационных технологий и в свете прогресса в информационном обществе.
6. По 6 мая 2019 года комиссия рассматривает иные правовые акты, принимаемые Союзом, регламентирующих обработку компетентным органам для целей, изложенных в статье 1(1), в том числе указанных в статье 60, для того, чтобы оценить необходимость приведения их в соответствие с настоящей директивой и, при необходимости, необходимые предложения по внесению изменений в эти акты в целях обеспечения последовательного подхода к защите персональных данных в рамках настоящей Директивы.

Статья 63

Транспозиция

1. Государства-члены должны принять и опубликовать до 6 мая 2018, законы, правила и административные положения, необходимые для выполнения этой Директивы. Они должны незамедлительно сообщить комиссии текст этих положений. Они должны применяться те положения, которые с 6 мая 2018 года. Когда государства-члены принимают эти положения, они должны содержать ссылку на настоящую Директиву или должны сопровождаться такой ссылкой в случае их официальной публикации. Государства-члены должны определить каким образом принимается.
2. В отступление от пункта 1, государство-член может предусмотреть, в исключительных случаях, где это предполагает несоизмеримо больших усилий, для автоматизированных систем обработки созданы до 6 мая 2016 года должны быть приведены в соответствие со статьей 25(1) до 6 мая 2023 года.
3. В отступление от пунктов 1 и 2 настоящей статьи, государство-член может, в исключительных обстоятельствах, привести автоматизированную систему обработки, указанные в пункте 2 настоящей статьи, в соответствии со статьей

25(1) в течение определенного периода после окончания срока, указанного в пункте 2 настоящей статьи, если оно могло бы вызвать серьезные трудности для функционирования данной автоматизированной системы обработки. Соответствующее государство-член уведомляет комиссию из оснований для те серьезные трудности и оснований для указанного периода, в течение которого он должен принести этой конкретной автоматизированной системе обработки в соответствии со статьей 25(1). Указанный срок в любом случае не позднее 6 мая 2026 года.

4. Государства-члены должны сообщить комиссии текст основных положений национального законодательства, которые они принимают в области, охватываемой данной директивой.

Статья 64

Вступление в силу

Настоящая Директива вступает в силу на следующий день после его опубликования в *официальном журнале Европейского Союза*.

Статья 65

Адресатам

Настоящая Директива адресована государствам-членам.
Совершено в Брюсселе, 27 апреля 2016.