Постоянному бюро
Парламента Республики Молдова

В соответствии с положениями статьи 73 Конституции Республики Молдова и статьи 47 Регламента Парламента представляется в порядке законодательной инициативы проект Закона о защите персональных данных.

Прилагаются:
1) проект закона;
2) пояснительная записка;
3) Заключения органов власти.

Депутаты Парламента:

С. Сырбу

В. Стратан

К. Цуцу

Е. Никифорчук

К. Падневич

В. Иванов

И. Время

А. Загородный

А. Канду

Е. Бодарев

А. Горилэ

С. Стати

В. Неделя

М. Рэдукан

Р. Апольский

SECRETARIATUL PARLAMENTULUI
REPUBLICII MOLDOVA
D.D.P. Nr. 422
"22" 11 2018
Ora

Перевод

ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

З А К О Н
о защите персональных данных

В целях обеспечения соблюдения основного права человека на непрекосновенность интимной, семейной и частной жизни, закрепленного статьей 28 Конституции Республики Молдова;

Осознавая взятые на себя Республикой Молдова при присоединении к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера № 108 и Дополнительному протоколу к ней относительно органов надзора и трансграничных потоков данных;

Настоящий закон перелагает Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки личных данных и о свободном движении таких данных, а также об отмене Директивы 95/46/ЕС (общее регулирование защиты данных) и Директиву (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 года 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, опубликованных в Официальном журнале ЕС L 119 от 4 мая 2016 года.

Парламент принимает настоящий органический закон.

Глава I
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель закона

Целью настоящего закона является обеспечение права на защиту персональных данных, вытекающего в том числе из конституционного права на неприкосновенность интимной, семейной и частной жизни.

Статья 2. Материальная область применения

(1) Настоящий закон регулирует обработку персональных данных, осуществляемую полностью или частично автоматизированными средствами, а также обработку средствами, отличными от автоматизированных, персональных данных какой-либо системы учета или предназначенных для введения в такую систему.

(2) Действие настоящего закона распространяется на:

а) обработку персональных данных на территории Республики Молдова, в том числе содержащихся в информации, отнесенной к государственной тайне, профессиональной тайне, банковской тайне, врачебной тайне, коммерческой тайне,

налоговой тайне, и в иной информации ограниченного доступа, или административные операции, осуществляемые в связи с ведением гражданского, правонарушительного или уголовного дела, а также на используемые для этого средства;

b) обработку персональных данных в дипломатических представительствах и консульских учреждениях Республики Молдова, а также иными контролерами, находящимися за пределами страны, но на территории, где на основании международного публичного права применяется внутреннее законодательство Республики Молдова;

c) обработку персональных данных субъектов, находящихся на территории Республики Молдова, контролерами, находящимися за пределами Республики Молдова, в случае такой обработки в связи с предоставлением за плату или безвозмездно товаров или услуг этим субъектам в Республике Молдова либо в связи с мониторингом поведения последних в Республике Молдова, за исключением обработки персональных данных в целях транзитной передачи через территорию Республики Молдова;

d) обработку персональных данных, выполняемую контролерами-правоохранительными органами, обладающими установленными законом полномочиями по предотвращению и расследованию преступлений и/или уголовному преследованию, исполнению уголовных наказаний, предварительному заключению, в том числе по предотвращению и пресечению угроз общественному порядку, национальной и государственной безопасности, или по специальной розыскной деятельности;

e) обработку персональных данных умерших, за исключением таких категорий данных, как фамилия, имя, дата, месяц и год рождения или смерти, а также при осуществлении прав наследования.

(3) Действие настоящего закона не распространяется на:

a) обработку персональных данных физическими лицами исключительно для личных или семейных нужд, не связанных с профессиональной или коммерческой деятельностью;

b) обработку персональных данных агентуры и источников информации в рамках разведывательной и контрразведывательной деятельности, осуществляемую в соответствии с законом;

c) обезличенные персональные данные;

d) операции по обработке и трансграничной передачи персональных данных виновных в совершении преступлений геноцида, военных преступлений и преступлений против человечества или жертв таких преступлений.

Статья 3. Основные понятия

Термины и выражения, используемые в настоящем законе, имеют следующее значение:

персональные данные – любая информация, идентифицирующая или содействующая идентификации субъекта персональных данных. Существует две категории персональных данных: обычная и особая;

обычная категория персональных данных – следующие данные, не ограничиваясь ими: фамилия, имя, отчество, государственный идентификационный номер, адрес, номер телефона, регистрационный номер автомобиля, данные о месте

нахождения, голос, идентификатор в режиме реального времени либо на один или несколько факторов, специфичных для физической, физиологической, экономической, культурной или социальной идентичности физического лица;

особая категория персональных данных – данные, раскрывающие расовое или этническое происхождение лица, политические убеждения, религиозные или философские воззрения, принадлежность к профессиональным союзам, генетические и биометрические данные, позволяющие идентифицировать физическое лицо, данные, касающиеся состояния здоровья или половой жизни, половой ориентации, а также данные, касающиеся уголовных наказаний и совершенных преступлений, принудительных процессуальных мер или санкций за правонарушения;

генетические данные – персональные данные, касающиеся унаследованных или приобретенных генетических характеристик физического лица, предоставляющих уникальную информацию о его физиологии или состоянии здоровья в результате анализа биологического материала соответствующего лица;

биометрические данные – персональные данные, полученные в результате применения техник специальной обработки физических, физиологических или поведенческих характеристик физического лица, позволяющих его идентифицировать или подтвердить идентификацию, такие как изображения лица или дактилоскопические данные;

данные о состоянии здоровья – персональные данные, связанные со состоянием физического или психического здоровья физического лица, включая данные об оказанных медицинских услугах, раскрывающие информацию о состоянии здоровья соответствующего лица;

субъект персональных данных (далее - *субъект данных*) – идентифицированное или идентифицируемое физическое лицо. Умерший не может быть субъектом данных;

обработка персональных данных – любая операция или набор операций, выполняемых над персональными данными или набором персональных данных, как автоматизированными средствами, так и без таковых, такие как сбор, запись, организация, структурирование, хранение, восстановление, адаптация или изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространения или предоставления иного доступа, группировка или комбинирование, блокирование, стирание или уничтожение;

трансграничная обработка персональных данных – обработка персональных данных, осложненная иностранным элементом, в которой участвует находящееся в другом государстве физическое лицо либо юридическое лицо публичного или частного права;

создание профилей – любая форма автоматизированной обработки персональных данных, состоящая в использовании персональных данных для оценки определенных аспектов, касающихся физического лица, в частности, его достижений на рабочем месте, экономического положения, состояния здоровья, личных предпочтений, интересов, жизнеспособности, поведения, места нахождения или перемещений;

контролер – физическое лицо или юридическое лицо публичного или частного права, включая орган публичной власти, любое иное учреждение, организация или авторизованное лицо, которое самостоятельно или совместно с другими определяет цели и/или средства обработки персональных данных, обрабатывает или намеревается обрабатывать эти данные;

ассоциированный контролер – два или более контролеров, совместно определяющих цели и/или средства обработки персональных данных;

обработчик – физическое лицо или юридическое лицо публичного или частного права, включая орган публичной власти, любое иное учреждение, организация или авторизованное лицо, которое обрабатывает персональные данные от имени контролера. Как правило, обработчиком является физическое или юридическое лицо, иное чем контролер;

система учета персональных данных – любой автоматически, вручную или смешанным образом структурированный набор личных данных, являющихся доступными в соответствии с определенными критериями, централизованный, децентрализованный или распределенный на функциональной или географической основе. Системой учета персональных данных являются, не ограничиваясь ими, реестры, дела, базы данных, информационные системы, в которых хранятся и автоматически, вручную в форме картотеки или смешанным образом обрабатываются персональные данные для определенной цели;

получатель – любое физическое лицо или юридическое лицо, орган публичной власти, любое иное учреждение, организация или авторизованное лицо, которому раскрываются персональные данные, независимо от того, является ли оно третьей стороной. В рамках операций по обработке персональных данных получатель соблюдает положения законодательства о защите персональных данных, касающиеся ограничения целей и обеспечения режима конфиденциальности и безопасности. Не считаются получателями органы публичной власти, которым персональные данные передаются в рамках осуществления согласно закону расследований, в том числе судебные инстанции при осуществлении правосудия и правоохранительные органы при реализации целей, предусмотренных пунктом d) части (2) статьи 2; обработка персональных данных этими органами публичной власти осуществляется по применимым правилам охраны персональных данных в соответствии с целью обработки;

третья сторона – физическое лицо или юридическое лицо публичного или частного права, орган публичной власти, учреждение, агентство, кроме субъекта персональных данных, контролера, обработчика и лиц, которые уполномочены обрабатывать персональные данные с прямой санкции контролера или обработчика;

согласие субъекта персональных данных – любое волеизъявление, свободное, конкретное, информированное и безоговорочное, данное в форме заявления или недусмысленного действия, которым субъект персональных данных соглашается на обработку касающихся его персональных данных;

нарушение безопасности персональных данных – нарушение правил безопасности, приводящее к случайным или умышленным уничтожению, утрате, изменению или несанкционированному разглашению персональных данных, неправильно переданных, хранящихся или обработанных, а также к несанкционированному доступу к ним;

прямой маркетинг – методы изучения рынка, распространения товаров и услуг, в которых использованы маркетинговые концепции, техники и инструменты, в том числе посредством почты, услуг электронных коммуникаций или других услуг по доставке, и которые конкретизируются в непосредственном посыле субъекту персональных данных с целью оценки его реакции;

псевдообезличивание персональных данных – обработка персональных данных таким образом, чтобы их нельзя было бы относить к их субъекту без использования дополнительной информации, которая хранится отдельно и доступ к ней ограничен

техническими и организационными мерами, препятствующими их отождествление с идентифицированным или идентифицируемым лицом;

обезличивание персональных данных – изменение персональных данных так, что детали личного или материального положения более не дают возможности отождествить персональные данные с идентифицированным или идентифицируемым лицом. Обезличенные данные не являются персональными данными;

правоохранительный орган в смысле настоящего закона:

– орган публичной власти или его подразделение, обладающие полномочиями по предотвращению, расследованию, раскрытию преступлений в рамках уголовного производства, уголовного преследования или исполнения уголовных наказаний, в том числе по предотвращению и пресечению угроз общественному порядку, такие как, не ограничиваясь ими: полиция, органы прокуратуры, таможенные органы, пенитенциарные учреждения, органы по предупреждению и борьбе с коррупцией, отмыванием денег, финансированием терроризма, органы по возмещению добытого преступным путем имущества, органы государственной безопасности;

- орган публичной власти или его подразделение, обладающие полномочия по национальной или государственной безопасности, осуществляющие специальную розыскную деятельность;

юридические лица публичного права в смысле настоящего закона – Парламент Республики Молдова, Аппарат Президента Республики Молдова, Правительство Республики Молдова, министерства, другие отраслевые органы центрального публичного управления и органы местного публичного управления I и II уровней, автономные органы публичной власти и публичные учреждения, подведомственные им публичные учреждения, государственные предприятия и подобные им организации, образовательные учреждения, учреждения здравоохранения, культуры и др., не ограничиваясь данным перечислением;

юридические лица частного права в смысле настоящего закона – юридические лица, преследующие цель извлечения прибыли и не преследующие такой цели;

представитель – физическое или юридическое лицо с местонахождением в Республике Молдова или в одном из государств-членов Европейского Союза, ответственных за Республику Молдова, письменно назначенное контролером или обработчиком в соответствии со статьей 32, представляющее контролера или обработчика относительно их обязанностей, предусмотренных настоящим законом;

международная организация – регулируемые международным публичным правом организация и подчиненные ей структуры или любая организация, учрежденная соглашением, заключенным двумя или более странами, либо на основании такого соглашения;

предприятие – физическое или юридическое лицо, осуществляющее экономическую деятельность независимо от организационно-правовой формы, в том числе партнерства и ассоциации, осуществляющие экономическую деятельность на постоянной основе;

группа предприятий – контролирующее предприятие и контролируемые им предприятия;

обязательные корпоративные правила – политика в области защиты персональных данных, которой должны руководствоваться контролер или обработчик с местонахождением в Республике Молдова при передаче персональных данных контролеру или обработчику, находящемуся в одной или нескольких странах, в

рамках группы предприятий или группы предприятий, осуществляющих общую экономическую деятельность;

услуги информационного общества – любая дистанционная услуга, оказываемая через электронные средства по индивидуальному запросу получателя услуги.

Глава II
ОСНОВНЫЕ УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 4. Принципы обработки персональных данных

(1) Персональные данные обрабатываются с соблюдением следующих принципов:

a) принципы законности, справедливости и прозрачности - персональные данные должны обрабатываться законно, справедливо и прозрачно для субъекта данных. Требование прозрачности не относится к обработке, производимой правоохранительными органами при осуществлении деятельности, предусмотренной пунктом d) части (2) статьи 2;

b) принцип ограничения целью - персональные данные должны собираться для определенных четко сформулированных и законных целей и не подлежат обработке в порядке, противоречащем этим целям. Последующая обработка для архивирования в общественных интересах, для научных и исторических исследований или в статистических целях в соответствии со статьями 14, 15 и 16 не считается противоречащей первоначальным целям;

c) принцип минимизации данных – обработке подлежат соответствующие адекватные персональные данные, ограниченные необходимыми для достижения целей обработки;

d) принцип точности - персональные данные должны быть точными и, при необходимости, актуализированными. Следует принять все необходимые меры для незамедлительного удаления, уничтожения или исправления неточных персональных данных с учетом целей их обработки;

e) принцип ограничения хранения - персональные данные подлежат хранению в форме, позволяющей идентифицировать субъект персональных данных в течение срока, необходимого для достижения целей обработки таковых. Срок хранения персональных данных может быть более продолжительным, если таковые обрабатываются исключительно для архивирования в общественных интересах, для научных и исторических исследований или в статистических целях в соответствии со статьями 14, 15 и 16, при условии, что принимаются предусмотренные настоящим

законом надлежащие технические и организационные меры для гарантирования прав и свобод субъектов данных;

f) принципы целостности и конфиденциальности - персональные данные должны обрабатываться таким образом, чтобы была обеспечена их надлежащая безопасность, в том числе их защита от несанкционированной или незаконной обработки, от случайного или незаконного удаления, уничтожения или искажения путем принятия соответствующих технических и организационных мер.

(2) Персональные данные подлежат маркировке при их передаче другим контролерам, третьим сторонам или получателям. Порядок и форма маркировки утверждаются Правительством.

(3) Контролер несет ответственность за обеспечение соответствия с частью (1) и может доказать соблюдение предусмотренных ею принципов. Персональные данные подлежат обработке под ответственность контролера, который обеспечивает и доказывает соответствие каждой операции по обработке положениям настоящего закона.

Статья 5. Законность обработки

(1) Обработка является законной только при соблюдении и по мере соблюдения ходя бы одного из следующих условий:

a) субъект данных дал согласие на обработку своих персональных данных в одной или нескольких особых целях;

b) обработка необходима для исполнения договора, стороной которого является субъект данных, или для осуществления определенных действий по требованию субъекта данных до заключения договора;

c) обработка необходима для выполнения контролером своей законной обязанности;

d) обработка необходима для защиты жизни, физической целостности или здоровья субъекта данных или другого физического лица;

e) обработка необходима для решения задачи в общественных интересах или в порядке осуществления полномочий органа публичной власти, которыми обладает контролер;

f) обработка необходима в законных интересах контролера или третьей стороны, кроме случая, когда превалируют интересы или основные права и свободы субъекта данных относительно защиты персональных данных, особенно если таковым является ребенок. Пункт f) не применяется к обработке, производимой органами публичной власти при осуществлении своих полномочий.

(2) В случае если обработка с другой целью чем та, для которой были собраны персональные данные, производилась без согласия субъекта данных или без законного основания, представляющего собой необходимую и соразмерную в демократическом обществе меру по обеспечению достижения целей, указанных в части (1) статьи 28, для определения совместимости цели обработки с целью первоначального сбора персональных данных контролер должен принимать во внимание:

a) любую связь между целями сбора персональных данных и целями последующей запланированной их обработки;

b) обстоятельства сбора персональных данных, в частности, отношения между субъектом данных и контролером;

c) характеристики персональных данных, особенно в случае обработки особых категорий персональных данных;

d) возможные последствия последующей запланированной обработки для субъекта данных;

e) наличие надлежащих гарантий, таких как шифрование или псевдообезличивание.

(3) Установленные настоящей статьей требования обязательны как для обладателя персональных данных, так и для лица, намеревающегося ими обладать, которые обязаны доказать цель, законного основание и причинную связь между категориями персональных данных и причиной обращения/заявления, законным интересом.

(4) Обработка персональных данных производится в соответствии с положениями настоящего закона. Отказ от незаконной обработки персональных данных не влечет дисциплинарной, гражданской, правонарушительной или уголовной ответственности.

Статья 6. Надзорный орган

(1) Национальный центр по защите персональных данных (далее – *Центр*) является органом публичной власти, обеспечивающим право на защиту персональных данных, вытекающее также из конституционного права на неприкосновенность интимной, семейной и частной жизни, наделенным неотъемлемым правом осуществлять надзор, предупреждать нарушения настоящего закона (путем информирования, обучения, регулирования и других не противоречащих закону мер), проверять соблюдение принципов защиты персональных данных, предусмотренных действующим законодательством и т.д.

(2) Деятельность Центра регулируется Законом о Национальном центре по защите персональных данных, настоящим законом и другими нормативными актами по введению в действие этих законов.

(3) В своей деятельности Центр может руководствоваться документами институтов Европейского Союза в области защиты персональных данных и их безопасности, если это необходимо для решения поставленных перед ним задач.

(4) Надзор Центра не распространяется на деятельность судебных инстанций, связанную с судопроизводством. Такой деятельностью признается только деятельность судьи по осуществлению правосудия при условии, что персональные данные обрабатываются с законной целью и по законному основанию, кроме случая их сбора, раскрытия или обработки в иных целях и по другим основаниям самим судьей или по его поручению вне необходимых процессуальных действий. Организационные и административные процедуры получения, передачи, распоряжения и хранения персональных данных не признаются деятельностью по осуществлению правосудия.

Статья 7. Запрос информации, содержащей персональные данные

В случае если контролер, ассоциированный контролер, обработчик, получатель, любой другой субъект, не являющийся получателем, третья сторона, независимо от вида собственности, области деятельности и организационно-правовой формы, запрашивают информацию, содержащую персональные данные, запрос должен содержать обоснование, цель, законное основание запроса, категории запрашиваемых персональных данных и доказательство причинной связи между запрашиваемыми категориями персональных данных и преследуемым законным интересом.

Статья 8. Условия дачи согласия на обработку персональных данных

(1) В случае если для обработки персональных данных необходимо согласие субъекта данных, контролер должен быть способным доказать получение такого согласия.

(2) В случае если согласие субъекта данных выражено в письменном заявлении, содержащем и другие аспекты, оно должно быть четко отделено от других аспектов и сформулировано на понятном и доступном языке. Выраженное в заявлении согласие не имеет юридических последствий, если само заявление составлено с нарушением настоящего закона.

(3) В случае несовершеннолетнего субъекта данных или субъекта данных, в отношении которого установлена мера судебной охраны, согласие на обработку персональных данных в письменной или электронной форме, с соблюдением требований к электронной подписи и электронному документу, дает его законный представитель либо при особых обстоятельствах согласие субъекта данных может быть выражено проставлением галочки в специальном окошке или иным способом подтверждения подлинности согласия. Контролер прилагает все разумные усилия для проверки дачи или подтверждения согласия законным представителем с учетом имеющихся технологий.

(4) При предоставлении услуг информационным обществом непосредственно ребенку обработка его персональных данных признается законной в соответствии с пунктом a) части (1) статьи 5, если ребенку исполнилось 16 лет. Если же ребенок не достиг 16-летнего возраста, обработка его персональных данных будет законной только при даче или подтверждении согласия лицом, несущим родительскую ответственность за ребенка.

(5) Согласие, полученное после обработки персональных данных, не имеет обратной силы.

(6) Субъект данных может в любое время отозвать свое согласие. Отзыв согласия не делает незаконной обработку, произведенную на основании согласия до его отзыва. Субъект данных ставится в известность об этом перед дачей согласия. Процедура отзыва согласия так же проста, как и процедура дачи согласия.

(7) При оценке безусловности дачи согласия принимаются во внимание необходимость и объем соответствующих обработанных категорий персональных данных с учетом заявленной цели.

(8) Форма согласия должна соответствовать средствам сбора персональных данных.

(9) Наличие согласия не освобождает контролера от обязанности соблюдать требования статьи 4.

(10) В случае констатации нарушения настоящего закона, особенно его статьи 4, даже при наличии согласия субъекта данных Центр может принять решение о повторной обработке персональных данных в строгом соответствии с положениями настоящего закона.

Статья 9. Обработка особой категории персональных данных

(1) Обработка особой категории персональных данных запрещается.

(2) Часть (1) не применяется в случаях, когда:

a) субъект персональных данных специально дал свое согласие на обработку в одной или нескольких специальных целях, кроме случая, когда закон предусматривает, что согласие субъекта данных не отменяет запрета, установленного частью (1);

b) обработка необходима в целях исполнения обязательств и осуществления особых прав контролера или субъекта данных в сфере занятости, охраны труда и социальной защиты, при условии что это предусмотрено законом или коллективным трудовым договором, заключенном на основе закона, устанавливающим надлежащие гарантии соблюдения основных прав и законных интересов субъекта данных;

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

d) обработка осуществляется в ходе законной деятельности и с предоставлением надлежащих гарантий фондом, объединением или любой другой некоммерческой организацией политического, философского, религиозного или профсоюзного толка, при условии что обработка относится исключительно к членам или бывшим членам таковых или лицам, имеющим регулярные контакты с таковыми в связи с их целями, и что данные не раскрываются третьим сторонам без согласия субъекта данных;

e) обработка относится к данным, добровольно и явно сделанным общедоступными субъектом данных;

f) обработка необходима для определения, осуществления или защиты права субъекта данных в суде или в других случаях осуществления правосудия;

g) обработка производится компетентными органами в целях предупреждения, раскрытия, расследования преступлений, осуществления уголовного преследования или исполнения наказаний, при условии соблюдения прав субъекта данных и других требований и гарантий, предусмотренных настоящим законом. Только уполномоченный на то государственный орган может вести любую систему учета персональных данных в целях предупреждения, раскрытия, расследования преступлений, осуществления уголовного преследования или исполнения наказаний;

h) обработка необходима в целях, связанных с профилактикой заболеваний, гигиеной труда, определением трудоспособности работников, постановкой диагноза, оказанием медицинской или социальной помощи, назначением лечения, управлением системами и услугами здравоохранения или социальной помощи, в соответствии с законом или договором, заключенным с медицинским работником, при условии соблюдения требований и гарантий, предусмотренных частью (3);

i) обработка необходима в интересах общественного здоровья, таких как защита от серьезных трансграничных угроз здоровью или обеспечение высоких стандартов качества и безопасности медицинской помощи, лекарств и медицинских изделий, в соответствии с законом, устанавливающим надлежащие специальные меры по защите основных прав и свобод субъекта данных, особенно профессиональной тайны;

j) обработка необходима для архивирования в общественных интересах, для научных и исторических исследований или в статистических целях в соответствии со статьями 14, 15 и 16, соразмерна преследуемой цели, соблюдает сущность права на защиту персональных данных и предусматривает соответствующие специальные меры по защите основных прав и законных интересов субъекта данных;

k) обработка специально предусмотрена законом.

(3) Особая категория персональных данных может быть обработана в целях, указанных в пункте) части (2), профессионалом, взявшим на себя обязательство хранения профессиональной тайны, или под его ответственность либо другим лицом,

также имеющим обязательство конфиденциальности, а также в соответствии с нормативными актами.

Статья 10. Обработка, не требующая идентификации субъекта данных

(1) Если цели обработки персональных данных не требуют или более не требуют идентификации субъекта данных, контролер не обязан добывать, хранить или обрабатывать дополнительную информацию для идентификации субъекта данных с единственной целью соблюдения настоящего закона.

(2) Если в указанных в части (1) случаях контролер может доказать отсутствие необходимости в идентификации субъекта данных, он информирует последнего об этом при наличии такой возможности. В данных случаях статьи 20-25 не применяются, при условии что субъект данных не предоставит контролеру дополнительную информацию для его идентификации с целью осуществления прав, предусмотренных указанными статьями.

Статья 11. Минимизация персональных данных, обрабатываемых в целях идентификации субъекта данных

(1) Сбор персональных данных для идентификации субъекта данных допустим, только если цель их получения тесно связана с оказываемой услугой или определенным случаем.

(2) Контролер и/или обработчик обязаны доказать по требованию субъекта данных необходимость сбора каждой категории персональных данных.

(3) В случае если контролер обладает персональными данными, идентифицирующими субъект данных, таковые актуализируются и удостоверяются предъявлением оригинального документа, удостоверяющего личность субъекта, без его изъятия или получения копий.

(4) Изъятие или удержание в любой форме официальных документов, удостоверяющих личность субъекта, запрещается, за исключением случаев, предусмотренных законом.

(5) В случае если у контролера есть основания сомневаться в идентичности субъекта данных, он может запросить дополнительную информацию, необходимую для удостоверения личности субъекта данных.

Статья 12. Свобода выражения и доступ к информации в связи с обработкой персональных данных

(1) Предусмотренный настоящим законом правовой режим признает и обеспечивает любому лицу право на свободу выражения и на доступ к информации.

(2) Каждый имеет право обрабатывать персональные данные для целей своей академической, художественной или литературной деятельности, а журналисты вправе обрабатывать персональные данные только с целью распространения информации в общественных интересах.

(3) Правила настоящего закона, за исключением полномочий Центра и положений статей 1-4, 13, 36 и глав VIII и IX, не применяются к обработке персональных данных в академических, художественных, журналистских или литературных целях, если необходимо уравновесить (сделать соразмерными) право на защиту персональных данных и свободу выражения, доступ к информации, при соблюдении следующих условий:

a) при обработке персональных данных с целью осуществления права на свободу выражения и на доступ к информации соблюдается право на защиту персональных данных, а у субъекта данных нет интересов, нуждающихся в защите, его гарантиям, физической и психической безопасности ничто не угрожает, принимая во внимание, что таковые имеют приоритет перед общественными интересами;

b) обработка персональных данных осуществляется с целью распространения информации в общественных интересах;

c) положения настоящего закона несовместимы и/или препятствуют осуществлению права на свободу выражения и на доступ к информации.

(4) Законом предусмотрены необходимые в демократическом обществе ограничения свободы выражения и доступа к информации в интересах национальной безопасности, территориальной целостности или общественной безопасности, для предупреждения беспорядков или преступности, охраны здоровья или нравственности, защиты репутации или прав других лиц, предупреждения разглашения конфиденциальной информации, поддержания авторитета и беспристрастия судебной системы.

(5) Для осуществления права на защиту персональных данных при обработке персональных данных в соответствии с настоящей статьей следует соотносить конкретную ситуацию с обязательностью обеспечения равновесия между правом на защиту персональных данных и правом на свободу выражения и на доступ к информации.

(6) Обработка персональных данных с соблюдением положений частей (1)-(5) исключает гражданскую, правонарушительную или уголовную ответственность.

Статья 13. Хранение и использование персональных данных

(1) Условия и сроки хранения и использования персональных данных устанавливаются законодательством с учетом положений статей 4 и 5.

(2) В случае если законодательством специально не предусмотрены условия и сроки хранения и использования персональных данных, таковые устанавливаются контролером. Органы публичной власти и публичные учреждения в своем качестве контролера устанавливают сроки хранения и использования персональных данных после консультаций с Центром.

(2) Персональные данные из государственных регистров с момента прекращения их использования могут оставаться на хранении, приобретая статус архивного документа.

(3) По достижении целей обработки персональных данных последние должны быть:

a) стерты или уничтожены без возможности восстановления;

b) преобразованы в архивные документы, представляющие интерес для общественности, и храниться в соответствии с законодальством об архивах с ограничением доступа к ним в течение всего срока хранения;

c) переданы другому контролеру в специально предусмотренных законом случаях;

d) обезличены или псевдообезличены.

(4) Государственные автоматизированные информационные системы, включая государственные реестры, обрабатывающие персональные данные, подлежат физическому хранению только в Республике Молдова.

Статья 14. Обработка персональных данных с целью их архивирования в общественных интересах

(1) Архивированные в общественных интересах персональные данные подлежат последующей обработке только в следующих случаях:

a) субъект данных, его законный представитель или наследники дали на то согласие;

b) для статистических целей или целей исторических или научных исследований;

c) для осуществления правосудия.

(2) Последующая обработка персональных данных в предусмотренных частью (1) случаях осуществляется в соответствии с настоящим законом.

(3) При обработке персональных данных с целью их архивирования в общественных интересах права на доступ, на ограничение, на исправление, на возражение и на передачу данных не осуществляются субъектами данных в той мере, в какой эти права могут сделать невозможным или воспрепятствовать достижению особых целей, а ограничение таких прав необходимо для достижения этих целей.

(4) Если указанная в части (3) обработка служит также другой цели, ограничение прав применяется только при обработке с целью архивирования персональных данных в общественных интересах.

(5) Обработка персональных данных с целью их архивирования в общественных интересах осуществляется с обеспечением гарантий соблюдения прав и свобод субъектов данных в соответствии с настоящим законом. Такими гарантиями служит принятие технических и организационных мер, необходимых для обеспечения соблюдения принципа минимизации данных. Эти меры могут включать псевдообезличивание при условии, что поставленные цели достигаются таким образом. Когда поставленные цели могут быть достигнуты последующей обработкой персональных данных, не позволяющей в дальнейшем идентифицировать субъект данных, эти цели достигаются таким образом.

Статья 15. Обработка персональных данных для статистических целей

(1) Обработка персональных данных для статистических целей означает любую операцию по сбору и обработке персональных данных, необходимую для статистических анкет или получения статистических результатов. Статистические цели предполагают, что результатом обработки являются не персональных данные, а сводные данные и что такой результат или данные не используются для принятия мер или решений в отношении конкретных физических лиц.

(2) Обработка персональных данных для статистических целей осуществляется с соблюдением в полной мере права на защиту персональных данных в соответствии с настоящим законом, а также нормативными актами, не противоречащими принципам защиты персональных данных.

(3) При обработке персональных данных для статистических целей права на доступ, на ограничение, на исправление и на возражение не осуществляются в той мере, в какой эти права могут сделать невозможным или воспрепятствовать достижению особых целей, а ограничение таких прав необходимо для достижения этих целей.

(4) Если указанная в части (3) обработка служит также другой цели, ограничение прав применяется только при обработке для статистических целей.

(5) Обработка персональных данных для статистических целей осуществляется с обеспечением гарантий соблюдения прав и свобод субъектов данных в соответствии с настоящим законом. Такими гарантиями служит принятие технических и организационных мер, необходимых для обеспечения соблюдения принципа минимизации данных. Эти меры могут включать псевдообезличивание при условии, что

поставленные цели достигаются таким образом. Когда поставленные цели могут быть достигнуты последующей обработкой персональных данных, не позволяющей в дальнейшем идентифицировать субъект данных, эти цели достигаются таким образом.

Статья 16. Обработка персональных данных для целей исторических или научных исследований

(1) Обработка персональных данных для целей научных исследований в широком смысле охватывает технологическое развитие, демонстрационную деятельность, фундаментальные исследования, прикладные исследования, исследования, финансируемые из частных источников.

(2) Под обработкой персональных данных для целей исторических исследований понимается обработка для исторических и генеалогических исследований.

(3) Обработка персональных данных для целей исторических или научных исследований осуществляется с соблюдением в полной мере права на интимную, семейную и частную жизнь, права на защиту персональных данных в соответствии с настоящим законом, а также нормативными актами, не противоречащими принципам защиты персональных данных.

(4) При обработке персональных данных для целей исторических или научных исследований права на доступ, на ограничение, на исправление и на возражение не осуществляются в той мере, в какой эти права могут сделать невозможным или воспрепятствовать достижению особых целей, а ограничение таких прав необходимо для достижения этих целей.

(5) Если указанная в части (4) обработка служит также другой цели, ограничение прав применяется только при обработке для целей исторических или научных исследований.

(6) Обработка персональных данных для целей исторических или научных исследований осуществляется с обеспечением гарантий соблюдения прав и свобод субъектов данных в соответствии с настоящим законом. Такими гарантиями служит принятие технических и организационных мер, необходимых для обеспечения соблюдения принципа минимизации данных. Эти меры могут включать псевдообезличивание при условии, что поставленные цели достигаются таким образом. Когда поставленные цели могут быть достигнуты последующей обработкой персональных данных, не позволяющей в дальнейшем идентифицировать субъект данных, эти цели достигаются таким образом.

Глава II

ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 17. Прозрачность информации, сообщений и порядка осуществления прав субъекта данных

(1) Предоставляемая субъекту данных информация в соответствии со статьями 18 и 19 и направляемые ему извещения в соответствии со статьями 20-27 и 38 должны быть сжатыми, прозрачными, понятными и легко доступными, должны быть изложены на понятном и простом языке, особенно если это касается информации, адресованной ребенку. Информация предоставляется в письменной или иной форме, в том числе электронной, если это целесообразно. По запросу субъекта данных предоставляется устная информация при условии, что личность субъекта данных проверена и удостоверена другими средствами.

(2) Контролер содействуют осуществлению прав субъекта данных, предусмотренных статьями 20-27. В указанных в части (2) статьи 10 случаях контролер удовлетворяет заявление субъекта данных, только если не докажет, что не может идентифицировать субъект данных.

(3) Контролер информирует субъекта данных о предпринятых действиях по его заявлению на основании статей 20-27 в течение не более месяца после поступления заявления. Этот срок может быть продлен при необходимости не более чем на два месяца, принимая во внимание сложность вопроса и количество заявлений, о чем контролер ставит в известность субъекта данных с уточнением причин продления срока. В случае поступления заявления субъекта данных по электронной почте информация для него также пересылается по электронной почте, только если субъект данных не предпочтет получать ее в другой форме.

(4) Если контролер не предпринимает никаких действий по заявлению субъекта данных, он незамедлительно или в течение не более месяца после поступления заявления информирует его о причинах этого и о возможности подать заявление в Центр или обратиться в судебную инстанцию.

(5) Предоставляемая субъекту данных информация в соответствии со статьями 18 и 19 и направляемые ему извещения в соответствии со статьями 20-27 и 38 являются бесплатными. В случае явно необоснованных, чрезмерных или повторных заявлений субъекта данных контролер может обоснованно, по обстоятельствам:

a) взыскать разумную плату за административные расходы по предоставлению информации и направлению извещений или за принятие запрашиваемых мер;

b) отказать в удовлетворении заявления.

(6) Без ущерба для положений статьи 10, в случае если у контролера есть основания сомневаться в идентичности лица, подающего заявление на основании

статей 20-26, он может запросить дополнительную информацию, необходимую для подтверждения личности субъекта данных.

(7) К информации, предоставляемой субъектам данных на основании статей 18 19, могут быть приложены стандатизированные изображения, наглядно и понятно представляющие соответствующую обработку. В случае если изображения представляются в электронном формате, они подлежат автоматическому считыванию.

Статья 18. Информирование субъекта данных

(1) В случае если персональные данные собираются непосредственно у субъекта данных, контролер или обработчик обязан бесплатно предоставить ему следующую информацию:

a) имя и контактные данные контролера/ассоциированных контролеров, обработчика или, по обстоятельствам, представителя контролера;

b) контактные данные ответственного за защиту персональных данных, по обстоятельствам;

c) цели и юридические основания обработки персональных данных, категории таковых;

d) законные интересы контролера или третьей стороны, в случае если обработка производится на основании пункта f) части (1) статьи 5;

e) получатели или категории получателей персональных данных;

f) намерение контролера передать персональные данные в другую страну или международной организации и наличие или отсутствие надлежащего уровня защиты таковых.

(2) По получении персональных данных контролер предоставляет субъекту данных следующую дополнительную информацию, необходимую для обеспечения справедливой по отношению к субъекту данных и прозрачной обработки таковых:

a) срок хранения персональных данных, а если таковой не установлен, критерии его установления, а также процедуры, которым подвергаются персональные данные по достижении целей их обработки;

b) наличие у субъекта данных права потребовать от контролера доступа к своим персональным данным, их исправления, удаления, ограничения обработки, а также прав на возражение против обработки и на передачу персональных данных;

c) при обработке персональных данных на основании согласия субъекта данных или пункта a) части (2) статьи 9 наличие у субъекта данных права на отзыв своего согласия в любое время без ущемления законности обработки, произведенной до отзыва согласия;

d) предоставление персональных данных их субъектом является законной или договорной обязанностью либо условием заключения договора, а при его обязательности последствия невыполнения этой обязанности;

e) наличие автоматизированного процесса принятия решений с созданием профилей, предусмотренного частями (1) и (4) статьи 27, а также по крайней мере в соответствующих случаях информация о предусмотренных логике, важности и последствиях такой обработки для субъекта данных;

f) наличие у субъекта данных права подать заявление в Центр.

(3) Субъект данных, как правило, информируется письменно, по электронной почте или иным способом, при условии что контролер может доказать, что проинформировал субъекта данных.

(4) В случае если контролер намеревается в дальнейшем обрабатывать персональные данные в иных целях, чем те, для которых они собирались, перед последующей обработкой он обязан сообщить субъекту данных цель такой обработки и другую информацию, предусмотренную частью (2).

(5) Положения частей (1), (2) и (4) не применяются, если субъект данных располагает соответствующей информацией.

Статья 19. Предоставление информации в случае получения персональных данных не от субъекта данных

(1) В случае получения персональных данных не от субъекта данных контролер предоставляет субъекту данных следующую информацию:

a) имя и контактные данные контролера/ассоциированных контролеров, обработчика или, по обстоятельствам, представителя контролера;

b) контактные данные ответственного за защиту персональных данных, по обстоятельствам;

c) цели и юридические основания обработки персональных данных;

d) категории обрабатываемых персональных данных;

e) получатели или категории получателей персональных данных, по обстоятельствам;

f) намерение контролера передать персональные данные зарубежному пользователю или международной организации (при наличии такового) и наличие или отсутствие решения Центра об обеспечении надлежащего уровня защиты персональных данных, в том числе в случае их передачи на основании статей 50, 51 и части (2) статьи 53.

(2) Помимо информации, указанной в части (1), контролер предоставляет субъекту данных следующую информацию, необходимую для обеспечения справедливой по отношению к субъекту данных и прозрачной обработки персональных данных:

a) срок хранения персональных данных, а если таковой не установлен, критерии его установления;

b) законные интересы контролера или третьей стороны, в случае если обработка производится на основании пункта f) части (1) статьи 5;

c) наличие у субъекта данных права потребовать от контролера доступа к своим персональным данным, их исправления, удаления, ограничения обработки, возражение против нее, а также права на передачу персональных данных;

d) при обработке персональных данных на основании пункта a) части (1) статьи 5 или пункта a) части (2) статьи 9 наличие у субъекта данных права на отзыв своего согласия в любое время без ущемления законности обработки, произведенной до отзыва согласия;

e) наличие у субъекта данных права подать заявление в Центр;

f) происхождение персональных данных и, по обстоятельствам, происхождение общедоступных источников;

g) наличие автоматизированного процесса принятия решений с созданием профилей, предусмотренного частями (1) и (4) статьи 27, а также по крайней мере в соответствующих случаях информация о предусмотренных логике, важности и последствиях такой обработки для субъекта данных.

(3) Указанная в частях (1) и (2) информация предоставляется контролером:

a) в разумный срок после получения персональных данных, но не более месяца, с учетом обстоятельств их обработки;

b) в момент первого контакта с субъектом данных, если целью сбора персональных данных было общение с их субъектом;

c) при первом раскрытии персональных данных другому получателю, если это предусмотрено целями их использования.

(4) В случае если контролер намеревается в дальнейшем обрабатывать персональные данные в иных целях, чем те, для которых они собирались, перед последующей обработкой он обязан сообщить субъекту данных цель такой обработки и другую информацию, предусмотренную частью (2).

(5) Положения частей (1)-(4) не применяются в следующих случаях:

a) субъект данных располагает соответствующей информацией;

b) предоставление информации оказывается невозможным или потребовало несоразмерных усилий, особенно в том, что касается обработки для архивирования в общественных интересах, для научных и исторических исследований или в статистических целях, с учетом требований и гарантий, предусмотренных статьями 14, 15 и 16, либо указанная в части (1) обязанность делает невозможным или значительно затрудняет достижение целей обработки. В таких случаях контролер принимает необходимые меры для защиты прав, свобод и законных интересов субъекта данных, включая обнародование информации;

c) получение или раскрытии персональных данных прямо предусмотрено законом, обязательным для исполнения контролером и предусматривающим адекватные меры по защите законных интересов субъекта данных;

d) законом предусмотрена конфиденциальность персональных данных в связи с обязанностью сохранения профессиональной тайны, включая законную обязанностью сохранения тайны.

Статья 20. Право доступа субъекта данных к своим персональным данным

(1) Субъект данных имеет право получить от контролера подтверждение или неподтверждение обработки своих персональных данных, а при подтверждение обработки – доступ к ним и предоставление следующей информации:

a) цели обработки персональных данных;

b) категории обрабатываемых персональных данных;

c) получатели или категории получателей, которым персональные данные уже раскрыты или подлежат раскрытию, особенно зарубежные получатели или международные организации;

d) срок хранения персональных данных, а если таковой не установлен, критерии его установления;

e) наличие у субъекта данных права потребовать от контролера исправления или удаления персональных данных, ограничения обработки, а также права на возражение против обработки;

f) наличие у субъекта данных права подать заявление в Центр;

g) любая информация об источнике персональных данных в случае их получения не от субъекта данных;

h) наличие автоматизированного процесса принятия решений с созданием профилей, предусмотренного статьей 27, а также по крайней мере в соответствующих случаях информация о предусмотренных логике, важности и последствиях такой обработки для субъекта данных.

(2) В случае передачи персональных данных в другую страну или международной организации субъект данных обязательно информируется об этом с уточнением наличия надлежащих гарантий передачи, предусмотренных статьей 50.

(3) По заявлению субъекта данных, содержащему его собственноручную подпись или электронную подпись, отвечающую требованиям электронного документа, контролер предоставляет ему копию персональных данных, подлежащих обработке. За любые другие копии контролер может взыскать разумную плату с учетом административных расходов на основании разработанного контролером положения. При поступлении электронного заявления информация предоставляется в обычном электронном формате, кроме случая запроса другого формата.

(4) Указанное в части (3) право на получение копии должно осуществляться таким образом, чтобы не ущемлять прав и свобод других субъектов данных.

(5) Субъект данных имеет право на основании заявления незамедлительно получить бесплатный физический доступ к своим персональным данным, хранящимся и обрабатываемым в системах учета, кроме случая, когда осуществление этого права противоречит требованиям обеспечиваемой безопасности, или невозможно по техническим причинам, или ущемляет права и свободы других субъектов данных.

Статья 21. Право на исправление

Субъект данных может на основании заявления незамедлительно получить у контролера право на:

a) исправление неточных или недостоверных касающихся его данных;

b) дополнение неполных касающихся его данных;

c) актуализацию касающихся его данных.

Статья 22. Право на удаление данных (право быть забытым)

(1) Субъект данных вправе потребовать от контролера удаления касающихся его персональных данных, а контролер обязан их незамедлительно удалить по одной из следующих причин:

a) отпала необходимость в персональных данных для достижения целей их сбора и обработки;

b) субъект данных отозвал свое согласие на обработку персональных данных, данное в соответствие с пунктом a) части (1) статьи 5 или пунктом a) части (2) статьи 9, при отсутствии другого юридического основания для обработки;

c) субъект данных возражает против обработки своих персональных данных на основании части (1) статьи 26 (при отсутствии другого юридического основания для обработки) либо на основании части (2) статьи 26;

d) произведена незаконная обработка персональных данных;

e) удаление персональных данных необходимо для соблюдения контролером предусмотренного законом требования;

f) персональные данные собраны в связи с оказанием услуг информационным обществом в соответствии с частью (4) статьи 8.

(2) В случае обнародования контролером персональных данных и его обязанности их удалить на основании части (1) он принимает разумные меры, в том числе технические, учитывая имеющуюся технологию и стоимость ее внедрения, для информирования контролеров, обрабатывающих персональные данные, о требовании субъекта данных удалить все ссылки на его персональные данные, а также любые копии или воспроизведения этих данных.

(3) В случае осуществления права на удаление персональных данных обрабатывающие их контролеры, обработчики, получатели, третья сторона и любые другие субъекты, не являющиеся получателями, обязаны незамедлительно или не позднее чем в месячный срок со дня получения извещения

внести изменения в свои операции по обработке персональных данных. Этот срок может быть продлен на 15 рабочих дней по причине сложности операций. О продлении срока и его причинах контролер информирует субъекта данных в течение 15 рабочих дней после поступления заявления. При поступлении электронного заявления информация предоставляется в электронном формате, кроме случая запроса другого формата.

(4) Положения частей (1)-(3) не применяются в той мере, в какой обработка оправдана и необходима:

a) для выполнения законной обязанности или решения задачи в общественных интересах либо для осуществления полномочий органа публичной власти, которыми обладает контролер;

b) в интересах общественного здоровья с соответствии с пунктами h) и i) части (2) и частью (3) статьи 9;

c) для установления, осуществления или защиты какого-либо права в судебной инстанции;

d) для архивирования в общественных интересах, для научных и исторических исследований или в статистических целях в соответствии со статьями 14, 15 и 16, в той мере, в какой указанное в части (1) право может сделать невозможным или значительно затруднить достижение целей обработки.

Статья 23. Право на ограничение обработки

(1) Субъект данных вправе потребовать от контролера ограничения обработки в одном их следующих случаях:

a) субъект данных оспаривает точность персональных данных – на период, достаточный для проверки их точности;

b) субъект данных считает обработку персональных данных незаконной, но вместо удаления персональных данных требует ограничения их использования;

c) персональные данные более не нужны контролеру для обработки, но они необходимы субъекту данных для установления, осуществления или защиты какого-либо права в судебной инстанции;

d) субъект данных возражает против обработки на основании части (1) статьи 26 – на период, достаточный для определения приоритета законных прав контролера или субъекта данных.

(2) В случае ограничения обработки персональных данных на основании части (1), за исключением хранения, таковые могут обрабатываться только с согласия субъекта данных, или для установления, осуществления или защиты какого-либо его права в судебной инстанции, а также для защиты прав физического или юридического лица, или в общественных интересах.

(3) Контролер информирует субъекта данных, добившегося ограничения обработки персональных данных на основании части (1), о сроке ограничения до его истечения.

Статья 24. Обязательное извещение об исправлении, удалении персональных данных или ограничении их обработки

Контролер сообщает каждому пользователю, которому он раскрыл персональные данные, о любом исправлении или удалении персональных данных либо об ограничении их обработки в соответствии со статьей 21, частью (1) статьи 22 и статьей 23, кроме случая, когда это оказывается невозможным или предполагает

несоразмерные усилия. Контролер информирует субъекта данных о таких пользователях по его запросу.

Статья 25. Право на передачу персональных данных

(1) Субъект данных имеет право на получение касающихся его персональных данных, которые он передал контролеру в обычно используемом структурированном формате, автоматически считываемом, и на передачу таковых другому контролеру без препятствий со стороны первого контролера, в случае если их обработка производится автоматизированными средствами на основании его согласия в соответствие с пунктом a) части (1) статьи 5 или пунктом a) части (2) статьи 9 либо на основании договора в соответствие с пунктом b) части (1) статьи 5.

(2) При осуществлении субъектом данных права на передачу персональных данных на основании части (1) таковые могут передаваться непосредственно от контролера к контролеру, если это осуществимо с технической точки зрения.

(3) Указанное в части (1) право осуществляется без ущерба для положений статьи 22. Такое право не осуществляется при обработке персональных данных для решения задачи в общественных интересах или в порядке осуществления полномочий органа публичной власти, которыми обладает контролер.

(4) Указанное в части (1) право осуществляется без ущемления прав и свобод других субъектов данных.

Статья 26. Право на возражение

(1) Субъект данных имеет право в любое время в связи с особой ситуацией, в которой он находится, возражать против обработки касающихся его персональных данных, в том числе против создания профилей, на основании пункта e) или f) части (1) статьи 5. В таком случае контролер прекращает обработку персональных данных, если только не докажет наличие законных и императивных оснований для обработки, которые имеют преимущество перед правами, свободами и интересами субъекта данных, либо что обработка производится для установления, осуществления или защиты какого-либо права в судебной инстанции.

(2) В случае если обработка персональных данных производится в интересах прямого маркетинга, субъект данных имеет право в любое время возражать против обработки касающихся его персональных данных, в том числе против создания профилей, в той мере, в какой такая обработка связана с прямым маркетингом.

(3) В случае если субъект данных возражает против обработки персональных данных в целях прямого маркетинга, персональные данные более не обрабатываются с этой целью.

(4) Указанное в частях (1) и (2) право доводится до субъекта данных не позднее первого контакта с ним, будучи представленным в ясной форме и отделено от другой информации.

(5) В рамках пользования услугами информационного общества субъект данных может осуществить свое право на возражение автоматизированными средствами, использующими технические спецификации.

(6) В случае если персональные данные обрабатываются для научных и исторических исследований или в статистических целях в соответствии со статьями 14, 15 и 16, субъект данных, исходя из особой ситуации, в которой он находится, имеет право возражать против обработки касающихся его персональных данных, кроме случая решения задачи в общественных интересах.

Статья 27. Автоматизированный процесс принятия частных решений, включающий создание профилей

(1) Субъект данных имеет право не быть объектом решения, порождающего серьезные юридические последствия для него и основанного исключительно на автоматизированной обработке персональных данных, включая создание профилей.

(2) Часть (1) не применяется, если решение:

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

b) санкционировано нормативным актом, применяемым к контролеру и устанавливающим меры для защиты прав, свобод и законных интересов субъекта данных;

c) основано на специальном согласии субъекта данных.

(3) В случаях, предусмотренных пунктами a) и c) части (2), контролер принимает надлежащие меры для защиты прав, свобод и законных интересов субъекта данных, по меньшей мере права на гуманное вмешательство контролера, на выражение своей точки зрения и на обжалование решения.

(4) Указанные в части (2) решения не основаны на особых категориях персональных данных, кроме случая применения пункта a) или g) части (2) статьи 9 и установления надлежащих мер для защиты прав, свобод и законных интересов субъекта данных.

Статья 28. Ограничения

(1) Права и обязанности, предусмотренные статьями 17-27 и 38, а также статьей 4 в той мере, в какой его положения соответствуют правам и обязанностям, предусмотренным статьями 17-27, могут быть ограничены законодательным актом при условии соблюдения сути основных прав и свобод и что это необходимо в демократическом обществе для:

a) защиты национальной и государственной безопасности;

b) охраны общественного порядка;

c) предотвращения, расследования, раскрытия преступлений, уголовного преследования или исполнения уголовных наказаний, включая защиту от угроз общественному порядку;

d) достижения важных общих целей государства, в частности в сфере экономики и финансов, включая денежную, бюджетную и налоговую области, здравоохранения и социальной безопасности;

e) защиты независимости судей и судопроизводства;

f) предотвращения, расследования, раскрытия и уголовного преследования нарушений профессиональной этики в случае регулируемых профессий;

g) мониторинга, инспектирования или регулирования, даже от случая к случаю, осуществления властных полномочий, предусмотренных пунктами a) - f);

h) защиты субъекта данных или прав и свобод других субъектов данных;

i) удовлетворения претензий гражданского права.

(2) Любая из перечисленных в части (1) законодательных мер в соответствии с настоящим законом должна содержать хотя бы положения, касающиеся:

a) целей или категорий обработки персональных данных;

b) категорий персональных данных;

c) сферы применения установленных ограничений;

d) гарантий от злоупотреблений, незаконных доступа или передачи персональных данных;

e) конкретного контролера или категорий контролеров;

f) сроков хранения персональных данных и применяемых гарантий с учетом характера и целей обработки таковых или категорий обрабатываемых персональных данных;

g) рисков для прав и свобод субъектов данных; и

h) права субъекта данных быть проинформированным об установленном ограничении, кроме случая, когда это может препятствовать достижению цели ограничения.

Глава VI
КОНТРОЛЕР И ОБРАБОТЧИК

Статья 29. Ответственность контролера

(1) Принимая во внимание характер, сферу применения, обстоятельства и цели обработки, а также риски различной степени вероятности и тяжести для прав и свобод физических лиц, контролер принимает надлежащие технические и организационные меры, позволяющие обеспечить и доказать соответствие обработки требованиям настоящего закона и/или регуляторных актов в области защиты персональных данных. Контролер обязан систематически проверять соблюдение установленных настоящим законом требований соответствия и безопасности и актуализировать их.

(2) Пропорциональные в отношении обработки меры, предусмотренные частью (1), предполагают реализацию контролером политики защиты персональных данных.

(3) Контролер обрабатывает персональные данные в соответствии с настоящим законом и обеспечивает соответствие обработки требованиям настоящего закона. Контролер несет ответственность за обработку персональных данных, если только не докажет, что правовые положения нарушены по вине обработчика в силу несоблюдения им требований договора или другого юридического акта.

(4) В случае если законодательством прямо не предусмотрены условия и сроки хранения и использования персональных данных, контролер устанавливает их в соответствии с положениями статьи 13.

(5) Обработанные контролером персональные данные могут быть переданы другому контролеру или ассоциированному контролеру для обработки в аналогичных целях или иных, чем те, в которых они собирались, но только на законном основании, указанном в части (1) статьи 5, и с соблюдением принципов, указанных в части (1) статьи 4.

(6) Присоединение к утвержденным кодексам поведения в установленном статьей 46 порядке или утвержденным механизмам сертификации, предусмотренным статьей 47, может служить доказательством выполнения контролером своих обязанностей.

Статья 30. Предполагаемое обеспечение защиты персональных данных с момента их появления

(1) Принимая во внимание нынешний уровень развития технологий, стоимость их внедрения, характер, сферу применения, обстоятельства и целей обработки, а также риски различной степени вероятности и тяжести для прав и свобод физических лиц в связи с обработкой персональных данных, при определении средств обработки и в процессе самой обработки контролер принимает надлежащие технические и организационные меры (такие как псевдообезличивание, обезличивание данных и др.), призванные обеспечить соблюдение принципов защиты персональных данных (таких как минимизация данных), необходимых гарантий при обработке, требований настоящего закона и защитить права субъекта данных.

(2) Принимаемые контролером надлежащие технические и организационные меры предположительно гарантируют обработку только персональных данных, необходимых для специальной цели обработки. Гарантии распространяются на объем собираемых персональных данных, степень их обработки, сроки хранения и доступ к ним. В частности, такие меры делают недоступными персональные данные для неограниченного числа лиц без вмешательства их субъекта.

(3) Для обеспечения защиты персональных данных, их предполагаемой конфиденциальности и конфиденциальности с момента появления контролер обязан

согласовать с Центром создание систем учета персональных данных, если они предполагают обработку особой категории персональных данных.

(4) Органы публичной власти и публичные учреждения согласовывают с Центром создание любой системы учета, предполагающей обработку персональных данных.

(5) Заключение Центра о соответствии обработки в момент изучения ситуации основывается в соответствии с настоящим законом на оценке влияния обработки на защиту персональных данных и на представленных заявителем информации и материалов. Для получения заключения Центра заявитель указывает в своем заявлении:

a) ответственность контролера, ассоциированных контролеров и обработчиков, по обстоятельствам, особенно если обработка производится в рамках группы предприятий;

b) цели и средства предполагаемой обработки;

c) предусмотренные настоящим законом меры и гарантии защиты прав и свобод субъектов данных;

d) контактные данные ответственного за защиту персональных данных, при необходимости;

e) влияние обработки на защиту персональных данных; и

f) любые другие сведения, запрашиваемые Центром в связи с обработкой персональных данных.

(6) Выдача заключения не исключает вмешательства Центра на любом этапе при появлении новых обстоятельств и/или выявления рисков для осуществления прав и свобод субъектов данных.

(7) Механизм сертификации, утвержденный в установленном статьей 47 порядке, может служить доказательством выполнения требований, предусмотренных частями (1) и (2). Настоящая часть не применяется к обработке персональных данных в соответствии с пунктом d) части (2) статьи 2.

Статья 31. Ассоциированные контролеры

(1) Ассоциированные контролеры устанавливают соглашением или другим юридическим актом в условиях прозрачности ответственность каждого из них за исполнение обязанностей, вменяемых им настоящим законом, в частности, за осуществление прав субъектов данных и предоставление информации, предусмотренной статьями 18 и 19, при условии и в той мере, в какой такая ответственность не определена законом, обязательным для исполнения ассоциированными

контролерами. Соглашение или юридический акт может содержать положение об определении пункта для контакта с субъектами данных.

(2) Указанное в части (1) соглашение устанавливает роли ассоциированных контролеров и их отношения с субъектами данных. Соглашение доводится до сведения субъекта данных, если этим не ставятся под угрозу применяемые контролером меры безопасности; в противном случае сообщается только суть соглашения.

(3) Независимо от положений соглашения, указанного в части (1), субъект данных может осуществлять свои права в отношениях с каждым контролером в соответствии с настоящим законом.

Статья 32. Представители контролеров или лиц с местонахождением вне Республики Молдова

(1) В случае применения пункта c) части (2) статьи 2 контролеры и обработчики с местонахождением вне Республики Молдова обязаны письменно назначить своего представителя в Республике Молдова или представителя в государстве-члене Европейского Союза, ответственном за Республику Молдова.

(2) Предусмотренная частью (1) обязанность не распространяется на:

a) одноразовую обработку, в общем не охватывающую особые категории персональных данных и не несущую риски для прав и свобод субъектов данных, принимая во внимание характер, сферу применения, обстоятельства и цели обработки;

b) органы публичной власти и публичные учреждения.

(3) Для обеспечения соблюдения настоящего закона представитель уполномочен контролером и обработчиком решать все вопросы, связанные с обработкой персональных данных, с которыми к нему обращаются Центр и субъект данных.

(4) Назначение контролером или обработчиком своего представителя не препятствует предъявлению законных исков к контролеру или обработчику.

Статья 33. Обработчик

(1) Для обработки от имени контролера последний привлекает только обработчиков, предоставляющих достаточные гарантии применения надлежащих технических и организационных мер для обеспечения соблюдения предусмотренных настоящим законом требований и защиты прав субъектов данных.

(2) Обработчик не может заключить договор с другим обработчиком без предварительного получения письменного специального или общего разрешения контролера. В случае письменного общего разрешения обработчик информирует контролера о своем намерении привлечь новых обработчиков или заменить имеющихся, что дает возможность контролеру возразить против таких изменений.

(3) Обработка персональных данных обработчиком регулируется договором или другим юридическим актом, обязательным для сторон и устанавливающим предмет и продолжительность обработки, характер и цель обработки, вид персональных данных, категории субъектов данных, обязанности и права контролера. Соответствующий договор или юридический акт предусматривает, в частности, что обработчик:

a) обрабатывает персональные данные только на основании задокументированных инструкций контролера, в том числе касающихся передачи персональных данных другой стране или международной организации, кроме случая, когда это является обязанностью обработчика. В данном случае он извещает об этом контролера до обработки, если только правом не запрещено такое извещение в общественных интересах;

b) удостоверился, что авторизованные обрабатывать персональные данные лица обязались соблюдать конфиденциальность либо что соблюдение конфиденциальности является их уставной обязанностью;

c) принял все необходимые меры в соответствии со статьей 36;

d) соблюдает предусмотренные частями (2) и (4) условия заключения договора с другим обработчиком;

e) учитывая характер обработки, принятием по мере возможности надлежащих технических и организационных мер оказывает контролеру помощь в обеспечении условий для осуществления субъектом данных прав, предусмотренных главой III;

f) оказывает контролеру помощь в выполнении им обязательств, предусмотренных статьями 36, 37, 38, 40, 41, с учетом характера обработки и имеющейся у него информации;

g) по желанию контролера стирает или возвращает ему все персональные данные по прекращении предоставления услуг, связанных с обработкой, и удаляет имеющиеся копии, если законом не предусмотрено иное;

h) предоставляет контролеру всю информацию, необходимую для доказательства выполнения обязательств, предусмотренных настоящей статьей, позволяет и содействует проведению аудита, включая инспекции, контролером или уполномоченным аудитором. В случае если считает, что какая-либо инструкция нарушает настоящий закон или другие нормативные акты в области персональных данных, незамедлительно доводит это до сведения контролера.

(4) В случае заключения обработчиком договора на осуществление работ, связанных с обработкой персональных данных от имени контролера, с другим обработчиком, последний обязан выполнять в соответствии с частью (3) те же обязательства

по защите персональных данных, предусмотренные договором или другим юридическим актом, заключенным между контролером и обработчиком, которые на него возлагаются договором или другим юридическим актом, в частности по предоставлению достаточных гарантий применения надлежащих технических и организационных мер для соблюдения требований настоящего закона к обработке. В случае невыполнения вторым обработчиком своих обязательств по защите персональных данных первый обработчик несет за это ответственность в полном объеме перед контролером.

(5) Присоединение обработчика к утвержденному кодексу поведения, указанному в статье 45, или к утвержденному механизму сертификации, указанному в статье 47, может служить доказательством предоставлению достаточных гарантий, предусмотренных частями (1) и (4) настоящей статьи.

(6) Без ущерба для индивидуального договора, заключенного между контролером и обработчиком, указанный в частях (3) и (4) договор или другой юридический акт может содержать полностью или частично стандартные договорные условия, предусмотренные частями (7) и (8) настоящей статьи, в том числе если таковые являются частью сертификации, предоставляемой контролеру или обработчику в соответствии со статьями 47 и 48.

(7) Центр может установить стандартные договорные условия для аспектов, предусмотренных частями (3) и (4).

(8) Договор или другой юридический акт, указанный в частях (3) и (4), составляется в письменной форме, в том числе в электронном формате с соблюдением требований к электронной подписи и электронному документу.

(9) Без ущерба для статей 88 и 89, в случае нарушения обработчиком настоящего закона путем установления целей и средств обработки персональных данных обработчик признается контролером в отношении соответствующей обработки.

(10) Обработка персональных данных признается осуществленной обработчиком под ответственность контролера в случае ее соответствия правовому режиму, предусмотренному настоящим законом.

Статья 34. Обработка персональных данных от имени контролера или обработчика

(1) Обработчик и любое другое лицо, действующее от имени контролера или обработчика и имеющее доступ к персональным данным, обрабатывают последние только с соблюдением инструкций контролера при условии, что законом не предусмотрено иное.

(2) Обработка персональных данных лицами, находящимися в трудовых правоотношениях с контролером или обработчиком в соответствии с договором или другим юридическим актом, признается осуществленной контролером.

(3) Если указанная в части (1) обработка персональных данных произведена в иных, чем установленные контролером, целях, осуществившее ее лицо признается по отношению к ней контролером независимо от того, находится ли оно в трудовых правоотношениях с контролером.

Статья 35. Учет деятельности по обработке

(1) Контролер и, по обстоятельствам, его представитель ведут учет деятельности по обработке персональных данных, осуществляемой под их ответственность. Учету подлежит следующая информация:

a) наименование контролера, имя и данные обработчика, ассоциированного контролера, представителя контролера и ответственного за защиту персональных данных;

b) цель и законное основание обработки;

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

d) категории получателей, которым предоставлены или будут предоставлены персональные данные, включая зарубежных получателей или международные организации;

e) если таковая имела место, передача персональных данных другой стране или международной организации с указанием соответствующей страны или международной организации и – в случае передачи, указанной в части (2) статьи 53, - документации, подтверждающей наличие надлежащих гарантий;

f) предельные сроки удаления различных категорий персональных данных, если их установление возможно;

g) если это возможно, общее описание технических и организационных мер безопасности, предусмотренных частью (1) статьи 36.

(2) Каждый контролер и, по обстоятельствам, обработчик ведут учет всех видов деятельности по обработке персональных данных, осуществляемых от имени контролера, охватывая следующую информацию:

a) имя и контактные данные обработчика или обработчиков и каждого контролера, от имени которого действует обработчик (действуют обработчики), а также представителя контролера или представителя обработчика, по обстоятельствам;

b) операции по обработке персональных данных, осуществленные от имени контролера, с указанием цели и законного основания обработки;

c) если таковая имела место, передача персональных данных другой стране или международной организации с указанием соответствующей страны или международной организации и – в случае передачи, указанной в части (2) статьи 53, - документации, подтверждающей наличие надлежащих гарантий;

d) если это возможно, общее описание технических и организационных мер безопасности, предусмотренных частью (1) статьи 36.

(3) Учет деятельности по обработке персональных данных ведется в автоматизированной, смешанной или ручной форме с сохранением учетных данных в течение пяти лет.

(4) Контролер или, по обстоятельствам, обработчик, представитель контролера или представитель обработчика, а также субъекты, не являющиеся получателями, третья сторона независимо от вида собственности, области деятельности и организационно-правовой формы предоставляют Центру, по его требованию, учетные данные о деятельности по обработке персональных данных. При необходимости Центр может запросить дополнительную информацию об учете деятельности по обработке персональных данных.

(5) Положения частей (1), (2) и (3) не применяются к юридическим лицам публичного или частного права, имеющим менее 20 работников, если только производимая ими обработка персональных данных не сопряжена с риском для прав и свобод субъектов обрабатываемых данных, не является случайной и не касается особых категорий персональных данных, предусмотренных частью (1) статьи 9.

(6) Центральные и местные органы публичной власти всех уровней, являющиеся контролерами, утверждают подробные внутренние регламенты выполнения требований и внутреннего контроля за их выполнением.

Глава II
БЕЗОПАСНОСТЬ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 36. Безопасность обработки

(1) С учетом уровня развития технологий, расходов на их внедрение, характера и области применения, обстоятельств и целей обработки, а также рисков различных степеней вероятности и тяжести для прав и свобод физических лиц контролер, ассоциированный контролер, обработчик, получатель, а также субъекты, не являющиеся получателями, третья сторона независимо от вида собственности, области деятельности и организационно-правовой формы принимают адекватные риску

технические и организационные меры для обеспечения надлежащего уровня безопасности, включающие помимо прочего:

a) безопасность помещений, в которых обрабатываются и хранятся персональные данные, в том числе безопасность средств обработки и хранения персональных данных;

b) выявление и авторизацию лиц, имеющих доступ к системам учета, содержащим персональные данные;

c) внедрение процедур авторизации и предоставления права доступа к системам учета и принятие контрольных мер (разрешение на доступ с учетом уровня иерархии, установление прав, обязанностей, ограничений, осуществление контроля мер по безопасности, повышение ответственности работников, мониторинг срочных мероприятий);

d) установку и/или изменение средств, программного/аппаратного обеспечения, составление их списка, а также установление правил управления временными картотеками;

e) защиту носителей для хранения персональных данных (учет носителей для хранения персональных данных, контроль использования, способ блокировки неавторизованного использования, удаление, псевдообезличивание и шифрование персональных данных или обезличивание хранящихся персональных данных);

f) антивирусную защиту (обеспечение антивирусной защиты и актуализация средств обеспечения защиты от вредных программ и вирусных подписей);

g) защиту от проникновений, в том числе с использованием беспроводных технологий;

h) целостность персональных данных (обеспечение хранения информации, содержащей персональные данные, с ее первоначальными атрибутами и ее изменения только авторизованными лицами. При передаче информации, содержащей персональные данные, должны использоваться средства криптографической защиты и электронная подпись. При хранении, обработке или передаче персональных данных должны приниматься надлежащие меры от случайного или незаконного уничтожения или изменения, от случайной утраты или искажения, от незаконных хранения, обработки, доступа или обнародования);

i) доступность персональных данных (обеспечение при помощи технических средств доступа к информации в течение установленного отрезка времени согласно технической спецификации, производство резервных копий информации, содержащей персональные данные, обеспечение возможности их восстановления в течение определенного отрезка времени);

j) конфиденциальность персональных данных (обеспечение, в том числе при помощи технических средств, доступа к информации, содержащей персональные данные, только авторизованным лицам и только к персональным данным, доступ к которым разрешен);

k) маркировку информации, содержащей персональные данные;

l) сохранение в системе персональных данных в течение пяти лет учетных данных о мероприятиях, событиях и/или действиях, зарегистрированных в системе аудита безопасности;

m) управление инцидентами безопасности персональных данных в соответствии со статьями 37 и 38;

n) внутреннюю проверку безопасности, осуществляемую ежегодно или по мере необходимости (выявление и анализ слабых мест управляемых систем учета, проверка соблюдения внедренных мер безопасности и периодическая оценка эффективности технических и организационных мер для обеспечения безопасности персональных данных);

o) обеспечение мер безопасности, предусмотренных настоящей главой, также при использовании виртуальной среды.

(2) При оценке уровня безопасности принимаются во внимание риски случайных или умышленных уничтожения, утраты, изменения, обнародования или незаконного доступа к передаваемым, хранящимся или обрабатываемым персональным данным, другие факторы, способные повлиять на безопасность персональных данных.

(3) Контролер и обработчик должны принять меры, чтобы действующие от их имени лица, имеющие доступ к персональным данным, обрабатывали последние исключительно по требованию контролера, только если такая обязанность не вменяется им законодательством.

(4) Детальное описание мер безопасности обработки персональных данных утверждается, при необходимости, постановлением Парламента.

(5) Контролер, ассоциированный контролер, обработчик, получатель, а также субъекты, не являющиеся получателями, третья сторона независимо от вида собственности, области деятельности и организационно-правовой формы должны предоставлять Центру, по его требованию, подробную информацию о принятых мерах безопасности. Центр обеспечивает конфиденциальность и неразглашение такой информации.

Статья 37. Уведомление Центра о случаях нарушения безопасности персональных данных

(1) В случае нарушения безопасности персональных данных контролер незамедлительно, но не позднее 72 часов после того, как это стало ему известным, уведомляет о нем Центр, если только такое нарушение угрожает правам и свободам субъектов данных. Уведомление, направленное с нарушением установленного срока, должно содержать объяснение задержки.

(2) Обработчик сообщает контролеру без необоснованных задержек о ставшим ему известным нарушении безопасности персональных данных.

(3) Уведомление должно содержать:

a) описание характера нарушения безопасности персональных данных, если это возможно, категории и примерное число субъектов, безопасность персональных данных которых нарушена, а также примерное число регистраций и категории персональных данных безопасность которых нарушена;

b) имя и контактные данные ответственного за защиту персональных данных или контактные данные пункта, в котором можно получить необходимую информацию;

c) описание возможных последствий нарушения безопасности персональных данных;

d) принятые контролером или предложенные ему меры для устранения нарушения безопасности персональных данных, в том числе для уменьшения вреда от возможных последствий;

e) другую необходимую информацию.

(4) При невозможности предоставления всей информации одновременно таковая сообщается поэтапно, но без необоснованных задержек.

(5) По всем случаям нарушения безопасности персональных данных контролер должен хранить документы, содержащие описание фактической ситуации нарушения безопасности персональных данных, последствий нарушения и принятых мер для их устранения. Такая документация дает возможность Центру проверить соблюдение настоящей статьи.

(6) С учетом положений настоящей статьи Центр своим приказом утверждает порядок и сроки уведомления об инцидентах безопасности, а также соответствующие приложения.

Статья 38. Сообщение субъектам данных о нарушении безопасности их персональных данных

(1) В случае если нарушение безопасности персональных данных представляет значительную угрозу для прав и свобод субъектов данных, контролер без необоснованных задержек сообщает о нем субъекту данных.

(2) Направляемое субъектам данных сообщение в соответствии с частью (1) настоящей статьи должно содержать ясное и простое описание характера нарушения безопасности персональных данных, а также по меньшей мере информацию, указанную в пунктах b), c) и d) части (3) статьи 37.

(3) В предусмотренном частью (1) сообщении нет необходимости при одном из следующих обстоятельств:

a) в отношении персональных данных, которых коснулось нарушение безопасности, контролером приняты надлежащие технические и организационные меры безопасности, такие как шифрование, делающие персональные данные непонятными для лиц, не имеющих законного доступа к ним;

b) контролером приняты последующие меры, обеспечивающие устранение значительной угрозы для прав и свобод субъектов данных, указанной в части (1);

c) если направление сообщения каждому субъекту данных предполагает чрезмерные усилия, такое сообщение публикуется в средствах массовой информации либо соответствующая информация доводится до сведения субъектов данных другим столь же эффективным способом.

Статья 39. Требования к доступу и обнародованию персональных данных

(1) Лица, имеющие доступ к персональным данным, обязаны обрабатывать их в соответствии со статьями 4 и 5.

(2) Лицо имеет право доступа к информации, включая персональные данные, в следующих случаях:

a) обработке подлежат персональные данные, обнародованные по воле и с выраженного согласия субъекта таковых;

b) персональные данные обезличены;

c) персональные данные подверглись псевдообезличиванию при условии снижения риска нарушения защиты персональных данных;

d) при наличии законного основания.

(3) Обработка обнародованных персональных данных, опубликование таковых или предоставление неограниченного доступа к ним не исключает соблюдения правового режима обработки персональных данных, предусмотренного настоящим законом.

(4) Органы публичной власти не имеют права передавать информацию, содержащую персональные данные, юридическим лицам публичного или частного права и физическим лицам, если только для этого нет законного основания, предусмотренного статьей 5.

Статья 40. Оценка причинения ущерба защите персональных данных

(1) В случае если обработка персональных данных, в частности с использованием новых технологий, может представлять значительную угрозу для прав и свобод субъектов данных, до ее осуществления контролер производит оценку приченения ущерба защите персональных данных предполагаемыми операциями по обработке, принимая во внимание характер, область применения, обстоятельства и цели обработки. Аналогичные операции по обработке с одинаковым уровнем рисков могут быть подвергнуты единой оценке.

(2) Для оценки приченения ущерба защите персональных данных контролер запрашивает заключение ответственного за защиту персональных данных, если такой назначен.

(3) Предусмотренная частью (1) оценка приченения ущерба защите персональных данных обязательна в частности:

a) при систематической и всеобъемлющей оценке личных аспектов субъектов данных, основанной на автоматизированной обработке, включая создание профилей, и лежащей в основе решений, имеющих юридические последствия для субъекта данных или иным образом значительно влияющих на него;

b) при широкомасштабной обработке особых категорий персональных данных, предусмотренных частью (1) статьи 9;

c) при широкомасштабном систематическом мониторинге доступной общественности зоны.

(4) Центр устанавливает и публикует на своей официальной веб-странице перечень видов операций по обработке, подлежащих оценке причинения ущерба защите персональных данных.

(5) Центр может установить и опубликовать на своей официальной веб-странице перечень видов операций по обработке, в отношении которых не производится оценка причинения ущерба защите персональных данных.

(6) Оценка предполагает:

a) системное описание предусмотренных операций по обработке и целей обработки с указанием, при необходимости, законных интересов контролера;

b) оценку необходимости и адекватности операций по обработке с учетом их целей;

c) оценку указанных в части (1) угроз для прав и свобод субъектов данных;

d) установление мер устранения угроз и предоставления гарантий, включая меры безопасности и механизмы, позволяющие обеспечить защиту персональных данных и доказать соблюдение законодательства в том, что касается прав и законных интересов субъектов данных и других заинтересованных лиц;

e) оценку ущерба, причиняемого операциями по обработке;

f) изучение другой информации.

(7) Контролер испрашивает, когда это уместно, мнение субъекта данных или его представителя относительно обработки персональных данных, если это не наносит ущерб коммерческим или общественным интересам либо безопасности операций по обработке.

(8) Части (1)-(7) настоящей статьи не применяются, если юридическое основание обработки, предусмотренное пунктами c) и e) части (1) статьи 5, регулирует особую операцию по обработке или ряд особых операций по обработке, при условии оценки причинения ущерба защите персональных данных в рамках оценки причинения общего ущерба в связи применением соответствующего юридического основания.

(9) При необходимости контролер определяет, учитывается ли оценка причинения ущерба защите персональных данных при обработке последних, по меньшей мере при изменении риска, предполагаемого операциями по обработке.

Статья 41. Предварительная консультация

(1) Контролер консультируется с Центром до производства обработки, если предусмотренная статьей 40 оценка причинения ущерба защите персональных данных говорит о том, что обработка сопряжена с высоким риском, если контролером не будут приняты меры для снижения такого риска.

(2) В случае если Центр сочтет, что предусмотренная частью (1) обработка приведет к нарушению настоящего закона, особенно когда риск не установлен или не снижен, он в срок не более двух месяцев срок со дня поступления заявления о консультировании предоставляет контролеру или, по обстоятельствам, обработчику письменную консультацию и может воспользоваться любым полномочием из предоставленных ему настоящим законом или Законом о Национальном центре по защите персональных данных. Указанный срок может быть продлен не более чем на два месяца с учетом сложности предполагаемой обработки. Центр в месячный срок со дня поступления заявления информирует контролера или, по обстоятельствам,

обработчика о любом продлении срока для предоставления консультации с указанием причин такого продления. Течение срока прерывается до получения Центром запрошенной информации в связи с соответствующей консультацией.

(3) Для получения предварительной консультации контролер предоставляет Центру следующую информацию:

a) ответственность контролера, ассоциированных контролеров и обработчиков, по обстоятельствам, особенно в связи с обработкой группой предприятий;

b) цели и средства предполагаемой обработки;

c) принимаемые меры и предоставляемые гарантии для защиты прав и свобод субъектов данных в соответствии с настоящим законом;

d) при необходимости, контактные данные ответственного за защиту персональных данных;

e) оценка причинения ущерба защите персональных данных, предусмотренная статьей 40; и

f) любую другую запрашиваемую Центром информацию.

(4) Органы публичной власти обязаны получить заключение Центра на проекты нормативных актов, касающихся или затрагивающих обработку персональных данных, в том числе в областях общественного порядка, государственной безопасности, социальной защиты и общественного здоровья.

(5) В отступление от части (1) контролер обязан проконсультироваться с Центром и получить его предварительное разрешение на обработку персональных данных для выполнения в общественных интересах поставленной перед ним задачи, в том числе связанной с общественным порядком, социальной защитой и общественным здоровьем.

Статья 42. Назначение ответственного за защиту персональных данных

(1) Контролер и обработчик назначают ответственных за защиту персональных данных каждый раз, когда:

a) обработка персональных данных производится органом публичной власти или учреждением, оказывающим государственные услуги, за исключением судебных органов;

b) основная деятельность контролера или обработчика состоит в обработке персональных данных, которая в силу своего характера, области применения и/или целей требует периодического и систематического мониторинга субъектов данных в широком масштабе;

c) основная деятельность контролера или обработчика состоит в широкомасштабной обработке особой категории персональных данных, предусмотренной статьей 9.

(2) Группа предприятий, ассоциаций, концернов, консорциумов может назначить единого ответственного за защиту персональных данных при условии, что он будет доступен для каждого предприятия.

(3) В случае если контролером или обработчиком является орган публичной власти или публичное учреждение, для нескольких таких органов или учреждений, не имеющих статуса юридического лица, может быть назначен единый ответственный за защиту персональных данных с учетом их организационной структуры и численности персонала.

(4) В случаях, не указанных в части (1), контролер или обработчик либо их ассоциации или учреждения, представляющие категории контролеров или обработчиков, могут назначить или – если того требует нормативный акт – назначают ответственного за защиту персональных данных. Ответственный за защиту персональных данных может действовать в интересах таких ассоциаций или учреждений.

(5) Ответственным за защиту персональных данных назначается лицо, обладающее профессиональными навыками и, в частности, специальными знаниями в области защиты персональных данных или информационной безопасности и способное выполнять задачи, предусмотренные статьей 44.

(6) Ответственный за защиту персональных данных может быть включен в штат контролера или обработчика либо решать поставленные перед ним задачи на основе гражданского договора.

(7) Контролер или обработчик публикует на своей официальной веб-странице и вывешивает в месте своего нахождения контактные данные своего ответственного за защиту персональных данных.

(8) Принимая во внимание численность персонала, объем и категории обрабатываемых персональных данных, сопутствующие риски, контролер или обработчик, правоохранительные органы могут создавать структурные подразделения, ответственные за защиту персональных данных.

Статья 43. Должность ответственного за защиту персональных данных

(1) Контролер и обработчик должны быть уверены, что ответственный за защиту персональных данных своевременно принимает надлежащие меры по любому аспекту защиты персональных данных.

(2) Контролер и обработчик оказывают содействие ответственному за защиту персональных данных в выполнении им задач, предусмотренных статьей 44,

обеспечивая его ресурсами, необходимыми для выполнения этих задач, получения доступа к персональных данным, операциям по обработке, документам, регулирующим обработку, а также для приобретения и умножения специальных знаний.

(3) Контролер и обработчик должны быть уверены, что ответственный за защиту персональных данных не получает никаких указаний относительно выполнения поставленных перед ним задач. Контролер или обработчик не может уволить или наказать ответственного за защиту персональных данных за законно выполняемые им задачи.

(4) Ответственный за защиту персональных данных непосредственно отчитывается перед самым высокопоставленным лицом из руководства контролера или обработчика.

(5) Субъекты данных могут обращаться к ответственному за защиту персональных данных по всем вопросам, связанным с обработкой персональных данных и осуществлением прав на основании настоящего закона.

(6) При исполнении своих обязанностей ответственный за защиту персональных данных обязан в установленном законом порядке, даже после увольнения, обеспечить конфиденциальность информации, к которой он имеет доступ.

(7) Ответственный за защиту персональных данных может также выполнять другие задачи и обязанности. Однако, контролер и обработчик должны быть уверены в том, что такие задачи и обязанности не порождают конфликт интересов или не мешают, не препятствуют выполнению основных задач.

Статья 44. Задачи ответственного за защиту персональных данных

(1) Перед ответственным за защиту персональных данных стоят следующие задачи:

a) информирование и консультирование контролера или обработчика, а также их работников, занимающихся обработкой персональных данных, относительно их обязанностей, предусмотренных настоящим законом и нормативными положениями о защите персональных данных;

b) мониторинг соблюдения настоящего закона и нормативных положений о защите персональных данных, мониторинг политики контролера или обработчика в области защиты персональных данных, включающей распределение ответственности, привлечение внимания к проблеме и обучение персонала, занимающегося обработкой персональных данных, проведение аудита;

c) консультирование, по обращению, относительно оценки причинения ущерба защите персональных данных и мониторинг такой процедуры в соответствии со статьей 40;

d) сотрудничество с Центром;

e) предоставление Центру любой информации, связанной с обработкой персональных данных, в том числе предусмотренной статьей 41, а также консультирование его по любому другому вопросу, при необходимости;

f) выполнение других задач, предусмотренных законом.

(2) При выполнении поставленных перед ним задач ответственный за защиту персональных данных долным образом учитывает риск операций по обработке, принимая во внимание характер, сферу применения, обстоятельства и цели обработки.

(3) Ответственный за защиту персональных данных обязан письменно или по электронной почте сообщать руководству контролера или обработчика о любом нарушении принципов защиты персональных данных, в том числе о ситуациях, способных породить риски, вызвать ущемление прав субъектов данных, вызвать несоблюдение условий соответствия и безопасности обработки персональных данных.

Статья 45. Кодексы поведения

(1) В целях правильного применения настоящего закона ассоциации и другие организации, представляющие категории контролеров или обработчиков, могут разрабатывать кодексы поведения, учитывающие особенности различных секторов обработки, либо вносить изменения или дополнения в существующие кодексы для приведения их в соответствие со следующими требованиями настоящего закона:

a) справедливая и прозрачная обработка;
b) законные интересы контролеров при различных обстоятельствах;
c) сбор персональных данных;
d) псевдообезличивание персональных данных;
e) информирование общественности и субъектов данных;
f) осуществление прав субъектов данных;
g) информирование и защита ребенка, порядок получения согласия его законного представителя на обработку персональных данных ребенка;

h) ответственность контролера и принимаемые им меры для обеспечения защиты персональных данных с момента их появления, включающие соблюдение конфиденциальности и меры безопасности обработки персональных данных, в соответствии со статьями 29, 30 и 36;

i) извещение Центра о нарушении безопасности персональных данных и информирование субъектов данных о таких нарушениях;

j) передача персональных данных другим странам и международным организациям;

k) внесудебная процедура и другие процедуры разрешения споров между контролерами и субъектами данных относительно обработки, не отменяющие право субъекта данных обратиться в Центр либо обжаловать решение контролера или обработчика.

(2) Кодекс поведения должен предусматривать механизмы, которые бы позволили организации, компетентной быть экспертом по вопросам кодекса, осуществлять обязательный мониторинг его соблюдения контролерами или обработчиками, которые обязуются его применять без ущерба для задач и компетенции Центра.

(3) К кодексам поведения, утвержденным в соответствии с частью (4) и получившим общее признание в соответствии с частью (7), могут присоединиться контролеры или обработчики, как подпадающие под действие настоящего закона, так и не подпадающие под него, чтобы предоставлять надлежащие гарантии в случае трансграничной передачи персональных данных в соответствии с пунктом e) части (2) статьи 51. Такие контролеры или обработчики берут на себя посредством договора или других обязательных юридических инструментов обязательные для исполнения обязательства по предоставлению надлежащих гарантий и соблюдению смежных прав субъектов данных.

(4) Ассоциации и другие организации, представляющие категории контролеров или обработчиков, намеревающиеся издать новый кодекс поведения или внести изменения в существующий кодекс, представляют Центру проект нового или измененного кодекса для получения заключения на него относительно соблюдения настоящего закона, а в случае его утверждения Центр регистрирует и публикует кодекс поведения.

(5) При выявлении несоблюдения настоящего закона Центр в своем заключении на проект нового, измененного или дополненного кодекса указывает недостатки, подлежащие устранению ассоциацией и другой организацией, предусмотренной частью (4), в установленный им срок.

(6) В случае устранения ассоциацией и другой организацией, предусмотренной частью (4), в установленный им срок указанных в заключении недостатков Центр утверждает, регистрирует и публикует кодекс поведения.

(7) В случае если проект нового, измененного или дополненного кодекса поведения касается деятельности по обработке персональных данных в других странах, до его утверждения Центр может запросить на него заключение у надзорных органов соответствующих стран.

(8) Настоящая статья не применяется к обработке персональных данных органами публичной власти и публичными учреждениями.

Статья 46. Мониторинг утвержденных кодексов поведения

(1) На основании статьи 45 мониторинг соблюдения кодекса поведения без ущерба для задач и компетенции Центра осуществляются организацией, компетентной быть экспертом по вопросам кодекса и аккредитованной Центром.

(2) Указанная в части (1) организация получает аккредитацию для мониторинга соблюдения кодекса поведения, если:

a) надлежаще доказала Центру, что обладает независимостью и компетентна быть экспертом по вопросам кодекса поведения;

b) установила процедуры оценки способности контролеров и обработчиков применять кодекс поведения, осуществлять мониторинг его соблюдения и периодически пересматривать таковой;

c) создала прозрачные для субъектов данных и общественности процедуры и структуры, призванные рассматривать заявления о нарушениях кодекса поведения и следить за порядком применения такового контролерами или обработчиками, и надлежаще доказала Центру, что задачи и функции таких процедур и структур не приводят к конфликту интересов.

(3) Указанная организация должна предоставлять достаточные гарантии принятия надлежащих мер, без ущерба для задач и компетенции Центра, в случае нарушения контролером или обработчиком кодекса поведения, в том числе временное или постоянное исключение из списка соблюдающих соответствующий кодекс. Она информирует Центр о принятых мерах и причинах их принятия.

(4) Центр отзывает аккредитацию в случае, если организация более не соответствует условиям аккредитации или принятыми мерами нарушила настоящий закон, либо по заявлению организации.

Статья 47. Сертификация

(1) Каждый контролер или обработчик может получить сертификаты или марки, подтверждающие соблюдение настоящего закона при обработке персональных данных контролером или обработчиком.

(2) Сертификация является добровольной, доступной и прозрачной процедурой.

(3) Механизмы сертификации защиты персональных данных и установленные настоящий законом марки внедряются не только для подтверждения соблюдения настоящего закона контролерами или обработчиками, подпадающими под его действие, но и для доказательства наличия надлежащих гарантий, предоставляемых контролерами или обработчиками, не подпадающими под действие настоящего закона, в случае трансграничной передачи персональных данных в соответствии с пунктом f) части (2) статьи 50. Такие контролеры или обработчики берут на себя

посредством договора или других обязательных юридических инструментов обязательные для исполнения обязательства по предоставлению надлежащих гарантий и соблюдению смежных прав субъектов данных.

(4) Для получения сертификата контролер или обработчик предоставляет сертификационному органу или, по обстоятельствам, Центру всю информацию, необходимую для процедуры сертификации, а также доступ к соответствующей деятельности по обработке.

(5) Сертификационный орган несет ответственность за надлежащую оценку, являющуюся основанием для выдачи или отзыва сертификата или марок.

(6) Сертификационный орган доводит до сведения Центра основания выдачи или отзыва сертификата или марки.

(7) Сертификат выдается контролеру или обработчику сроком на три года с возможностью его продления на условиях выдачи и при соответствии условиям сертификации. Сертификат отзывается сертификационным органом или, по обстоятельствам, Центром, если контролер или обработчик более не соответствует условиям сертификации.

(8) Получение сертификата в соответствии с настоящей статьей не снимает ответственности контролера или обработчика за несоблюдение настоящего закона и не влияет на задачи и компетенции Центра.

(6) Порядок выдачи сертификатов или марок, а также их образцы утверждаются Центром.

Статья 48. Сертификационные органы

(1) Сертификационные органы получают аккредитацию Центра. По обращению сертификационного органа Цент предоставляет или продлевает ему аккредитацию, если он достаточно компетентен в области защиты персональных данных.

(2) Сертификационный орган получает аккредитацию, только если он:

a) надлежаще доказал Центру, что обладает независимостью и компетентен быть экспертом по вопросам, связанным с объектом сертификации;

b) обязался соблюдать утвержденные Центром критерии;

c) установил процедуры предоставления и отзыва сертификата, а также периодического пересмотра сертификации в области защиты персональных данных;

d) создал прозрачные для субъектов данных и общественности процедуры и структуры, призванные рассматривать заявления о нарушении условий

сертификации и следить за соответствием контролера или обработчика условиям сертификации;

е) надлежаще доказал Центру, что выполняемые задачи и функции не приводят к конфликту интересов.

(3) Аккредитация сертификационных органов, указанных в частях (1) и (2), осуществляется на основе утвержденных Центром критериев, опубликованных в Официальном мониторе Республики Молдова.

(4) Аккредитация предоставляется сроком на пять лет с возможностью ее продления на условиях предоставления, если сертификационный орган соответствует требованиям настоящей статьи и информация об аккредитации публикуется в Официальном мониторе Республики Молдова.

(5) Без ущерба для положений главы IX Центр отзывает аккредитацию, предоставленную в соответствии с частью (1), в случае если организация не соответствует или более не соответствует условиям аккредитации либо принятыми мерами нарушила настоящий закон.

Глава VI
ПЕРЕДАЧА ТРАНСГРАНИЧНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 49. Трансграничная передача персональных данных

(1) Трансграничная передача другому государству персональных данных, являющихся предметом обработки или собираемых с целью обработки, осуществляется на любом носителе или любыми средствами.

(2) Персональные данные, предназначенные для передачи другому государству, защищаются в соответствии с настоящим законом.

(3) Передача персональных данных другой стране или международной организации может быть осуществлена, если Центр вынес решение о том, что страна, территория или один либо несколько указанных секторов этой страны или соответствующей международной организации обеспечивают адекватный уровень защиты. Передача в этих условиях не требует специальных разрешений. Решение предусматривает механизм периодического пересмотра, по крайней мере, каждые четыре года, учитывающий все показательные достижения в этой стране или международной организации.

(4) Решение об адекватном уровне защиты выносится Центром с учетом соблюдения следующих условий:

а) правовое государство, соблюдение основных прав и свобод человека, релевантное общее и секторальное законодательство, в том числе в области общественного порядка, обороны, национальной и государственной безопасности, уголовного и гражданского права, а также доступ органов публичной власти к персональным данным, введение в действие этого законодательства, нормы защиты персональных

данных, профессиональные нормы и меры безопасности, включая нормы по последующей передаче персональных данных другой стране или международной организации, которые соблюдаются в соответствующей стране или международной организации, юриспруденция, а также наличие фактических и имеющих исковую силу прав субъектов данных и наличие инструментов, применимых для фактического административного и судебного возмещения ущерба субъектов данных, чьи личные данные передаются;

b) существование и эффективное функционирование независимого надзорного органа в соответствующей стране или в юрисдикции которого находится определенная международная организация, ответственного за обеспечение и наложение требования соблюдения норм защиты персональных данных, включая адекватные полномочия по обеспечению соблюдения применения в целях оказания поддержки и проведения консультаций с субъектами данных об осуществлении их прав и для сотрудничества с Центром; и

c) международные обязательства, к которым присоединилась соответствующая страна или международная организация, или другие обязательства, вытекающие из юридически обязательных конвенций или инструментов, а также из ее участия в многосторонних или региональных системах, особенно в области защиты персональных данных.

(5) При установлении адекватного уровня защиты Центр принимает во внимание решения Комиссии Европейского Союза, если третья страна, территория или один либо несколько указанных секторов в соответствующей третьей стране или международной организации обеспечивают адекватный уровень защиты.

(6) Если, в частности после указанного в части (3) пересмотра, имеющаяся информация раскрывает, что страна, территория или указанный сектор этой страны или международной организации более не обеспечивают адекватный уровень защиты в соответствии с частью (4) настоящей статьи, Центр при необходимости отменяет, изменяет или приостанавливает посредством другого административного акта указанное в части (3) решение без обратной силы.

(7) Принятое в соответствии с частью (4) решение не наносит ущерба передаче персональных данных стране, территории или одному или нескольким указанным секторам этой страны или соответствующей международной организации в соответствии со статьями 50–53.

(8) Центр публикует в Официальном мониторе и на официальной веб-странице список стран, территорий и указанных секторов страны и международных организаций, в случае которых было принято решение, что адекватный уровень защиты обеспечен или более не обеспечивается.

(9) Трансграничная передача персональных данных государству-члену Европейской экономической зоны не требует разрешения Центра.

(10) Контролер и обработчик обрабатывают персональные данные, управляемые в системах учета, расположенных за пределами территории Республики

Молдова, в соответствии с положениями настоящего закона и принимают необходимые меры для устранения нарушений, допущенных при обработке этих данных.

(11) Контролер и обработчик несут ответственность согласно настоящему закону в случае трансграничной передачи персональных данных.

Статья 50. Трансграничная передача на основе адекватных гарантий

(1) При отсутствии адекватного уровня защиты персональных данных в смысле части (3) статьи 49 контролер или обработчик передает персональные данные стране, которая не является членом Европейской экономической зоны, или международной организации, только если контролер или обработчик предоставил адекватные гарантии и при условии, что существуют имеющие исковую силу права и эффективный порядок обжалования для субъектов данных.

(2) В соответствии с частью (1) адекватные гарантии предоставляются без специального разрешения Центра путем:

a) юридически обязательного и подлежащего исполнению инструмента между органами публичной власти;

b) обязательных корпоративных правил согласно статье 51;

c) стандартных положений о защите персональных данных, принятых Центром;

d) стандартных положений о защите персональных данных, принятых Европейской комиссией или другими ответственными органами Европейского Союза, которые, по необходимости, одобряются Центром;

e) утвержденного в соответствии со статьей 45 кодекса поведения и сопутствующего обязательного и подлежащего исполнению обязательства контролера или обработчика другой страны применять адекватные гарантии, включая по правам соответствующих лиц;

f) механизма сертификации, утвержденного в соответствии со статьей 47, вместе с обязательными и подлежащими исполнению обязательствами контролера или обработчика страны применять соответствующие гарантии, включая по правам субъектов данных.

(3) При условии получения разрешения Центра соответствующие указанные в части (1) гарантии могут быть предусмотрены, в частности, путем:

a) договорных условий между контролером или обработчиком и контролером, обработчиком или получателем персональных данных другой страны или международной организации;

b) положениями, которые вносятся в административные соглашения между органами публичной власти, включающими имеющие исковую силу и фактические права субъектов данных.

(4) В указанных в части (3) случаях Центр учитывает существующий в Европейском Союзе механизм по обеспечению согласованности.

(5) Контролер и обработчик несут ответственность за нарушение положений настоящего закона в случае трансграничной передачи персональных данных, даже

если существуют адекватные гарантии для трансграничной передачи персональных данных.

Статья 51. Обязательные корпоративные правила

(1) Центр утверждает обязательные корпоративные правила при условии, что они:

a) обязательны и применяются к каждому заинтересованному члену группы предприятий или группы предприятий, осуществляющих совместную экономическую деятельность, включая их работников, и выполняются соответствующими членами;

b) прямо предоставляют субъектам данных имеющие исковую силу права по обработке их персональных данных;

c) соответствуют предусмотренным в части (2) требованиям.

(2) Обязательные корпоративные правила включают:

a) структуру и контактные данные группы предприятий или группы предприятий, вовлеченных в совместную экономическую деятельность, и каждого из ее членов;

b) передачу или набор передач данных, включая категории персональных данных, тип и цели обработки, тип соответствующих субъектов данных и идентификацию страны или стран, которой (которым) передаются данные;

c) их юридически обязательный характер как на внутреннем, так и на международном уровне;

d) применение общих принципов защиты данных, в частности ограничение цели, минимизация данных, ограниченные сроки хранения, качество данных, защита данных с момента их создания и на подразумеваемом этапе, правовая основа для обработки, обработка особых категорий персональных данных, безопасность данных и требования к их будущей передаче органам, на которые не распространяются обязательные корпоративные нормы;

e) права субъектов данных в отношении обработки и порядка реализации этих прав, включая право не быть предметом решений, основанных исключительно на автоматизированной обработке, в том числе создание профилей в соответствии со статьей 27, право подать заявление в Центр в соответствии со статьей 78, требовать возмещения в компетентных инстанциях Республики Молдова в соответствии со статьей 89 и, по обстоятельствам, компенсации за нарушение обязательных корпоративных норм в соответствии со статьей 90;

f) принятие контролером или обработчиком, с местоположением в Республике Молдова, ответственности за любое нарушение обязательных корпоративных норм любым соответствующим членом, не имеющим своего местоположения в Республике Молдова. Контролер или обработчик освобождается от этой ответственности, полностью или частично, только если доказывает, что соответствующий член не несет ответственности за обстоятельство, нанесшее ущерб;

g) порядок предоставления субъектам данных информации об обязательных корпоративных правилах, в частности указанных в пунктах d), e) и f), для дополнения указанной в статьях 18 и 19 информации;

h) обязанности любого лица, ответственного за защиту персональных данных, назначенного в соответствии со статьей 42, или любого другого физического или юридического лица, которому поручено проводить мониторинг соблюдения обязательных корпоративных правил в группе предприятий или группе предприятий, осуществляющих совместную экономическую деятельность, обучения персонала и управления заявлениями;

i) процедуры оформления заявлений;

j) механизмы в группе предприятий или группе предприятий, осуществляющих совместную экономическую деятельность, для обеспечения проверки соответствия обязательным корпоративным правилам. Эти механизмы включают аудиты защиты данных и методы обеспечения корректирующих действий для защиты прав субъекта данных. Результаты такой проверки должны быть сообщены указанному в пункте (h) физическому или юридическому лицу и административному совету предприятия, которое контролирует группу предприятий или группу предприятий, осуществляющих совместную экономическую деятельность, и по запросу предоставляются Центру.

k) механизм отчетности и регистрации внесенных в правила изменений и представления Центру отчетов об этих изменениях;

l) механизм сотрудничества с Центром для обеспечения соблюдения любым членом группы предприятий или группы предприятий, осуществляющих совместную экономическую деятельность, в частности, путем предоставления в распоряжение Центру результатов проверки мер, указанных в пункте j);

m) механизмы представления Центру отчетов о правовых требованиях, предъявляемых к члену группы предприятий или группы предприятий, осуществляющих совместную экономическую деятельность, в стране за пределами Европейской экономической зоны или в третьей стране, территории или в одном или нескольких указанных секторах в этой третьей стране или международной организации, обеспечивают адекватный уровень защиты, признанный Европейской комиссией, который может отрицательно сказаться на гарантиях, предоставляемых обязательными корпоративными правилами;

n) надлежащую подготовку по защите данных персонала, который имеет постоянный или периодический доступ к персональным данным;

o) другие релевантные аспекты.

(3) Центр может указать формат и процедуры, применимые к обязательным корпоративным правилам в смысле настоящей статьи, а также может принять во внимание любое решение Европейской комиссии по аналогичным вопросам.

Статья 52. Несанкционированная передача или раскрытие информации

(1) Без ущерба для положений статьей 49 и 50, передача персональных данных осуществляется на условиях, установленных специальным законом или международным договором либо соглашением, ратифицированным Республикой Молдова, в частности если передача осуществляется с целью предотвращения или расследования преступлений. Специальный закон, международный договор или соглашение должны содержать достаточно гарантий для защиты прав лиц, являющихся объектом персональных данных.

(2) Любое решение судебной инстанции и любое решение административного органа другой страны, требующее от контролера или обработчика с местоположением в Республике Молдова передавать или раскрывать персональные данные в этой стране, могут быть признаны или исполнены только если основаны на международном соглашении, таком как договор о взаимной правовой помощи, на основе установленных Центром адекватных гарантий, действующих между страной-заявителем и Республикой Молдова. Это не наносит ущерба другим основаниям для передачи в соответствии с настоящей главой.

Статья 53. Отступления в особых случаях

(1) При отсутствии решения об адекватности защиты в соответствии с частью (3) статьи 49 или адекватных гарантий в соответствии со статьей 50, включая обязательные корпоративные нормы, передача или набор передач персональных данных другой стране или международной организации осуществляется только при соблюдении одного из следующих условий:

a) субъект данных явно согласился с предложенной передачей после того, как его проинформировали о возможных рисках, которые такие передачи могут повлечь для субъекта данных в результате отсутствия решения об адекватном уровне защиты и адекватных гарантиях;

b) передача необходима для исполнения договора между субъектом данных и лицом, которое контролирует или осуществляет преддоговорные меры, принятые по запросу субъекта данных;

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

d) передача необходима по важным причинам, представляющим общественный интерес;

e) передача необходима для установления, осуществления или защиты права в судебной инстанции;

f) передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных не имеет физической или юридической возможности выразить свое согласие;

g) передача производится из реестра, который, согласно закону Республики Молдова, имеет целью информирование общественности и открыт для консультирования либо для широкой общественности, либо для лица, которое может доказать

законный интерес, но только в той степени, в которой условия, предусмотренные законом для консультирования, выполняются в конкретном случае.

(2) Если передача не может быть основана на положении статьи 49, включая положения об обязательных корпоративных правилах, и не применимо ни одно из отступлений для особых случаев, изложенных в части (1), передача другой стране или международной организации может иметь место только в том случае, если передача не повторна, относится только к ограниченному числу субъектов данных, необходима для реализации серьезных законных интересов, преследуемых контролером в отношении которого интересы или права и свободы субъекта данных не имеют преимущественной силы, и контролер оценил все обстоятельства передачи персональных данных и на основе этой оценки предоставил соответствующие гарантии в отношении защиты персональных данных. Контролер информирует Центр о передаче. Контролер предоставляет указанную в статьях 18 и 19 информацию и информирует субъекта данных о передаче и серьезных законных интересах, которые он преследует.

(3) Передача на основании пункта g) части (1) не подразумевает все персональные данные или все категории персональных данных, содержащихся в реестре. Если к реестру обращаются лица, имеющие законный интерес, передача осуществляется только по запросу соответствующих лиц или если они являются получателями.

(4) Пункты a), b) и c) части (1) и часть (3) не распространяется на деятельность, осуществляемую органами публичной власти при осуществлении ими своих публичных полномочий, если обрабатывается ограниченный объем персональных данных.

(5) Указанный в пункте d) части (1) общественный интерес признается национальным законодательством, под действие которого подпадает контролер.

(6) При отсутствии решения Центра об адекватном уровне защиты законодательство, по основаниям общественного интереса, может прямо устанавливать пределы для передачи определенных категорий персональных данных стране за пределами Европейской экономической зоны или другой третьей стране, территории или одному либо нескольким указанным секторам в соответствующей третьей стране или международной организации.

(7) Контролер или обработчик должны документально подтвердить в учетной записи, указанной в статье 35, соответствующие указанные в части (2) гарантии.

Статья 54. Международное сотрудничество в области защиты персональных данных

Что касается трансграничной обработки персональных данных, Центр принимает необходимые меры для:

a) разработки механизмов международного сотрудничества для содействия эффективному применению законодательства о защите персональных данных;

b) оказания международной взаимной помощи в применении законодательства о защите персональных данных, в том числе посредством обращения, уведомления о заявлениях, содействия в расследовании и обмене информацией, при условии соблюдения адекватных гарантий для защиты персональных данных и других основных прав и свобод;

c) взаимодействия с релевантными заинтересованными сторонами в дискуссиях и мероприятиях, направленных на продвижение международного сотрудничества в применении законодательства о защите персональных данных;

d) продвижения обмена и документирования законодательства и практики по защите персональных данных, в том числе в связи с юрисдикционными конфликтами с другими странами.

Глава VII
ОСОБЫЕ ПОЛОЖЕНИЯ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

Статья 55. Особые положения

(1) Для целей, указанных в пункте d) части (2) статьи 2, контролеры – правоохранительные органы применяют особые нормы по обработке персональных данных. К обработке персональных данных, осуществляемой правоохранительными органами вне указанных в пункте d) части (2) статьи 2 целей, применяются другие требования настоящего закона.

(2) Применение особых норм не исключает обязанность правоохранительных органов соблюдать другие требования настоящего закона при отсутствии специального регулирования.

Статья 56. Законность обработки

(1) Обработка персональных данных правоохранительными органами допускается только на основании специального закона и только в той степени, в которой такая обработка необходима для выполнения задачи правоохранительным органом для целей пункта d) части (2) статьи 2.

(2) Обработка персональных данных правоохранительными органами для особых целей, указанных в пункте d) части (2) статьи 2, применяется для целей, отличных от указанных в пункте d) части (2) статьи 2, в той степени, в какой закон требует от контролера обработки таких данных, а обработка необходима и пропорциональна этой другой цели в соответствии с законом.

(3) Нормативные акты, регулирующие сферу деятельности правоохранительных органов, устанавливают цель обработки персональных данных, категории подлежащих обработке персональных данных и другие детали, касающиеся обработки персональных данных.

(4) Правоохранительные органы создают эффективные внутренние механизмы для поощрения конфиденциального разоблачения случаев нарушения

настоящего закона в этих органах. При направлении Центру разоблачительного заявления необходимо обеспечить конфиденциальность личности заявителя.

Статья 57. Срок хранения и пересмотра

(1) Срок хранения персональных данных определяется в соответствии с целью обработки, обеспечивая периодический пересмотр необходимости их хранения.

(2) Срок хранения устанавливается особой нормой, предусмотренной специальным законом. Если закон не предусматривает такой срок, контролер установит соответствующий срок после консультирования с Центром.

(3) Контролер устанавливает процедурные механизмы для обеспечения соблюдения сроков хранения.

(4) По истечении срока хранения персональные данные удаляются, уничтожаются или преобразуются в архивный документ в соответствии с действующим законодательством.

Статья 58. Разграничение категорий субъектов данных

Контролер обязан проводить четкое разграничение, насколько это возможно, с необходимой аргументацией при обработке персональных данных различных категорий субъектов данных, таких как подозреваемые, обвиняемые, свидетели, потерпевшие, третьи лица, субъекты пробации, осужденные, задержанные, арестованные и другие лица.

Статья 59. Разграничение персональных данных на основе фактов и на основе оценок

(1) Правоохранительный орган проводит разграничение, насколько это возможно, с необходимой аргументацией, персональных данных на основе фактов и на основе оценок.

(2) Правоохранительный орган принимает все необходимые меры для удостоверения в том, что неточные, неполные или устаревшие персональные данные не передаются или не предоставляются. С этой целью каждый компетентный орган, по возможности, проверяет качество персональных данных до их передачи или предоставления. Любая передача персональных данных дополняется, по возможности, необходимой информацией, позволяющей оценить степень точности, целостности, надежности и актуальности персональных данных.

(3) Получатель немедленно уведомляется об установлении факта передачи неверных персональных данных или незаконной передачи персональных данных. В таком случае персональные данные исправляются или удаляются, либо их обработка ограничивается.

Статья 60. Обработка особых категорий персональных данных

Правоохранительный орган обрабатывает особые категории персональных данных только в случае крайней необходимости, при условии соблюдения соответствующих гарантий прав и свобод субъекта данных:

a) если это разрешено специальным законом;

b) для защиты жизни, физической неприкосновенности или здоровья субъекта данных или другого физического лица;

c) когда такая обработка относится к персональным данным, которые явно обнародованы субъектом данных.

Статья 61. Автоматизированный индивидуальный процесс принятия решений, в том числе создание профилей

(1) Решение, основанное исключительно на автоматической обработке, включая создание профилей, которое оказывает негативное правовое воздействие на субъекта данных или наносит существенный ущерб, запрещается, если это не разрешено специальным законом, применяемым правоохранительному органу и предусматривающим адекватные гарантии прав и свобод субъекта данных, по крайней мере, право на получение содействия контролера.

(2) Указанные в части (1) решения не основываются на особых категориях персональных данных, за исключением персональных данных, связанных с осуждением по уголовному делу, если существуют адекватные меры по защите прав и свобод субъекта данных и его законных интересов при консультировании с Центром.

(3) Запрещается создавать профили, которые приводят к дискриминации субъектов данных на основе особых категорий персональных данных.

Статья 62. Сообщение и способы реализации прав субъектов данных

(1) Правоохранительные органы бесплатно передают субъекту данных информацию относительно обработки в соответствии со статьей 63 и в связи со статьями 61, 64–67 и 70 в краткой, понятной и легко доступной форме, используя ясный и простой язык. Информация передается любыми подходящими способами, в том числе электронными средствами. Как правило, контролер передает информацию в том же формате, в каком было получено заявление.

(2) Статьи 18–26 не распространяются на обработку персональных данных правоохранительными органами.

(3) Контролер реализует права субъекта данных согласно статьям 61 и 64–67.

(4) Контролер, без необоснованной задержки, письменно информирует соответствующее лицо о способе удовлетворения его зявления.

(5) Если зявления субъекта данных являются явно необоснованными или чрезмерными, повторными, мотивированный контролер может в соответствующих случаях:

a) взимать разумную плату, принимая во внимание административные расходы на предоставление информации или сообщение либо принятие запрошенных мер;

b) отказать в удовлетворении заявления.

(6) Если у контролера имеются обоснованные сомнения относительно личности субъекта данных, подающего заявление, указанное в статьях 64 или 66, он может запросить предоставление дополнительной информации, необходимой для подтверждения личности субъекта данных.

Статья 63. Информация, которую необходимо предоставить в распоряжение субъекту данных

(1) Контролер предоставляет в распоряжение субъекту данных следующую информацию:

a) личность и контактные данные контролера;

b) контактные данные лица, ответственного за защиту персональных данных, по обстоятельствам;

c) цели, для которых обрабатываются персональные данные;

d) право подать заявление в Центр и контактные данные надзорного органа;

e) наличие права требовать от контролера доступа и исправления или удаления персональных данных и ограничения обработки персональных данных, относящихся к субъекту данных;

f) другая релевантная информация.

(2) В дополнение к информации, указанной в части (1), контролер в некоторых случаях предоставляет субъекту данных следующую дополнительную информацию, позволяющую реализовать его права:

a) правовую основу обработки;

b) период, в течение которого будут храниться персональные данные, или, если это невозможно, критерии, используемые для определения этого периода;

c) по обстоятельствам, категории получателей персональных данных, в том числе в других странах или международных организациях;

d) при необходимости, дополнительную информацию, особенно если персональные данные собираются без ведома субъекта данных.

(3) Если это предусмотрено специальным законодательством, контролер может отложить, ограничить или исключить предоставление информации субъекту данных в соответствии с частью (2), по мере необходимости и соразмерности в демократическом обществе, при соблюдении основных прав и законных интересов физического лица, с тем чтобы:

a) избежать воспрепятствования проведению расследований правоохранительными органами и/или процессуальным действиям, проводимым в соответствии с законом;

b) не наносить ущерба предотвращению, выявлению, расследованию или судебному преследованию за уголовные преступления или исполнению уголовных наказаний;

c) обеспечить охрану общественного порядка;

d) обеспечить защиту национальной безопасности;

e) обеспечить защиту государственной безопасности;

f) обеспечить защиту прав и свобод других физических лиц.

Статья 64. Право доступа субъекта данных

Субъект данных имеет право получить от контролера подтверждение того, обрабатываются ли относящиеся к нему персональные данные или нет, и если это так, он имеет доступ к соответствующим данным и следующей информации:

a) цели и правовая основа обработки;

b) категории соответствующих персональных данных;

c) получатели или категории получателей, которым были переданы персональные данные, в частности получатели из других государств или международных организаций;

d) когда это применимо, срок хранения персональных данных, или, если это невозможно, критерии, использованные для определения этого срока;

e) наличие права запрашивать исправление или удаление контролером персональных данных или ограничение обработки персональных данных, относящихся к субъекту данных;

f) право подать заявление и контактные данные Центра;

g) передача обрабатываемых персональных данных и любой доступной информации об их происхождении.

Статья 65. Ограничение права доступа

(1) Контролер может полностью или частично ограничить осуществление права доступа субъекта данных, если это оправдано и представляет собой необходимую и соразмерную меру, при условии, что специальный закон предусматривает такую процедуру, с тем, чтобы:

a) избежать воспрепятствования проведению расследований правоохранительными органами и/или процессуальным действиям, проводимым в соответствии с законом;

b) не наносить ущерба предотвращению, выявлению, расследованию или судебному преследованию за уголовные преступления или исполнению уголовных наказаний;

c) обеспечить охрану общественного порядка;

d) обеспечить защиту национальной и государственной безопасности;

e) обеспечить защиту прав и свобод других лиц.

(2) В случае полного или частичного ограничения осуществления права доступа субъекта данных, контролер письменно информирует субъекта данных без неоправданной задержки об отказе или ограничении доступа и причинах отказа или ограничения. Такая информация может быть пропущена, если предоставление противоречит одной из целей части (1). Такое ограничение на предоставление информации субъекту данных ограничено во времени в соответствии с правовыми положениями.

(3) Контролер должен сообщить субъекту данных о возможности подачи заявления в Центр или о праве на подачу иска.

(4) Контролер должен документально подтвердить фактические и юридические основания, на которых основано решение, и занести это в Автоматизированный реестр применения исключений. Эта информация предоставляется в распоряжение Центру.

Статья 66. Право на исправление или удаление персональных данных и ограничение обработки

(1) Субъект данных имеет право без неоправданной задержки потребовать от контролера исправления касающихся его неточных персональных данных. Если это возможно и с учетом целей обработки, субъект данных имеет право дополнить неполные персональные данные, в том числе путем предоставления дополнительной декларации.

(2) Субъект данных имеет право запросить удаление персональных данных и контролер должен удовлетворить такой запрос, если обработка нарушает положения статьей 4, 56 или 60, или если персональные данные должны быть удалены для выполнения правового обязательства, возложенного на контролера в соответствии со статьей 57.

(3) Вместо удаления контролер ограничивает обработку, когда:

a) точность персональных данных оспаривается субъектом данных, а их точность или неточность не могут быть точно установлены;

b) персональные данные должны храниться в качестве доказательства.

Если обработка ограничена в соответствии с пунктом a), контролер информирует субъекта данных перед снятием ограничений на обработку.

(4) Контролер письменно информирует субъекта данных о любом отказе исправить или удалить персональные данные или ограничить обработку, а также о причинах отказа. Контролер может ограничить, частично или, если это оправдано, полностью, предоставление такой информации, если это прямо предусмотрено специальным законодательством. Такое ограничение допустимо в той мере, в какой оно является необходимой и соразмерной мерой в демократическом обществе, при соблюдении основных прав и законных интересов соответствующего физического лица, с тем, чтобы:

a) избежать воспрепятствования проведению расследований правоохранительными органами и/или процессуальным действиям, проводимым в соответствии с законом;

b) не наносить ущерба предотвращению, выявлению, расследованию или судебному преследованию за уголовные преступления или исполнению уголовных наказаний;

c) обеспечить охрану общественного порядка;

d) обеспечить защиту национальной и государственной безопасности;

e) обеспечить защиту прав и свобод других лиц.

(5) Если основание ограничений части (4) более не применимо, контролер принимает меры, запрашиваемые субъектом данных, за исключением случая, когда это не будет наносить ущерба указанным в части (4) целям.

(6) Контролер сообщает компетентному органу, передавшему неточные персональные данные, об их исправлении.

(7) Если персональные данные были исправлены или удалены, либо обработка была ограничена в соответствии с частями (1), (2) и (3), контролер уведомляет получателей, а получатели исправляют или удаляют персональные данные или ограничивают обработку персональных данных, находящихся под их ответственностью.

(8) Контролер сообщает субъекту данных о возможности подать заявление в Центр или обратиться в судебную инстанцию, если субъект данных считает необоснованным отказ исправить или удалить персональные данные.

Статья 67. Уведомление Центра правоохранительным органом о нарушении безопасности персональных данных

(1) Правоохранительный орган уведомляет Центр о нарушении безопасности персональных данных в соответствии со статьей 37.

(2) Если нарушение безопасности персональных данных касается персональных данных, переданных контролером из другого государства или такому контролеру, указанная в части (3) статьи 37 информация доводится до сведения контролера соответствующего государства без необоснованной задержки.

Статья 68. Сообщение субъекту данных правоохранительным органом о нарушении безопасности персональных данных

(1) Правоохранительный орган сообщает субъекту данных о нарушении безопасности персональных данных в соответствии со статьей 38.

(2) В отступление от статьи 38, сообщение субъекту данных о нарушении безопасности персональных данных может быть задержано, ограничено или, если это оправдано, пропущено, если это необходимо и соразмерно, с тем, чтобы:

a) избежать воспрепятствования проведению расследований правоохранительными органами и/или процессуальным действиям, проводимым в соответствии с законом;

b) не наносить ущерба предотвращению, выявлению, расследованию или судебному преследованию за уголовные преступления или исполнению уголовных наказаний;

c) обеспечить охрану общественного порядка;

d) обеспечить защиту национальной и государственной безопасности;

e) обеспечить защиту прав и свобод других лиц.

(3) Если основания для ограничения в соответствии с частью (2) более не применимы, контролер информирует субъекта данных о нарушении безопасности персональных данных, за исключением ситуаций, когда это нанесло бы ущерб цели, указанной в части (2) для другого случая.

Статья 69. Учет деятельности по обработке

(1) Правоохранительный орган обязан вести учет операций по обработке персональных данных в автоматизированной, смешанной или ручной системе: сбор, консультирование, изменение, раскрытие, распространение, печать, передача, слияние и удаление.

(2) Учет деятельности по обработке должен позволять определение цели и правовой основы, даты и времени, определение лица, получившего доступ или раскрывшего данные, а также личность получателей персональных данных.

(3) Учет деятельности по обработке может быть использован только для проверки законности обработки данных, внутренних проверок, обеспечения целостности и безопасности персональных данных и в ходе уголовного преследования.

(4) Правоохранительный орган, действующий в качестве контролера или обработчика, предоставляет в распоряжение Центра, по запросу, учет деятельности по обработке, с указанием в том числе цели получения доступа к данным, даты и времени этих операций, личности лица, получившего доступ к информации, а также их получателя. Центр может запросить дополнительную информацию об учете деятельности по обработке и, таким образом, правоохранительный орган предоставляет Центру необходимую дополнительную информацию.

Статья 70. Обязательство правоохранительного органа в соотношении с полномочиями Центра

(1) Если заявление было подано правоохранительным органом Центру в соответствии со статьей 75 о деятельности по обработке, в том числе, не ограничиваясь предусмотренными статьями 65 и 66 исключениями, контролер, обработчик или третья сторона должны удовлетворить требование Центра предоставить запрошенную информацию.

(2) Предоставляя Центру информацию в соответствии с частью (1) правоохранительный орган предоставляет информацию об обрабатываемых персональных данных, цели, правовом основании и причинно-следственной связи между субъектом данных, его статусом и выполненными операциями, включая личность лица, получившего доступ к информации, и получателя.

(3) На основании мотивированного запроса Центра правоохранительный орган предоставляют дополнительную информацию и документы для подтверждения предоставленной информации.

(4) По завершении расследования Центр информирует субъекта данных, а также правоохранительный орган о принятом по делу решении.

(5) В случаях, когда на основании обоснованной информации правоохранительного органа информирование субъекта данных, предусмотренное в части (4), может подорвать цель обработки, Центр информирует субъекта данных о том, что он провел расследование и все необходимые проверки. Такое исключение по предоставлению информации субъекту данных ограничено во времени на срок в 30 дней

с возможностью обоснованного продления правоохранительным органом до шести месяцев. Если устанавливается, что обработка персональных данных необоснованна и не имеет причинно-следственной связи с заявленной целью, Центр требует от правоохранительного органа информировать субъекта данных о проведенной обработке.

(6) Правоохранительный орган и/или субъект данных может оспорить решение Центра подачей административного искового заявления. Дело рассматривается в закрытом заседании, в отсутствие субъекта данных, с участием Центра и правоохранительного органа.

Статья 71. Применение исключений и их регистрация

(1) Для целей пункта d) части (2) статьи 2 правоохранительный орган применяет исключения по предоставлению информации субъекту данных, касающейся обработки персональных данных в любой информационной системе.

(2) Правоохранительный орган в случае применения исключений, указанных в части (1), обязан вести их учет путем записи в Автоматизированном реестре применения исключений, находящимся в ведении Центра, созданным и регулируемым Постановлением Парламента.

(3) Указанные в части (1) исключения применяются только если специальный закон определяет случаи их применения, предельный срок и периодичность их продления, способ проверки и информирования субъекта данных.

(4) Неприменение исключений, пропущение срока для продления или превышения исключений, устраняет возможность применения исключений на тех же правовых основаниях.

(5) После исчерпания ситуации, которая оправдывает применение частей (1)–(4), правоохранительные органы обязаны информировать в письменной или электронной форме, в соответствии с требованиями электронного документа и электронной подписи, субъектов данных в порядке, установленном статьями 63 и 64.

(6) В случаях, предусмотренных частями (4)–(5), при осуществлении право доступа к персональным данным, контролеры вправе информировать субъекта данных и не несут ответственности за такое информирование.

(7) Учет деятельности по обработке персональных данных, связанной с применением исключения, должен храниться не менее 10 лет с момента применения.

Статья 72. Трансграничная передача персональных данных между правоохранительными органами

(1) Любая передача персональных данных правоохранительными органами, которые обрабатываются или предназначены для обработки в контексте передачи за пределы Республики Молдова в Европейскую экономическую зону или в международную организацию либо в другую страну, территорию либо один или несколько указанных секторов в этой стране либо международной организации, которая обеспечивает адекватный уровень защиты, признанный Европейской комиссией, в том

числе для последующей передачи другой стране или международной организации, допускается только при следующих условиях:

a) передача необходима для целей, предусмотренных пунктом d) части (2) статьи 2;

b) персональные данные передаются контролеру в стране или международной организации, который является компетентным органом для целей, указанных пунктом d) части (2) статьи 2;

c) передача разрешена только после того, как Центр предоставил разрешение в соответствии с частью (3) статьи 49 или передача разрешена в соответствии с частью (1) статьи 52.

(2) Условия части (1) статьи 53 не применяется, если передача осуществляется в соответствии с настоящей статьей.

Статья 73. Отступления в особых ситуациях

(1) В исключительных случаях, если не выполняются условия части (1) статьи 72, передача или категория передачи персональных данных другой стране или международной организации может осуществляться только в том случае, если передача необходима:

a) для защиты жизни, физической неприкосновенности или здоровья субъекта данных или другого лица;

b) для защиты законных интересов субъекта данных, если это предусмотрено специальным законом;

c) для предотвращения непосредственной и серьезной угрозы общественному порядку Республики Молдова или другой страны;

d) в отдельных случаях для целей, предусмотренных пунктом d) части (2) статьи 2;

e) в индивидуальном случае установления, осуществления или защиты законных требований, связанных с целями, предусмотренными пунктом d) части (2) статьи 2.

(2) Персональные данные не передаются, если передающий их правоохранительный орган устанавливает, что права и основные свободы соответствующего субъекта данных превосходят общественный интерес при передаче, предусмотренный пунктами d) и e) части (1).

(3) Если передача основана на части (1), она документируется, а документация предоставляется в распоряжение Центру по запросу, включая дату и время передачи, информацию о компетентном органе – получателе, основания и причины передачи, переданные персональные данные.

Статья 74. Передача персональных данных другим получателям за пределами Республики Молдова

(1) Если получатель не является назначенным пунктом b) части (1) статьи 72 органом и без ущерба для любого международного соглашения, заключенного и

ратифицированного Республикой Молдова с другими государствами в области судебно-уголовного и полицейского сотрудничества, содержащего гарантии по охране прав субъекта данных, правоохранительные органы в отдельных и особых случаях передают персональные данные непосредственно получателям с местоположением за пределами Республики Молдова только при соблюдении других положений настоящего закона и выполнении следующих условий:

a) передача является строго необходимой для выполнения задачи правоохранительного органа, осуществляющего передачу, и предусмотрен специальным законом для целей, указанных в пункте d) части (2) статьи 2;

b) правоохранительный орган, передающий персональные данные, устанавливает, что ни одно из соответствующих основных прав и свобод субъекта данных не превышает общественный интерес, требующий этой передачи;

c) правоохранительный орган, передающий персональные данные, считает, что передача компетентному органу другой страны для целей, указанных в пункте d) части (2) статьи 2, является неэффективной или неадекватной, так как, в частности, передача не может быть осуществлена своевременно;

d) компетентный орган другой страны для целей, указанных в пункте d) части (2) статьи 2, информируется без необоснованной задержки, за исключением случая, когда это является неэффективным или неадекватным;

e) правоохранительный орган, передающий персональные данные, информирует получателя о конкретной цели или целях, для которых персональные данные должны быть обработаны только им, при условии, что такая обработка необходима.

(2) Правоохранительный орган информирует Центр об осуществленных передачах в соответствии с настоящей статьей до осуществления передачи или в течение двух дней с момента передачи, в противном случае Центр констатирует нарушение принципов защиты персональных данных и положений этой нормы.

(3) Если передача основана на части (1), она документируется. В документации должны быть указаны дата и время передачи, информация о компетентном органе – получателе, обоснования и причины передачи, переданные персональные данные и связь между переданными персональными данными и предусмотренными в пункте a) части (1) условиями.

Глава VIII
УСЛОВИЯ ПОДАЧИ ЗАЯВЛЕНИЙ, ПРОЦЕДУРА РАССМОТРЕНИЯ И ПРОВЕДЕНИЯ РАССЛЕДОВАНИЯ, ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ, ИСПОЛНЕНИЕ РЕШЕНИЙ, КОНФИДЕНЦИАЛЬНОСТЬ, ДОСТУП И ХРАНЕНИЕ СЛЕДСТВЕННЫХ МАТЕРИАЛОВ

Статья 75. Право на подачу заявления

(1) Если субъект данных считает, что обработка относящихся к нему персональных данных нарушает закон, он имеет право подать заявление в Центр в течение трех месяцев с момента обнаружения предполагаемого нарушения.

(2) Если заявление относится к реализации прав субъектов данных, изложенных в главе III, это заявление будет первоначально представлено контролерам данных в соответствии с законом. Если субъект данных не получает ответа от контролера в установленные главой III сроки или когда ответ или предпринимаемые контролером действия считаются неадекватными либо не разрешают запрос, субъект данных, в течение 30 дней с момента, когда он получил ответ или должен был получить ответ, имеет право подать заявление в Центр.

(3) Заявления, поданные в нарушении процедуры и сроков давности, предусмотренных в соответствии с частями (1) и (2), не рассматриваются, и Центр информирует об этом субъекта данных в течение 10 рабочих дней.

(4) Для субъекта данных, который по обоснованным и уважительным причинам пропустил срок давности, срок может быть восстановлен в соответствии с положениями Гражданского процессуального кодекса.

Статья 76. Требования для подачи заявления

(1) Заявление может быть подано непосредственно в Центр, почтовым отправлением или электронной почтой, в соответствии с требованиями электронной подписи и электронного документа, лично субъектом данных или его представителем, используя утвержденный Центром печатный или электронный бланк. При подаче заявления представителем представляются должным образом возложенные субъектом данных на представителя полномочия в отношениях с Центром и объем персональных данных, которые представитель имеет право обрабатывать.

(2) Форма и содержание поданного в Центр заявления должны включать:

a) фамилию, имя, адрес субъекта данных и, по необходимости, фамилию, имя представителя, номер телефона, адрес электронной почты;

b) подробное описание фактических и правовых обстоятельств дела;

c) фамилию, имя или наименование, адрес, номер телефона контролера и/или обработчика;

d) другую необходимую информацию, по обстоятельствам, в том числе если предмет заявления рассматривается или был рассмотрен судебной инстанцией, органом публичной власти в процессе посредничества или арбитража между теми же сторонами;

e) дату оформления заявления;

f) собственноручную или электронную подпись субъекта данных или его представителя.

(3) Во всех случаях к заявлениям прилагаются соответствующие доказательства, подтверждающие предполагаемые нарушения. Представленные копии доказательств и других документов, в свою очередь, должны быть надлежащим образом заверены записью «копия соответствует оригиналу» и проставлением даты и собственноручной или электронной подписи для представленных в электронном формате заявлений. К заявлению прилагаются только информация и документы,

которые имеют отношение к делу и не являются чрезмерными по отношению в заявленному деянию.

(4) Центр может идентифицировать и выслушать субъекта данных и/или его представителя.

(5) Рассмотрение заявления, не отвечающего требованиям положений частей (1)–(4), приостанавливается. В этом случае Центр в течение 10 рабочих дней информирует субъекта данных о необходимости устранения допущенных несоответствий. Если субъект данных не предоставляет запрашиваемую Центром информацию в течение 30 рабочих дней с момента получения извещения, заявление считается недопустимым и остается нерассмотренным, о чем информируется субъект данных. В течение трех месяцев после получения ответа Центра субъект данных имеет право подать в Центр другое заявление, отвечающее всем требованиям закона.

(6) Если поданное в Центр заявление с тем же предметом и с теми же сторонами рассматривается судебной инстанцией или органом публичной власти в процессе посредничества или арбитража, Центр отклоняет заявление или приостанавливает его рассмотрение до завершения рассмотрения и/или, по обстоятельствам, до принятия окончательного решения, информируя заявителя о причинах, которые привели к отклонению заявления или приостановлению его рассмотрения в течение 10 рабочих дней с моммента установления данного факта.

(7) Если заявление приостановлено, заявитель обязан проинформировать Центр об устранении указанных в части (6) обстоятельств. В случае отклонения заявления, если срок его подачи истек в результате рассмотрения в судебной инстанции, органе публичной власти, в рамках процесса посредничества или арбитража, субъект данных может повторно подать завление в Центр в течение трех месяцев со дня получения решения по делу.

(8) В отступление от части (6), если могут быть ущемлены права других субъектов данных или затронуты меры безопасности, либо если Центр считает предмет заявления показательным, он может распорядиться о проведении необходимых расследований.

(9) Повторные заявления, не содержащие новых аргументов или информации или являюшиеся явно необоснованными, не рассматриваются, о чем информируется субъект данных.

(10) Заявления, содержащие нецензурную или оскорбительную лексику, угрозы национальной безопасности, общественному порядку, жизни и здоровью должностного лица и членов его семьи, не рассматриваются.

Статья 77. Компетенция рассмотрения

(1) Центр обладает компетенцией расследовать и разрешать случаи нарушения нормативных положений в области защиты персональных данных с выездом на место или без него, в следующих ситуациях:

а) при подаче заявления субъекта данных или законного представителя о несоблюдении условий обработки персональных данных;

b) при реагировании по собственной инициативе или когда Центр был проинформирован о массовом, системном или серьезном нарушении принципов защиты персональных данных, социально значимых случаях или в случаях надзора и предотвращения.

(2) Если предполагаемое нарушение обработки персональных данных выходит за рамки применения настоящего закона, Центр по запросу субъекта данных оказывает содействие в исполнении Конвенции о защите физических лиц при автоматизированной обработке персональных данных.

(3) Если заявление касается обработки трансграничных данных или касается иностранного элемента, Центр применяет, по обстоятельствам, механизмы сотрудничества, установленные в соответствии со статьей 54 настоящего закона и, по обстоятельствам, частями 7–10 статьи 6 Закона о Национальном центре по защите персональных данных. Это положение применяется только в том случае, если обычное местожительство или место работы субъекта данных либо местоположение контролера или обработчика, являющегося предметом заявления, находится в Республике Молдова.

Статья 78. Расследование

(1) Расследование – это деятельность, осуществляемая инспекторами по защите данных, руководителями специализированных подразделений Центра с целью проверки соблюдения требований настоящего закона и других нормативных актов, касающихся области защиты персональных данных: контролерами, ассоциированными контролерами, обработчиками, получателями, а также органами, которые не считаются получателями, третьими лицами, независимо от вида собственности и сферы деятельности, организационно-правовой формы организации. Расследование сложных и крупномасштабных дел может проводиться группой инспекторов по защите с указанием лица, рукодящего расследованием.

(2) В ходе расследования Центр принимает решения как по соответствию обработки данных, так и по средствам, которыми осуществлялась обработка персональных данных.

(3) Центр запрашивает у субъектов данных и/или субъектов права, указанных в части (1), документы, информацию и, по обстоятельствам, средства, необходимые для подтверждения или опровержения предполагаемых нарушений законодательства о защите персональных данных, указывает правовую основу и цель запроса информации, устанавливает срок предоставления информации, указывает взыскания, предусмотренные законом за непредоставление информации или предоставление неточной, неполной или вводящей в заблуждение информации.

(4) Для сбора доказательств, необходимых для подтверждения или опровержения нарушения законодательства о защите персональных данных, Центр может принять решение в рамках того же расследования или другого расследования о выезде на место.

(5) В случае расследования с выездом на место, директор Центра, заместитель директора или другое ответственное лицо, назначаемое с этой целью приказом директора Центра, выносит решение, в котором указываются цель и предмет расследования, лица, которым поручено проводить расследование, срок, а также права и обязанности сторон, вовлеченных в расследование.

(6) Решение о проведении расследования с выездом на место доводится до сведения под подписью лица, подследственного субъекта или законного представителя. В случае отказа в получении и подписании решения составляется акт в присутствии свидетеля, а в случае видео- и аудиозаписей, фиксирующих тот факт, свидетель не обязан присутствовать.

(7) Инспекторы по защите данных исполняют свои права при проведении расследований на месте в пределах полномочий, предусмотренных в решении в соответствии с положениями настоящего закона, Закона о Национальном центре по защите персональных данных, а также других внутренних нормативных актов.

(8) В ходе расследования инспекторы по защите данных имеют следующие права:

a) иметь доступ и проверять системы учета персональных данных, программное и аппаратное обеспечение, персональные данные и любые документы, связанные с предметом и целью расследования, независимо от оборудования и/или носителя, на котором хранятся данные;

b) входить в помещения, зоны или транспортные средства, находящиеся в собственности или пользовании субъектов права, указанных в части (1);

c) изымать средства, с помощью которых осуществляется обработка персональных данных, собирать, получать копии или выписки в любой форме из систем учета и документы, содержащие персональные данные;

d) опечатывать помещения и средства, где и с помощью которых обрабатываются персональные данные, системы учета и документы, относящиеся к предмету и цели расследования, на срок и в объеме, необходимом для проведения расследования. Запечатывание и распечатывание может быть осуществлено только Центром, с занесением данного факта в протокол, подписанный заинтересованными лицами;

e) заслушивать и запрашивать у лица, подследственного субъекта или законного представителя либо у других лиц, которые могут предоставить Центру информацию, необходимую для разрешения заявления, касающегося обработки персональных данных в ходе расследования, и регистрировать с предварительным уведомлением подследственного лица, в том числе с помощью аудио, видео или других средств, их ответы;

f) запрашивать и получать информацию, касающуюся предмета и цели расследования, хранящуюся на компьютерах или других электронных устройствах, в форме, которая разрешает их изъятие и транспортировку, видимую и разборчивую;

g) проводить расследования безопасности в любых системах учета, содержащих персональные данные или с помощью которых можно обрабатывать персональные данные, включая технические меры для имитации схемы доступа к системам

учета персональных данных, с целью проверки их уровня защиты и предотвращения возможных случаев незаконного или случайного доступа к таким системам, выявления уязвимостей в механизмах их защиты, при необходимости, в сотрудничестве с другими органами;

h) обращаться за поддержкой к компетентным подразделениям правоохранительных органов, которые обязаны оказывать необходимую помощь работникам Центра. В проведение расследования могут быть задействованы также, по обстоятельствам, эксперты в определенных областях, уполномоченных Центром;

i) другие права, предусмотренные настоящим законом, Законом о Национальном центре по защите персональных данных и другими нормативными актами.

(9) В ходе расследования инспекторы по защите данных и эксперты, уполномоченные Центром в этом отношении, обязаны:

a) информировать подследственное лицо о его правах и обязанностях;

b) проводить расследование в соответствии с полномочиями, предусмотренными настоящим законом, с учетом его предмета и цели.

(10) В ходе расследования проверяемое лицо имеет следующие права:

a) получать информацию и копию решения о проведении расследования на месте;

b) представлять доказательства в ходе расследования;

c) давать объяснения, зарегистрированные в любой форме, касающиеся предмета и цели расследования;

d) идентифицировать данные и информацию, составляющую секретную и другую конфиденциальную информацию, предоставленную в ходе расследования, с внесением соответствующих записей;

e) получать перечень средств, систем учета и документов, изъятых в ходе расследования, подписанный инспектором по защите данных;

f) получать помощь адвокатов, других уполномоченных по закону представителей. Если подследственное лицо запрашивает присутствие адвоката, расследование приостанавливается до прихода адвоката, но не более чем на 2 часа.

(11) Все органы/субъекты и физические лица обязаны подчиняться расследованию, проводимому Центром, в том числе путем обеспечения условий для надлежащего проведения расследования.

(12) Следственные действия проводятся в любое время, релевантное для сбора информации, необходимой для разрешения дела.

(13) Расследование на месте проводится в рабочие часы подследственного органа/субъекта. В нерабочее время расследование может продолжаться только с согласия представителя подследственного субъекта.

(14) Результаты расследования с выездом на место фиксируются в акте, составляемом в двух экземплярах, страницы пронумеровываются, на каждой странице инспекторы по защите данных проставляют свои подписи. Акт доводится до сведения подследственного лица под подпись в течение 10 рабочих дней после завершения расследования с выездом на место. Подследственное лицо обязано подтвердить

подписью, в том числе через ответственное лицо или другого своего представителя, получение копии акта, даже в случае несогласия с находящимися в нем выводами. Если представитель подследственного лица отказывается получить и подтвердить подписью получение копии акта, в нем указывается отказ в получении копии акта и/или подтверждении подписью получения копии документа, подписанного инспекторами по защите данных, которые провели расследование, а акт будет отправлен подследственному лицу заказным письмом с подтверждением получения.

(15) Условия, сроки и порядок хранения средств, копий или выписок, систем учета и документов, изъятых в соответствии с настоящей статьей, устанавливаются Центром в соответствии с нормативными актами.

(16) При наличии обоснованного подозрения, что носители информации о деятельности и предмете расследования, которые могут иметь рашеющее значение для доказательства нарушения законодательства о защите персональных данных, хранятся в других помещениях, зонах и транспортных средствах, включая жилье членов руководящих органов или субъектов, указанных в части (1), иных, чем указанных в решении о проведении расследования с выездом на место, расследование может быть продлено и проведено в отношении этого имущества при письменном согласии соответствующих лиц или их законного представителя. Описанная ситуация относится к любому типу собственности, пользования, владения, приобретательной давности, таким как, но не ограничиваясь этим, аренда, имущественный наем, лизинг.

(17) Доступ представителей Центра в жилье, здание или помещения, зоны и транспортные средства, к оборудованию для обработки, программам и приложениям, а также документам, записям, касающимся обработки персональных данных, принадлежащих, находящимся во владении или в пользовании подследственного лица, при отсутствии письменного согласия, допускается только на основании судебного ордера, выданного в соответствии с положениями настоящей статьи и представленного подследственному лицу или его представителю.

(18) Во избежание воспрепятствования расследованию в отношении сокрытия, изменения, удаления, уничтожения систем учета персональных данных, оборудования для обработки, программ и приложений, а также любого документа или записи, относящихся к обработке персональных данных, Центр может запросить непосредственно у судебной инстанции выдачу судебного ордера. Запрос судебного ордера рассматривается с участием Центра в течение не более 48 часов с даты его регистрации. Определение мотивируется и сообщается Центру немедленно, но не позднее, чем через 48 часов после оглашения.

(19) Судебный ордер может быть выдан, если:

а) существует обоснованное подозрение, что в жилье, здании или в помещениях, транспортных средствах находятся системы учета персональных данных, средства обработки, программы и приложения, а также хранятся документы или записи, относящиеся к обработке персональных данных или другие документы, которые могли быть сокрыты, устранены, удалены, изменены или уничтожены; либо

b) существует обоснованное подозрение, что в жилье, здании или в помещениях, зонах и транспортных средствах, подлежащих следствию, находятся системы учета персональных данных, средства обработки, программы и приложения, а также любые документы или записи, относящиеся к обработке персональных данных или другие документы, представление которых было запрошено Центром в соответствии с настоящим законом, но которые не были представлены в установленный срок.

(20) Судебный ордер действует в течение 30 дней со дня выдачи и может быть продлен еще на 30 дней. Постановление/решение об отказе в выдаче судебного ордера может быть обжаловано в кассационном порядке в течение 10 дней с момента информирования.

(21) При запросе судебного ордера судебная инстанция обязана проверить, не являются ли расследование и принимаемые меры произвольными или чрезмерными с учетом предмета расследования.

(22) При необходимости судебная инстанция может запросить дополнительно у Центра подробные объяснения, в частности об основаниях, обуславливающих подозрения Центра о нарушении законодательства о защите персональных данных, о серьезности предполагаемого нарушения, важности искомых доказательств, характере вовлечения контролера или обработчика и разумной вероятности того, что системы учета персональных данных, средства обработки, программы и приложения, а также документы или записи, относящиеся к обработке персональных данных, в связи с предметом расследования, хранятся или находятся в месте, для которого запрашивается ордер. При рассмотрении запроса на судебный ордер судебная инстанция соответственно применяет положения настоящей статьи.

(23) При проведении расследования инспектор по защите данных руководствуется правовыми положениями, принимает решение о направлении расследования и выполняет следственные действия, за исключением случаев, когда необходимо одобрить, санкционировать, подтвердить или проверить его действия со стороны руководителей, по обстоятельствам, руководителей Центра или судебной инстанции. Любое вмешательство в деятельность инспектора по охране запрещено.

(24) Расследование проводится в разумные сроки в зависимости от серьезности предполагаемого нарушения и других критериев, которые бы определяли его продолжительность, но не более двух лет.

(25) Общий контроль за соблюдением разумного срока проведения расследования возлагается на заместителя директора и судебную инстанцию.

(26) Если по истечении двухлетнего срока у Центра не будет достаточно доказательств, чтобы с уверенностью оценить наличие или отсутствие нарушения, расследование может быть приостановлено максимум на один год, информируя подавшего заявление субъекта данных. Возобновление расследования может иметь место в установленный срок, при условии появления новых доказательств, значительных и убедительных для разрешения дела.

(27) Если по истечении срока приостановления, предусмотренного в части (26), не возникает значимых обстоятельств для возобновления расследования, Центр

выносит решение об отсутствии нарушения с соответствующим информированием подавшего заявление субъекта данных.

(28) Центр информирует субъекта данных по его запросу о ходе и результатах расследования сколько раз это необходимо или каждые три месяца.

(29) Центр разрабатывает и утверждает Положение о проведении расследования в соответствии с положениями настоящего закона и Закона о Национальном центре по защите персональных данных.

Статья 79. Доказательства

(1) Центр может использовать любые средства доказательства и информацию, которые служат для установления наличия или отсутствия нарушения.

(2) Для целей применения этого закона Центр допускает как прямые, так и косвенные доказательства:

a) прямые доказательства – это показания свидетелей или других лиц, вещественные доказательства, записи, аудио- и/или видеозаписи, заключения экспертов и любые другие доказательства, прямо свидетельствующие о наличии или отсутствии нарушения закона;

b) косвенные доказательства – это доказательства, которые прямо не доказывают наличие или отсутствие нарушения закона, но могут привести к некоторым логическим выводам с другими прямыми или косвенными доказательствами того, что нарушение закона существует или существовало в определенный момент или не существует и не существовало в определенный момент.

(3) В случае отсутствия или недостаточности доказательств, подтверждающих наличие нарушения, Центр по решению констатирует отсутствие нарушения.

Статья 80. Конфиденциальность расследования

(1) Лица, которые в силу своих прав и обязанностей, возложенных на них на основании настоящего закона, ознакомились с результатами расследования, в том числе другие лица, которым стала известна такая информация, обязаны обеспечить их конфиденциальность, подлежа предусмотренным законодательством взысканиям.

(2) Персональные данные, которые были обработаны в ходе расследований Центра, являются конфиденциальными и не могут быть изъяты, перехвачены, получены и/или использованы любым другим способом, кроме случаев, когда субъект данных дал свое явное согласие на такую обработку или на условиях авторизованной передачи Центром и не могут быть использованы, если это может ухудшить положение субъекта данных.

(3) Инспектор по защите данных, субъект данных или другие лица, которые в силу своих прав и обязанностей, возложенных на них на основании настоящего закона, ознакомились или им стала известна информация, полученная в ходе расследования, не могут быть заслушаны или допрошены другими органами или организациями относительно сущности информации, полученной в ходе расследования, за

исключением судебной инстанции. Информация, документы и следственные материалы могут быть использованы только с разрешения Центра.

(4) Деятельность, документы, информация и материалы Центра подлежат только судебному контролю при условии обеспечения конфиденциальности и безопасности таких данных.

(5) Следственные материалы не могут быть обнародованы, если они могут создавать существенные риски для права на личную, семейную и частную жизнь субъекта данных. Центр может обнародовать общую информацию из следственных материалов, такую как предмет расследования, данные о контролерах, обработчиках, третьих сторонах, получателях и субъектах, не являющихся получателями, относительно хода и/или результатах расследования, в целях информирования общества.

Статья 81. Доступ к следственным материалам и их хранение

(1) Субъект данных, подавший заявление, или другие лица, имеющие отношение к расследованию, могут запросить в письменной или электронной форме, в соответствии с требованиями электронной подписи и электронного документа, доступ к следственным материалам. Выдача копий следственных материалов предоставляется бесплатно один раз, за последующие запросы взимается плата, размер которой определяется Центром в соответствии с разрабатываемым и утверждаемым положением. Взимаемая плата переводится в государственный бюджет.

(2) До завершения расследования доступ к собранным материалам может быть предоставлен только в том случае, если инспектор по защите данных сочтет это возможным, получив разрешение руководителя, соблюдая презумпцию невиновности, не ущемляя интересы других лиц, не препятствуя и/или не противодействуя расследованию либо процессуальным действиям, проводимым в соответствии с законом.

(3) Если следственные материалы содержат информацию, относящуюся к государственной тайне, коммерческой тайне, банковской тайне или делам особого производства, конфиденциальную информацию правонарушительного или уголовного производства или другую официальную информацию ограниченного доступа, Центр ограничивает доступ к ней.

(4) При рассмотрении заявления разглашение информации о личной, семейной и частной жизни субъектов данных не допускается без письменного согласия или в электронном виде в соответствии с требованиями электронной подписи и электронного документа и в соотвтетствии с законом.

(5) Право доступа не включает доступа к внутренним документам или переписке Центра.

(6) Доступ к следственным материалам предоставляется при условии, что информация используется только при проводимом Центром расследовании или связанном с ним судебном разбирательстве.

(7) Центр не обязан переводить запрашиваемые материалы и информацию.

(8) По завершении расследования материалы, не рассмотренные судебной инстанцией, хранятся в архиве Центра в течение 10 лет.

(9) Рассмотренные судебной инстанцией следственные материалы хранятся в архиве судебной инстанции, которая рассмотрела дело в первой инстанции.

(10) Следственные материалы, содержащие государственную тайну, хранятся в архиве Центра или судебной инстанции, по обстоятельствам.

(11) Доступ к следственным материалам, хранящимся в соответствии с условиями, предусмотренными в настоящей статье, разрешается руководством Центра или другим лицом, уполномоченным с этой целью директором Центра, по обстоятельствам, председателем судебной инстанции, в котором они хранятся, в соответствии с положениями этой главы.

Статья 82. Вынесение и сообщение решений

(1) По завершении расследования ответственный за ресследование инспектор по защите данных или, по обстоятельствам, инспекторы по защите, руководитель группы представляет обоснованное заключение по результатам проведенного расследования с подробным описанием фактических и правовых обстоятельств, и предлагает, по обстоятельствам, меры по устранению и исправлению несоответствий и денежное взыскание, которое налагается при принятии решения.

(2) В зависимости от результата и фактов, выявленных в ходе расследования, Центр своим решением констатирует неприменимость закона или отсутствие нарушения, либо может предписать, отдельно или в совокупности, следующее:

a) исправление, приостановку, блокировку, запрет, прекращение обработки и/или намерения обрабатывать персональные данные, включая, по обстоятельствам, по отношению к средствам, которые используются или подлежат использованию для обработки, не соблюдающие положения Закона о защите персональных данных, или которые могут создавать существенные риски для права на личную, семейную и частную жизнь человека при сборе, регистрации, организации, хранении, сохранении, восстановлении, адаптации или изменении, извлечении, консультировании, использовании, раскрытии, распространении или другое;

b) уничтожение или удаление персональных данных, с или без удаления или дезактивации технического программного и аппаратного обеспечения, средств в области информационных технологий, задействованых для нарушения законадательства о защите персональных данных;

c) восстановление прав субъектов данных.

(3) Решения подписываются директором Центра, заместителем директора или другим ответственным лицом, назначенным в этом отношении приказом директора Центра.

(4) Решение сообщается соответствующему лицу в течение 10 рабочих дней со дня его вынесения посредством заказного письма либо в электронной форме в соответствии с требованиями электронной подписи и электронного документа или любыми средствами, подтверждающими его получение.

(5) Если сообщение о решении не может быть выполнено на предусмотренных в части (4) условиях на основании того, что соответствующее лицо не было найдено или по другим причинам, относящимся к данному лицу или лицам, Центр может опубликовать объявление в национальной или местной газете, указывающее о принятии решения, которое можно получить в Центре. В случае публикации данного объявления, по истечении пяти дней, соответствующее лицо будет считаться информированным.

Статья 83. Исполнение решений Центра

(1) Решения вступают в силу и подлежат исполнению в течение указанного в них срока с обязательством письменно информировать Центр о принятых мерах. Центр может установить срок исполнения решения до 6 месяцев.

(2) В случае неисполнения в установленный срок соответствующими лицами решения Центра о мерах, установленных в пунктах a), b), c) части (2) статьи 82, судебный исполнитель осуществляет его принудительное исполнение согласно положениям настоящего закона и Исполнительного кодекса.

(3) Во всех случаях судебная инстанция выдает заключения по всем средствам, изъятым Центром в результате расследования, включая их передачу органу, уполномоченному продавать их, без участия Центра.

Статья 84. Вызов повесткой в суд

(1) Повестка должна быть индивидуальной и включать:

a) фамилию, имя или наименование вызываемого лица с указанием предмета дела;

b) адрес вызываемого лица, который должен включать: населенный пункт, улицу, номер дома, квартиры, а также любые другие данные, необходимые для указания адреса вызываемого лица;

c) время, день, месяц и год, место явки вызываемого лица с указанием правовых последствий в случае неявки;

d) указание о том, что вызываемое лицо имеет право на помощь адвоката, с которым он может явиться в установленный срок.

(2) Повестка в суд направляется по месту его жительства или юридическому адресу, а если это неизвестно, по месту его работы.

(3) В случае изменения адреса вызываемого лица повестка в суд направляется по его новому адресу только в том случае, если он проинформировал Центр об изменении или если Центр установил на основании полученных данных, что произошла смена адреса.

(4) Соответствующее лицо должно не позднее, чем в течение трех дней, уведомить Центр об изменении места жительства.

(5) Повестка в суд повторно направляется по месту нахождения или месту жительства законного представителя, если соответствующее лицо не явилось после законно выполненного первого вызова в суд.

(6) Повестка вручается лично вызываемому лицу, которое подписывает подтверждение о получении.

(7) Центр может запросить для вызова в суд поддержку органа полиции. Если вызываемое лицо отказывается от получения повестки, отказ в получении заносится в протокол об отказе в получении повестки.

(8) Если вызов в суд осуществлен в соответствии с частями (2) и (5), администрации соответствующих учреждений обязаны незамедлительно вручить повестку вызываемому лицу, под его подпись, заверяя его подпись в подтверждении о получении или указывая причину, по которой его подпись не была получена. Подтверждение о получении направляется Центру.

(9) Если вызываемое лицо отсутствует дома, повестка вручается супругу/супруге, родственнику или любому лицу, проживающему с ним, или которое обычно получает его корреспонденцию. Вызов не может быть вручен несовершеннолетнему в возрасте до 14 лет или психически больному.

(10) Вызов в суд также может быть осуществлен по телефону или телеграфу, телефаксу, электронной почте или любой другой системе электронных сообщений, если Центр располагает техническими средствами, необходимыми для доказательства того, что повестка была получена или вызов в суд осуществлен.

Статья 85. Рассмотрение других обращений

Обращения, не соответствующие условиям, изложенным в настоящем законе, рассматриваются в соответствии с другими правовыми положениями, без вынесения решений.

Глава IX
ОБЖАЛОВАНИЕ, ОТВЕТСТВЕННОСТЬ И ВЗЫСКАНИЯ

Статья 86. Право на эффективный судебный порядок обжалования административных актов, изданных Центром

(1) Решения, изданные Центром и сообщенные в соответствии с частью (4) и (5) статьи 82, могут быть оспорены/обжалованы у руководителя лица, подписавшего решение, или непосредственно в административном суде. Решения, подписанные директором, прямо оспариваются в судебной инстанции.

(2) Протест может быть подан в течение 30 дней с момента доведения решения до сведения. Руководитель рассматривает протест в течение 30 рабочих дней. Решение, принятое руководителем в результате рассмотрения протеста, может быть оспорено/обжаловано в судебной инстанции в течение 30 дней с момента доведения решения до сведения.

(3) Если субъект данных не был проинформирован в соответствии с частью (28) статьи 78 или заявление не было рассмотрено в соответствии с положениями настоящего закона, он может оспорить действия или бездействие Центра в соответствии с частью (1).

(4) В отступление от правовых положений до окончательного урегулирования дела исполнение решений Центра не может быть приостановлено, за исключением случаев применения денежных взысканий, предписания уничтожения или удаления персональных данных или если ущерб может превысить преследуемый частный или общественный интерес.

(5) Судебное определение о приостановлении или отказе в приостановлении решения Центра может быть обжаловано в кассационном порядке в течение 15 дней. Кассационная жалоба против определения рассматривается в течение кратчайшего периода, не превышающего 10 дней с даты подачи кассационной жалобы.

Статья 87. Право на эффективный судебный порядок обжалования действий контролера или обработчика

(1) Любой субъект данных имеет право подать заявление непосредственно в судебную инстанцию, если предполагаемое нарушение имело место в Республике Молдова, без ущерба для прав и полномочий Центра.

(2) Если заявление касается осуществления прав субъектов данных, предусмотренных в главе III, оно первоначально подается контролеру данных или обработчику в соответствии с положениями закона. Если субъект данных не получает ответ от контролера или обработчика в установленный главой III срок, или если ответ или предпринятые ими действия считаются неадекватными или не разрешают запрос, субъект данных подает заявление непосредственно в судебную инстанцию в установленном законодательством порядке, без ущерба для прав и полномочий Центра.

Статья 88. Право на возмещение ущерба и ответственность

(1) Любое лицо, понесшее материальный или моральный ущерб в результате нарушения настоящего закона, имеет право на получение возмещения за понесенный ущерб от контролера или обработчика.

(2) Любой контролер, вовлеченный в операции по обработке, несет ответственность за ущерб, нанесенный операциями по обработке, нарушившими положения настоящего закона и других нормативных актов в области защиты персональных данных. Обработчик несет ответственность за ущерб, нанесенный обработкой, только в том случае, если он действовал за пределами или в противоречии законным инструкциям контролера либо не выполнил свои обязанности, предусмотренные настоящим законом и другими нормативными актами в области защиты персональных данных.

(3) Контролер или обработчик освобождается от ответственности согласно части (2), если он доказывает, что не несет никакой ответственности за обстоятельство, повлекшее ущерб.

(4) Если несколько контролеров или обработчиков, или контролер и обработчик вовлечены в ту же операцию обработки и несут ответственность, согласно частям (2) и (3), за любой ущерб, вызванный обработкой, каждый контролер или

обработчик несет ответственность за весь ущерб, чтобы обеспечить фактическое возмещение ущерба соответствующего лица.

(5) Если контролер или обработчик полностью возместил ущерб в соответствии с частью (4), то он имеет право требовать от других контролеров или обработчиков, вовлеченных в ту же операцию обработки, возврата части возмещенного ущерба, соответствующей их части ответственности за ущерб, согласно изложенным в части (2) условиям.

(6) Заявление о возмещении ущерба подается в судебную инстанцию, если установлен контролер или обработчик. Субъект данных может подать заявление в судебную инстанцию, в территориальной юрисдикции которой находится его местожительство. Если оператор или обработчик является органом публичной власти, действующим при осуществлении своих публичных полномочий, исковое заявление подается в судебную инстанцию, в территориальной юрисдикции которой находится орган публичной власти.

Статья 89. Административная ответственность за нарушение положений настоящего закона

(1) В случае нарушения положений настоящего закона по решению выносится предупреждение или налагается денежное взыскание. Вынесение предупреждения или наложение денежного взыскания не исключает применения мер по устранению и исправлению несоответствий.

(2) Административная ответственность юридического лица публичного или частного права не исключает, по обстоятельствам, привлечения к ответственности за совершенное деяние должностного или руководящего лица.

(3) В случае наложения денежного взыскания его размер определяется отдельно в каждом конкретном случае с учетом следующих аспектов:

a) характер, серьезность и длительность нарушения, принимая во внимание характер, область применения или цель соответствующей обработки, а также число затронутых лиц и степень нанесенного им ущерба;

b) было ли нарушение совершено преднамеренно или по небрежности;

c) любое действие, предпринятое контролером или обработчиком для уменьшения ущерба, нанесенного субъекту данных;

d) степень ответственности контролера или обработчика, с учетом технических и организационных мер, принятых ими в соответствии со статьями 30 и 42;

e) предыдущие показательные нарушения, совершенные контролером или обработчиком;

f) степень сотрудничества с Центром для устранения нарушения и смягчения возможных негативных последствий нарушения;

g) категории персональных данных, затронутых нарушением;

h) способ, которым нарушение было доведено до сведения Центра, в частности, если и в какой степени контролер или обработчик уведомил о нарушении;

i) соблюдение ранее предписанных мер по устранению и исправлению несоответствий в отношении контролера или обработчика и того же объекта;

j) оборот или годовой доход контролера (физического лица);

k) соблюдение утвержденных кодексов поведения в соответствии со статьей 45 или утвержденных механизмов сертификации в соответствии со статьей 47;

l) любой другой усугубляющий или смягчающий фактор, применимый к обстоятельствам дела, такой как полученные финансовые выгоды или убытки, которые прямо или косвенно были предотвращены вследствие нарушения.

(4) Если контролер или обработчик преднамеренно или по небрежности нарушает по одной и той же операции обработки или по сопутствующим операциям обработки несколько положений настоящего закона, общий размер денежного взыскания не может превышать сумму, предусмотренную для самого серьезного нарушения.

(5) За нарушение следующих положений, в соответствии с частью (3), налагаются денежные взыскания в размере до одного миллиона леев или, в случае предприятия, до 1% общего годового оборота за предыдущий финансовый год с учетом наибольшего размера:

a) обязанности контролера и обработчика в соответствии с частью (4) статьи 8, статьями 10, 30–44, 47–48;

b) обязанности органа по сертификации согласно статьям 47 и 48;

c) обязанности органа по мониторингу согласно статье 46.

(6) За нарушение положений, изложенных в части (5), контролером или обработчиком – юридическим лицом публичного права, будет вынесено предупреждение с применением, по обстоятельствам, мер по устранению и исправлению несоответствий. Если будет установлено, что контролер или обработчик – юридическое лицо публичного права, не полностью выполнил меры по устранению и исправлению несоответствий, будет наложено денежное взыскание в размере до 100 тыс. леев.

(7) За нарушение следующих положений, в соответствии с частью (3), налагаются денежные взыскания в размере до 2 млн. леев или, в случае предприятия, до 2% общего годового оборота предыдущего финансового года с учетом наибольшего размера:

a) основные принципы обработки, в том числе условия согласия, в соответствии со статьями 4, 5, 8 и 9;

b) права соотвтетствующих субъектов согласно статьям 17–27;

c) передача личных данных получателю из другой страны или международной организации в соответствии со статьями 49–54;

d) любые обязательства на основании национального законодательства, принятые в соответствии со статьями 12, 14, 15, 16 и 92;

e) несоблюдение приказа, инструкции, положения или любого другого административного акта или временного или окончательного ограничения обработки или приостановки потоков данных, изданных Центром, или непредоставление доступа.

(8) За неисполнение решения Центра, за меры, установленные в пунктах a), b) и c) части (2) статьи 82, налагаются в соответствии с частью (3), денежные взыскания в размере до 2 млн. леев или, в случае предприятия, до 2% общего годового оборота предыдущего финансового года с учетом наибольшего размера.

(9) За нарушение положений, изложенных в частях (7) и (8), контролером или обработчиком – юридическим лицом публичного права, выносится предупреждение с применением , по обстоятельствам, мер по устранению и исправлению несоответствий. Если устанавливается, что контролер или обработчик – юридическое лицо публичного права не полностью выполнил меры по устранению и исправлению несоответствий, налагается денежное взыскание в размере до 100 тыс. леев.

(10) В случае несоблюдения предписанных мер или в случае отказа предоставить всю информацию и документы, запрашиваемые в ходе следственной процедуры, Центр может по своему решению предписать наложение денежного взыскания в размере до 50 тыс. леев за каждый день задержки, рассчитанный с установленного решением дня. Расчет будет произведен с учетом непрерывности нарушения.

(11) В случае незначительного нарушения, если стороны примирились или заявление было отозвано субъектом данных, а размер налагаемого денежного взыскания стал бы непропорциональным бременем для контролера – физического лица, вместо денежного взыскания выносится предупреждение.

(12) В случае денежного взыскания в отношении правоохранительных органов принимаются во внимание применимые положения главы VII в соотношении с упомянутыми выше нормами.

(13) Срок привлечения к административной ответственности за нарушение положений настоящего закона составляет пять лет с момента совершения нарушения. Непрерывное нарушение считается исчерпанным в момент прекращения действия или бездействия нарушения либо возникновения обстоятельств, предотвращающих это действие. Продленное нарушение считается исчерпанным в момент совершения последнего действия или бездействия нарушения.

(14) Лицо не может быть привлечено к административной ответственности за нарушение положений настоящего закона и расследование прекращается в следующих случаях:

a) деяние нарушения отсутствует;

b) срок привлечения к административной ответственности за нарушение положений настоящего закона истек;

c) для того же деяния и в отношении того же лица существует окончательное решение/постановление;

d) злоумышленик не установлен.

Статья 90. Обработка и публичный доступ к официальным документам

Обработка персональных данных и доступ к таким данным из официальных документов осуществляются при условии соразмерности и баланса между правом на

личную, семейную и частную жизнь в связи с обработкой персональных данных и правом на доступ к информации и свободой слова.

Статья 91. Особые положения об административной ответственности

(1) Суммы денежных взысканий, налагаемых Центром, зачисляются в государственный бюджет.

(2) Решение о наложении денежных взысканий включает предельный срок для уплаты. Предельный срок для уплаты не может превышать 30 дней со дня сообщения о решении по наложению денежного взыскания.

(3) Решения о наложении денежного взыскания, по обстоятельствам, публикуются на официальной веб-странице Центра сохраняя конфиденциальность или анонимность персональных данных, по обстоятельствам.

(4) Если лица, указанные в решении о наложении денежного взыскания, уплатили его в течение пяти дней со дня уведомления, они имеют право на 25-ти процентное освобождение от суммы рассчитанного взыскания.

(5) Лица, указанные в решении о наложении денежного взыскания, информируют Центр о мерах, принятых для исполнения решения, в том числе о мерах по устранению и исправлению несоответствий и/или уплате денежного взыскания в установленный срок, с представлением доказательств в этом отношении.

Статья 92. Обработка государственного идентификационного номера

(1) Обработка государственного идентификационного номера, в том числе посредством сбора или разглашения документов, его содержащих, осуществляется в ситуациях, предусмотренных частью (1) статьи 5.

(2) Обработка государственного идентификационного номера, в том числе посредством сбора или разглашения документов, его содержащих, для цели, предусмотренной пунктом f) части (1) статьи 5, соответственно для реализации законных интересов, преследуемых контролером или третьей стороной, осуществляется путем установления следующих гарантий:

a) принятие адекватных технических и организационных мер, в частности для минимизации данных, а также для обеспечения безопасности и конфиденциальности обработки персональных данных в соответствии со статьей 36;

b) назначение ответственного по защите данных в соответствии со статьей 42;

c) соблюдение кодекса поведения, утвержденного в соответствии со статьей 45;

d) установление сроков хранения в зависимости от характера данных и цели обработки, в соответствии со статьей 13;

e) периодический инструктаж по своим обязанностям лиц, которые под непосредственным руководством контролера или обработчика, обрабатывают персональные данные.

Статья 93. Обработка персональных данных в контексте трудовых отношений

Если используются системы мониторинга с помощью электронных средств связи и/или с помощью видео-, аудионаблюдения на рабочем месте, обработка персональных данных работников для реализации законных интересов работадателя, допускаются только при соблюдении следующих условий:

a) преследуемые работодателем законные интересы относятся к деятельности особого значения, основательно обоснованной, и превалирут над интересами или правами и свободами соответствующих лиц;

b) работодатель в обязательном порядке, в полной и ясной мере предварительно проинформировал работников;

c) работодатель проконсультировался с профсоюзом или, по обстоятельствам, с представителями работников до введения системы мониторинга;

d) соблюдается разумная зона интимности;

e) другие формы и способы, менее интрузивные/навязчивые для достижения преследуемой работодателем цели ранее доказали свою неэффективность; и

f) продолжительность хранения персональных данных соразмерна с целью обработки, но не более чем 30 дней, за исключением специально регулируемых законом ситуаций или в основательно обоснованных случаях.

Статья 94. Обработка генетических и биометрических данных

Обработка генетических и биометрических данных в целях обеспечения автоматизированного процесса принятия решений или создания профилей запрещена, за исключением обработки, выполняемой органами публичной власти или под их контролем в пределах полномочий, возложенных на них законом, и на условиях, установленных специальными законами, регулирующими эти сферы и обеспечивающими адекватные гарантии для соответсвующих лиц.

Глава XI
ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

Статья 95. Заключительные положения

(1) Настоящий закон вступает в силу с 2 мая 2019 года.

(2) После вступления в силу настоящего закона признать утратившим силу Закон о защите персональных данных № 133/2011.

Статья 96. Переходные положения

(1) С момента вступления в силу настоящего закона, из окончательной суммы денежного взыскания, налагаемого Центром в соответствии с положениями настоящего закона, соответствующие лица обязаны уплатить:

a) в первый год – 30 процентов суммы налагаемого денежного взыскания;

b) во второй год – 50 процентов суммы налагаемого денежного взыскания;

c) в третий год – 100 процентов суммы налагаемого денежного взыскания.

(2) Положения части (1) не влияют на критерии индивидуализации.

(3) Жалобы и дела, по которым процедура рассмотрения Центром не завершена до вступления в силу настоящего закона, рассматриваются в соответствии с процедурой и материалами, предусмотренными настоящим законом. Если настоящий закон предусматривает более серьезное наказание, за нарушение, совершенное до вступления в силу настоящего закона, будут наложены взыскания в соответствии с нормативными актами, действующими на момент его совершения. Если, согласно настоящему закону, деяние более не считается нарушением, взыскания не налагаются, даже если оно совершено до дня вступления в силу.

(4) Споры, которые на день вступления в силу настоящего закона находятся на рассмотрении, подлежат разрешению в соответствии с законодательством, действующим на день возникновения спора.

(5) Решения, разрешающие или не разрешающие операции по обработке персональных данных и о регистрации или об отказе в регистрации в качестве контролера, с вступлением в силу настоящего закона не имеют правового действия. Контролерам необходимо пересмотреть способ обработки данных и привести свои акты в соответствие с настоящим законом.

(6) В течение девяти месяцев со дня опубликования настоящего закона, Правительству:

a) разработать и представить Парламенту предложения по приведению действующего законодательства в соответствие с настоящим законом;

b) привести свои нормативные акты в соответствие с настоящим законом;

c) обеспечить приведение нормативных актов центральных органов публичной власти с настоящим законом.

(7) В течение девяти месяцев со дня опубликования настоящего закона Центру:

a) разработать и принять нормативные акты, необходимые для выполнения настоящего закона;

b) привести свои нормативные акты в соответствие с положениями настоящего закона.

ПРЕДСЕДАТЕЛЬ ПАРЛАМЕНТА