

Неофициальный перевод с эстонского языка. Юридическую силу имеет только текст закона на эстонском языке. Перевод выполнен по сводному тексту, вступившему в силу 01.10.2026 (RT I, 30.06.2026, 52), в шапке которого дата окончания действия редакции не указана (действующая редакция).

Издатель: Рийгикогу

Вид акта: закон

Вид текста: сводный текст

Дата вступления редакции в силу: 01.10.2026

Окончание действия редакции: не указано (действующая редакция)

Опубликовано: RT I, 30.06.2026, 52

Закон о защите персональных данных¹

Принят 12.12.2018

RT I, 04.01.2019, 11

Вступил в силу 15.01.2019

Изменён следующими актами:

22.02.2023 — RT I, 11.03.2023, 1 — вступило в силу 01.11.2023

11.12.2024 — RT I, 30.12.2024, 1 — вступило в силу 01.01.2025 (на основании части 12 § 105.19 Закона о Правительстве Республики слово «Justiitsministeerium» заменено словами «Justiits- ja Digiministeerium» в соответствующем падеже)

18.12.2024 — RT I, 31.12.2024, 5 — вступило в силу 01.01.2025

17.06.2025 — RT I, 12.07.2025, 1 — вступило в силу 01.10.2025

18.02.2026 — RT I, 06.03.2026, 2 — вступило в силу 16.03.2026

02.06.2026 — RT I, 30.06.2026, 1 — вступило в силу 01.10.2026

1 глава

ОБЩИЕ ПОЛОЖЕНИЯ

§ 1. Сфера регулирования закона

(1) Настоящий закон регулирует:

1) защиту физических лиц при обработке персональных данных в той мере, в какой он уточняет и дополняет положения Регламента (ЕС) 2016/679 Европейского парламента и Совета о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент по защите данных) (ELT L 119, 04.05.2016, стр. 1–88);

2) защиту физических лиц при обработке персональных данных правоохранительными учреждениями при предотвращении, выявлении правонарушений и производстве по ним, а также при исполнении наказаний.

(2) Настоящий закон устанавливает:

1) нормы для применения Регламента (ЕС) 2016/679 Европейского парламента и Совета;

2) нормы для имплементации Директивы (ЕС) 2016/680 Европейского парламента и Совета о защите физических лиц при обработке персональных данных компетентными учреждениями в целях предотвращения, расследования, выявления правонарушений и привлечения за них к ответственности или исполнения уголовных наказаний и о свободном перемещении таких данных, которой отменяется Рамочное решение Совета 2008/977/ЮВД (ELT L 119, 04.05.2016, стр. 89–131);

- 3) порядок осуществления государственного и административного надзора за соблюдением требований к обработке персональных данных;
- 4) ответственность за нарушение требований к обработке персональных данных.

§ 2. Особенности применения настоящего закона и Регламента (ЕС) 2016/679 Европейского парламента и Совета

Настоящий закон и Регламент (ЕС) 2016/679 Европейского парламента и Совета применяются:

- 1) к производству по делам о правонарушениях и судебному производству с особенностями, установленными процессуальными кодексами;
- 2) к конституционным институтам в той мере, в какой это не затрагивает исполнение ими конституционных задач и не урегулировано в специальных законах, касающихся их.

§ 2¹. Компетенция Инспекции по защите данных в производстве по коллективному представительному иску

Инспекция по защите данных является компетентным подразделением в значении §§ 60² и 66² Закона о защите прав потребителей и может от имени Эстонской Республики для защиты коллективных интересов субъектов данных обращаться с внутригосударственным коллективным представительным иском в уездный суд, а также с трансграничным коллективным представительным иском в суд другого государства — члена Европейского союза.

[RT I, 31.12.2024, 5 — вступило в силу 01.01.2025]

§ 3. Применение Закона об административной процедуре

К административной процедуре, предусмотренной настоящим законом, применяются положения Закона об административной процедуре с учётом особенностей настоящего закона.

2 глава ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ 4. Обработка персональных данных в журналистских целях

Персональные данные могут обрабатываться без согласия субъекта данных в журналистских целях, в частности обнародоваться в средствах массовой информации, если для этого имеется общественный интерес и это соответствует принципам журналистской этики. Обнародование персональных данных не должно чрезмерно ущемлять права субъекта данных.

§ 5. Обработка персональных данных для целей академического, художественного и литературного самовыражения

Персональные данные могут обрабатываться без согласия субъекта данных в целях академического, художественного и литературного самовыражения, в частности обнародоваться, если это не ущемляет чрезмерно права субъекта данных.

§ 6. Обработка персональных данных для нужд научного или исторического исследования и государственной статистики

(1) Персональные данные могут обрабатываться без согласия субъекта данных для нужд научного или исторического исследования или государственной статистики, в частности в псевдонимизированном виде или в виде, обеспечивающем равноценный уровень защиты данных. Перед передачей персональных данных для обработки в целях научного или

исторического исследования или государственной статистики персональные данные заменяются данными в псевдонимизированном виде или в виде, обеспечивающем равноценный уровень защиты данных.

(2) Депсевдонимизация или иной способ, которым данные, не позволяющие идентифицировать лицо, вновь делаются позволяющими идентификацию, допускается только для нужд дополнительных научных или исторических исследований или государственной статистики. Лицо, обрабатывающее персональные данные, поимённо определяет лицо, имеющее доступ к данным, позволяющим провести депсевдонимизацию.

(3) Обработка относящихся к субъекту данных без его согласия для нужд научного или исторического исследования или государственной статистики в виде, позволяющем идентифицировать субъекта данных, допускается лишь при выполнении следующих условий:

- 1) после удаления данных, позволяющих идентификацию, цели обработки данных более недостижимы или их достижение было бы неоправданно затруднительным;
- 2) по оценке лица, проводящего научное или историческое исследование или государственную статистику, для этого существует преобладающий общественный интерес;
- 3) на основании обрабатываемых персональных данных не изменяется объём обязанностей субъекта данных и иным образом чрезмерно не ущемляются его права.

(4) Если научное или историческое исследование основывается на персональных данных особых категорий, комитет по этике соответствующей области, образованный законом или на его основании, проверяет перед проведением исследования выполнение условий, установленных настоящим параграфом. Если в области науки комитет по этике отсутствует, соблюдение требований проверяет Инспекция по защите данных. В отношении персональных данных, хранящихся в Национальном архиве, права комитета по этике принадлежат Национальному архиву.

[RT I, 12.07.2025, 1 — вступило в силу 01.10.2025]

(5) В значении настоящего закона научным исследованием считаются также анализы и исследования исполнительной государственной власти, проводимые в целях формирования политики. Для их подготовки исполнительная государственная власть вправе делать запросы в базу данных другого ответственного или уполномоченного обработчика и обрабатывать полученные персональные данные. Инспекция по защите данных проверяет перед началом обработки указанных персональных данных выполнение условий, установленных настоящим параграфом, за исключением случая, когда цели исследования, проводимого для формирования политики, и объём обработки персональных данных вытекают из правового акта.

(5¹) Если законом не установлено иное, обязанность проверки комитетом по этике, установленная частью 4 настоящего параграфа, не применяется к анализам и исследованиям исполнительной государственной власти, указанным в части 5, проводимым в целях формирования политики. Инспекция по защите данных может консультироваться с комитетом по этике, указанным в § 26 Закона об организации научно-исследовательской и опытно-конструкторской деятельности и инноваций, если, по оценке Инспекции по защите данных, исследование или анализ, проводимые для формирования политики, нуждаются в этической оценке.

[RT I, 12.07.2025, 1 — вступило в силу 01.10.2025]

(5²) Если Инспекция по защите данных консультируется с комитетом по этике в соответствии с частью 5¹ настоящего параграфа, плату, запрашиваемую комитетом по этике за консультацию, оплачивает заказчик анализов и исследований исполнительной государственной власти.

(6) Если персональные данные обрабатываются в целях научного или исторического исследования или государственной статистики, ответственный или уполномоченный обработчик может ограничить права субъекта данных, установленные в статьях 15, 16, 18 и 21 Регламента (ЕС) 2016/679 Европейского парламента и Совета, в той мере, в какой осуществление этих прав, вероятно, сделает невозможным достижение цели научного или исторического исследования или государственной статистики или существенно затруднит его.

§ 7. Обработка персональных данных в целях архивирования в общественных интересах

(1) Если персональные данные обрабатываются в целях архивирования в общественных интересах, ответственный или уполномоченный обработчик может ограничить права субъекта данных, установленные в статьях 15, 16 и 18–21 Регламента (ЕС) 2016/679 Европейского парламента и Совета, в той мере, в какой осуществление этих прав, вероятно, сделает невозможным достижение цели архивирования в общественных интересах или существенно затруднит его.

(2) Права субъекта данных, указанные в части 1 настоящего параграфа, могут быть ограничены для того, чтобы не создавать угрозу состоянию, подлинности, достоверности, целостности и пригодности для использования архивных документов.

3 глава

ИНЫЕ СЛУЧАИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ 8. Обработка персональных данных ребёнка при предоставлении услуг информационного общества

(1) Если применяется пункт «а» части 1 статьи 6 Регламента (ЕС) 2016/679 Европейского парламента и Совета в связи с предоставлением услуг информационного общества непосредственно ребёнку, обработка персональных данных ребёнка допускается только в том случае, если ребёнку исполнилось не менее 13 лет.

(2) Если ребёнок младше 13 лет, обработка персональных данных допускается лишь в том случае и в том объёме, на которые дал согласие законный представитель ребёнка.

§ 9. Обработка персональных данных после смерти субъекта данных

(1) Согласие субъекта данных действует при жизни субъекта данных и 10 лет после его смерти, если субъект данных не решил иначе. Если субъект данных умер несовершеннолетним, его согласие действует 20 лет после смерти субъекта данных.

(2) После смерти субъекта данных обработка его персональных данных допускается с согласия наследника субъекта данных, за исключением случаев, когда:

- 1) со дня смерти субъекта данных прошло 10 лет;
- 2) со дня смерти умершего несовершеннолетним субъекта данных прошло 20 лет;
- 3) персональные данные обрабатываются на ином правовом основании.

(3) При наличии нескольких наследников обработка персональных данных субъекта данных допускается с согласия любого из них.

(4) Согласие, указанное в части 1 настоящего параграфа, не требуется, если обрабатываемыми персональными данными являются исключительно имя, пол, дата рождения и смерти субъекта данных, факт смерти, а также время и место захоронения.

§ 10. Обработка персональных данных в связи с нарушением долговых отношений

(1) Передача персональных данных, связанных с нарушением долговых отношений, третьему лицу и обработка переданных данных третьим лицом допускаются в целях оценки кредитоспособности субъекта данных или в иной аналогичной цели и только в том случае, если ответственный или уполномоченный обработчик проверил правильность передаваемых данных и правовое основание для передачи персональных данных и зарегистрировал передачу данных.

(2) В цели, указанной в части 1 настоящего параграфа, собирать данные и передавать их третьему лицу не допускается, если:

- 1) речь идёт об обработке персональных данных особых категорий в значении части 1 статьи 9 Регламента (ЕС) 2016/679 Европейского парламента и Совета;
- 2) речь идёт о данных о совершении правонарушения или о том, что лицо стало его жертвой, до публичного судебного заседания либо до вынесения решения по делу о правонарушении или прекращения производства по делу;
- 3) это чрезмерно ущемило бы права или свободы субъекта данных;
- 4) с момента нарушения договора прошло менее 30 дней;
- 5) с момента прекращения нарушения обязательства прошло более пяти лет.

§ 11. Обработка персональных данных в общественном месте

Если законом не установлено иное, при записи звука или изображения в общественном месте в целях обнародования согласие субъекта данных заменяется его уведомлением в такой форме, которая позволяет ему понять факт записи звука или изображения и при желании избежать записи себя. Обязанность уведомления не действует в отношении публичных мероприятий, запись которых в целях обнародования можно разумно предполагать.

4 глава

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРАВООХРАНИТЕЛЬНЫМ УЧРЕЖДЕНИЕМ ПРИ ПРЕДОТВРАЩЕНИИ, ВЫЯВЛЕНИИ ПРАВОНАРУШЕНИЯ И ПРОИЗВОДСТВЕ ПО НЕМУ, А ТАКЖЕ ПРИ ИСПОЛНЕНИИ НАКАЗАНИЯ

1 раздел

Общие положения

§ 12. Применение настоящей главы

(1) Настоящая глава применяется к обработке персональных данных правоохранительным учреждением при предотвращении, выявлении правонарушения и производстве по нему, а также при исполнении наказания.

(2) Настоящая глава не применяется к обработке персональных данных при осуществлении государственного надзора или административного надзора.

(3) Настоящей главой предусматриваются особенности, применяемые к правоохранительному учреждению. Регламент (ЕС) 2016/679 Европейского парламента и Совета не применяется к правоохранительному учреждению, если из настоящего закона не вытекает иное.

§ 13. Термины

(1) В настоящей главе термины используются в значении статьи 4 и части 1 статьи 9 Регламента (ЕС) 2016/679 Европейского парламента и Совета.

(2) В настоящей главе правоохранительным учреждением считается учреждение или структурное подразделение учреждения, компетентное на основании закона предотвращать и выявлять правонарушение, вести производство по нему или исполнять наказание.

2 раздел Принципы

§ 14. Принципы обработки персональных данных

При обработке персональных данных необходимо соблюдать следующие принципы:

- 1) законность и справедливость – персональные данные обрабатываются законно и справедливо;
- 2) целевое назначение – персональные данные собираются для точно и ясно определённых законных целей и не обрабатываются способом, противоречащим этим целям;
- 3) качество – персональные данные должны быть достаточными и уместными и не должны быть чрезмерными с учётом целей обработки данных;
- 4) точность – персональные данные должны быть точными и при необходимости актуализированными; разумными мерами обеспечивается, что неточные с точки зрения цели обработки данных персональные данные удаляются или исправляются без промедления;
- 5) хранение – персональные данные хранятся в форме, позволяющей идентифицировать субъекта данных, лишь до тех пор, пока это необходимо для достижения цели, для которой персональные данные обрабатываются;
- 6) безопасность – персональные данные обрабатываются способом, обеспечивающим их безопасность, в том числе защищающим от несанкционированной или незаконной обработки и от случайной потери, уничтожения или повреждения, с применением соответствующих технических или организационных мер.

§ 15. Законность обработки персональных данных

Правоохранительное учреждение может обрабатывать персональные данные на основании закона, если их обработка необходима для выполнения задачи, вытекающей из цели предотвращения, выявления правонарушения или производства по нему либо исполнения наказания.

§ 16. Обработка персональных данных в цели, отличной от первоначальной

(1) Обработка персональных данных тем же или другим контролёром в иной цели, установленной частью 1 § 12 настоящего закона, чем первоначальная цель, для которой персональные данные собираются, допускается в той мере, в какой:

- 1) у контролёра имеется для обработки персональных данных в такой цели основание, вытекающее из закона или правового акта Европейского союза, и
- 2) такая обработка персональных данных необходима в соответствии с законом или правовым актом Европейского союза и соразмерна поставленной цели.

(2) Персональные данные, собранные или собираемые правоохранительным учреждением в целях, установленных частью 1 § 12 настоящего закона, нельзя обрабатывать в иных целях, за исключением случаев, установленных частью 1 настоящего параграфа, или если такая обработка допускается законом или правовым актом Европейского союза. Если персональные данные обрабатываются в такой иной цели, применяется Регламент (ЕС) 2016/679 Европейского парламента и Совета, за исключением случая, когда персональные данные обрабатываются в ходе деятельности, не относящейся к сфере применения

указанного регламента. В ситуации, когда цель обработки не относится к сфере применения указанного регламента, применяется право Эстонии.

(3) Если правоохранительное учреждение в соответствии с законом выполняет также иные задачи, чем те, что выполняются в целях, установленных частью 1 § 12 настоящего закона, к обработке персональных данных в такой цели применяется Регламент (ЕС) 2016/679 Европейского парламента и Совета. В ситуации, когда цель обработки не относится к сфере применения указанного регламента, применяется право Эстонии.

§ 17. Хранение персональных данных

(1) Для обрабатываемых персональных данных законом или постановлением устанавливается срок хранения. В исключительном случае, если срок хранения персональных данных не установлен законом или постановлением, этот срок должен установить контролёр.

(2) Срок хранения, установленный на основании части 1 настоящего параграфа, допускается продлевать лишь в обоснованном случае, за исключением случая, когда срок хранения установлен нормативным правовым актом.

(3) Если конкретный срок хранения установить невозможно, контролёр должен применять правовые и технологические меры, позволяющие постоянно оценивать необходимость дальнейшей обработки данных.

(4) По окончании срока хранения персональных данных контролёр и обработчик обязаны окончательно удалить персональные данные. Для этого контролёр должен применять надлежащие правовые и технологические меры.

§ 18. Различение разных категорий субъектов данных

При возможности и в соответствующих случаях контролёр при обработке персональных данных различает в качестве разных категорий субъектов данных лиц, в отношении которых ведётся производство, подозреваемых, обвиняемых, потерпевших, свидетелей, заключённых, лиц, находящихся под арестом, лиц, находящихся под уголовным надзором, и других лиц.

§ 19. Различение персональных данных, основанных на оценках

Контролёр по возможности различает персональные данные, основанные на фактах, и персональные данные, основанные на личных оценках.

§ 20. Особенности обработки персональных данных особых категорий

(1) Обработка персональных данных особых категорий допускается только тогда, когда это строго необходимо, и лишь в следующих случаях:

- 1) допустимость обработки установлена правовым актом;
- 2) обработка необходима для защиты жизненно важных интересов субъекта данных или другого физического лица или
- 3) обрабатываются персональные данные, которые субъект данных сам явно обнаружил.

(2) К обработке персональных данных особых категорий, указанных в части 1 настоящего параграфа, применяются соответствующие меры защиты прав и свобод субъекта данных.

§ 21. Автоматизированная обработка

(1) Запрещается принимать решение, основанное исключительно на автоматизированной обработке, в том числе профилирование, если оно влечёт для субъекта данных неблагоприятные правовые последствия или оказывает на него иное существенное влияние. Такое решение может быть принято, если принятие решения допускается законом, в котором

установлены соответствующие меры защиты прав, свобод и законных интересов субъекта данных.

(2) Субъект данных вправе в отношении решения, указанного в части 1 настоящего параграфа, представить контролёру возражения для защиты своего законного интереса.

(3) Решение, указанное в части 1 настоящего параграфа, не должно основываться на персональных данных особых категорий, за исключением случая применения надлежащих мер защиты прав, свобод и законных интересов субъекта данных.

(4) Запрещается решение, основанное на профилировании, в результате которого физические лица подвергаются дискриминации на основании персональных данных особых категорий.

3 раздел

Права субъекта данных

§ 22. Информация, предоставляемая в доступном для субъекта данных виде

(1) Контролёр обязан обнародовать следующую информацию:

- 1) планируемая цель обработки персональных данных;
- 2) право лица знакомиться со своими данными и исправлять, удалять или ограничивать их, а также порядок осуществления этих прав;
- 3) имя (наименование) и контактные данные контролёра и специалиста по защите данных;
- 4) контактные данные Инспекции по защите данных;
- 5) право подать жалобу в Инспекцию по защите данных, если при обработке персональных данных были нарушены права субъекта данных.

(2) Обнародованием, указанным в части 1 настоящего параграфа, считается обнародование информации на веб-сайте контролёра или в ином легкодоступном для субъекта данных месте.

§ 23. Информация, предоставляемая при уведомлении субъекта данных

(1) Если законом установлена обязанность уведомить субъекта данных об обработке его персональных данных, контролёр предоставляет субъекту данных следующую дополнительную информацию:

- 1) информацию, указанную в части 1 § 22 настоящего закона;
- 2) правовое основание обработки персональных данных;
- 3) срок хранения персональных данных или основания определения срока хранения;
- 4) категории получателей, которым разрешено передавать персональные данные;
- 5) при необходимости иную дополнительную информацию.

(2) В случаях, установленных законом, контролёр может предоставить информацию, указанную в части 1 настоящего параграфа, субъекту данных позднее, ограничить её предоставление или не предоставлять, если это может:

- 1) воспрепятствовать или нанести ущерб предотвращению, выявлению правонарушения или производству по нему либо исполнению наказания;
- 2) нанести ущерб правам и свободам другого лица;
- 3) создать угрозу государственной безопасности;
- 4) создать угрозу охране общественного порядка;
- 5) воспрепятствовать официальному расследованию или производству.

§ 24. Право субъекта данных получать информацию и относящиеся к нему персональные данные

(1) Субъект данных вправе получить от контролёра подтверждение того, что его персональные данные обрабатываются. По желанию субъекта данных контролёр должен сообщить субъекту данных:

- 1) относящиеся к нему персональные данные и категории соответствующих персональных данных;
- 2) имеющуюся информацию о происхождении персональных данных;
- 3) цель и правовое основание обработки персональных данных;
- 4) получателей или их категории, которым персональные данные субъекта данных были обнародованы;
- 5) планируемый срок хранения персональных данных или основания определения срока хранения;
- 6) право требовать от контролёра исправления, удаления или ограничения обработки персональных данных субъекта данных;
- 7) право подать жалобу в Инспекцию по защите данных и контактные данные Инспекции по защите данных.

(2) В случаях, установленных законом, контролёр может предоставить информацию, указанную в части 1 настоящего параграфа, субъекту данных позднее, ограничить её предоставление или отказаться от её выдачи, если это может:

- 1) воспрепятствовать или нанести ущерб предотвращению, выявлению правонарушения или производству по нему либо исполнению наказания;
- 2) нанести ущерб правам и свободам другого лица;
- 3) создать угрозу государственной безопасности;
- 4) создать угрозу охране общественного порядка;
- 5) воспрепятствовать официальному расследованию или производству.

(3) Контролёр без промедления письменно уведомляет субъекта данных об ограничении ознакомления с информацией, указанной в части 1 настоящего параграфа, или об отказе в таком ознакомлении и о причинах этого. Контролёр может не приводить обоснования, если предоставление такой информации привело бы к возникновению какого-либо из обстоятельств, указанных в части 2 настоящего параграфа.

(4) При уведомлении субъекта данных в соответствии с частью 3 настоящего параграфа контролёр уведомляет субъекта данных о его праве обратиться для оспаривания решения в Инспекцию по защите данных или в суд.

(5) Контролёр документирует фактические и правовые основания решения, принятого на основании части 2 настоящего параграфа, и при необходимости обеспечивает доступность информации для Инспекции по защите данных.

§ 25. Право субъекта данных требовать исправления и удаления персональных данных

(1) Субъект данных вправе требовать от контролёра исправления относящихся к нему неточных персональных данных, основанных на фактах.

(2) Субъект данных вправе требовать от контролёра дополнения относящихся к нему неполных персональных данных, если это уместно с учётом цели обработки персональных данных.

(3) Субъект данных вправе требовать от контролёра удаления собранных персональных данных, если:

- 1) обработка персональных данных не допускается на основании закона;
- 2) при обработке персональных данных не были учтены принципы обработки персональных данных или
- 3) контролёр обязан удалить данные во исполнение обязанности, вытекающей из закона, судебного решения, международного договора или иного обязывающего соглашения.

(4) Вместо удаления персональных данных контролёр ограничивает их обработку, если:

- 1) субъект данных оспаривает правильность персональных данных, и установить их правильность или неправильность невозможно или
- 2) персональные данные необходимо хранить в целях доказывания.

(5) Если контролёр вместо удаления персональных данных применил предусмотренное пунктом 1 части 4 настоящего параграфа ограничение обработки персональных данных, контролёр должен уведомить субъекта данных о снятии такого ограничения.

(6) Контролёр обязан без промедления письменно уведомить субъекта данных, если он отказывается исправлять или удалять персональные данные либо ограничивать их обработку, и указать причины отказа. Контролёр может не приводить обоснования, если предоставление такой информации привело бы к возникновению какого-либо из обстоятельств, указанных в части 2 § 24 настоящего закона.

(7) При уведомлении субъекта данных в соответствии с частью 6 настоящего параграфа контролёр уведомляет субъекта данных о его праве обратиться для оспаривания решения в Инспекцию по защите данных или в суд.

§ 26. Обязанность контролёра уведомлять об исправлении, удалении персональных данных и ограничении их обработки

(1) При исправлении персональных данных контролёр обязан без промедления уведомить об исправлении и его содержании компетентное учреждение, от которого были получены неточные персональные данные.

(2) Если персональные данные были исправлены или удалены на основании § 25 настоящего закона или их обработка была ограничена, контролёр обязан уведомить получателей, которым данные были ранее переданы.

(3) Получатели, указанные в части 2 настоящего параграфа, обязаны исправить или удалить относящиеся к их ответственности персональные данные либо ограничить их обработку.

§ 27. Порядок осуществления прав субъекта данных

(1) Контролёр обязан отвечать на запрос субъекта данных в краткой, понятной и легкодоступной форме, используя ясные и простые формулировки. На запрос субъекта данных по возможности отвечают желаемым субъектом данных способом.

(2) Контролёр без необоснованной задержки, в течение одного месяца после получения запроса, уведомляет субъекта данных о действиях, совершённых на основании запроса субъекта данных.

(3) Контролёр может запросить у субъекта данных возмещение разумных расходов, связанных с исполнением запроса, установленных законом или изданным на его основании правовым актом, либо отказаться от принятия запрошенных мер, если запрос субъекта данных необоснован или чрезмерен.

(4) Контролёр устанавливает личность субъекта данных и его право получать информацию и относящиеся к нему персональные данные либо право требовать исправления и удаления персональных данных.

§ 28. Право субъекта данных обратиться в Инспекцию по защите данных

(1) Если субъект данных считает, что при обработке персональных данных нарушаются его права, он вправе обратиться с жалобой в Инспекцию по защите данных.

(2) Инспекция по защите данных уведомляет субъекта данных о решении, принятом на основании его жалобы, и о праве обратиться в суд для оспаривания решения Инспекции по защите данных.

(3) Если рассматривать жалобу субъекта данных компетентен надзорный орган другого государства — члена Европейского союза, Инспекция по защите данных направляет жалобу субъекта данных для подачи в компетентный надзорный орган другого государства — члена Европейского союза.

4 раздел

Обязанности контролёра и обработчика

§ 29. Контролёр и обработчик

(1) Контролёр применяет соответствующие технические и организационные меры, чтобы обеспечить при обработке персональных данных соблюдение требований настоящего закона. Контролёр обязан при необходимости доказывать выполнение требований, установленных настоящим законом.

(2) Контролёр даёт обработчику обязательные указания по обработке персональных данных и отвечает за то, чтобы обработчик соблюдал требования к обработке персональных данных.

(3) Контролёр может использовать только таких обработчиков, которые дают достаточные гарантии того, что они применяют соответствующие технические и организационные меры таким образом, чтобы обработка персональных данных отвечала требованиям настоящего закона, и обеспечивают защиту прав субъекта данных.

(4) Обработчик может привлекать к обработке персональных данных других обработчиков только на основании закона или изданного на его основании правового акта либо с письменного разрешения контролёра и при условии, что не превышаются полномочия, предоставленные обработчику. При полномочии, предоставленном на основании письменного разрешения, обработчик должен всегда уведомлять контролёра о добавлении или замене другого обработчика. В этом случае контролёр может выдвинуть возражения относительно изменений.

(5) Если обработчик, нарушая настоящий закон, определяет цели и средства обработки персональных данных, то этот обработчик является в отношении такой обработки контролёром.

§ 30. Назначение обработчика и его обязанности

(1) Контролёр может поручить обработчику обрабатывать персональные данные на основании закона, изданного на его основании правового акта или письменного договора, в котором устанавливаются содержание, продолжительность, характер и цель обработки персональных данных, категории обрабатываемых персональных данных и категории субъектов данных, а также обязанности и права контролёра.

(2) В законе, изданном на его основании правовом акте или договоре, указанных в части 1 настоящего параграфа, устанавливается, в частности, что обработчик обязан:

- 1) действовать исключительно на основании указаний контролёра;

- 2) обеспечить, чтобы уполномоченное на обработку персональных данных лицо сохраняло в тайне персональные данные, ставшие ему известными при исполнении служебных обязанностей;
- 3) обеспечить защиту прав субъекта данных;
- 4) после окончания оказания услуги по обработке данных по выбору контролёра удалить или вернуть контролёру все персональные данные и удалить имеющиеся копии, если законом не установлено иное;
- 5) предоставить контролёру информацию, связанную с обработкой персональных данных, необходимую для доказательства выполнения требований, установленных настоящим параграфом;
- 6) соблюдать условия привлечения другого обработчика, установленные частью 4 § 29 и настоящим параграфом.

§ 31. Совместные контролёры

- (1) Если два или более контролёра совместно определяют цели и средства обработки персональных данных, они являются совместными контролёрами.
- (2) Ответственность и объём обязанностей совместного контролёра определяются законом, изданным на его основании правовым актом или договором, заключённым между совместными контролёрами.
- (3) В договоре, указанном в части 2 настоящего параграфа, для субъектов данных определяется контактный пункт, через который субъект данных может осуществлять свои права.
- (4) Субъект данных может осуществлять вытекающие из настоящего закона права в отношении каждого контролёра.

§ 32. Обработка персональных данных от имени контролёра и обработчика

- (1) Лицо, обрабатывающее персональные данные от имени контролёра или обработчика, обязано обрабатывать их исключительно в соответствии с указаниями контролёра, если законом не установлено иное.
- (2) Право лица обрабатывать персональные данные от имени контролёра или обработчика должно вытекать из закона, изданного на его основании правового акта, договора, заключённого между контролёром или обработчиком и лицом, либо акта, регулирующего служебные отношения.

§ 33. Встроенная защита данных и защита данных по умолчанию

- (1) Контролёр и обработчик принимают для определения средств обработки и для обработки персональных данных соответствующие технические и организационные меры и применяют их последовательно.
- (2) Контролёр и обработчик применяют соответствующие технические и организационные меры, которыми обеспечивается, что по умолчанию обрабатываются только персональные данные, необходимые для достижения каждой конкретной цели обработки.

§ 34. Требования к обработке персональных данных

Контролёр и обработчик при обработке персональных данных обязаны:

- 1) исправлять неточные персональные данные;
- 2) удалять персональные данные, если их обработка не допускается на основании закона или не соответствует принципам обработки персональных данных;
- 3) уведомлять получателя, если персональные данные были переданы незаконно или были переданы неточные персональные данные;

4) сотрудничать с Инспекцией по защите данных.

§ 35. Требования к передаче персональных данных

(1) Контролёр обязан принимать и применять соответствующие меры для того, чтобы неполные, неточные или устаревшие персональные данные не передавались и не делались доступными.

(2) Контролёр при передаче персональных данных по возможности прилагает необходимую информацию, позволяющую получающему данные компетентному учреждению оценить правильность, полноту, достоверность и актуальность персональных данных.

(3) Если к обработке персональных данных применяются особые условия, контролёр при передаче таких персональных данных уведомляет получателя об этих условиях и о необходимости их соблюдения.

(4) При передаче персональных данных другим получателям, находящимся в Европейском союзе, и учреждениям, созданным в соответствии с главами 4 и 5 раздела V Договора о функционировании Европейского союза, не применяются дополнительные особые условия обработки персональных данных по сравнению с теми, которые применяются к передаче персональных данных внутри государства.

§ 36. Ведение журналов

(1) Контролёр и обработчик ведут журналы как минимум о следующих операциях по обработке персональных данных, совершаемых в автоматизированных системах:

- 1) сбор;
- 2) изменение;
- 3) чтение;
- 4) обнародование;
- 5) передача;
- 6) объединение;
- 7) удаление.

(2) Журналы, отражающие чтение, обнародование и передачу, должны позволять установить обоснование, дату и время совершения указанных операций и сведения о лице, которое читало, обнародовало или передавало персональные данные, а также наименования получателей таких персональных данных.

(3) Журналы допускается использовать для проверки законности операций по обработке персональных данных, внутреннего контроля, обеспечения целостности и безопасности персональных данных и ведения производства по делу о правонарушении.

(4) По запросу Инспекции по защите данных контролёр и обработчик обеспечивают доступность информации, указанной в части 1 настоящего параграфа, для Инспекции по защите данных.

(5) Контролёр устанавливает сроки хранения журналов.

§ 37. Регистрация операций по обработке персональных данных

(1) Контролёр регистрирует все виды операций по обработке персональных данных, совершаемых под его ответственностью. Необходимо зарегистрировать следующую информацию:

- 1) имя (наименование) и контактные данные контролёра и, в соответствующем случае, совместного контролёра;
- 2) имя и контактные данные специалиста по защите данных;

- 3) цели обработки персональных данных;
 - 4) получатели или их категории, которым персональные данные были или будут обнародованы;
 - 5) описание категорий субъектов данных и категорий персональных данных;
 - 6) в соответствующем случае использование профилирования;
 - 7) в соответствующем случае виды передачи персональных данных третьему государству или международной организации;
 - 8) информация о правовом основании обработки персональных данных;
 - 9) по возможности предусмотренные сроки удаления персональных данных особых категорий;
 - 10) по возможности описание организационных и технических мер безопасности обработки персональных данных, принятых на основании § 43 настоящего закона.
- (2) Обработчик регистрирует все виды операций, связанных с обработкой персональных данных, совершаемых от имени контролёра. Необходимо зарегистрировать следующую информацию:
- 1) имя (наименование) и контактные данные обработчика, а также контролёра, от имени которого обработчик действует;
 - 2) в соответствующем случае имя и контактные данные должностного лица по защите данных;
 - 3) виды обработки персональных данных, совершаемой от имени контролёра;
 - 4) в соответствующем случае передача персональных данных третьему государству или международной организации, в том числе данные для идентификации такого третьего государства или международной организации;
 - 5) по возможности описание организационных и технических мер безопасности обработки персональных данных, принятых на основании § 43 настоящего закона.
- (3) Информация, указанная в частях 1 и 2 настоящего параграфа, регистрируется в форме, позволяющей письменное воспроизведение.
- (4) По запросу Инспекции по защите данных ответственный или уполномоченный обработчик обеспечивает доступность документов, указанных в частях 1 и 2 настоящего параграфа, для Инспекции по защите данных.

§ 38. Оценка воздействия на защиту данных

- (1) Контролёр до обработки персональных данных оценивает влияние планируемых операций по обработке персональных данных на защиту персональных данных, если в результате обработки персональных данных с учётом характера, объёма, контекста и целей обработки может возникнуть высокий риск для прав и свобод физического лица.
- (2) Оценка воздействия должна включать как минимум следующее:
- 1) систематическое описание планируемых операций по обработке персональных данных и целей обработки;
 - 2) оценку необходимости и соразмерности операций по обработке персональных данных с учётом целей обработки персональных данных;
 - 3) оценку рисков, затрагивающих права и свободы субъекта данных;
 - 4) меры, запланированные для устранения рисков, в том числе гарантии, меры безопасности и механизмы обеспечения защиты персональных данных и доказательства соблюдения настоящего закона с учётом прав и законных интересов субъекта данных и других заинтересованных лиц.

§ 39. Консультация с Инспекцией по защите данных

(1) Если ответственный или уполномоченный обработчик намерен обрабатывать персональные данные, которые вносятся во вновь создаваемый массив данных, он должен предварительно проконсультироваться с Инспекцией по защите данных в следующих случаях:

- 1) из оценки воздействия на защиту данных, проведённой на основании § 38 настоящего закона, следует, что в результате обработки персональных данных при отсутствии мер, принимаемых контролёром для смягчения риска, возник бы высокий риск;
- 2) характер обработки персональных данных влечёт высокий риск для прав и свобод субъекта данных.

(2) Для оценки соответствия требованиям к обработке персональных данных контролёр представляет Инспекции по защите данных следующую информацию:

- 1) оценку воздействия на защиту данных, предусмотренную § 38 настоящего закона;
- 2) цель и средства планируемой обработки персональных данных;
- 3) меры и гарантии, предусмотренные для защиты прав и свобод субъекта данных;
- 4) в соответствующем случае контактные данные должностного лица по защите данных;
- 5) в соответствующем случае области ответственности контролёра, совместных контролёров и обработчиков при обработке персональных данных;
- 6) иную информацию, запрошенную Инспекцией по защите данных.

(3) Если, по оценке Инспекции по защите данных, планируемая обработка персональных данных, указанная в части 1 настоящего параграфа, нарушала бы требования настоящего закона, Инспекция по защите данных даёт контролёру и в соответствующем случае обработчику письменную рекомендацию о том, как привести обработку данных в соответствие с требованиями настоящего закона.

(4) Инспекция по защите данных даёт контролёру или обработчику рекомендацию в течение шести недель со дня получения информации, указанной в части 2 настоящего параграфа.

(5) Срок, указанный в части 4 настоящего параграфа, может быть продлён на один месяц с учётом сложности планируемой обработки персональных данных. Инспекция по защите данных уведомляет контролёра или обработчика о продлении срока в течение одного месяца со дня получения запроса о консультации. Продление срока необходимо обосновать.

(6) Инспекция по защите данных может составить перечень операций по обработке персональных данных, для которых необходима предварительная консультация, указанная в части 1 настоящего параграфа.

5 раздел

Специалист по защите данных

§ 40. Назначение специалиста по защите данных

(1) Правоохранительное учреждение назначает специалиста по защите данных. От этой обязанности освобождены суды при выполнении функции отправления правосудия.

(2) Правоохранительное учреждение может назначить одного специалиста по защите данных для нескольких учреждений или органов в зависимости от их организационной структуры и размера.

(3) При назначении специалиста по защите данных исходят из его профессиональных навыков и экспертных знаний в области правовых актов и практики по защите данных, а также способности выполнять задачи, установленные § 41 настоящего закона.

(4) Специалист по защите данных может быть должностным лицом или работником, находящимся на службе в правоохранительном учреждении, либо выполнять задачи на основании договора об оказании услуг.

§ 41. Задачи специалиста по защите данных

(1) Специалист по защите данных выполняет как минимум следующие задачи:

1) информирует и консультирует правоохранительное учреждение и по его поручению обрабатывающих персональные данные должностных лиц и работников в связи с их обязанностями, вытекающими из настоящего закона и иных норм по защите данных Европейского союза или его государств-членов;

2) обеспечивает соответствие настоящему закону, при необходимости иным нормам по защите данных Европейского союза или его государств-членов и внутренним правилам контролёра, касающимся принципов защиты персональных данных и повышения осведомлённости и обучения участвующих в обработке персональных данных должностных лиц и работников;

3) консультирует в связи с оценкой воздействия на защиту данных и следит за её функционированием в соответствии с § 38 настоящего закона;

4) сотрудничает с Инспекцией по защите данных;

5) выступает по вопросам обработки персональных данных в качестве контактного лица Инспекции по защите данных, в том числе в ходе предварительной консультации, предусмотренной § 39 настоящего закона, и при необходимости консультирует также по иным вопросам.

(2) Специалист по защите данных суда не выполняет задачи, указанные в части 1 настоящего параграфа, в отношении деятельности суда, связанной с отправлением правосудия.

(3) Специалист по защите данных может выполнять иные задачи и обязанности. Ответственный или уполномоченный обработчик обеспечивает, чтобы такие задачи и обязанности не приводили к конфликту интересов у специалиста по защите данных.

§ 42. Служебное положение специалиста по защите данных

(1) Контролёр обеспечивает надлежащее и своевременное привлечение специалиста по защите данных ко всем вопросам защиты персональных данных.

(2) Контролёр поддерживает специалиста по защите данных при выполнении задач, указанных в § 41 настоящего закона, предоставляя ему необходимые для выполнения этих задач и поддержания уровня экспертных знаний средства, а также доступ к персональным данным и операциям по их обработке.

(3) К служебному положению специалиста по защите данных применяется то, что установлено частями 3–6 статьи 38 Регламента (ЕС) 2016/679 Европейского парламента и Совета.

6 раздел

Меры безопасности обработки персональных данных и уведомление о нарушениях, связанных с персональными данными

§ 43. Меры безопасности обработки персональных данных

Контролёр и обработчик обязаны принимать и применять организационные и технические меры безопасности для защиты персональных данных, чтобы:

- 1) запретить неуполномоченным лицам доступ к средствам обработки данных, используемым для обработки персональных данных;
- 2) предотвратить самовольное чтение, копирование, изменение и удаление носителей данных;
- 3) предотвратить самовольный ввод персональных данных и ознакомление с хранимыми персональными данными, их изменение или удаление;
- 4) предотвратить использование системы обработки данных неуполномоченными лицами с помощью средств передачи данных;
- 5) обеспечить, чтобы пользователю, имеющему разрешение на использование автоматизированной системы обработки данных, был предоставлен доступ только к тем персональным данным, которые охвачены его разрешением на доступ;
- 6) обеспечить возможность доказать и определить, каким учреждениям персональные данные были переданы или сделаны доступными с помощью средств передачи данных и каким учреждениям их можно передавать или делать доступными;
- 7) обеспечить возможность доказать и установить, какие персональные данные были введены в автоматизированную систему обработки данных, а также когда и кем они были введены;
- 8) предотвратить несанкционированное чтение, копирование, изменение или удаление персональных данных при их передаче или перевозке носителей данных;
- 9) обеспечить возможность восстановления установленных систем обработки данных в случае сбоя;
- 10) обеспечить функционирование системы обработки данных и уведомление о возникающих в её работе ошибках;
- 11) предотвратить искажение персональных данных в результате сбоев системы.

§ 44. Уведомление Инспекции по защите данных о нарушении, связанном с персональными данными

- (1) Если нарушение, связанное с персональными данными, вероятно, создаёт угрозу правам и свободам физического лица, контролёр сообщает о нарушении Инспекции по защите данных без промедления, по возможности в течение 72 часов после того, как ему стало об этом известно.
- (2) Обработчик уведомляет контролёра без промедления после того, как ему стало известно о нарушении, связанном с персональными данными.
- (3) В сообщении, указанном в части 1 настоящего параграфа, необходимо представить следующую информацию:
 - 1) суть нарушения, в том числе характер нарушения, связанного с персональными данными, по возможности категории и приблизительное число затронутых субъектов данных, а также категории и приблизительное число затронутых персональных данных;
 - 2) имя и контактные данные должностного лица по защите данных;
 - 3) описание возможных последствий нарушения, связанного с персональными данными;
 - 4) меры, принятые или запланированные контролёром для устранения нарушений, связанных с персональными данными, в том числе меры по смягчению возможных неблагоприятных последствий нарушения.

(4) Если Инспекцию по защите данных уведомляют о нарушении, связанном с персональными данными, по истечении 72 часов после того, как стало об этом известно, по этому поводу представляется обоснование.

(5) Если нарушение, связанное с персональными данными, затрагивает персональные данные, переданные контролёром другого государства — члена Европейского союза или контролёру другого государства — члена Европейского союза, информация, указанная в части 3 настоящего параграфа, передаётся без необоснованной задержки контролёру этого государства-члена.

(6) Контролёр документирует все нарушения, связанные с персональными данными, указанные в части 1 настоящего параграфа, в том числе обстоятельства нарушения, его влияние и принятые меры по исправлению.

§ 45. Уведомление субъекта данных о нарушении, связанном с персональными данными

(1) Если нарушение, вероятно, создаёт высокий риск для прав и свобод физического лица, контролёр без промедления уведомляет субъекта данных о нарушении, связанном с персональными данными.

(2) При уведомлении, указанном в части 1 настоящего параграфа, ясным и простым языком описывается характер нарушения, связанного с персональными данными, и представляется как минимум информация, указанная в пунктах 2–4 части 3 § 44 настоящего закона.

(3) Уведомление, указанное в части 1 настоящего параграфа, не требуется, если выполнено хотя бы одно из следующих условий:

- 1) контролёр применил соответствующие технологические и организационные меры защиты, и они были применены к персональным данным, затронутым нарушением, связанным с персональными данными;
- 2) контролёр принял последующие меры, исключающие реализацию высокого риска для прав и свобод субъекта данных, указанного в части 1 настоящего параграфа;
- 3) индивидуальное уведомление субъекта данных повлекло бы несоразмерные расходы, а общественность о нарушении была уведомлена.

(4) Если контролёр ещё не уведомил субъекта данных о нарушении, связанном с персональными данными, Инспекция по защите данных может после оценки тяжести нарушения решить, требуется ли уведомление субъекта данных о нарушении, связанном с персональными данными, или имеет место один из случаев, указанных в части 3 настоящего параграфа.

(5) О нарушении, указанном в части 1 настоящего параграфа, субъекта данных можно уведомить позднее, в ограниченном объёме или не уведомлять, если это может:

- 1) воспрепятствовать или нанести ущерб предотвращению, выявлению правонарушения или производству по нему либо исполнению наказания;
- 2) нанести ущерб правам и свободам другого лица;
- 3) создать угрозу государственной безопасности;
- 4) создать угрозу охране общественного порядка;
- 5) воспрепятствовать официальному расследованию или производству.

7 раздел

Передача персональных данных третьему государству и международной организации

§ 46. Общие условия передачи персональных данных третьему государству и международной организации

(1) Персональные данные допускается передавать третьему государству или международной организации только при выполнении всех следующих условий:

- 1) передача необходима для предотвращения, выявления правонарушения или производства по нему либо исполнения наказания;
- 2) персональные данные передаются контролёру в третьем государстве или международной организации, компетентному предотвращать и выявлять правонарушение, вести производство по нему или исполнять наказание;
- 3) имеется согласие другого государства — члена Европейского союза на дальнейшее использование данных, если передаваемые данные получены от этого государства-члена;
- 4) Европейская комиссия приняла в соответствии со статьёй 36 Директивы (ЕС) 2016/680 Европейского парламента и Совета решение об адекватности защиты, а при отсутствии такого решения приняты достаточные меры защиты, указанные в § 47 настоящего закона, либо при их отсутствии применяется исключение, указанное в § 48 настоящего закона;
- 5) при передаче персональных данных обеспечивается, что передающий данные контролёр дал предварительное согласие на дальнейшую передачу персональных данных другому третьему государству или международной организации.

(2) Если разрешение на передачу персональных данных, указанное в пункте 3 части 1 настоящего параграфа, невозможно получить вовремя, а передача персональных данных необходима для предотвращения непосредственной и серьёзной угрозы общественному порядку государства или третьего государства либо для защиты существенного интереса государства, персональные данные могут быть переданы без разрешения, указанного в пункте 3 части 1 настоящего параграфа. О предусмотренном настоящей частью обмене данными без промедления уведомляется компетентное учреждение государства — члена Европейского союза, передавшего персональные данные.

(3) При даче согласия, указанного в пункте 5 части 1 настоящего параграфа, ответственный или уполномоченный обработчик учитывает, среди прочего, тяжесть правонарушения, цель первоначальной передачи персональных данных и уровень защиты персональных данных в том третьем государстве или международной организации, куда персональные данные передаются дальше.

(4) Если Европейская комиссия приняла решение, указанное в части 5 статьи 36 Директивы (ЕС) 2016/680 Европейского парламента и Совета, персональные данные могут быть переданы третьему государству или международной организации на основании §§ 47 и 48 настоящего закона.

§ 47. Передача персональных данных при применении соответствующих мер защиты

При отсутствии решения Европейской комиссии об адекватности защиты, указанного в пункте 4 части 1 § 46 настоящего закона, персональные данные могут быть переданы третьему государству или международной организации в следующих случаях:

- 1) соответствующие меры защиты персональных данных установлены в юридически обязывающем акте;

2) контролёр оценил все обстоятельства, связанные с передачей персональных данных, и пришёл к выводу, что приняты все соответствующие с точки зрения защиты персональных данных меры защиты.

§ 48. Передача персональных данных в исключительных случаях

(1) При отсутствии решения Европейской комиссии об адекватности защиты, указанного в пункте 4 части 1 § 46 настоящего закона, или соответствующих мер защиты, указанных в § 47, передача персональных данных третьему государству или международной организации допускается, если она необходима:

- 1) для защиты прав и свобод субъекта данных или другого лица;
- 2) для защиты законных интересов субъекта данных;
- 3) для предотвращения непосредственной и серьёзной угрозы общественному порядку;
- 4) для предотвращения, выявления конкретного правонарушения или производства по нему либо исполнения наказания или
- 5) для составления, предъявления или защиты конкретного правового требования, связанного с целью предотвращения, выявления конкретного правонарушения или производства по нему либо исполнения наказания.

(2) Если права субъекта данных весомее интереса, установленного в пунктах 4 и 5 части 1 настоящего параграфа, передача персональных данных не допускается.

§ 49. Передача персональных данных получателю в третьем государстве

Персональные данные могут быть переданы непосредственно получателю в третьем государстве, если выполнены все следующие условия:

- 1) передача строго необходима для выполнения задачи, передающего персональные данные правоохранительного учреждения в целях предотвращения, выявления правонарушения или производства по нему либо исполнения наказания;
- 2) общественный интерес весомее прав и свобод субъекта данных;
- 3) передача персональных данных учреждению третьего государства, компетентному предотвращать и выявлять правонарушение, вести производство по нему или исполнять наказание, неэффективна или нецелесообразна;
- 4) учреждение третьего государства, компетентное предотвращать и выявлять правонарушение, вести производство по нему или исполнять наказание, уведомляется без промедления, за исключением случая, когда это неэффективно или нецелесообразно;
- 5) получателя уведомляют о конкретной цели обработки персональных данных и указывают ему обрабатывать персональные данные только в этой цели.

§ 50. Уведомление Инспекции по защите данных и документирование передачи персональных данных

(1) Ответственный или уполномоченный обработчик предоставляет Инспекции по защите данных обзор передач персональных данных, состоявшихся на основании пункта 2 § 47 и § 49 настоящего закона, не реже одного раза в год.

(2) Если персональные данные передаются на основании пункта 2 § 47, части 1 § 48 или § 49 настоящего закона, ответственный или уполномоченный обработчик документирует такую передачу, в том числе дату и время передачи, данные принимающего компетентного учреждения, пояснение к передаче и переданные персональные данные.

(3) По запросу Инспекции по защите данных ответственный или уполномоченный обработчик обеспечивает ей доступность документов, указанных в части 2 настоящего параграфа.

5 глава **ГОСУДАРСТВЕННЫЙ И АДМИНИСТРАТИВНЫЙ НАДЗОР**

1 раздел **Назорный орган**

§ 51. Образование независимого надзорного органа

(1) Независимым надзорным органом в значении части 1 статьи 51 Регламента (ЕС) 2016/679 Европейского парламента и Совета и статьи 41 Директивы (ЕС) 2016/680 Европейского парламента и Совета является Инспекция по защите данных.

(2) Инспекция по защите данных при выполнении своих задач независима и действует, исходя из настоящего закона, Регламента (ЕС) 2016/679 Европейского парламента и Совета, иных законов и изданных на их основании правовых актов.

§ 52. Квалификация, требуемая для назначения на должность руководителя Инспекции по защите данных

(1) Руководителем Инспекции по защите данных может работать лицо с управленческим опытом и высшим образованием, обладающее знаниями о правовом регулировании защиты персональных данных и об информационных и коммуникационных технологиях, в том числе об информационных системах.

(2) Руководитель Инспекции по защите данных не вправе в период пребывания в должности участвовать в деятельности политических партий или работать на иной оплачиваемой трудовой должности или должности на службе, за исключением педагогической и научной работы.

§ 53. Проверка безопасности кандидата на должность руководителя Инспекции по защите данных

(1) Кандидат на должность руководителя Инспекции по защите данных должен до назначения на должность руководителя Инспекции по защите данных пройти проверку безопасности, за исключением случая, когда у него имеется действующее разрешение на доступ к государственной тайне уровня «совершенно секретно» или когда на момент становления кандидатом он занимает должность, с которой связано должностное право доступа ко всем уровням государственной тайны.

(2) Проверку безопасности кандидата на должность руководителя Инспекции по защите данных проводит Департамент полиции безопасности в порядке, предусмотренном Законом об учреждениях безопасности.

(3) Для прохождения проверки безопасности кандидат на должность руководителя Инспекции по защите данных заполняет анкету лица, ходатайствующего о разрешении на доступ к государственной тайне, и подписывает согласие, которым разрешает проводящему проверку безопасности учреждению получать во время проведения проверки безопасности сведения о себе от физических и юридических лиц, а также от учреждений и органов государства и местного самоуправления, и представляет их через Министерство юстиции и цифровых дел в Департамент полиции безопасности.

[RT I, 30.12.2024, 1 — вступило в силу 01.01.2025, на основании части 12 § 105.19 Закона о Правительстве Республики слово «Justiitsministeerium» заменено словами «Justiits- ja Digiministeerium» в соответствующем надежде]

(4) Департамент полиции безопасности передаёт данные, собранные в результате проверки безопасности, ответственному за соответствующую сферу министру в течение трёх месяцев со дня получения документов, указанных в части 3 настоящего параграфа, прилагая своё мнение о соответствии кандидата на должность руководителя Инспекции по защите данных условиям получения разрешения на доступ к государственной тайне.

(5) Если полномочия руководителя Инспекции по защите данных закончились до окончания срока, проверку безопасности необходимо провести в отношении кандидата на должность руководителя Инспекции по защите данных в течение трёх месяцев со дня получения документов, указанных в части 3 настоящего параграфа. С разрешения руководителя проводящего проверку безопасности учреждения срок проведения проверки безопасности может быть продлён на один месяц, если имеет место обстоятельство, указанное в пункте 1 или 2 части 4 § 33 Закона о государственной тайне и засекреченной иностранной информации, или если в течение одного месяца возможно выявление обстоятельства, указанного в пункте 3 или 4 той же части.

[RT I, 30.06.2026, 1 — вступило в силу 01.10.2026]

(6) На основании данных, собранных в ходе проведённой проверки безопасности, кандидата на должность руководителя Инспекции по защите данных можно назначить на должность в течение девяти месяцев со дня, когда Департамент полиции безопасности передал собранную в ходе проверки безопасности информацию ответственному за соответствующую сферу министру. По истечении этого срока кандидата на должность руководителя Инспекции по защите данных можно назначить на должность после прохождения новой проверки безопасности.

§ 54. Назначение на должность и освобождение от должности руководителя Инспекции по защите данных

(1) Руководителя Инспекции по защите данных назначает на должность на пять лет по предложению ответственного за соответствующую сферу министра Правительство Республики, предварительно заслушав мнение Конституционной комиссии Рийгикогу.

(2) Перед досрочным освобождением руководителя Инспекции по защите данных от должности заслушивается мнение Конституционной комиссии Рийгикогу.

§ 55. Компетенция Инспекции по защите данных при аккредитации сертификационных органов

Компетентным учреждением в значении части 1 статьи 43 Регламента (ЕС) 2016/679 Европейского парламента и Совета, компетентным аккредитовать сертификационные органы, обладающие соответствующими экспертными знаниями в сфере защиты данных, является Инспекция по защите данных.

2 раздел

Осуществление государственного и административного надзора

§ 56. Компетенция Инспекции по защите данных при осуществлении государственного и административного надзора

(1) Государственный и административный надзор за соблюдением требований, установленных настоящим законом, изданными на его основании правовыми актами и Регламентом (ЕС) 2016/679 Европейского парламента и Совета, а также требований, установленных к обработке персональных данных иными законами, осуществляет Инспекция по защите данных.

(2) Помимо предусмотренного в статье 57 Регламента (ЕС) 2016/679 Европейского парламента и Совета, в компетенцию Инспекции по защите данных входит:

- 1) повышать осведомлённость и понимание общественности, контролёров и обработчиков в отношении рисков при обработке персональных данных, действующих норм и мер защиты, касающихся обработки, а также прав, связанных с обработкой персональных данных; для выполнения этой задачи Инспекция по защите данных может давать рекомендательные указания;
 - 2) давать субъекту данных по его запросу информацию об осуществлении его прав, вытекающих из настоящего закона, и в соответствующем случае сотрудничать для этого с надзорными органами других государств — членов Европейского союза;
 - 3) при необходимости возбуждать производство о проступке и применять наказание, если иными административно-правовыми мерами невозможно добиться соблюдения требований, установленных законом или Регламентом (ЕС) 2016/679 Европейского парламента и Совета;
 - 4) сотрудничать с международными организациями по надзору в области защиты данных и другими учреждениями по надзору в области защиты данных, а также иными компетентными учреждениями и лицами иностранных государств;
 - 5) отслеживать соответствующие тенденции в той мере, в какой они влияют на защиту персональных данных, в частности развитие информационных и коммуникационных технологий;
 - 6) консультировать по операциям по обработке персональных данных, указанным в § 39 настоящего закона;
 - 7) участвовать в Европейском совете по защите данных;
 - 8) применять административное принуждение на основаниях, в объёме и порядке, предусмотренных законами;
 - 9) по собственной инициативе или по запросу представлять мнения по вопросам, связанным с защитой персональных данных, Рийгикогу, Правительству Республики, Канцлеру права и другим учреждениям, а также общественности;
 - 10) выполнять иные задачи, вытекающие из законов.
- (3) Помимо предусмотренного в статье 57 Регламента (ЕС) 2016/679 Европейского парламента и Совета, Инспекция по защите данных вправе:
- 1) предупреждать контролёра и обработчика о том, что планируемые операции по обработке персональных данных, вероятно, нарушают настоящий закон;
 - 2) требовать исправления персональных данных;
 - 3) требовать удаления персональных данных;
 - 4) требовать ограничения обработки персональных данных;
 - 5) требовать прекращения обработки персональных данных, в том числе уничтожения или передачи в архив;
 - 6) для предотвращения ущерба правам и свободам лица при необходимости применять без промедления организационные, физические и информационно-технические меры безопасности для защиты персональных данных в порядке, установленном Законом о замещающем исполнении и принудительном денежном взыскании, за исключением случая, когда персональные данные обрабатывает государственное учреждение;
 - 7) устанавливать временное или постоянное ограничение обработки персональных данных, в том числе запрет обработки персональных данных;
 - 8) возбуждать надзорное производство по жалобе или по собственной инициативе.

§ 57. Особые меры государственного надзора

Инспекция по защите данных может для осуществления предусмотренного настоящим законом государственного надзора применять особые меры государственного надзора, установленные в §§ 30–32, 44 и 49–53 Закона об охране правопорядка, на основаниях и в порядке, предусмотренных Законом об охране правопорядка.

§ 58. Особенности государственного надзора

(1) Инспекция по защите данных может для осуществления государственного надзора применять меры, установленные в статье 58 Регламента (ЕС) 2016/679 Европейского парламента и Совета.

(2) Инспекция по защите данных может сделать запрос предпринимателю в области электронной связи о данных, необходимых для установления конечного пользователя, связанного с идентификационными признаками, используемыми в общедоступной сети электронной связи, за исключением данных, связанных с фактом передачи сообщения, если иным способом установить конечного пользователя, связанного с идентификационными признаками, невозможно.

§ 59. Особенности административного надзора

(1) Инспекция по защите данных может при осуществлении административного надзора в соответствии с частью 7 статьи 83 Регламента (ЕС) 2016/679 Европейского парламента и Совета и положениями §§ 75¹ и 75² Закона о Правительстве Республики в случае неисполнения выданного предписания обратиться к вышестоящему учреждению, лицу или органу получателя предписания для организации служебного надзора или для возбуждения дисциплинарного производства в отношении должностного лица.

(2) Осуществляющий служебный надзор или лицо, имеющее право возбуждать дисциплинарное производство, обязано рассмотреть ходатайство в течение одного месяца со дня его получения и представить своё обоснованное мнение Инспекции по защите данных. В случае возбуждения служебного надзора или дисциплинарного производства осуществляющий надзор или лицо, имеющее право возбуждать дисциплинарное производство, обязано без промедления уведомить Инспекцию по защите данных о результатах соответствующего производства.

(3) Если обрабатывающее персональные данные государственное учреждение не исполнило предписание Инспекции по защите данных в установленный в нём срок, Инспекция по защите данных обращается в административный суд с протестом в порядке, установленном Кодексом административного судопроизводства.

§ 60. Размер принудительного денежного взыскания

В случае неисполнения предписания Инспекции по защите данных верхний предел принудительного денежного взыскания, применяемого в порядке, установленном Законом о замещающем исполнении и принудительном денежном взыскании, при каждом применении составляет до 20 000 000 евро или, в случае предпринимателя, до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 61. Срок рассмотрения жалобы

(1) Инспекция по защите данных разрешает жалобу в течение 30 дней со дня подачи жалобы в Инспекцию по защите данных.

(2) Для дополнительного выяснения обстоятельств, необходимых для разрешения жалобы, Инспекция по защите данных может продлить срок рассмотрения жалобы до 60 дней. О продлении срока необходимо письменно уведомить подавшего жалобу.

(3) Если для разрешения жалобы необходимо сотрудничество с другими заинтересованными надзорными органами, рассмотрение жалобы продлевается на разумное время, необходимое для заслушивания мнения сотрудничающих надзорных органов или представления своего мнения.

6 глава ОТВЕТСТВЕННОСТЬ

§ 62. Нарушение обязанности контролёра и обработчика

(1) За нарушение обязанности контролёра или обработчика, установленной в статьях 8, 11, 25–39, 42 и 43 Регламента (ЕС) 2016/679 Европейского парламента и Совета, –

наказывается денежным штрафом до 10 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 10 000 000 евро или до 2 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 63. Нарушение порядка сертификации

(1) За нарушение порядка сертификации, установленного в статьях 42 и 43 Регламента (ЕС) 2016/679 Европейского парламента и Совета, –

наказывается денежным штрафом до 10 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 10 000 000 евро или до 2 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 64. Нарушение порядка осуществления надзора за соблюдением кодекса поведения

(1) За нарушение порядка осуществления надзора за соблюдением кодекса поведения, установленного в части 4 статьи 41 Регламента (ЕС) 2016/679 Европейского парламента и Совета, –

наказывается денежным штрафом до 10 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 10 000 000 евро или до 2 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 65. Нарушение принципов обработки персональных данных

(1) За нарушение принципов обработки персональных данных, установленных в статье 5 Регламента (ЕС) 2016/679 Европейского парламента и Совета, а также за нарушение порядка дачи согласия субъекта данных, установленного в статьях 5–7 и 9 указанного регламента, –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 66. Нарушение прав субъекта данных

(1) За нарушение права субъекта данных, установленного в статьях 12–22 Регламента (ЕС) 2016/679 Европейского парламента и Совета, –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 67. Нарушение порядка передачи персональных данных

(1) За нарушение порядка передачи персональных данных, установленного в статьях 44–49 Регламента (ЕС) 2016/679 Европейского парламента и Совета, –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 68. Нарушение порядка, установленного в отношении особенностей обработки персональных данных

(1) За нарушение порядка, установленного в отношении особенностей обработки персональных данных главой 2 настоящего закона, –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 69. Неисполнение распоряжения Инспекции по защите данных

(1) За неисполнение распоряжения, предусмотренного в части 2 статьи 58 Регламента (ЕС) 2016/679 Европейского парламента и Совета, –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 70. Нарушение обеспечения доступа для Инспекции по защите данных

(1) За неисполнение распоряжения, выданного на основании полномочия по расследованию, установленного в части 1 статьи 58 Регламента (ЕС) 2016/679 Европейского парламента и Совета, если этим не обеспечивается доступ Инспекции по защите данных к персональным данным, иной информации или помещениям, –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до 4 процентов его общемирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше.

§ 71. Незаконная обработка персональных данных вне исполнения трудовых или служебных обязанностей

За незаконный сбор, просмотр, чтение, использование персональных данных, доступ к ним или составление запросов либо выписок о них лицом, имеющим доступ к персональным данным в силу своих трудовых или служебных обязанностей, если отсутствуют составы правонарушений, предусмотренные §§ 157 и 157¹ Уголовного кодекса, –

наказывается денежным штрафом до 200 штрафных единиц.

§ 71¹. Нарушение требований к методам таргетирования и распространения рекламы в связи с интернет-политической рекламой

(1) За нарушение требований, установленных в статьях 18 и 19 Регламента (ЕС) 2024/900 о прозрачности и таргетировании политической рекламы (ELT L, 2024/900, 20.03.2024), –

наказывается денежным штрафом до 20 000 000 евро.

(2) За то же деяние, если оно совершено юридическим лицом, –

наказывается денежным штрафом до 20 000 000 евро или до четырёх процентов его общемирового годового оборота за предыдущий финансовый год.

[RT I, 06.03.2026, 2 — вступило в силу 16.03.2026]

§ 72. Нарушение иных требований к обработке персональных данных

За нарушение требований к защите персональных данных, если отсутствуют составы правонарушений, предусмотренные §§ 62–71¹ настоящего закона и §§ 157 и 157¹ Уголовного кодекса, –

наказывается денежным штрафом до 200 штрафных единиц.

[RT I, 06.03.2026, 2 — вступило в силу 16.03.2026]

§ 73. Производство

(1) Срок давности проступков, установленных настоящей главой, составляет три года.

(2) Внесудебным органом, ведущим производство по проступкам, установленным настоящей главой, является Инспекция по защите данных.

[RT I, 11.03.2023, 1 — вступило в силу 01.11.2023]

7 глава

ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

§ 74. Регистр лиц, обрабатывающих персональные данные, и лиц, ответственных за защиту персональных данных

(1) Данные регистра лиц, обрабатывающих персональные данные, и лиц, ответственных за защиту персональных данных, хранятся в архивированном виде до пяти лет со дня вступления в силу настоящего закона. По наступлении срока данные регистра удаляются.

(2) Для доступа к данным регистра подаётся ходатайство в Инспекцию по защите данных.

(3) Запись в регистре об обработке деликатных персональных данных имеет информативное значение до окончания, установленного для нее первоначального срока действия.

§ 75. Признание утратившим силу Закона о защите персональных данных

[Из настоящего текста исключено.]

§ 76. Вступление закона в силу

Настоящий закон вступает в силу 15 января 2019 года.

¹ Директива (ЕС) 2016/680 Европейского парламента и Совета о защите физических лиц при обработке персональных данных компетентными учреждениями в целях предотвращения, расследования, выявления правонарушений и привлечения за них к ответственности или исполнения уголовных наказаний и о свободном перемещении таких данных, которой отменяется Рамочное решение Совета 2008/977/ЮВД (ELT L 119, 04.05.2016, стр. 89–131).