МИНИСТЕРСТВО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РЕСПУБЛИКИ КАРЕЛИЯ

П Р И К А З

13.03.2024

№ 140

г. ПЕТРОЗАВОДСК

Об утверждении порядка оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»

В соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее - Федеральный закон), приказом Роскомнадзора от 27 октября 2022 года №178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», в целях проведения мероприятий в области обеспечения защиты информации в Министерстве экономического развития Республики Карелия (далее – Министерство) приказываю:

1. Утвердить Порядок оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», соотношения указанного возможного вреда и принимаемых Министерством экономического развития Республики Карелия мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом (далее - Порядок), в соответствии с приложением к настоящему приказу.

2. Главному специалисту Министерства обеспечить размещение настоящего приказа на официальном сайте Министерства.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр О.А. Ермолаев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 38114F7A51839A35BB4550DD48BAA428
Владелец **Ермолаев Олег Александрович**
Действителен с 04.08.2023 по 27.10.2024

Приложение
к приказу Министерства экономического развития
Республики Карелия от ___ февраля 2024 года №____

Порядок оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», соотношения указанного возможного вреда и принимаемых Министерством экономического развития Республики Карелия мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом

1. Общие положения

1.1. Настоящий Порядок оценки возможного вреда субъектам персональных данных (далее - Порядок) определяет методику и порядок оценки вреда, который может быть причинен субъекту персональных в случае нарушения требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» (далее - Закон о персональных данных), и отражает соотношение указанного возможного вреда и принимаемых Министерством экономического развития Республики Карелия (далее - Министерство) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.

1.2. Настоящий Порядок принят в целях обеспечения соответствия процессов обработки персональных данных требованиям Закона о персональных данных и приказа Роскомнадзора от 27 октября 2022 года №178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

1.3. Настоящий документ применяется:

- к процессам Министерства, в которых ведется обработка персональных данных;

- ко всем структурным подразделениям Министерства.

1.4. Порядок предназначен для:

- ответственного за организацию обработки персональных данных (далее - Ответственный);

- комиссии по защите информации Министерства (далее - Комиссия).

1.5. Порядок действует с момента утверждения. Порядок подлежит уточнению (изменению) в случае изменения требований законодательства, изменения оценки рисков информационной безопасности. Изменения в документ вносятся путем издания новой версии.

2. Основные понятия

2.1. В настоящем Порядке используются следующие основные понятия с соответствующими определениями:

Информация - сведения (сообщения, данные) независимо от формы их представления;

Безопасность информации - состояние защищенности информации, при которой обеспечены ее конфиденциальность, доступность и целостность;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;

Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать его беспрепятственно;

Убытки - расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

Моральный вред - физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;

Оценка возможного вреда - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. Методика оценки возможного вреда субъектам персональных данных в случае нарушения Закона о персональных данных

3.1. Возможный вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.

3.2.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных.

3.2.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

3.2.4. Нарушение права субъекта персональных данных требовать от Министерства уточнения его персональных данных, их блокирования или уничтожения является нарушением целостности информации.

3.2.5. Нарушение права субъекта персональных данных на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.

3.2.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

3.2.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.

3.2.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренного федеральными законами, является нарушением конфиденциальности персональных данных.

3.3. Вред, который может быть причинен субъекту персональных данных, определяется в виде:

3.3.1. Убытков - расходов, которые субъект персональных данных, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб).

3.3.2. Недополученного дохода, который этот субъект персональных данных получил бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

3.3.3. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права субъекта персональных данных либо посягающими на принадлежащие субъекту персональных данных другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4. В оценке вреда определяется одна из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных:

3.4.1. Высокая в случаях:

- обработки сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;

- обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

- обработки персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации;

- поручения иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации;

- сбора персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.

3.4.2. Средняя в случаях:

- распространения персональных данных на официальном сайте в информационно-телекоммуникационной сети «Интернет» Министерства, а именно предоставлению персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;

- обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;

- продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор;

- получения согласия на обработку персональных данных посредством реализации на официальном сайте в информационно-телекоммуникационной сети «Интернет» функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;

- осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

3.4.3. Низкая в случаях:

- ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Закона о персональных данных;

- назначения в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником Министерства.

3.4.4. В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии подпунктами 3.4.1 - 3.4.3 пункта 3.4 настоящего Порядка могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Министерством мер

4.1. Оценка возможного вреда субъектам персональных данных осуществляется Ответственным или Комиссией, который может быть причинен субъектам персональных данных в случае нарушения требований Закона о персональных данных, соотношение указанного возможного вреда и принимаемых Министерством мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом, в соответствии с Методикой, описанной в разделе 3 настоящего Порядка.

4.2. Результаты оценки вреда оформляются актом оценки вреда.

4.3. Акт оценки вреда должен содержать:

а) наименование и адрес Министерства;

б) дату издания акта оценки вреда;

в) дату проведения оценки вреда;

г) фамилию, имя, отчество, должность Ответственного (членов Комиссии), проводивших оценку вреда, а также его (их) подпись;

д) степень вреда, которая может быть причинена субъекту персональных

данных, в соответствии с пунктами 3.4.1 - 3.4.3 раздела 3 настоящего Порядка;

е) меры, принимаемые Министерством, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом.

Акт составляется согласно форме, указанной в приложении 1 к настоящему Порядку.

4.4. Состав реализуемых Министерством мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных, определяется Ответственным или Комиссией исходя из правомерности и разумной достаточности указанных мер. При необходимости допускается привлечение сторонних экспертов в области защиты информации.

Приложение 1
к Порядку
оценки возможного вреда, который может быть
причинен субъектам персональных данных в случае
нарушения требований Федерального закона
от 27 июля 2006 года № 152-ФЗ «О персональных данных»,
соотношения указанного возможного вреда и принимаемых
Министерством экономического развития Республики Карелия мер,
направленных на обеспечение выполнения обязанностей,
предусмотренных указанным Федеральным законом

Форма Акта
оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона

АКТ
оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона

Министерство экономического развития Республики Карелия
(185028, Республика Карелия, г. Петрозаводск, ул. Андропова, д. 2)

г. Петрозаводск "__" _____ 20__ г.

1. Настоящий Акт составлен Ответственным за организацию обработки персональных данных_____(далее - Ответственный)
ФИО
/комиссией по защите информации Министерства экономического развития Республики Карелия (далее - Комиссия), назначенным(ой) приказом от «__» _____ 20__ г. № _____ «_____» /в составе:

Председатель комиссии: И.О. Фамилия, должность
_____

Члены комиссии: И.О. Фамилия, должность
_____

И.О. Фамилия, должность)
_____

с целью оценки возможного вреда субъектам персональных данных категорий, указанных в Правилах обработки персональных данных в Министерстве, утвержденных приказом от «__» _____ 20__ г. № ____ «_____».

2. В ходе проведения оценки возможного вреда субъектам персональных данных Ответственный /Комиссия руководствовался/руководствовалась следующими документами:

- Порядком оценки возможного вреда субъектам персональных данных, утвержденным приказом от «__» _____ 20__ г. № ____ «Об утверждении Порядка оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона»;
- Правилами обработки персональных данных в Министерстве, утвержденных приказом от «__» _____ 20__ г. № ____ «_____»;
- Требованиями к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», утвержденными приказом Роскомнадзора от 27 октября 2022 г. № 178.

Результаты оценки возможного вреда субъектам персональных данных приведены в таблице 1.

Таблица 1 - Исходные данные для определения необходимого уровня защищенности

№	Требования Закона, которые могут быть нарушены	Возможные нарушения безопасности информации и причинённый субъекту персональных данных вред		Уровень возможного вреда для субъекта персональных данных	Меры, принимаемые Министерством
1.	порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	в соответствии с законодательством в области защиты информации и Правилами обработки персональных данных в Министерстве
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
2.	порядок и условия применения средств защиты информации	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	в соответствии с технической документацией на систему защиты информационных систем персональных данных
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
3.	эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	программа и методика испытаний систем защиты информации
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средн	

				ий/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
4.	состояние учета машинных носителей персональных данных	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	инструкция по учету машинных носителей информации
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
5.	соблюдение правил доступа к персональным данным	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	в соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
6.	наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	мониторинг средств защиты информации на наличие фактов доступа к персональным данным
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	

		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
7.	мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	применение резервного копирования
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	
8.	осуществление мероприятий по обеспечению целостности персональных данных	Убытки (Недополученный доход) и моральный вред	+/-	Отсутствует/Низкий/Средний/Высокий	организация режима доступа к техническим и программным средствам
		Конфиденциальность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Целостность	+/-	Отсутствует/Низкий/Средний/Высокий	
		Доступность	+/-	Отсутствует/Низкий/Средний/Высокий	

Вывод:

_____

_____

Ответственный _____ _____

(Подпись) (Фамилия и инициалы)

/

Председатель комиссии: _____ _____
(Подпись) (Фамилия и инициалы)

Члены комиссии: _____ _____
(Подпись) (Фамилия и инициалы)

_____ _____
(Подпись) (Фамилия и инициалы)

_____ _____
(Подпись) (Фамилия и инициалы)