МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное учреждение науки
Федеральный исследовательский центр «Коми научный центр Уральского отделения Российской академии наук»
(ФИЦ Коми НЦ УрО РАН)

РОССИЯСА НАУКА ДА ВЫЛЫС ВЕЛӧДЧАН МИНИСТЕРСТВО

«Россияса наукаяс академиялӧн Урал юкӧнса Коми наука шӧрин» туялан удж нуӧдысь федеральнӧй шӧрин
Федеральнӧй канму сьӧмкуд наука учреждение
(ТФШ РНА УрЮ Коми НШ)

ПРИКАЗ

20.11.2024 № 316

г. Сыктывкар

Об утверждении Регламента проведения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» в ФИЦ Коми НЦ УрО РАН

В целях исполнения требований Федерального закона от 27.07.2006 № 152-Ф «О персональных данных», приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Регламент проведения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» в ФИЦ Коми НЦ УрО РАН согласно приложению к настоящему приказу.
2. Руководителям структурных и обособленных подразделений, осуществляющих обработку персональных данных в ФИЦ Коми НЦ УрО РАН:
2.1. Обеспечить ознакомление с настоящим приказом работников, участвующих в обработке персональных данных под роспись.
2.2. Акты оценки вреда, который может быть причинен субъектам персональных данных, предоставлять ответственному за организацию обработки персональных данных в ФИЦ Коми НЦ УрО РАН (Полле А.Я.) в срок до 10 декабря ежегодно.
3. Контроль исполнения настоящего приказа оставляю за собой.

Временно исполняющий обязанности директора А.Я. Полле

Приложение

Утверждено
приказом ФИЦ Коми НЦ УрО РАН
от 20.11.2024 № 316

РЕГЛАМЕНТ
проведения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» в ФИЦ Коми НЦ УрО РАН

1. Общие положения

1.1. Настоящий Регламент проведения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» в ФИЦ Коми НЦ УрО РАН (далее – Регламент, Центр), при нарушении Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон 152-ФЗ) определяет порядок проведения оценки и методику оценки вреда.

1.2. Регламент принят с целью обеспечения соответствия деятельности Центра требованиям пункта 5 части 1 статьи 18.1 Федерального закона № 152-ФЗ и приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (далее – приказ Роскомнадзора от 27.10.2022 № 178).

1.3. Регламент предназначен для членов комиссии по оценке вреда, работников Центра, ответственных за обработку персональных данных, а также иных заинтересованных лиц, имеющих доступ к персональным данным.

2. Определения и термины

2.1. Обработка персональных данных – любое действие (операция) или совокупность действий, совершаемых с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, использование, передачу, распространение, обезличивание, блокирование, уничтожение.

2.2. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.3. Персональные данные – любая информация, прямо или косвенно относящаяся к определенному или определяемому физическому лицу (субъекту данных).

2.4. Уровни вреда – уровни возможного вреда, который может быть причинен субъекту персональных данных, классифицируются на высокую, среднюю и низкую степень.

3. Область действия

Действие настоящего Регламента распространяется на все структурные и обособленные подразделения Центра.

4. Порядок проведения оценки вреда

4.1. Для проведения оценки вреда, который может быть причинен субъектам персональных данных, при нарушении Федерального закона № 152-ФЗ создается комиссия, назначаемая приказом Центра (в обособленных подразделениях – руководителем обособленного подразделения), в количестве не менее трех человек.

4.1.1. Субъекту персональных данных может быть причинен вред в форме:

а) убытков – расходов, 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;

б) морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

4.1.2. Вред субъекту персональных данных может быть причинен 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. Оценка степени вреда, который может быть причинен субъекту персональных данных, осуществляется в соответствии с приказом Роскомнадзора от 27.10.2022 № 178.

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

- неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;
- неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
- неправомерное изменение персональных данных является нарушением целостности персональных данных;
- нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;
- нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
- обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;
- неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
- принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

4.2. Комиссия для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона № 152-ФЗ.

4.3. Методика оценки возможного вреда субъекту персональных данных

4.3.1. Высокая степень вреда устанавливается в случаях:

- обработки биометрических персональных данных, если оператор использует их для установления личности субъекта, которому они принадлежат. Исключение – случаи, когда обработка таких данных прямо предусмотрена законом;
- обработки персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости. Исключение – случаи, установленные федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;
- обработки персональных данных несовершеннолетних для исполнения или заключения договора, стороной которого такой несовершеннолетний является в случаях, не предусмотренных законом;

- обезличивания персональных данных (в том числе для проведения оценочных (скоринговых) исследований), оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также других исследований, не предусмотренных пунктом 9 части 1 статьи 6 Закона Федерального закона № 152-ФЗ;

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

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

4.3.2. Средняя степень вреда устанавливается в случаях:

- распространения персональных данных на официальном сайте оператора, а также их предоставление неограниченному кругу лиц, кроме случаев, установленных пунктом 1.1. статьи 3 Федерального закона № 152-ФЗ;

- обработки персональных данных в целях, отличных от первоначальной цели сбора (например, если изначально предполагались сбор и хранение, а затем потребовалась их передача третьему лицу);

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

- получения согласия на обработку персональных данных на сайте оператора, который не предусматривает дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;

- обработки персональных данных с получением согласия на передачу права их обработки третьими лицам в целях, которые несовместимы с целями сбора таких данных (часть 2 статьи 5 Федерального закона № 152-ФЗ).

4.3.3. Низкая степень вреда устанавливается в случаях:

- ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Федерального закона № 152-ФЗ (например, справочники, адресные книги и т. д.);

- назначения ответственным за обработку персональных данных лица, которое не является штатным сотрудником оператора.

При выявлении факторов, относящихся к разным степеням риска, выбирается более высокая степень.

5. Документирование результатов

5.1. Результаты оценки вреда, который может быть причинен субъекту персональных данных, оформляются актом оценки вреда по форме согласно приложению № 1 к настоящему Регламенту).

5.2. Акт оценки вреда содержит:

- наименование или Ф.И.О. (при наличии) и адрес оператора персональных данных;
- дата издания акта оценки вреда;
- дата проведения оценки вреда;
- фамилия, имя, отчество (при наличии), должность лиц (лица), проводивших оценку вреда, а также их (его) подпись;

5.3. Акт оформляют как на бумажном носителе, так и в электронной форме. Бумажный акт подписывается лицом, которое проводило оценку вреда. Электронный акт должен быть подписан усиленной квалифицированной электронной подписью (далее – УКЭП).

5.4. Допускается оформление одного акта на несколько категорий субъектов персональных данных.

5.5. Проведение оценки проводится:

- Планово – не реже одного раза в год (до 1 декабря текущего года).
- Внепланово – в случае поступления оператору информации о неправомерной (незаконной) обработке персональных данных оператором, а именно:

• запроса субъекта персональных данных или его представителя;
• запроса Роскомнадзора;
• требования Роскомнадзора о представлении уведомления;
• запроса иного заинтересованного лица.

Оценка вреда осуществляется также для определения типа угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных.

6. Меры по снижению риска

6.1. В целях минимизации риска причинения вреда субъектам данных Центр разрабатывает и внедряет комплекс превентивных мер, включающих:

- регулярные аудиты безопасности;
- обучение персонала по вопросам защиты данных.
- введение многофакторной аутентификации и иных технических средств защиты.

6.2. В случае выявления угрозы нарушения безопасности данных Центр обязан незамедлительно принять меры по устранению рисков, уведомив при этом субъекты данных в соответствии с законодательством.

7. Пересмотр Регламента

7.1. Регламент подлежит пересмотру не реже одного раза в три года, а также в случае:

- изменений в законодательстве;
- существенных изменений в процессах обработки данных;
- выявления новых рисков или угроз.

7.2. Пересмотр Регламента осуществляется комиссией, назначенной директором Центра. Итоги пересмотра утверждаются приказом и доводятся до сведения всех заинтересованных сторон.

8. Ответственность

8.1. Ответственность за соблюдение требований настоящего регламента несут руководители подразделений, участвующих в обработке персональных данных, и члены комиссии по оценке вреда.

8.2. В случае нарушения требований регламента к виновным лицам могут быть применены дисциплинарные меры в соответствии с внутренними нормативными актами Центра и законодательством Российской Федерации.

Приложение
к Регламенту проведения оценки вреда, который
может быть причинен субъектам персональных
данных в случае нарушения Федерального закона
«О персональных данных» в ФИЦ Коми НЦ УрО РАН

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное
бюджетное учреждение науки
Федеральный исследовательский центр
«Коми научный центр Уральского отделения
Российской академии наук»
(ФИЦ Коми НЦ УрО РАН)

РОССИЯСА НАУКА ДА ВЫЛЫС ВЕЛӧДЧАН МИНИСТЕРСТВО

«Россияса наукаяс академиялӧн
Урал юкӧнса Коми наука шӧрин»
туялан удж нуӧдысь федеральнӧй шӧрин
Федеральнӧй канму
сьӧмкуд наука учреждение
(ТФШ РНА УрЮ Коми НШ)

АКТ

_____ № _____

г. Сыктывкар

оценки вреда, который может быть
причинен субъектам персональных данных
в случае нарушения Федерального закона
«О персональных данных»

Акт составлен комиссией, действующей на основании приказа ФИЦ Коми НЦ УрО РАН от ___. _____202_ года № ____, в составе:

председателя комиссии:
_____
членов комиссии:
_____
_____,

Комиссия, во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» провела оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и установила следующее:

1. Персональные данные обрабатываются в следующих информационных системах ФИЦ Коми НЦ УрО РАН:

- Информационная система «Кадры»

2. ФИЦ Коми НЦ УрО РАН осуществляет обработку следующих персональных данных:

- специальных категорий персональных данных - состояния здоровья, сведений о судимости для целей трудоустройства на работу и соблюдения трудового законодательства;

- 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. Степень вреда, который может быть причинен субъектам персональных данных - высокая.

4. Защищенность информации в информационных системах ФИЦ Коми НЦ УрО РАН соответствует требованиям, установленным требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119

Настоящий акт составил:
Председатель комиссии:

_____ ФИО

Содержание акта подтверждаем

_____ ФИО

_____ ФИО