

Приложение №6
к приказу КОГПОБУ «КЛПК»
от 30.12.2022 г. № 138-д

ПОРЯДОК
оценки вреда субъектам персональных данных

Киров, 2022

Содержание

1. Общие положения.....	3
1.1. Назначение	3
1.2. Цель разработки Порядка	3
1.3. Область применения	3
1.4. Аудитория	3
1.5. Нормативные ссылки	3
1.6. Срок действия и порядок внесения изменений	3
2. Порядок проведения оценки вреда субъекту персональных данных.....	4
Приложение № 1. Типовая форма акта оценки вреда субъекту персональных данных	6

1. Общие положения

1.1. Назначение

Настоящий Порядок оценки вреда субъектам персональных данных (далее – Порядок) определяет правила оценки вреда, который может быть причинён субъекту персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в «*Название организации*» (далее – Организация), а также форму акта оценки вреда.

1.2. Цель разработки Порядка

Настоящий Порядок принят в целях обеспечения соответствия процессов обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Область применения

Настоящий документ применяется:

- к процессам Организации, в которых ведется обработка персональных данных.
- ко всем обособленным подразделениям Организации;
- ко всем офисам и удаленным сотрудникам, независимо от их местоположения.

1.4. Аудитория

Порядок предназначен для следующих категорий сотрудников Организации:

- сотрудник, ответственный за организацию обработки персональных данных;
- руководители подразделений, обрабатывающих персональные данные;
- владельцы процессов, связанных с обработкой персональных данных;
- лица, которым Организацией поручено обрабатывать персональные данные.

Под сотрудниками в настоящем Порядке понимаются лица, состоящие в трудовых или договорных отношениях с Организацией.

Перечисленные сотрудники перед предоставлением доступа к персональным данным должны быть ознакомлены с настоящим документом в соответствии с *Порядком предоставления доступа к персональным данным*.

1.5. Нормативные ссылки

Положение разработано в целях реализации требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с требованиями 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».

1.6. Срок действия и порядок внесения изменений

Порядок действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим. Порядок подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, требований со стороны партнеров, изменения оценки рисков информационной безопасности. Изменения в документ вносятся путем издания новой версии и ознакомления с ним сотрудников, а также лиц, осуществляющих обработку персональных данных.

Срок хранения после прекращения действия: постоянно.

2. Порядок проведения оценки вреда субъекту персональных данных

2.1. Организация для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

2.1.1. Высокую 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;

обезличивания персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований;

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

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

2.1.2. Среднюю в случаях:

распространения персональных данных на официальном сайте в информационно-телекоммуникационной сети «Интернет» оператора, а равно предоставление 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.

2.1.3. Низкую 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 оператора.

2.2. В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии подпунктами 2.1.1 - 2.1.3 пункта 2 настоящего Порядка могут быть причинены различные степени вреда, подлежит применению **более высокая степень вреда**.

2.3. Оценка вреда субъекту персональных данных осуществляется ответственным за организацию обработки персональных данных либо комиссией, образуемой Организацией.

2.3.1. По результатам оценки степени вреда субъекту персональных данных оформляется акт оценки вреда субъекту персональных данных (далее – Акт).

2.3.2 Акт может быть оформлен на бумажном носителе, подписанном собственноручно лицом (лицами), производившими оценку, либо в виде электронного документа, подписанного в соответствии электронной подписью.

2.3.3. Типовая форма Акта приведена в Приложении № 1.

2.3.4. Оценка вреда подлежит пересмотру **не реже 1 раза в год**.

Приложение № 1. Типовая форма акта оценки вреда субъекту персональных данных

УТВЕРЖДАЮ

<Должность>

<Название организации>

_____/_____
« ____ » _____ 20__ г.

АКТ № ____

оценки вреда субъектам персональных данных

г. Киров

« ____ » _____ 20__ г.

1. Настоящий Акт составлен Комиссией по обеспечению безопасности персональных данных КОГПОБУ «КЛПК» назначенной 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 вреда субъекту персональных данных.

2. Оценка вреда субъектам персональных данных проводится « ____ » _____ 20__ г.

3. Исходные данные для определения оценки вреда субъектам персональных данных:
Оператором персональных данных

(наименование юридического лица/ФИО физического лица)

(адрес оператора персональных данных)

осуществляется:

№/№	Действие	Значение показателя (да/нет)
Высокая степень вреда		
1	Обработка 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	
2	Обработка 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	

№/№	Действие	Значение показателя (да/нет)
3	Обработка 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	
4	Обезличивание персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований	
5	Поручение иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации	
6	Сбор персональных данных с использованием баз данных, находящихся за пределами Российской Федерации	
Средняя степень вреда		
1	Распространение персональных данных на официальном сайте в информационно-телекоммуникационной сети «Интернет» оператора, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки	
2	Обработка персональных данных в дополнительных целях, отличных от первоначальной цели сбора	
3	Продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор	
4	Получение 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	
5	Осуществление 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	
Низкая степень вреда		
1	Ведение общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»	
2	Назначения в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником оператора	

По результатам проведения оценки определяется _____ степень вреда, который
(высокая, средняя, низкая)

может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /

_____ / _____ /