Утверждено Приказом

Индивидуального предпринимателя

Трофимова Я.А.

№ 03/25 от 08.04.2025г.

**Положение**

**о недопущении Оператором**

**вреда при обработке персональных данных**

|  |  |
| --- | --- |
|  |  |

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Положение об обработке персональных данных издано и применяется Индивидуальным предпринимателем Трофимовым Ярославом Алексеевичем ИНН 021202992345 (далее - Положение и Оператор соответственно) в соответствии с [п. 2 ч. 1 ст. 18.1](https://login.consultant.ru/link/?req=doc&base=LAW&n=482686&date=08.04.2025&dst=100360&field=134) Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных".

1.2. Настоящее Положение устанавливает процедуры, направленные на выявление причин, которые могут повлечь причинение вреда субъекту персональных данных и/или Оператору и их предотвращение, а также на устранение последствий такого вреда при обработке персональных данных.

1.3. Под вредом для целей настоящего Положения понимается моральный вред и/или материальный ущерб субъекта персональных данных и/или Оператора, который реально причинен или может быть причинен в случае нарушения Оператором требований Федерального [закона](https://login.consultant.ru/link/?req=doc&base=LAW&n=482686&date=08.04.2025) от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - вред). Размер вреда определяется в соответствии со [ст. ст. 15](https://login.consultant.ru/link/?req=doc&base=LAW&n=482692&date=08.04.2025&dst=100091&field=134), [151](https://login.consultant.ru/link/?req=doc&base=LAW&n=482692&date=08.04.2025&dst=100875&field=134), [152](https://login.consultant.ru/link/?req=doc&base=LAW&n=482692&date=08.04.2025&dst=690&field=134), [1101](https://login.consultant.ru/link/?req=doc&base=LAW&n=493202&date=08.04.2025&dst=102766&field=134) Гражданского кодекса Российской Федерации. Соотношение вреда и принимаемых Оператором мер, направленных на предупреждение, недопущение и/или устранение его последствий, установлены настоящим Положением.

1.4. Недопущение вреда является одним из направлений обеспечения общей безопасности Оператора и представляет собой комплекс правовых, организационных и технических мер. Правовые меры состоят из изучения и применения законодательства по вопросам недопущения вреда, разработки локальных актов и их применения в данной сфере деятельности Оператора. Организационные меры включают тщательный отбор, обучение и расстановку кадров, повышение их мотивации в вопросах недопущения вреда. Технические меры объединяют создание условий и реализацию мероприятий по недопущению вреда, в том числе:

1.4.1. Обеспечение сохранности собственности Оператора, в том числе материальных носителей информации, путем установления и поддержания соответствующих режимов безопасности.

1.4.2. Недопущение попадания конфиденциальной информации Оператора, в том числе информации, составляющей коммерческую и служебную тайны, неуполномоченным лицам путем выделения специальных помещений для обработки и хранения персональных данных.

1.4.3. Обеспечение информационной безопасности Оператора, бесперебойного функционирования технических средств обработки персональных данных. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1.4.4. Обеспечение физической защиты объектов, находящихся на балансе Оператора, путем установления внутриобъектового и режима пожаробезопасности.

1.4.5. Обеспечение физической защиты работников Оператора при исполнении ими служебных обязанностей, комфортного морально-психологического климата и обстановки делового сотрудничества среди работников Оператора.

1.4.6. Обеспечение личной безопасности руководителей Оператора.

1.4.7. Незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.4.8. Постоянный контроль за обеспечением уровня защищенности персональных данных.

1.5. В целях недопущения вреда Оператор самостоятельно отвечает за организацию обработки персональных данных либо назначает ответственного по направлению.

1.5.1. Ответственный по направлению получает указания непосредственно от Оператора и подотчетен ему.

1.5.2. Ответственный по направлению осуществляет внутренний контроль за соблюдением другими работниками Оператора законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

1.5.3. Ответственный по направлению проводит ориентировочную оценку размера вреда, устанавливает, какие меры были приняты в целях недопущения вреда, и их соотношение.

1.6. Руководящими документами при обработке персональных данных в первую очередь являются [ст. 19](https://login.consultant.ru/link/?req=doc&base=LAW&n=482686&date=08.04.2025&dst=100368&field=134) Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", [Постановление](https://login.consultant.ru/link/?req=doc&base=LAW&n=137356&date=08.04.2025) Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", [Положение](https://login.consultant.ru/link/?req=doc&base=LAW&n=496432&date=08.04.2025&dst=100010&field=134) об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 № 687, "Методический [документ](https://login.consultant.ru/link/?req=doc&base=LAW&n=378330&date=08.04.2025). Методика оценки угроз безопасности информации", утв. ФСТЭК России 05.02.2021.

1.7. Настоящее Положение и изменения к нему утверждаются Оператором и вводятся приказом Оператора.

1.8. Ответственный по направлению, сотрудники Оператора, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под роспись до начала работы с настоящим Положением и изменениями к нему, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на Операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности.

1.9. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного Оператором или ответственным по направлению.

1.10. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в [п. 1.9](#P39) настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) Оператора.

1.11. В целях предотвращения и уменьшения вреда при обнаружении нарушений порядка предоставления персональных данных Оператор незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

1.12. Режим конфиденциальности персональных данных Оператор обеспечивает в соответствии с принятыми локальными актами по вопросам конфиденциальности.

1.13. Опубликование или обеспечение иным образом неограниченного доступа к настоящему Положению, иным документам, определяющим политику Оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных Оператор проводит в соответствии с Положением Оператора о раскрытии информации.

1.14. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

**2. СТРУКТУРНЫЕ ПОДРАЗДЕЛЕНИЯ ОПЕРАТОРА ПО НЕДОПУЩЕНИЮ ВРЕДА**

**ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

2.1. Обработку персональных данных, в том числе реализацию общих мер по недопущению вреда, организует Оператор лично или лицо ответственное по направлению.

2.2. Лицо ответственное по направлению находится в непосредственном подчинении Оператора.

2.3. Реализация специальных мер по недопущению вреда возложена на Оператора или лица ответственного по направлению.

2.4. Оператор или лицо ответственное по направлению:

1) координирует действия всех подразделений и работников Оператора по вопросам недопущения вреда;

2) организует правовое, методическое и техническое сопровождение обработки персональных данных сотрудниками Оператора с целью недопущения вреда;

3) рассматривает обращения и запросы субъектов персональных данных, которым причинен вред, принимает меры по устранению его последствий.

**3. ПРОЦЕДУРЫ ПО НЕДОПУЩЕНИЮ ВРЕДА**

**И ПО УСТРАНЕНИЮ ЕГО ПОСЛЕДСТВИЙ**

3.1. Процедуры, направленные на предупреждение вреда:

3.1.1. Соблюдение сотрудниками Оператора установленных законодательством и локальными актами Оператора регламентов получения, обработки, хранения, предоставления и распространения персональных данных (далее - регламент).

3.1.2. Выявление нарушений со стороны сотрудников и/или субъектов персональных данных установленных регламентов и доведение информации о нарушениях до Оператора.

3.1.3. Разработка и утверждение Оператором правил определения возможных форм причинения вреда и оценки его размера.

3.1.4. Ознакомление сотрудников Оператора с правилами определения возможных форм причинения вреда и оценки его размера.

3.1.5. Предупреждение субъектов персональных данных о рисках причинения вреда в ходе обработки персональных данных.

3.1.6. Внеочередной инструктаж всех сотрудников Оператора по вопросам недопущения вреда в случае обнаружения факта причинения вреда.

3.2. Процедуры, направленные на устранение вреда:

3.2.1. Своевременное обнаружение допущенных нарушений регламентов и незамедлительное пресечение таких нарушений.

3.2.2. Оценка уже причиненного вреда, фиксация мер, принятых Оператором по недопущению вреда, и их сопоставление.

3.2.3. Информирование субъектов персональных данных о допущенных нарушениях, о рисках и о подлежащих принятию мерах.

3.2.4. Компенсация причиненного вреда на основе определенных Оператором форм причинения вреда и оценки его размера.

3.2.5. Привлечение к ответственности сотрудников Оператора, допустивших причинение вреда.

3.3. Процедуры, направленные на устранение последствий вреда:

3.3.1. Восстановление деловой репутации Оператора.

3.3.2. Корректировка регламентов и программ обучения сотрудников.

**4. ОБЯЗАННОСТИ ОПЕРАТОРА И ЕГО РАБОТНИКОВ**

4.1. Оператор:

- оказывает содействие лицу ответственному по направлению в выполнении им своих обязанностей;

- организует устранение выявленных нарушений законодательства Российской Федерации, нормативных правовых актов уполномоченного федерального органа исполнительной власти, внутренних документов, а также причин и условий, способствовавших совершению нарушения;

- организует рассмотрение случаев причинения вреда и выплату компенсаций.

4.2. Лицо ответственное по направлению:

- оказывает содействие Оператору в выполнении им своих обязанностей в части работы с персональными данными;

- незамедлительно доводят до сведения Оператора информацию обо всех случаях причинения вреда другими сотрудниками Оператора или контрагентами Оператора.

**5. КОНТРОЛЬ, ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ**

**ИЛИ НЕИСПОЛНЕНИЕ ПОЛОЖЕНИЯ**

5.1. Контроль за исполнением Положения возложен на Оператора.

5.2. Лица, нарушающие или не исполняющие требования Положения, привлекаются к дисциплинарной, административной ([ст. ст. 5.39](https://login.consultant.ru/link/?req=doc&base=LAW&n=483238&date=08.04.2025&dst=2057&field=134), [13.11](https://login.consultant.ru/link/?req=doc&base=LAW&n=483238&date=08.04.2025&dst=101137&field=134), [13.14](https://login.consultant.ru/link/?req=doc&base=LAW&n=483238&date=08.04.2025&dst=101154&field=134) Кодекса Российской Федерации об административных правонарушениях) или уголовной ответственности ([ст. ст. 137](https://login.consultant.ru/link/?req=doc&base=LAW&n=500185&date=08.04.2025&dst=100774&field=134), [272](https://login.consultant.ru/link/?req=doc&base=LAW&n=500185&date=08.04.2025&dst=969&field=134), [272.1](https://login.consultant.ru/link/?req=doc&base=LAW&n=500185&date=08.04.2025&dst=3306&field=134), [274](https://login.consultant.ru/link/?req=doc&base=LAW&n=500185&date=08.04.2025&dst=987&field=134) Уголовного кодекса Российской Федерации).

5.3. Лицо ответственное по направлению несет персональную ответственность.