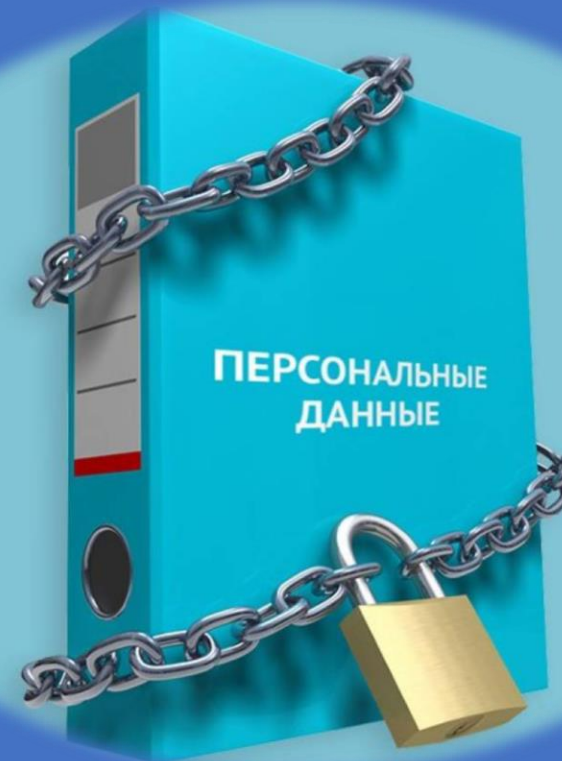


Персональные данные в НКО: основы и риски

Спикер: Виктория Павлюк

***С использованием материалов Ассоциации
«Юристы за гражданское общество»**



Нормативные правовые акты в области ПДн

1

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»

2

Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»

3

Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

4

Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

5

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.12.2021 N 253 «Об утверждении формы проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами»

Нормативные правовые акты в области ПДн

- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 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"»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»

Уполномоченные органы власти

- **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)** – уполномоченный орган по защите прав субъектов персональных данных;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК) – вопросы применения технических средств защиты информации;
- Федеральная служба безопасности (ФСБ) – вопросы применения средств криптографической защиты информации (шифрования);
- Государственные инспекции труда (ГИТ) – вопросы соблюдения работодателями требований по защите персональных данных работников (гл. 14 Трудового кодекса РФ);
- Органы прокуратуры – надзор за соблюдением законов.

Персональные данные

– любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Виды персональных данных

Общие

Биометрические

Специальные



Специальные категории ПДн

касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, **состояния здоровья**, интимной жизни, сведения о судимости.



Биометрические ПДн

сведения, 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.

Оператор ПДн

Оператор – государственный орган, муниципальной орган, юридическое или физическое лица, 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

Обработка персональных данных

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Цель обработки персональных данных

- Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей – **этим определяется и срок обработки;**
- Не допускается обработка ПДн, несовместимая с целями сбора ПДн – **нельзя что-либо делать с ПДн «заодно» и «про запас»;**
- Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки – **они не должны быть избыточными.**

Случаи обработки ПДн

- 1. Согласие субъекта ПДн;**
2. Исполнение международных договоров РФ или выполнение оператором возложенных на него законом обязанностей;
3. Осуществление правосудия;
4. Исполнительное производство;
5. Предоставление государственных или муниципальных услуг;
- 6. Заключение и исполнение договора, стороной которого является субъект ПДн;**
7. Защита жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия невозможно;

Случаи обработки ПДн 2 часть

- 8.** Осуществление прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- 9.** Профессиональная деятельность журналиста и СМИ, научная, литературная или иная творческая деятельность;
- 10.** Статистические или иные исследовательские цели, при условии обязательного обезличивания ПДн;
- 11.** Обезличенные ПДн при внедрении технологий искусственного интеллекта;
- 12.** ПДн подлежат опубликованию или обязательному раскрытию в соответствии с законом.

Виды согласий

В соответствии с действующим законодательством можно выделить два отдельных согласия:

- 1) **Согласие на обработку персональных данных** (статья 9 Федерального закона «О персональных данных»)
- 2) **Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения** (статья 10.1 Федерального закона «О персональных данных»).

Согласие на обработку персональных данных.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем **в любой позволяющей подтвердить факт его получения форме**, если иное не установлено федеральным законом.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на **оператора**.

В случаях, предусмотренных федеральным законом (**обработка биометрических данных, специальных данных, трансграничная передача**), обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя информацию, предусмотренную статьей 9 Федерального закона «О персональных данных».

1. ФИО, адрес субъекта ПДн, номер и сведения о выдаче основного документа, удостоверяющего его личность;
2. ФИО, адрес представителя субъекта ПДн, номер и сведения о выдаче основного документа, удостоверяющего его личность, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя;
3. Наименование или ФИО и адрес оператора, получающего согласие субъекта ПДн;
4. Цель обработки ПДн;
5. Перечень ПДн, на обработку которых дается согласие субъекта ПДн;
6. Наименование или ФИО и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;
7. Перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
8. Срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
9. Подпись субъекта ПДн.

В марте 2021 вступили в силу важные изменения в Федеральный закон «О персональных данных». Появился термин «персональные данные, разрешенные для распространения» – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Также в правовом поле появился новый документ – согласие на обработку персональных данных, разрешенных для распространения. Порядок работы с ним изложен в статье 10.1 Федерального закона «О персональных данных» и Приказе Роскомнадзора от 24.02.2021 N 18.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется **отдельно** от иных согласий субъекта персональных данных на обработку его персональных данных.

1. ФИО субъекта ПДн (или его представителя);
2. Контактная информация (телефон, e-mail или почтовый адрес);
3. Сведения об операторе-организации (наименование, адрес в ЕГРЮЛ, ИНН, ОГРН);
4. Сведения об операторе-физлице (ФИО, место жительства или пребывания);
5. Сведения об операторе-ИП (ФИО, ИНН, ОГРН);
6. Сведения об информационных ресурсах (http/https, www, домен и имя страницы);
7. Цель (цели) обработки ПДн;
8. Категории и перечень ПДн (ПДн, специальные категории ПДн, биометрические ПДн);
9. Категории и перечень ПДн, для обработки которых субъект устанавливает условия и запреты, и их перечень (по желанию субъекта);
10. Условия передачи ПДн по внутренней сети оператора, через интернет, либо без передачи (по желанию субъекта);
11. Срок действия согласия.



Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются **только с согласия этого гражданина**. После смерти гражданина его изображение может использоваться только с согласия детей и пережившего супруга, а при их отсутствии - с согласия родителей. Такое согласие не требуется в случаях, когда:

- 1)** использование изображения осуществляется в государственных, общественных **(ППВС №16 от 15.06.10)** или иных публичных интересах **(ППВС №25 от 23.06.15)**;
- 2)** **изображение гражданина получено при съемке, которая проводится в местах**, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;
- 3)** гражданин позировал за плату.

- Перечень ПДн;
- Перечень действий (операций);
- Цели обработки;
- Конфиденциальность;
- Хранение на территории РФ;
- Представление сведений по запросу оператора;
- Безопасность и требования к защите ПДн.





Меры, предпринимаемые оператором ПДн

1. Назначение ответственного за обработку ПДн;
2. Издание документов, определяющих политику оператора в отношении обработки ПДн и локальных актов по вопросам обработки ПДн;
3. Применение правовых, организационных и технических мер по обеспечению безопасности ПДн;
4. Осуществление внутреннего контроля;
5. Оценка возможного вреда;
6. Ознакомление работников с положениями законодательства и локальных актов по вопросам ПДн.



Документ, определяющий политику оператора ПДн в отношении обработки ПДн

- Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.
- Рекомендации Роскомнадзора по составлению политики в отношении обработки ПДн



Содержание политики обработки ПДн

Для каждой цели обработки ПДн:

- категории и перечень обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- способы, сроки их обработки и хранения;
- порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований.



Меры по обеспечению безопасности ПДн

1. Определение угроз безопасности;
2. Применение организационных и технических мер безопасности, обеспечивающих уровни защищенности;
3. Применение сертифицированных средств защиты информации;
4. Оценка эффективности принимаемых мер;
5. Учет машинных носителей ПДн;
6. Обнаружение фактов несанкционированного доступа к ПДн;
7. Восстановление модифицированных или уничтоженных ПДн;
8. Установление правил доступа к ПДн и учета всех действий с ними;
9. Контроль за принимаемыми мерами и уровнем защищенности.

Уведомление о деятельности в Роскомнадзор

Оператор **до начала обработки** персональных данных **обязан уведомить** уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев обработки ПДн:

- 1.** включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- 2.** в случае, если оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;
- 3.** обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Порядок подачи уведомления в Роскомнадзор

Уведомление заполняется на сайте Роскомнадзора:

<https://pd.rkn.gov.ru/operators-registry/notification/form/> (при заполнении можно руководствоваться Приказом Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»).

Уведомление может быть направлено тремя способами:

- в бумажном виде;
- в электронном виде с использованием усиленной ЭЦП;
- в электронном виде с использованием средств аутентификации ЕСИА (портал Госуслуг).

Трансграничная передача ПДн



Инциденты (утечка)

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан уведомить Роскомнадзор:

- **24 часа** – об инциденте, о предполагаемых причинах, о предполагаемом вреде, о принятых мерах по устранению последствий, об уполномоченном лице;
- **72 часа** – о результатах внутреннего расследования, о виновных лицах.

Ответственность за нарушения в сфере ПДн (с 01.05.2025 г.)

- Статья 13.11 КоАП РФ (12 составов, штраф от 30 тыс. до 18 млн. руб.)
- Статья 19.7 КоАП РФ (Неподача уведомления в Роскомнадзор – от 3 до 5 тыс. руб.)
- Статья 19.5 КоАП РФ (Неисполнение предписания – от 10 до 20 тыс. руб., а для должностных лиц – дисквалификация)

Готовимся к проверке Роскомнадзора

https://base.garant.ru/403583410/#block_1000 – проверочный лист на основании которого можно выделить основные моменты, на которые **следует обратить внимание при подготовке к проверке:**

1. Регистрация в Реестре операторов.
2. Назначение ответственного за организацию обработки персональных данных.
3. Разработка и обеспечение неограниченного доступа к Политике по обработке персональных данных.
4. Локальные нормативные акты.
5. Организация хранения и своевременное уничтожение персональных данных.
6. Наличие согласий на обработку персональных данных (в случае отсутствия иных правовых оснований), соответствие письменных согласий требованиям ч. 4 ст. 9 Федерального закона «О персональных данных».
7. Обеспечение надлежащей защиты персональных данных, обрабатываемых в информационных системах.
8. Ознакомление сотрудников, работающих с персональными данными, с требованиями законодательства, а также с локальными актами по вопросам обработки персональных данных.
9. Своевременное реагирование на жалобы, требования и запросы со стороны субъектов персональных данных (в случае их поступления).
10. Прекращение обработки персональных данных в случаях, предусмотренных законом.



Для создания документов, которые проверяет РКН, вы можете воспользоваться сервисом [152DOC](#). Он поможет подготовить Политику обработки персональных данных, Согласие на обработку ПДн и все необходимые регламенты и приказы.

СПАСИБО



**Защита
персональных
данных**