The image features a central black circle containing white text. This central circle is surrounded by several concentric, thin grey circles. Scattered around these circles are various geometric shapes: small black dots, larger grey dots, and a single black square. The overall composition is minimalist and modern, with a focus on geometric forms and a limited color palette of black, white, and grey.

**Персональные
данные и
профсоюзные
организации:
ТОЧКИ
соприкосновения**



1

Что такое персональные данные и зачем их защищать

2

Кто отвечает за обработку персональных данных в профсоюзной организации

3

Как организовать обработку персональных данных внутри профсоюзной организации

4

Передал персональные данные третьему лицу: что дальше?

5

Сколько и где хранить персональные данные, и как их уничтожить

6

Сессия вопросов и ответов



**Что такое
персональные
данные и зачем их
защищать**

Определения понятия «персональные данные»

- Любая информация об определенном или поддающемся определению физическом лице (п.«а» ст.2 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 №108)
- Любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных) (п.1.ст.4 GDPR)
- Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п.1 ст.3 ФЗ-152)
- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (п.1 Перечня сведений конфиденциального характера, утвержденного Указом Президента РФ от 06.03.1997 №188)

Матрица персональных данных

- Если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными, даже если они не включают в себя данные документов, удостоверяющих личность.
- При этом данные нельзя считать персональными в том случае, если без использования дополнительной информации они не позволяют идентифицировать физическое лицо.

Данный подход допустимо рассматривать как учитывающий баланс интересов всех участников отношений.

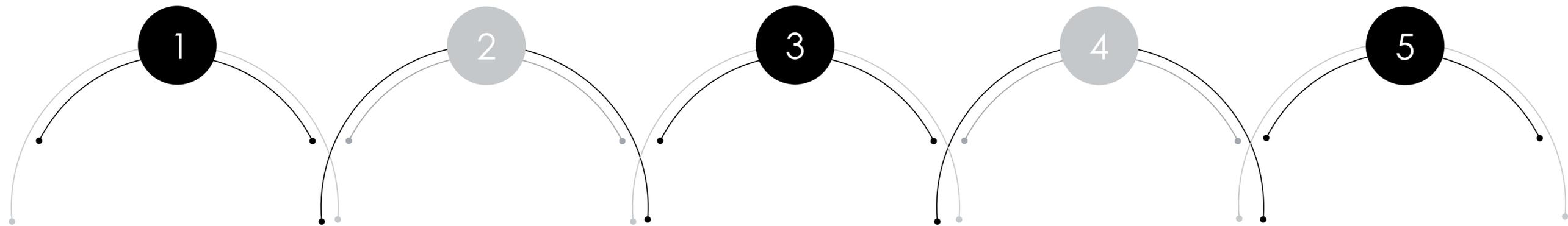
НЕ являются Персональными данными

К числу данных, которые не могут рассматриваться **по отдельности друг от друга** в качестве персональных: фамилия, имя, отчество; адрес проживания; адрес электронной почты; номер контактного телефона; дата рождения.

Другие идентификаторы (например, табельный номер) сами по себе не определяют однозначно конкретное физическое лицо. Такие данные должны быть отнесены к персональным данным только в том случае, если они хранятся и обрабатываются совместно с идентификаторами, которые сами по себе определяют физическое лицо.

Вопрос:

Номер телефона –
это персональные данные или нет?



Номер телефона и адрес электронной почты – персональные данные, но не всегда*

Абонентский номер или адрес электронной почты **могут быть** признаны персональными данными в случае, когда такая информация относится к прямо или косвенно определенному или определяемому физическому лицу.

Например, абонентский номер, принадлежащий юридическому лицу, не может рассматриваться в качестве персональных данных (Письмо Минкомсвязи России от 07.07.2017 № П11-15054-ОГ «О разъяснении норм федерального законодательства»).

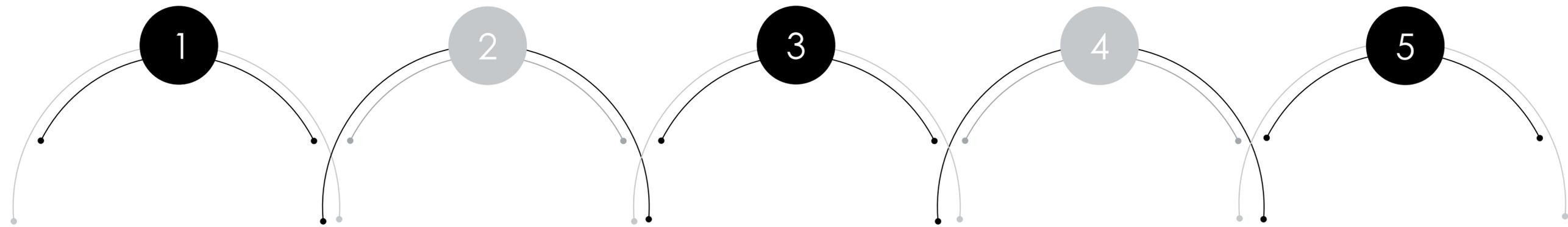
*учитывая матрицу персональных данных

Персональные данные-идентификаторы

Среди массива данных о субъекте можно выделить данные-идентификаторы, которые, как правило, присваивает государство, и которые позволяют **однозначно идентифицировать лицо**.

Вопрос:

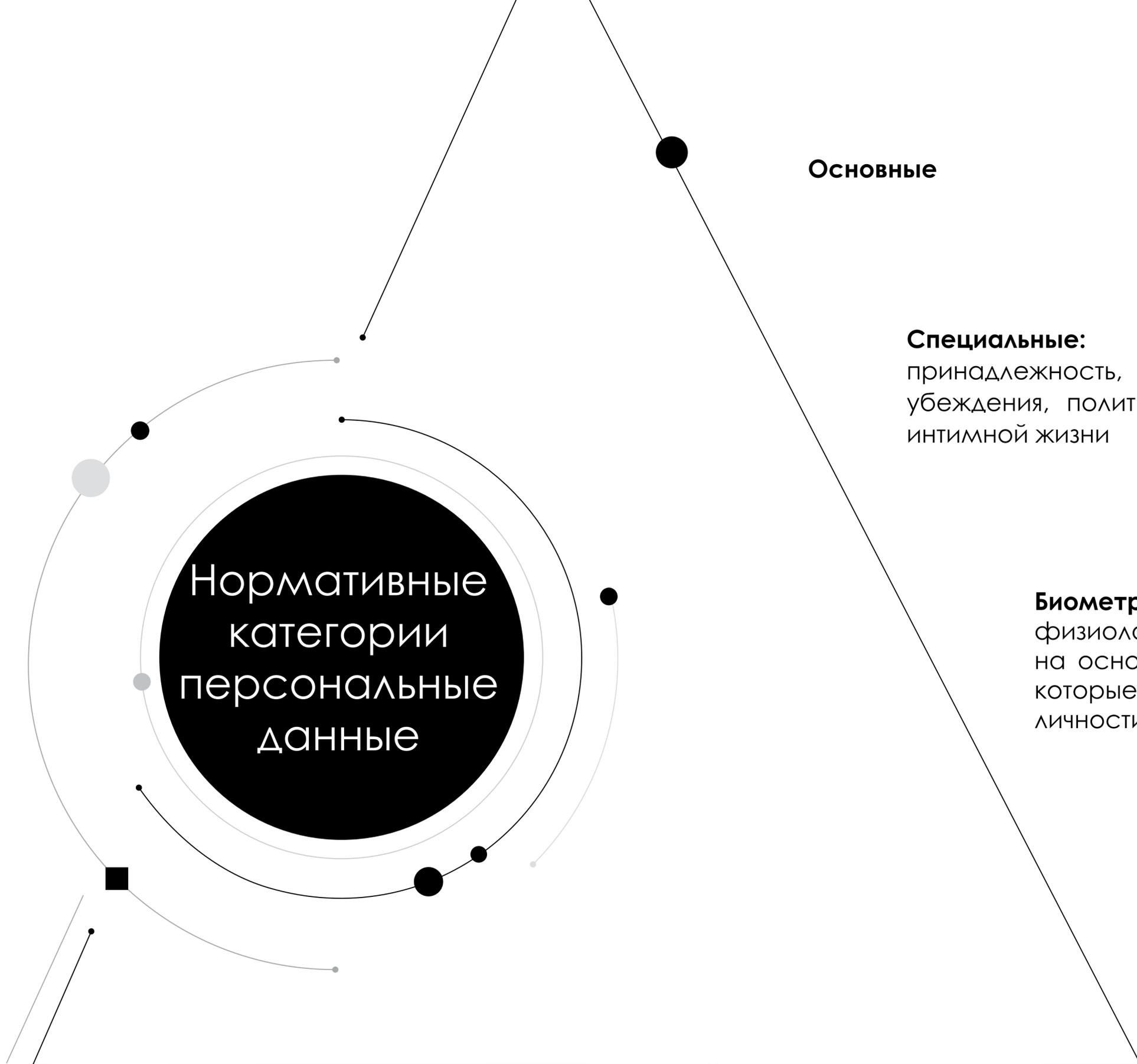
Вася Пупкин, 1990 г.р., инженер –
персональные данные или нет?



Персональные данные с вероятностью совпадения

Персональными считаются данные, несмотря на то, что в их отношении **сохраняется некоторый аспект вероятного совпадения:**

- Фамилия, имя, отчество, дата рождения + иная информация о субъекте (например: место рождения; адрес проживания; наименование должности; сведения о семейном, социальном, имущественном положении; сведения об образовании, квалификации, профессии; контактные сведения и т.д.);
- Фамилия, имя, отчество (возможно, фамилия и инициалы) + любая информация, выделяющая субъекта из уже ограниченного круга лиц



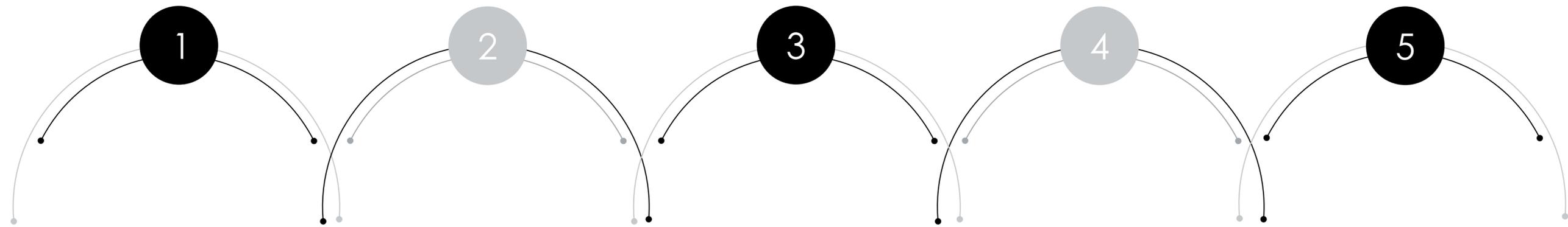
Основные

Специальные: расовая принадлежность, национальная принадлежность, религиозные убеждения, философские убеждения, политические взгляды, состояние здоровья, состояние интимной жизни

Биометрические - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта

Вопрос:

Cookies – это персональные данные?



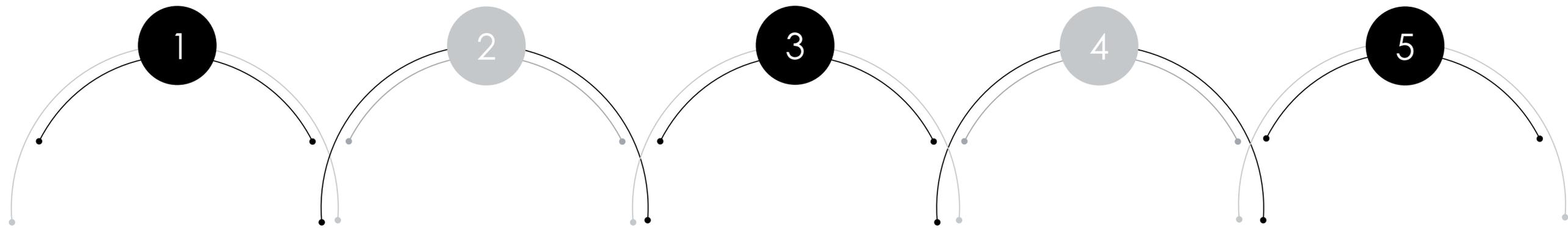
Cookies - персональные данные

Cookies:

- специальные файлы, которые находятся на диске компьютера пользователя и содержат текстовую информацию, которая нужна серверу для функционирования какого-либо сайта
- применяются для сохранения данных о пользователе и обычно используются для аутентификации пользователя, хранения персональных предпочтений и настроек пользователя, отслеживания состояния сессии доступа пользователя, ведения статистики о пользователях.
- **являются персональными данными** (ст.30 GDPR; постановление Девятого арбитражного апелляционного суда от 23.05.2016 №09АП-17574/2016; решение Таганского районного суда г. Москвы от 19.12.2018 №02-4261/2018)

Вопрос:

IP – это персональные данные?



IP - персональные данные

IP-адреса представляют собой охраняемые персональные данные, поскольку они позволяют точно идентифицировать пользователей

- Scarlet Extended SA v. SABAM, ECJ, Case C 70/10. 24 November 2011

Данные о динамических IP-адресах, собранные онлайн-сервисом, являются персональными данными, поскольку есть потенциальная возможность связать их с данными о клиенте, содержащимися у интернет-провайдера, предоставившего соответствующий IP-адрес, и определить тем самым личность такого клиента

- Patrick Breyer v. Bundesrepublik Deutschland, ECJ, Case C-582/14. 19 October 2016

Вопрос:

Фото на пропуск –
это персональные данные или нет?

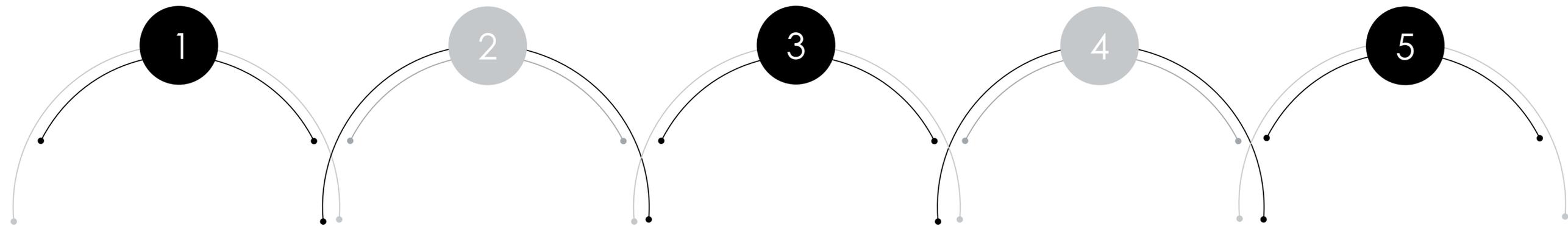


Фото на пропуск – биометрические персональные данные

Верховный Суд РФ отказал организации в отмене штрафа, назначенного за обработку биометрических персональных данных (фотографии) без специального письменного согласия субъекта.

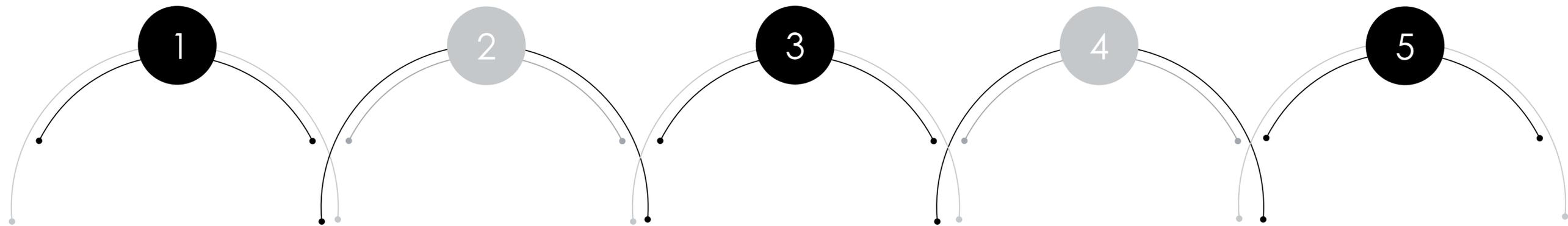
- ГУП Учебно-спортивный центр Мурманской области vs РКН - Решение ВС РФ от 05 марта 2018 по делу № 307-КГ18-101

Критерии биометрических данных:

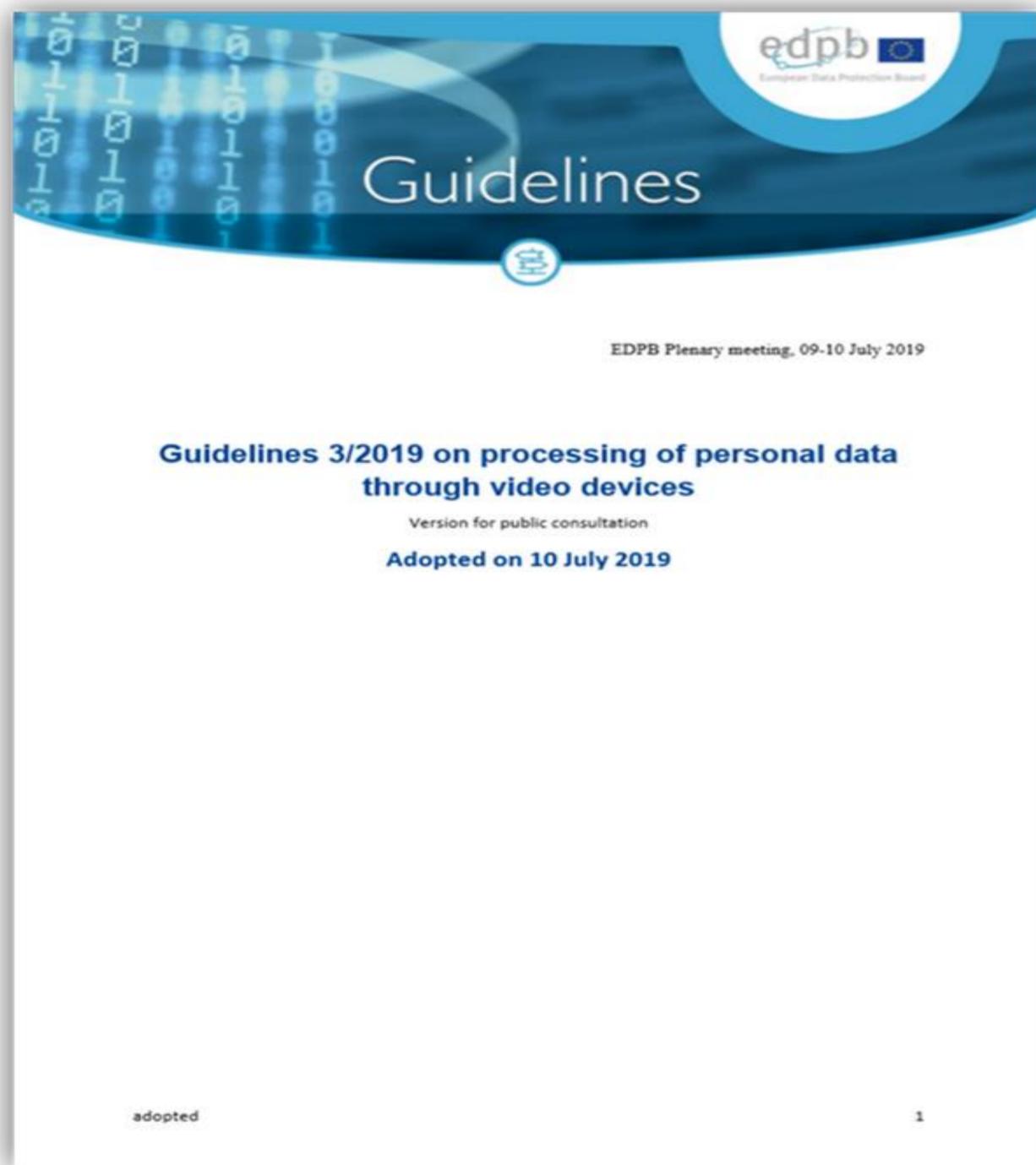
- данные должны содержать физиологические или биологические характеристики человека;
- данные должны позволять установить личность человека;
- данные должны использоваться оператором для установления личности субъекта.

Вопрос:

Видеозапись –
это персональные данные или нет?



Видеозапись – биометрические персональные данные



В России нет правового регулирования обработки персональных данных в формате видеозаписи.

В Европе действует с 2019 года отдельный документ: Руководство по обработке персональных данных с помощью видеоустройств.

Документ перечислил условия применения видеоустройств:

- законный интерес;
- ограничение во времени;
- ограничение по размещению;
- наличие предупреждающих надписей.

The background features a central black circle containing the text. This is surrounded by several concentric circles of varying radii. Scattered around these circles are various geometric shapes: small black dots, a larger grey dot, a black square, and a larger black circle. Some of these shapes are connected to the circles by thin, curved lines, creating a sense of movement or orbit.

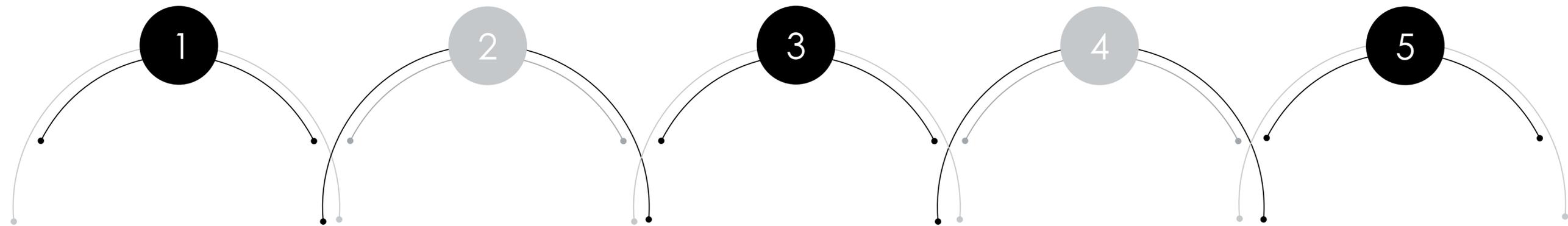
**Сессия
вопросов и ответов**

The background features several concentric circles of varying diameters. Scattered around these circles are various geometric shapes: solid black circles of different sizes, a solid grey circle, and a solid black square. Some of these shapes are connected to the circles by thin, curved lines, creating a sense of movement or orbit.

**Кто отвечает за
обработку
персональных
данных в
профсоюзной
организации**

Вопрос:

Является ли профсоюзная организация, которую Вы представляете, оператором персональных данных?



Профсоюзная организация – оператор персональных данных или нет?

Оператор персональных данных (ст.3 152-ФЗ) – это 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.

- Только те ПО, которые имеют статус юридического лица, **являются операторами** персональных данных
- ППО, являющиеся структурным подразделением ТООП и не обладающее статусом юридического лица, **НЕ является оператором** персональных данных

Если ППО – оператор, нужно ли уведомлять об этом Роскомнадзор ?

Не нужно, если:

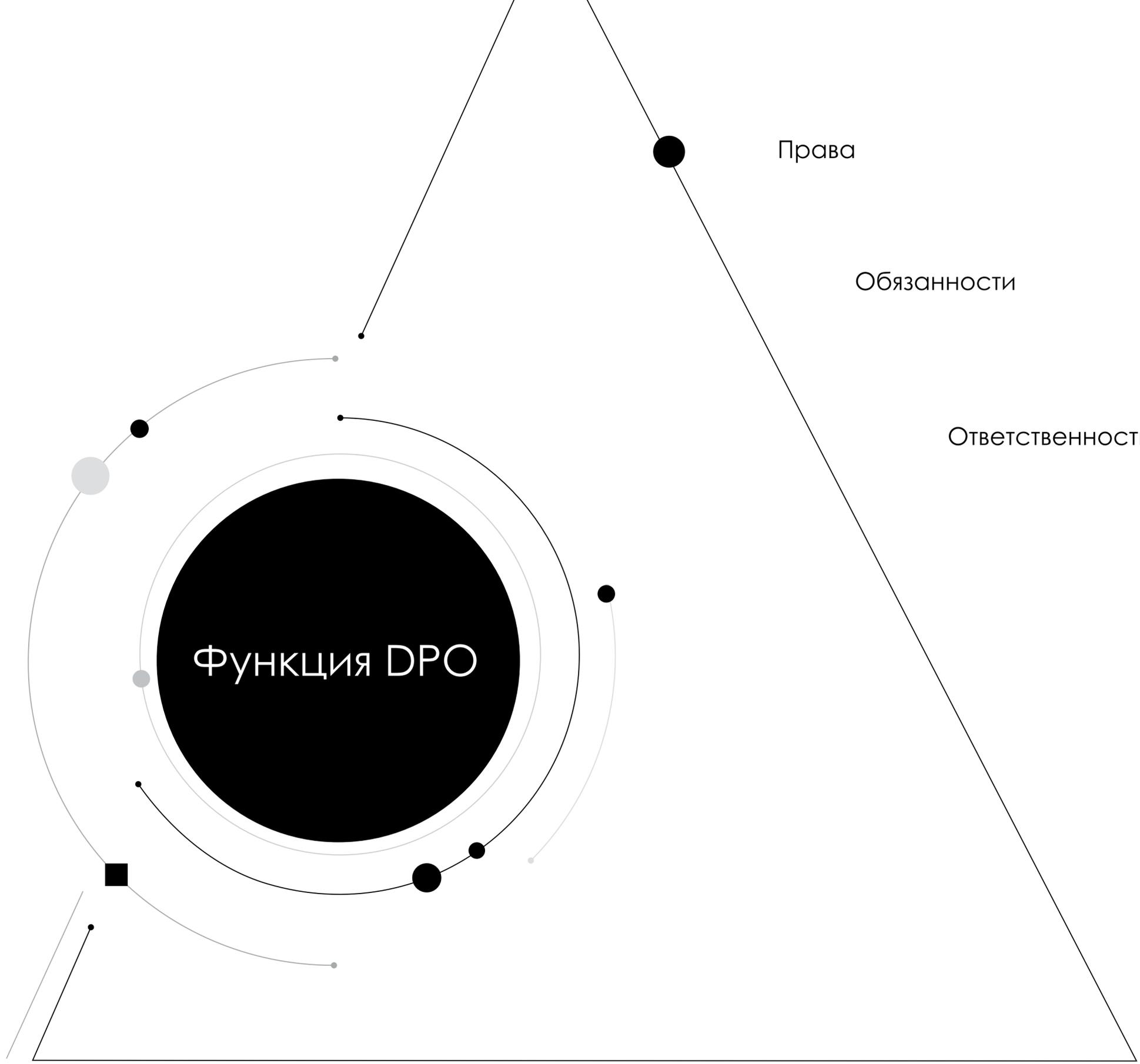
- ППО обрабатывают персональные данные **только членов профсоюза**
- обработка персональных данных осуществляется **только для достижения целей, предусмотренных учредительными документами**
- передача персональных данных осуществляется на основании **согласия в письменной форме**

Лицо, ответственное за обработку персональных данных: теория

- Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных
- Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему

Лицо, ответственное за обработку персональных данных: практика

- Лицо, ответственное за организацию обработки персональных данных, или DPO (Data Protection Officer) - штатная единица, не может быть назначен на общественных началах
- Председатель ППО как единоличный исполнительный орган своим распоряжением назначает штатного работника ППО лицом, ответственным за организацию обработки персональных данных
- Председатель ППО может возложить на себя обязанности DPO
- Отсутствие у оператора распоряжения о назначении DPO есть нарушение 152-ФЗ
- В дополнение к DPO необходимо назначить лицо, ответственное за обеспечение безопасности персональных данных (в соответствии с требованиями Постановления Правительства №1119 от 01.11.2012 г.)



Права

Обязанности

Ответственность

Функция ДРО

Права DPO

Право на доступ к информации, касающейся обработки персональных данных, а именно:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых способов обработки персональных данных;
- описание технических мер защиты ПДн, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- дата начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки

Обязанности DPO

- осуществлять внутренний контроль за соблюдением оператором законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов

Ответственность DPO

- Персональная ответственность по ст.13.11 КоАП РФ – штраф от 3 до 20 тыс. руб.
- В случае нарушения требований о локализации персональных данных (ч.8,9 ст.13.11 КоАП РФ) – штраф от 100 до 800 тыс. руб.
- Возможна дисквалификация до 3 лет в случае неисполнения предписания Роскомнадзора (ст.19.5. КоАП РФ)

Где фиксировать функцию DPO

- В локальном нормативном акте оператора – например, в Функциональном регламенте лица, ответственного за организацию обработки персональных данных,

ЛИБО

- В должностной инструкции лица, на которого возложены права и обязанности DPO

Кто имеет право работать с персональными данными, помимо DPO ?

Оператор издает локальный нормативный акт, утверждающий список лиц, имеющих право работать с персональными данными.

Например, председатель ТООП издает распоряжение об утверждении списка лиц членов профсоюза, выполнение служебных обязанностей которых связано с необходимостью доступа к персональным данным и уполномоченных на обработку персональных данных в ТООП:

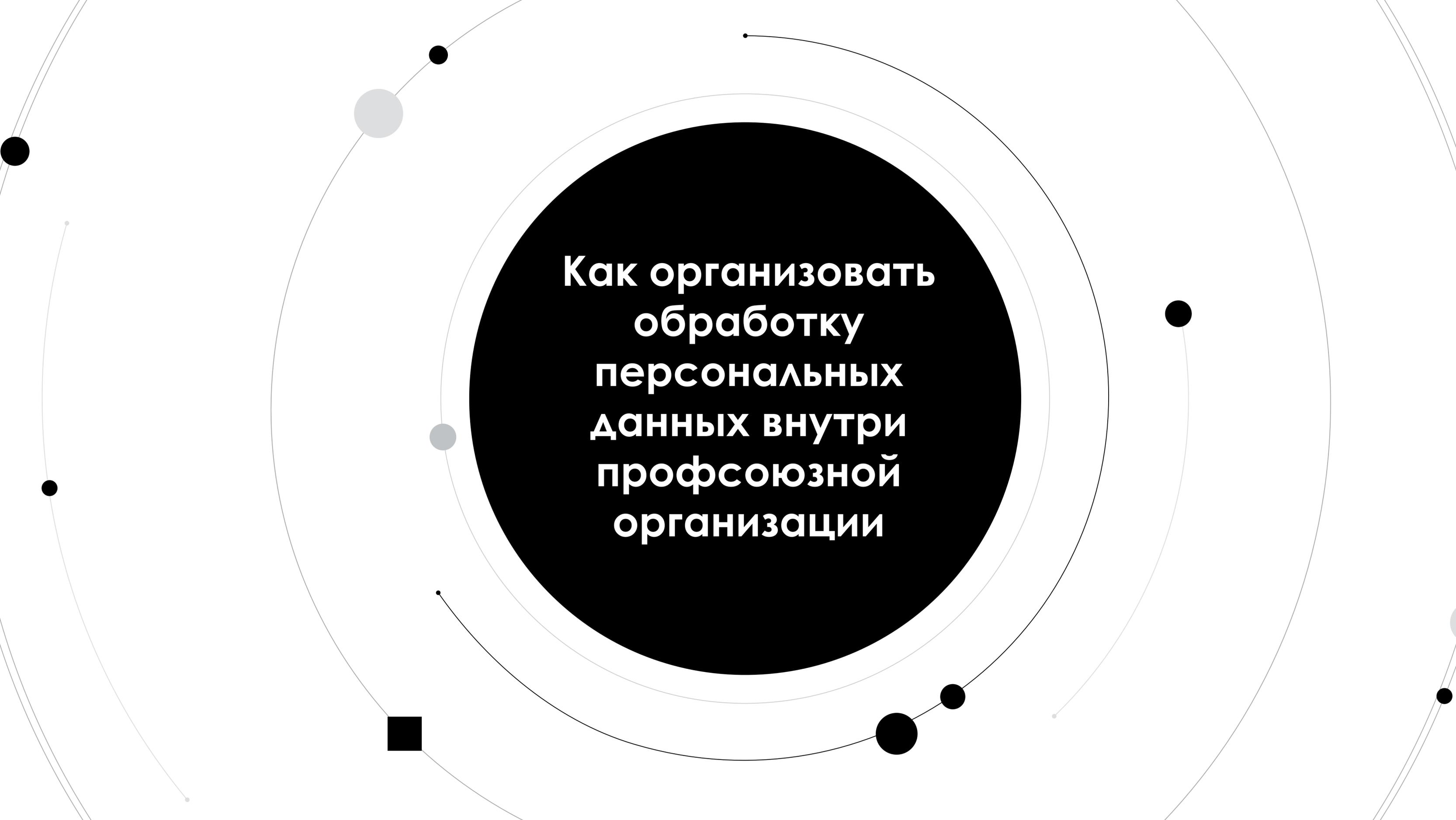
- Не освобожденные от основной работы председатели ППО, входящих в ТООП;
- Штатные председатели ППО, входящих в состав ТООП;
- Не освобожденные от основной работы члены профсоюзного комитета;
- Работники аппарата ТООП и пр.

Пример списка лиц членов профсоюза, выполнение служебных обязанностей которых связано с необходимостью доступа к персональным данным и уполномоченных на обработку персональных данных

№	ФИО	Уровень доступа
1	Иванов И.И.	Все ИСПДн
2	Петров С.С.	По заявке

The background features a central black circle containing the text. This is surrounded by several concentric, thin grey circles. Scattered around these circles are various geometric shapes: small black dots, a larger grey dot, a black square, and a larger black circle. Some of these shapes are connected to the concentric circles by thin, curved lines.

**Сессия
вопросов и ответов**

The background features several concentric circles of varying radii. Scattered around these circles are various geometric shapes: small black dots, larger grey circles, and a single black square. Some of these shapes are connected to the circles by thin, curved lines, creating a sense of movement or a network.

**Как организовать
обработку
персональных
данных внутри
профсоюзной
организации**

Какие локальные нормативные акты должны быть у оператора персональных данных

- Политика об обработке персональных данных
- Регламент обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных
- Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке
- Функциональный регламент лица, ответственного за организацию обработки персональных данных
- Положение о порядке обработки персональных данных работников
- Регламент уничтожения персональных данных при достижении целей обработки или наступления иных законных оснований
- Об утверждении перечня персональных данных
- Об утверждении перечня и описания информационных систем персональных данных
- Об утверждении модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Что включать в Политику обработки персональных данных

- Цель сбора персональных данных
- Правовые основания обработки персональных данных
- Объем и категории обрабатываемых персональных данных
- Категории субъектов персональных данных
- Порядок и условия обработки персональных данных
- Порядок актуализации, исправления, удаления, уничтожения и предоставления ответов на запросы субъектов на доступ к персональным данным

Какие формы документов должен иметь оператор

- Согласие на обработку персональных данных

Для членов профсоюза

Каждый член профсоюза должен дать согласие на передачу своих персональных данных 3-м лицам. Согласие должно быть дано в письменной форме.

Для работников

Общее правило: при передаче персональных данных **внутри одного юридического лица** согласие не требуется. Порядок передачи и работы с персональными данными регулируется локальным нормативным актом – Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке.

Каждый работник профсоюза, являющегося юридическим лицом, дает согласие на передачу своих персональных данных 3-м лицам в соответствии со ст.88 ТК РФ.

Если работник профсоюзной организации не является членом этой организации, то необходимо подписать согласие на обработку его данных в соответствии со ст.88 ТК РФ, если планируется передача его данных.

Если работник профсоюзной организации является членом этой организации, то необходимо собрать два согласия: согласие на обработку ПДн от члена профсоюза и согласие на обработку ПДн от работника (если планируется передача данных работника 3-м лицам), т.к. перечень данных, цели, сроки обработки будут разные.

Что должно быть в согласии?

Требования к согласию в письменной форме:

- ФИО, адрес, паспортные данные (номер, кем и когда выдан паспорт);
- наименование и адрес оператора;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие;
- перечень действий с персональными данными, на совершение которых дается согласие;
- общее описание используемых оператором способов обработки персональных данных;
- наименование и адрес 3-х лиц, которым может быть поручена обработка персональных данных от имени оператора;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва;
- подпись субъекта персональных данных.

Что должно быть в согласии - пример

Согласие на обработку персональных данных («Согласие»)

Я, _____
указать Ф.И.О.

адрес регистрации / проживания, номер основного документа, удостоверяющего личность,

сведения о дате выдачи указанного документа и выдавшем его органе

настоящим выражаю свое согласие на обработку, включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), в том числе трансграничную, обезличивание, блокирование, удаление, уничтожение,

следующих персональных данных («Персональные данные»): ФИО (на русском и английском языке), дата, год, месяц рождения; паспортные данные (серия, номер общегражданского паспорта, дата выдачи, наименование органа, выдавшего общегражданский паспорт); контактные телефоны (мобильный, домашний, служебный), адрес электронной почты; адрес регистрации по месту жительства и адрес фактического проживания; место работы и должность; сведения о составе семьи,

оператору Персональных данных («Оператор») – ***** с местоположением по адресу: *****,

в целях («Цели»): реализации прав и гарантий члену профсоюза, учета предоставленной мной информации в базах данных,

выражаю свое согласие и разрешаю Оператору обрабатывать Персональные данные с помощью неавтоматизированных способов обработки Персональных данных, а также автоматизированных систем управления базами данных (СУБД) и иных программных средств, специально разработанных по поручению Оператора. Работа с СУБД будет осуществляться по предписанному Оператору алгоритму (сбор, систематизация, накопление, хранение, уточнение, использование, блокирование, уничтожение).

Я соглашаюсь с тем, что, если это необходимо для реализации Целей обработки Персональных данных, Оператор вправе поручить обработку Персональных данных третьим лицам, а именно:

- *** с местоположением по адресу: ****,

при условии соблюдения требований применимого законодательства об обеспечении конфиденциальности Персональных данных и безопасности Персональных данных при их обработке. При передаче указанных данных Оператор предупреждает лиц, получающих Персональные данные, о том, что эти данные являются конфиденциальными и могут быть использованы лишь в целях, для которых они сообщены, и требует от этих лиц соблюдения этого правила. Хранение Персональных данных осуществляется исключительно на территории Оператора.

Требование об исключении или исправлении/дополнении неверных или неполных Персональных данных может быть подано в виде соответствующего письменного запроса в адрес Оператора.

Настоящее Согласие на обработку Персональных данных действует со дня его подписания в течение *** лет после окончания правовых отношений с Оператором либо до дня отзыва Согласия с правом Оператора продолжить обработку Персональных данных в установленных законодательством случаях.

Настоящее Согласие может быть отозвано путем предоставления письменного заявления в адрес Оператора.

Ф.И.О. полностью

подпись

дата

Что делать, если от субъекта персональных данных поступило обращение?

Субъект персональных данных имеет право:

- знать, какие данные обрабатываются = запрашивать информацию, касающуюся обработки персональных данных
- требовать уточнения персональных данных
- требовать блокировки персональных данных
- требовать уничтожения персональных данных
- отозвать свое согласие на обработку персональных данных



Реквизиты запроса субъекта

Запрос субъекта персональных данных должен содержать:

- ФИО субъекта
- паспортные данные
- номер, дата договора либо иные сведения, подтверждающие участие субъекта в отношениях с оператором
- ПОДПИСЬ субъекта



Алгоритм работы с запросами субъекта

- Независимо от канала поступления запроса (почта, личное обращение, электронное обращение) о запросе субъекта персональных данных должен быть проинформирован ДРО.
- Алгоритм работы предусмотрен локальным нормативным актом - Регламентом обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных
- Срок формирования ответа на запрос и его передачи для отправки субъекту персональных данных не может превышать 30 календарных дней с даты получения запроса



Хранение персональных данных на материальных носителях

Хранение материальных носителей персональных данных осуществляется в запираемых на ключ помещениях.

При этом при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

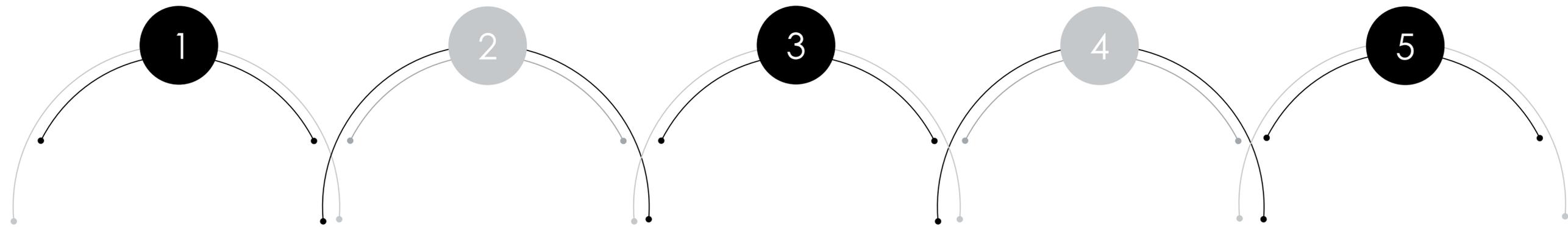
Обработка персональных данных без использования средств автоматизации, выполняется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Пример определения мест хранения:

№	Вид материальных носителей	Место хранения персональных данных
1.	Накопители на жестких магнитных дисках (серверные)	г. ***, ул. ***
2.	Накопители на магнитных лентах для резервного копирования	г. ***, ул. ***
3.	Переносные накопители	г. ***, ул. ***

Вопрос:

Можно ли хранить персональные данные в облаке?



Хранение персональных данных в информационных системах

Общее правило: основная база данных должна храниться на территории РФ - правило локализации

Поэтому хранить можно:

- на компьютере в локальной сети оператора, в том числе в удаленном режиме;
- в облачном хранилище, при условии соблюдения правила локализации.

Организация работ с информационными системами персональных данных (ИСПДн)

До начала проведения работ по обеспечению безопасности персональных данных проводится инвентаризация ИСПДн, составляется их описание, которое фиксируется в локальном акте - Об утверждении перечня и описания ИСПДн.

Для каждой ИСПДн разрабатывается Модель угроз в соответствии с:

- Нормативно-методическими документами ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», если в ИСПДн не используются криптографические средства;
- Нормативно-методическим документом ФСБ России «Методические рекомендации по обеспечению с помощью криптографических средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», если в ИСПДн используются криптографические средства.

Модель угроз утверждается локальным актом – Об утверждении модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Классификация ИСПДн по уровню защищенности

Все выявленные и вводимые в эксплуатацию ИСПДн должны классифицироваться по уровням защищенности персональных данных в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012 года № 1119.

Определение уровня защищенности проводится в следующей последовательности:

- создается Комиссия по определению уровня защищенности персональных данных при их обработке в ИСПДн;
- Комиссия проводит работы по определению уровня защищенности персональных данных, исходя из категорий и объема обрабатываемых персональных данных в ИСПДн, наличия актуальных угроз и типов угроз;
- Комиссия формирует Акты определения уровня защищенности для каждой ИСПДн.

Пример акта определения уровня защищенности

А К Т определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных «***»

г. ****

« » _____ 20__ г.

Комиссия по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных (далее – «Комиссия») в составе:

- Председатель Комиссии: ****;
- Члены Комиссии:
 - ****;
 - ****;

провела определение уровня защищенности персональных данных при их обработке в информационной системе персональных данных «***» (далее – ИСПДн «***»).



Комиссия, рассмотрев следующие характеристики ИСПДн «***»:

Категория обрабатываемых персональных данных	Иные
Объем обрабатываемых персональных данных	Менее 100 000.
Тип актуальных угроз	3-й тип угроз (<u>ИСПДн не содержат актуальные угрозы, связанные с наличием недекларированных возможностей в системном и прикладном программном обеспечении</u>)

в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»,

РЕШИЛА:

установить **третий уровень защищенности** персональных данных при их обработке в ИСПДн «***».

Подписи

Построение системы защиты персональных данных

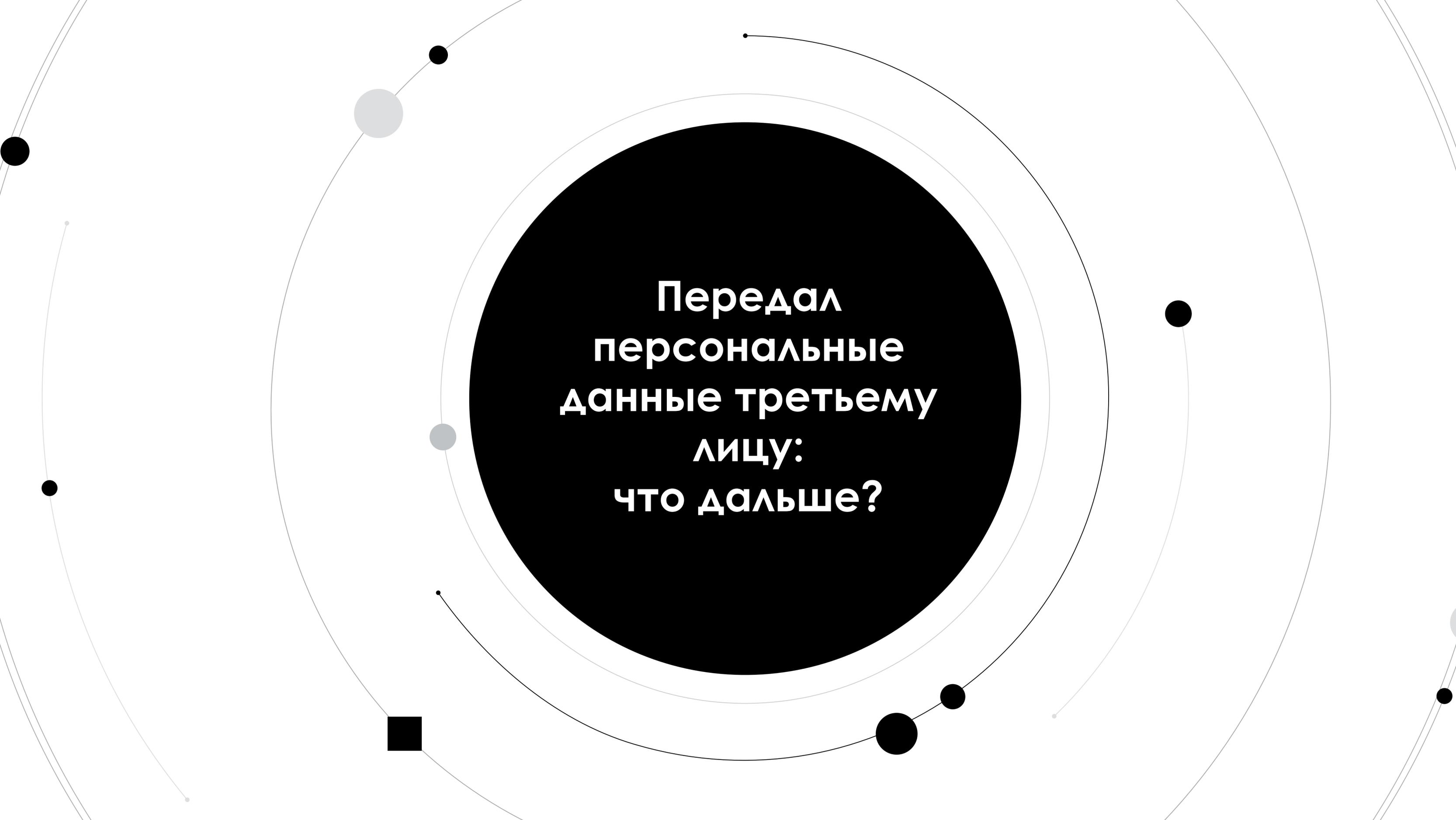
После того, как определены возможные угрозы и способы их нейтрализации в Модели угроз, внедряется система защиты персональных данных.

Работы по внедрению системы защиты персональных данных включают в себя техническое проектирование средств защиты персональных данных, внедрение средств защиты персональных данных, сопровождение средств защиты.

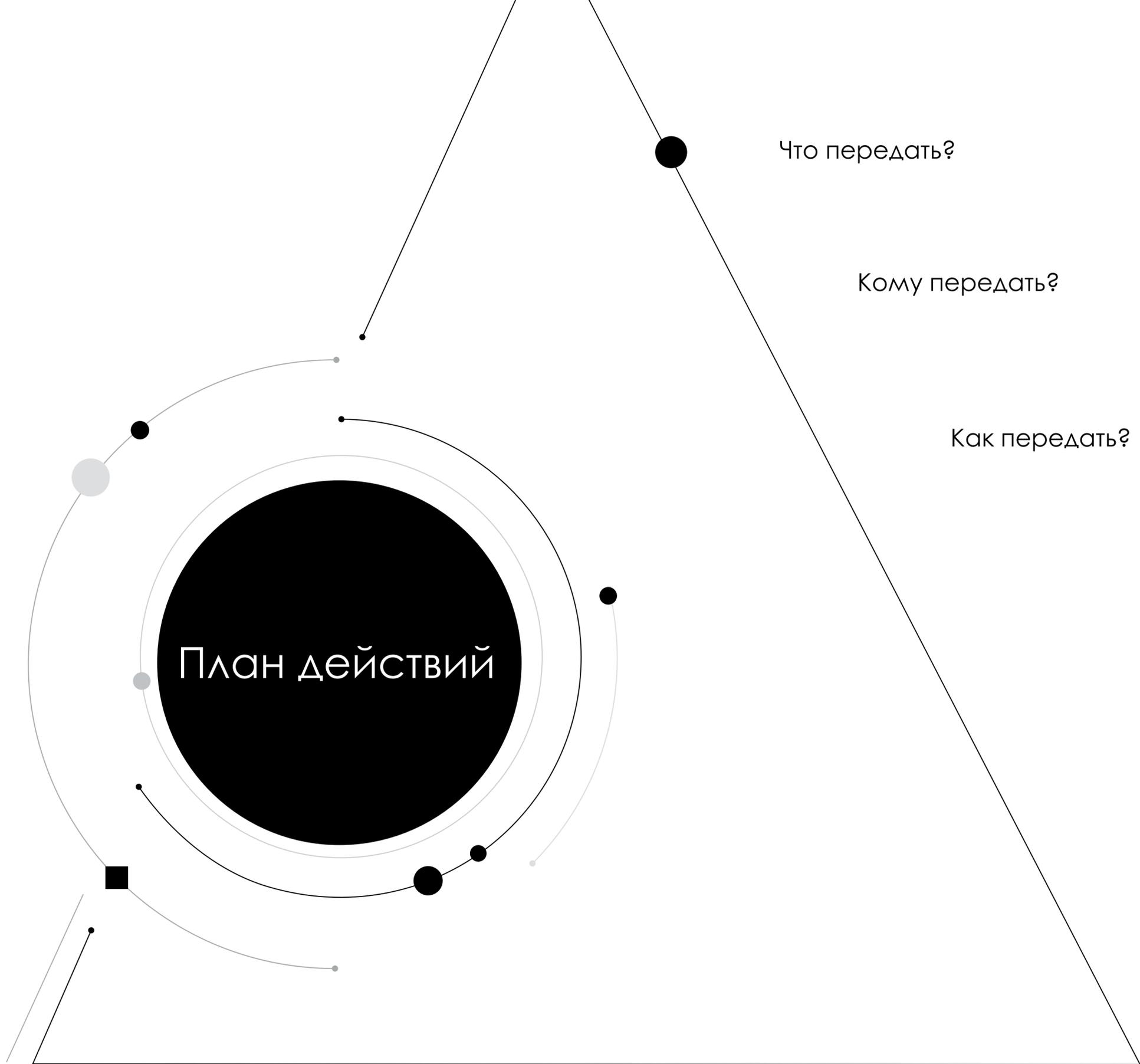
Для выполнения работ могут привлекаться подрядные организации, имеющие соответствующую лицензию ТЗКИ – техническая защита конфиденциальной информации.

The background features a central black circle containing the text. This is surrounded by several concentric, thin grey circles. Scattered around these circles are various geometric shapes: small black dots, a larger grey dot, a black square, and a larger black circle. Some of these shapes are connected to the concentric circles by thin, curved lines.

**Сессия
вопросов и ответов**

The background features several concentric circles of varying radii. Scattered around these circles are various geometric shapes: small black dots, larger grey dots, and a single black square. Some of these shapes are connected to the circles by thin, curved lines, creating a sense of movement or data points.

**Передал
персональные
данные третьему
лицу:
что дальше?**



План действий

Что передать?

Кому передать?

Как передать?

Кому передать?

- Обработчик персональных данных- лицо, осуществляющее обработку персональных данных по поручению оператора
- Контрагенты оператора, которым переданы персональные данные в обработку, есть обработчики
- Структурные подразделения оператора обработчиками не являются
- Обработка персональных данных третьим лицом должна осуществляться на основании заключаемого с этим лицом договора (п.3. ст.6 ФЗ-152)
- Со всеми обработчиками должны быть заключены Соглашение об обработке персональных данных либо Договор поручения на обработку персональных данных
- Обязательно уведомление о факте подписания такого договора DPO

Содержание Соглашения об обработке персональных данных

- Обработчик уполномочен оператором на обработку персональных данных от имени оператора
- Обработчик обязан обеспечить, чтобы информация, полученная от оператора, не раскрывалась неуполномоченным третьим сторонам
- Обработчик должен обрабатывать персональные данные исключительно в целях, определенных в договоре
- Обработчик обязан сообщить оператору об утечках, потерях данных или любых других существенных нарушениях, проявившихся в период обработки персональных данных
- Обработчик обязан уведомить оператора о запросах/ претензиях, полученных от субъектов персональных данных или третьих сторон (включая, государственные органы) в отношении персональных данных
- Обработчик по достижении целей обработки должен уничтожить все полученные от оператора персональные данные и направить в адрес оператора уведомление о выполнении обязательства
- Оператор вправе проверить исполнение Обработчиком взятых на себя обязательств.

Как передать?

Передача персональных данных по незащищенным каналам связи запрещена.

Защита канала связи может быть реализована как с помощью сертифицированных криптографических средств, так и с помощью иных средств защиты: архивирование и пароль.

Общее правило:

- заархивировать файл;
- установить пароль;
- направить файл и пароль разными каналами связи

Независимо от выбранной формы коммуникации, информация может разглашаться только уполномоченным получателям.

На что обращать внимание при работе с обработчиками

Ответственность перед субъектом персональных данных за действия обработчика несет оператор.

Поэтому **ВАЖНО** при работе с обработчиком:

- если есть утечки, потери данных - обработчик обязан сообщить оператору
- если есть запросы/ претензии субъектов персональных данных – обработчик обязан сообщить оператору
- если есть запросы/проверки со стороны РКН – обработчик обязан сообщить оператору
- если истек срок действия договора, обработчик обязан уничтожить полученные персональные данные и сообщить об этом оператору

The background features a central black circle containing the text. This is surrounded by several concentric circles of varying radii. Scattered around these circles are various geometric shapes: small black dots, a larger grey dot, a black square, and a black circle. Some of these shapes are connected to the circles by thin, curved lines, creating a sense of movement or orbit.

**Сессия
вопросов и ответов**

The background features several concentric circles of varying radii. Scattered around these circles are various geometric shapes: small black dots, larger grey dots, and a single black square. Some of these shapes are connected to the circles by thin, curved lines, creating a sense of movement or data points.

**СКОЛЬКО И ГДЕ
ХРАНИТЬ
ПЕРСОНАЛЬНЫЕ
ДААННЫЕ, И КАК ИХ
УНИЧТОЖИТЬ**

Правило локализации персональных данных

Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации (ст.18 152-ФЗ).

Нарушение правила влечет ответственность по ч.8.ст.13.11 КоАП РФ:

- Штраф на оператора от 1 до 6 млн. руб. (от до 18 млн. руб. за повторное нарушение)
- +
- Штраф на DPO от 100 до 200 тыс. руб. (от 500 до 800 тыс. руб. за повторное нарушение)

Сроки хранения персональных данных

Общее правило: персональные данные хранятся не дольше, чем того требует цель обработки

Сроки хранения персональных данных определяются в локальном нормативном акте - Об утверждении перечня персональных данных

Категории субъектов ПДн	Перечень ПДн	Место и способы обработки ПДн	Срок обработки ПДн	Условия прекращения обработки ПДн
Работник	ФИО; дата и место рождения; паспортные данные: серия и номер паспорта, кем, когда выдан, пол; ИНН; СНИЛС; адрес регистрации; фактический адрес проживания; контактный номер телефона (мобильный/домашний); адрес корпоративной электронной почты; данные об инвалидности (группа инвалидности); данные о семейном положении; сведения о составе семьи; сведения об образовании; занимаемая должность; информация о структурном подразделении; период нетрудоспособности из-за болезни; информация о премировании; размер заработной платы; сумма страховых взносов; дата приема на работу; дата увольнения; периоды трудовой деятельности; табельный номер; финансовая информация	<p><u>Способ обработки:</u> Смешанный.</p> На бумажных носителях ПДн хранятся в личных делах работников в выделенном помещении, запираемом на ключ, в департаменте управления персоналом Общества. В электронном виде хранение ПДн осуществляется в ИС «1С»	Бумажные носители, содержащие ПДн, уничтожаются по истечении 75 лет с момента увольнения работника. ПДн в электронном виде удаляются после уничтожения бумажных носителей.	ПДн подлежат уничтожению в случае отзыва субъектом ПДн согласия на обработку его ПДн (п. 5 ч. 1 ст. 21 № 152-ФЗ) либо по достижении цели обработки ПДн

Уничтожение персональных данных: теория

Общее правило: персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом (ст.5 ФЗ-152)

Алгоритм удаления прописывается в локальном нормативном акте - Регламенте уничтожения персональных данных при достижении целей обработки или наступления иных законных оснований

Удаление персональных данных: практика

- Достижение целей обработки для члена профсоюза – прекращение членства в профсоюзной организации
- Достижение целей обработки для работника – прекращение трудовых отношений. Приказ Росархива №236 от 20.12.2019 г. установил срок хранения кадровых документов – в течение 75 лет должны храниться кадровые документы, законченные делопроизводством до 01.01.2003 г., а документы, законченные делопроизводством после 01.01.2003 г., хранятся в течение 50 лет
- Персональные данные из баз данных и информационных систем удаляются после удаления бумажных носителей

Сроки удаления:

- по достижению целей обработки - в 30-дневный срок, если иное не предусмотрено иным соглашением между оператором и субъектом персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку персональных данных - в 30-дневный срок;
- при выявлении неправомерной обработки персональных данных - в срок, не превышающий 7 рабочих дней с даты выявления

Алгоритм действий при отзыве согласия



The background features a central black circle containing the text. This is surrounded by several concentric, thin grey circles. Scattered around these circles are various geometric shapes: small black dots, a larger grey dot, a black square, and a larger black circle. Some of these shapes are connected to the concentric circles by thin, curved lines.

**Сессия
вопросов и ответов**



Спасибо
за
ВНИМАНИЕ

1

Наталья Ковалева
к.ю.н., LLM
DPO Allianz Russia

2

[linkedin.com/in/natalya-kovaleva-a4314b95](https://www.linkedin.com/in/natalya-kovaleva-a4314b95)

Kovaleva.natalya@gmail.com