«УТВЕРЖДЕНО»

Директор
Плесского музея-заповедника

_____ А.В. Чаянова

Приказ № 880 от 19.08. 2025 года

ПОЛОЖЕНИЕ

о порядке обезличивания персональных данных в Государственном бюджетном учреждении Ивановской области «Плесский государственный историко-архитектурный и художественный музей-заповедник»

1. Общие положения

1.1. Назначение документа

Настоящее положение (далее – Положение) регулирует порядок проведения обезличивания персональных данных (далее — ПДн) в **Государственном бюджетном учреждении Ивановской области «Плесский государственный историко-архитектурный и художественный музей-заповедник»** (далее — Учреждение), описывает требования к процессу обезличивания, а также устанавливает правила обработки, хранения и защиты обезличенных данных.

1.2. Нормативно-правовые основания

Положение основано на положениях следующих нормативных правовых актов Российской Федерации:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер по защите прав субъектов персональных данных»;
- приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов обезличивания персональных данных»;
- приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств»;
- Федеральный закон от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон "О персональных данных" и Федеральный закон "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Термины и определения

Основные термины и определения, используемые в документе:

- обезличивание персональных данных — мероприятие, направленное на исключение из состава персональных данных информации, позволяющей идентифицировать субъект персональных данных без использования дополнительной информации;
- обезличенные данные — совокупность данных, прошедших процедуру обезличивания и не позволяющих идентифицировать физическое лицо без использования другой информации;

- дополнительная информация — любые данные, алгоритмы, программное обеспечение, предназначенные для реконструкции исходных персональных данных из обезличенных;
- оператор — юридическое лицо, осуществляющее сбор, обработку и обезличивание персональных данных в своей деятельности;
- информационная система персональных данных (ИСПДн) — совокупность информационных ресурсов и автоматизированных средств, предназначенных для обработки персональных данных;
- классификация информационной системы персональных данных (ИСПДн) — отнесение информационной системы к одному из четырех уровней значимости в зависимости от характера обрабатываемых данных;
- шифровальные (криптографические) средства защиты информации (СКЗИ) — сертифицированные средства криптографической защиты информации, обеспечивающие защиту обезличенных данных.

3. Цели и задачи обезличивания

3.1. Цель обезличивания состоит в снижении рисков нарушений конфиденциальности персональных данных и обеспечении сохранности обезличенных данных при условии сохранения достаточного объема данных для их дальнейшего эффективного использования.

3.2. Задачами обезличивания являются:

- исключение возможности идентификации физического лица по обезличенным данным без использования дополнительной информации;
- обеспечение возможности продолжения обработки обезличенных данных для нужд учреждения без прямого воздействия на физическую безопасность субъектов персональных данных;
- удовлетворение потребностей учреждения в предоставлении обезличенных данных партнерам и третьим сторонам.

4. Требования к обезличенным данным

Обезличенные данные должны отвечать ряду обязательных критериев, обеспечивающих их дальнейшую пригодность для обработки и анализа:

4.1. **Полнота**

Обезличенные данные должны сохранять весь объем доступной информации, за исключением непосредственно идентифицирующих признаков субъекта персональных данных (Ф. И. О., паспортные данные, контактные данные и т. д.). Информация, необходимая для анализа и поддержки бизнес-процессов учреждения, должна оставаться неизмененной.

4.2. **Структурированность**

Данные должны содержать структуру и логические связи между отдельными атрибутами. Связи между обезличенными данными сохраняются в такой мере, чтобы поддерживать релевантность данных и позволять эффективно осуществлять запросы и обрабатывать информацию без необходимости восстановления идентичности субъектов.

4.3. **Релевантность**

Обезличенные данные должны обеспечивать возможность полноценного анализа и обработки запросов, постановки диагноза или выработки решений без необходимости повторного деобезличивания. Вся информация должна быть достаточной для понимания сути и целей, ради которых проводилось обезличивание.

4.4. **Семантическая целостность**

Каждое значение атрибута в обезличенных данных должно соответствовать своему аналогу в исходных данных. При обезличивании недопустимо изменять смысловое содержание информации настолько, чтобы терялась способность правильно интерпретировать полученные выводы.

4.5. **Анонимность**

Обезличенные данные не должны допускать прямой или косвенной идентификации физического лица без использования дополнительной информации. Даже при наличии обезличенных данных восстановить оригинальную персону должно быть технически невозможно без особого доступа к дополнительному инструментарию, паролям или ключам.

4.6. **Исключение ограниченной информации**

Обезличенные данные не должны содержать сведений, доступ к которым ограничен федеральными законами. Проверка соответствия проводится перед передачей данных третьим лицам или формированием массивов данных.

5. Методы обезличивания

5.1. Методы обезличивания должны исключать возможность включения в обезличенные данные сведений, доступ к которым ограничен федеральными законами.

5.2. Учреждение использует следующие основные методы обезличивания:

5.2.1. **Метод введения идентификаторов**

Метод заключается в присвоении каждому объекту обработки уникальной метки (идентификатора), которая связывается с обезличенными данными и сохраняется отдельно от обезличенных данных. Связь идентификатора с обезличенными данными должна поддерживаться в отдельном реестре, доступ к которому ограничен специальным кругом лиц.

5.2.2. **Метод изменения состава или семантики**

Изменение состава или семантики подразумевает замену конкретных данных (таких как фамилии, имена, места жительства) общими характеристиками, такими как возрастные категории, регионы проживания и прочие агрегированные данные.

5.2.3. **Метод декомпозиции**

Декомпозиция предусматривает разбивку массива данных на самостоятельные блоки, содержащие разные виды данных, не допускающие идентификации физического лица без наличия дополнительных инструментов сопоставления.

5.2.4. **Метод перемешивания**

Перемешивание представляет собой случайное перераспределение записей в массиве данных с использованием сложных криптографических алгоритмов, обеспечивающих невозможность восстановления исходных данных без знания секретного ключа.

5.2.5 Выбор метода обезличивания

Выбор метода обезличивания зависит от задач.

Класс задач	Предпочтительные методы обезличивания
Статистические исследования	Метод декомпозиции
Хранение данных	Метод перемешивания, метод декомпозиции
Поиск по запросам	Метод введения идентификаторов
Интеграция данных	Метод введения идентификаторов, метод перемешивания
Передача данных в ГИС по запросу уполномоченных органов	Метод введения идентификаторов

6. Порядок обезличивания

Перед реализацией метода обезличивания проводится оценка, исключающая наличие в данных сведений, доступ к которым ограничен законом. Процедура обезличивания включает следующие этапы:

1. Оценка целесообразности и рисков обезличивания данных.
2. Выбор подходящего метода обезличивания.
3. Получение одобрения руководителя учреждения на проведение обезличивания.

4. Реализация выбранной методики обезличивания.
5. Проверка качества обезличивания специалистами информационной безопасности.
6. Архивация или уничтожение исходных персональных данных в установленном порядке.

7. Обработка обезличенных данных

7.1. Обезличенные данные могут использоваться без предварительной процедуры деобезличивания. Такие данные применяются исключительно для достижения заявленных целей обработки, таких как аналитика и статистика.
7.2. Запрещается передача обезличенных данных третьим лицам без согласования с руководством учреждения и подтверждения цели использования обезличенных данных. Допускается обмен обезличенными данными с внешними уполномоченными органами строго в объеме, необходимом для достижения поставленной цели.
7.3. Процедуру деобезличивания разрешается проводить исключительно в следующих случаях:

- по официальному запросу субъекта персональных данных (физического лица), чей запрос обоснован интересами защиты прав и свобод;
- в случае поступления мотивированного запроса от правоохранительных органов, судов или других официальных ведомств, наделенных правом запрашивать персональные данные;
- при выполнении обязательств учреждения, возложенных на него нормативными правовыми актами Российской Федерации.

7.4. Деобезличивание возможно только с участием специалиста по информационной безопасности. Деобезличенная информация подлежит немедленному возврату в состояние обезличенности сразу после ее использования в полном объеме.
7.5. Передача данных в государственную информационную систему
Обезличенные данные, полученные в результате обработки, предоставляются в государственную информационную систему уполномоченного органа в случаях, предусмотренных законом.

8. Меры защиты обезличенных данных

8.1. Обезличенные данные размещаются в выделенных сегментах информационных систем, оборудованных системами мониторинга и фильтрации доступа. Все обезличенные данные хранятся в закрытом режиме с высокой степенью защиты от несанкционированного доступа.
8.2. Для защиты обезличенных персональных данных применяются следующие меры защиты:
8.2.1. **Криптографическая защита:**

- используются аппаратно-программные комплексы и средства шифрования, сертифицированные ФСБ России и занесенные в официальный реестр. Сквозное шифрование применяется ко всем каналам передачи и местам хранения обезличенных данных;
- ключи шифрования регулярно обновляются по заранее установленному графику, утвержденному руководителем учреждения. Старые ключи уничтожаются в течение трех рабочих дней после замены новыми.

8.2.2. **Физическая защита:**

- серверные помещения, комнаты хранения носителей ключевой информации оснащаются охранными системами, видеонаблюдением и оборудованием пожарной сигнализации. Вход разрешен только авторизованным сотрудникам по предварительно согласованному списку лиц, утвержденному руководителем учреждения;
- система доступа регулируется регламентом допуска к персональным данным, предусматривающим выдачу пропусков и разрешение входа по электронным картам или биометрическим параметрам;

- режимы работы помещений: охранные режимы устанавливаются как для рабочего, так и для нерабочего времени. Во внерабочее время доступ ограничивается дополнительными мерами (наличием дежурных служб, блокировкой дверей и видеоконтролем).

8.2.3. Управление доступом:

- сотрудник получает доступ к обезличенным данным только в том случае, если это предусмотрено должностными обязанностями и обосновано производственными потребностями;
- лица, имеющие доступ к обезличенным данным, закреплены в официальном списке, утвержденном приказом руководителя учреждения. Список пересматривается раз в год и дополнительно изменяется в случае кадровых перестановок или иных обстоятельств, повышающих риск утечки данных.

9. Контроль и отчетность

9.1. **Отдел информационной безопасности** ежегодно проводит внутреннее тестирование уровня защищенности обезличенных данных и представляет руководству ежегодный отчет о состоянии дел. По результатам проверок выявляются возможные недостатки и принимаются оперативные меры по их устранению.

9.2. Учреждение ведет журнал передачи обезличенных данных в государственную систему, журнал допуска к персональным данным, журнал учета машинных носителей персональных данных, журнал уничтожения персональных данных.

10. Ответственность

Работники учреждения несут ответственность за нарушение правил обезличивания персональных данных, предусмотренную трудовым договором, должностными инструкциями и федеральными законами Российской Федерации. В частности, предусмотрена следующая ответственность:

- дисциплинарная ответственность — предупреждение, выговор, увольнение;
- административная ответственность — штрафы, предписания контролирующих органов;
- уголовная ответственность — наказание за преступления против тайны частной жизни (в зависимости от тяжести правонарушения).

Приложение №1
к положению о порядке обезличивания персональных данных

АКТ

об обезличивании персональных данных

(образец)

№ 1 _____ 2025 года

В соответствии с Положением об обезличивании персональных данных от 01.09.2025 Комиссия, назначенная приказом №_____от 01.09.2025, произвела обезличивание персональных данных сотрудников для последующей передачи в государственную информационную систему в ответ на запрос № _____от _____ на основании приказа директора № ____ от _____2025.

1. Комиссия произвела обезличивание следующих персональных данных работников:

- фамилия, имя отчество;
- год рождения;
- гражданство;
- адрес проживания.

2. Обезличивание выполнено методом идентификаторов. Персональные данные, указанные в пункте 1, обезличены таким образом, что данные не позволяют установить принадлежность к конкретному лицу, идентификация лица через обезличенные данные невозможна.

3. Состав обезличенных данных передан по защищенному каналу связи в государственную информационную систему _____2025 ____ ч ____ мин.

4. Копия состава обезличенных данных удалена из приложения для обезличивания персональных данных DFG в связи с достижением цели обработки. Уничтожение выполнено в присутствии комиссии методом форматирования _____2025 в ____ ч 00 мин.

Председатель
комиссии

_____

Члены комиссии:

Специалист по кадрам

_____

Заведующий
информационно-
техническим отделом

_____