КАДРОВОЕ ДЕЛО

«Обезличено». Что делать с данными уволенных работников с учетом новых требований закона о персданных

1 Когда работодателю придется обезличивать данные уволенных сотрудников

2 Придется ли изменять кадровые документы для обезличивания данных

3 Что грозит компании, если не вычистить во внутренних базах данные уволенных

С 1 сентября 2025 года вступают в силу новые требования к обезличиванию персональных данных. Они коснутся и персональных данных уволенных работников, которые продолжают «жить» во внутренних системах, даже когда их владельцы давно покинули организацию. Новый порядок требует пересмотра подходов к хранению и уничтожению информации. Мы собрали для вас пошаговый алгоритм, который поможет различить данные для хранения и обезличивания, а также подскажем, как действовать по новым правилам.

Наталья Ковалева
Руководитель практики персональных данных ООО «Хэдхантер», сертифицированный менеджер по конфиденциальности информации (CIPM), к. ю. н.

Что такое обезличивание

Обезличивание — это форма обработки, при которой становится невозможно определить, кому принадлежат данные, без доступа к дополнительной информации. Это позволяет сохранить смысл информации, но исключает возможность идентифицировать конкретного человека (подп. 9 п. 1 ст. 3 Закона от 27.07.2006 № 152-ФЗ, далее — Закон № 152-ФЗ).

Разница между уничтожением и обезличиванием следующая: если данные уничтожены, восстановить их невозможно. А обезличенные данные можно использовать дальше — например, для статистики, аналитики, обеспечения функционирования внутренних систем. Именно поэтому Закон № 152-ФЗ различает эти формы обработки и требует, чтобы каждая компания, являющаяся оператором персональных данных, знала, какая из этих форм обработки применима в каком случае.

Долгое время обезличивание фактически применялось только государственными и муниципальными органами — операторами персональных данных. Для остальных компаний порядок обезличивания оставался вне правового поля.

Ситуация изменится с 1 сентября 2025 года. В Законе № 152-ФЗ появится новая статья 13.1 — она устанавливает, как именно нужно работать с обезличенными персональными данными. В том числе — когда их нужно передавать государству, как обезличивать и кто может получить к ним доступ. К этому моменту также примут специальные правила, которые обяжут всех операторов — в том числе работодателей — использовать определенные методы обезличивания. Для кадровиков эти требования не совсем новые.

Правило про необходимость обезличивания было всегда: когда данные больше не нужны, их нужно либо уничтожить, либо обезличить (п. 7 ст. 5 Закона № 152-ФЗ). Но поскольку методика обезличивания работала только для государственных и муниципальных органов, компании просто не имели правовой возможности использовать обезличивание в своей практике.

Теперь, когда появляются конкретные требования к обезличиванию, ситуация может поменяться. В следующем разделе расскажем, как это повлияет на работу кадровой службы.

Когда и какие данные работников нужно обезличивать

Вопрос об обезличивании персональных данных для внутренних задач компании может возникнуть при работе с персональными данными уволенных работников. При расторжении трудового договора работодатель достигает цели обработки сведений о работнике — трудовые отношения прекращаются. Это означает, что данные должны быть либо уничтожены, либо обезличены, если нет иных правовых оснований для продолжения обработки персональных данных (п. 7 ст. 5 Закона № 152-ФЗ). Задача кадровика — понять, где хранятся такие данные.

Куда нужно будет передавать обезличенные данные

У обезличенных персональных данных есть две сферы применения: их можно будет использовать для внутренних задач компании, но также их придется предоставить по запросу государства. Так, например, Минцифры сможет запрашивать у организаций обезличенные наборы данных для мероприятий по борьбе с терроризмом при введении режима КТО, предупреждения эпидемий и отравлений во время карантина, а также для проведения исследований в экономической, социальной и туристической сферах (постановление Правительства от 24.04.2025 № 538). Обезличенные данные также понадобятся для реализации нацпроектов, госпрограмм и приоритетных инициатив.

Всю запрошенную информацию нужно будет безвозмездно направить в федеральную информационную систему — на Единую платформу национальной системы управления данными (постановление Правительства от 28.05.2025 № 740). Подключиться к системе нужно будет по запросу от Минцифры в течение 15 дней. Затем в течение трех рабочих дней нужно обезличить запрошенные данные, подписать их электронной подписью и загрузить в систему. Если сведения неполные или недостоверные, Минцифры вправе повторно направить запрос. В этом случае у оператора будет 10 рабочих дней на исправление (проект постановления Правительства, https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=154910).

Уничтожать или изменять кадровые документы, которые архивное законодательство требует длительно хранить, не придется

После этого — определить, нужно ли их уничтожить, обезличить или продолжить хранить на законном основании.

Сразу успокоим: уничтожать или изменять кадровые документы, которые архивное законодательство требует длительно хранить, не придется. Требования по обезличиванию их не касаются. Данные и в кадровых, и в бухгалтерских системах также можно и нужно хранить, если они связаны с исполнением обязательств перед уволенным работником. Например, личные дела уволенных сотрудников подлежат хранению в архиве 50 или 75 лет в соответствии с приказом Росархива от 20.12.2019 № 236. Эти данные можно сохранять в кадровых и бухгалтерских системах для обеспечения прав бывших работников при обращении в госорганы, например в Социальный фонд России.

Но нередко данные сотрудников остаются в других цифровых средах — базах знаний, CRM, таск-менеджерах, на корпоративном портале. При этом удаление таких данных может нарушить связность информации и работу внутренних систем. В этих случаях единственный законный путь — не уничтожать, а обезличить информацию, исключив возможность идентифицировать конкретного человека, но сохранив структуру и полезность массива данных.

Кадровикам стоит заранее определить, в каких случаях и каким способом будет применяться обезличивание. Лучше сделать это совместно с IT, специалистами по информационной безопасности и защите персданных, чтобы обеспечить соблюдение требований закона и исключить риски.

Для этого стоит сделать следующее:

— провести аудит: где остались данные уволенных работников, кроме личных дел и учетных систем;

— понять, какие данные нужно уничтожить, какие — сохранить, а какие — обезличить;

— зафиксировать это в локальных документах вместе с IT и специалистами по защите персданных.

Такой порядок позволит соблюсти требования закона и сохранить устойчивость внутренних процессов.

Рекомендуется издать приказ о проведении внутреннего аудита хранения и обработки персональных данных уволенных работников. В нем укажите следующую информацию.

Минцифры сможет запрашивать у организаций обезличенные наборы данных для мероприятий по борьбе с терроризмом, предупреждения эпидемий и отравлений во время карантина, а также для проведения исследований

Прежде всего обозначьте цель — выявить избыточные или неправомерно хранимые данные, определить зоны риска и точки, где требуется обезличивание.

В составе комиссии желательно объединить представителей кадровой службы, IT-отдела, специалистов по информационной безопасности и защите персданных, если такая роль выделена в компании. Комиссия должна составить перечень систем и документов, проверить, какие данные реально используются, а какие — остались без правового основания.

По результатам работы разработайте инструкцию или локальный нормативный акт, в котором пропишите:

— категории данных, подлежащих обезличиванию после увольнения сотрудника;

— сроки и процедуры обезличивания;

— ответственных лиц;

— используемые методы;

— порядок документирования действий по обезличиванию.

Это позволит не только организовать работу, но и продемонстрировать проверяющим наличие управляемого процесса.

Как обезличивать данные

Роскомнадзор предусмотрел пять методов обезличивания персональных данных. Именно их нужно использовать, в том числе и в кадровой работе (приказ РКН от 19.06.2025 № 140).

Введение идентификаторов. Этот метод подойдет, если данные сотрудника продолжают использоваться, но его имя должно быть скрыто. Например, в базе знаний или отчетах можно заменить Ф. И. О. сотрудника на уникальный идентификатор (например, HR-2023-017). Таблица соответствия с настоящими именами должна храниться отдельно, с ограниченным доступом. Это позволяет сохранить внутреннюю логику системы, не нарушая конфиденциальность.

Изменение состава данных. Если в документе избыточная информация, ее можно удалить или заменить.

Приказ о создании комиссии и проведении аудита

Возглавить комиссию лучше кадровику

Общество с ограниченной ответственностью «Альфа»
(ООО «Альфа»)

ПРИКАЗ

1 сентября 2025 г. № 37/о

Москва

О проведении внутреннего аудита хранения и обработки персональных данных уволенных работников

В соответствии с п. 4 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в целях осуществления внутреннего контроля и аудита соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам

ПРИКАЗЫВАЮ:

1. Провести внутренний аудит хранения и обработки персональных данных уволенных работников в срок до 15 октября 2025 года.

2. Утвердить состав комиссии по проведению аудита:
— Сергеева Ирина Михайловна, начальник отдела кадров — председатель комиссии;
— Плотников Антон Васильевич, инженер-программист отдела ИТ — член комиссии;
— Никитина Алла Геннадьевна, специалист по информационной безопасности — член комиссии;
— Михайлова Светлана Юрьевна, специалист по защите персональных данных (DPO) — член комиссии.

3. Комиссии в ходе работы:
— провести инвентаризацию информационных систем, где могут храниться данные уволенных работников (в том числе 1С:ЗУП, Bitrix24, HelpDesk, внутренние сетевые хранилища, электронная почта);
— составить перечень документов, файлов и записей, содержащих персональные данные уволенных сотрудников;
— определить, какие данные подлежат хранению на основании приказа Росархива от 20.12.2019 № 236, а какие — требуют уничтожения или обезличивания;
— выявить случаи хранения данных без правового основания и предложить меры по их устранению;
— разработать рекомендации по внесению изменений в локальные акты и настройку автоматического обезличивания в системах.

4. По результатам работы представить письменное заключение с выявленными рисками и предложениями по корректировке процедур в срок до 15 ноября 2025 года.

5. Контроль за исполнением настоящего Приказа возлагаю на начальника отдела кадров Сергееву И.М.

Генеральный директор *Львов* А.П. Львов

Перечислите возможные места хранения данных уволенных сотрудников

Инструкция по обезличиванию данных уволенных работников

Укажите условия обезличивания данных

...

ИНСТРУКЦИЯ

о порядке обезличивания персональных данных уволенных работников

1. Общие положения

1.1. Настоящая инструкция устанавливает порядок обезличивания персональных данных работников, трудовой договор с которыми прекращен.

1.2. Цель документа — обеспечить соблюдение требований п. 7 ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предотвратить неправомерное хранение персональных данных.

1.3. Обезличивание применяется в тех случаях, когда данные не подлежат архивному хранению, но их полное уничтожение может нарушить работу внутренних систем.

2. Категории данных, подлежащих обезличиванию

Обезличиванию подлежат следующие данные, если они сохраняются в информационных системах после увольнения работника и не входят в состав документов, подлежащих архивному хранению:

— имя, фамилия, отчество;
— адрес электронной почты;
— служебные номера телефонов;
— идентификаторы корпоративных аккаунтов;
— фото и иные изображения;
— ссылки на профили в мессенджерах и соцсетях;
— сведения о должности, подразделении, уровне доступа (если они сохраняются в сторонних системах вне кадрового контура — например, в CRM, HelpDesk, таск-трекерах и др.).

3. Сроки и порядок обезличивания

3.1. Обезличивание должно быть выполнено в срок не позднее 30 календарных дней с момента прекращения трудового договора, если иное не установлено законом.

3.2. Обезличивание проводится после подтверждения отсутствия оснований для дальнейшего хранения данных.

3.3. Системы, в которых сохраняются данные, подлежат учету и контролю в рамках перечня, утвержденного комиссией.

4. Ответственные лица

4.1. Ответственным за организацию обезличивания является начальник отдела кадров.

4.2. За выполнение технических процедур отвечают:

— ИТ-отдел — за очистку, настройку или доработку систем хранения и доступа;

Предусмотрите лиц, ответственных за обезличивание

— специалист по информационной безопасности — за контроль недоступности исходных данных;
— DPO (при наличии), специалист по защите персональных данных — за правовую оценку и ведение реестра обезличенных действий.

5. Методы обезличивания

В зависимости от возможностей системы применяются следующие методы:

— замена Ф. И. О. на уникальный идентификатор (введение идентификаторов);
— удаление или искажение полей (изменение состава данных);
— техническое разделение связанных данных (декомпозиция);
— обобщение до групповых признаков (агрегирование);
— автоматическое перемешивание записей при экспорте в аналитику.

6. Документирование

6.1. Факт обезличивания фиксируется в журнале учета операций обезличивания, где указываются:
— дата обезличивания;
— система, в которой выполнены действия;
— Ф. И. О. ответственного;
— примененный метод;
— обоснование необходимости (например, сохранение логики задач или проектов).

6.2. Журнал ведется в электронном виде и хранится у специалиста по защите персональных данных.

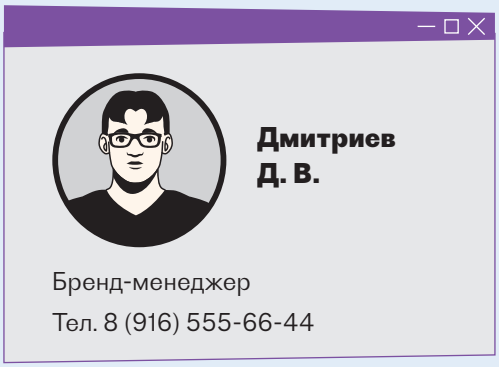
6.3. В случае запроса Роскомнадзора или иной уполномоченной инстанции журнал предоставляется по письменному требованию.

Например, оставить только название отдела без указания должности или имени. Или указать только регион проживания, а не полный адрес. Также можно заменить паспортные данные фиктивными номерами, если документ нужен только в демонстрационных или обучающих целях.

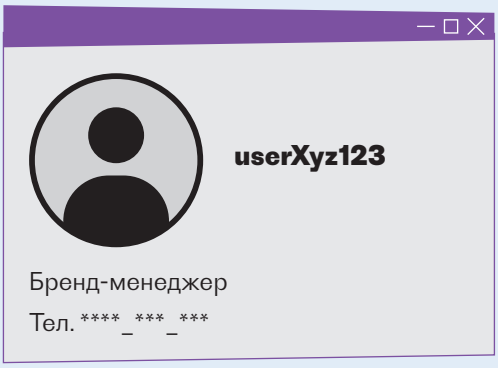
Декомпозиция. Этот способ можно применять, если в системе совмещены личные и рабочие данные. К примеру, можно разнести информацию по разным модулям: в одной части оставить должность и задачи, в другой — контакты. При этом между частями не должно быть связи, позволяющей восстановить полную картину о человеке.

Перемешивание. Используется, если система хранит большие таблицы с повторяющимися записями.

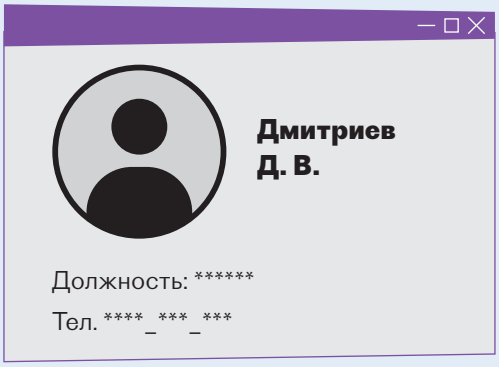
Как обезличить данные сотрудника на корпоративном портале



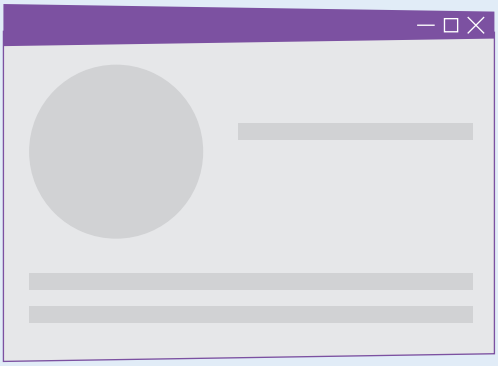
Так выглядит профиль сотрудника до увольнения



Замена имени и контактов на технический идентификатор



Очистка персональных данных, кроме минимальных полей



Полностью пустой профиль — только техническая оболочка

Например, можно случайным образом перемешать номера телефонов, e-mail или даты рождения между строками — так, чтобы каждая строка больше не соответствовала конкретному работнику. Метод особенно полезен при подготовке данных для внутренней аналитики.

Преобразование (агрегирование). Такой метод позволяет обезличить данные, сохранив общую статистику. Например, в отчетах по текучести кадров можно указать, что уволились три специалиста 25—35 лет из IT-отдела, без указания фамилий. Или — что на позиции в «поддержке» было оформлено 12 срочных договоров за год.

Выбор метода зависит от того, где хранятся данные и зачем они нужны. В любом случае важно зафиксировать, какой метод используется, в каком случае и кто за это отвечает.

Что будет, если проигнорировать правила обезличивания

Пока специальные штрафы за нарушение правил обезличивания данных предусмотрены только для государственных и муниципальных органов — от 6000 до 12 000 руб. для должностных лиц (п. 7 ст. 13.11 КоАП).

Вместе с тем есть общая норма, которая предусматривает штрафы за нарушение законодательства об обработке персональных данных (п. 1 ст. 13.11 КоАП). Поэтому штраф для компании может достигнуть 300 000 руб. и 100 000 руб. для должностного лица — директора или того лица, на которое возложили такие полномочия.

Высока вероятность, что и пункт 7 статьи 13.11 КоАП скоро будет распространяться на всех операторов персональных данных без исключения. Поэтому уже сейчас важно не просто формально знать о новых правилах, а внедрить их в повседневную практику работы