

Правила работы с обезличенными персональными данными В МБДОУ ДСКВ № 21 «Елочка»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными МБДОУ ДСКВ № 21 «Елочка» разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных» и Методических рекомендаций по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013).

1.2. Настоящие Правила определяют порядок работы с обезличенными данными Оператора.

1.3. Настоящие Правила утверждаются директором школы и действуют постоянно.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных» и Методическими рекомендациями по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»:

2.1.1 **атрибут персональных данных субъекта** - элемент структуры персональных данных (параметр персональных данных). Атрибут имеет название и может иметь множество возможных количественных и качественных значений применительно к конкретным субъектам персональных данных

2.1.2 **деобезличивание** - действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными

2.1.3 **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и

обеспечивающих их обработку информационных технологий и технических средств.

2.1.4 **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;

2.1.5 **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.1.6 **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.1.7 **семантика атрибута персональных данных** - смысловое значение названия атрибута, обозначения персональных данных

III. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

3.1. Требования к свойствам получаемых обезличенных данных:

3.1.1. сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);

3.1.2. сохранение структурированности обезличиваемых персональных данных;

3.1.3. сохранение семантической целостности обезличиваемых персональных данных;

3.1.4. анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания как, например, k-anonymity).

3.2. Требования к свойствам метода обезличивания:

3.2.1. обратимость (возможность проведения деобезличивания);

3.2.2. возможность обеспечения заданного уровня анонимности;

3.2.3. увеличение стойкости при увеличении объема обезличиваемых персональных данных.

3.3. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных Оператора и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.4. Способы обезличивания при условии дальнейшей обработки персональных данных:

3.2.1 Замена части сведений идентификаторами (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным). Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия

3.2.2 Метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений). Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта. При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

3.2.3 Метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств). Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

3.2.4 Метод перемешивания (перестановка отдельных записей, а так же групп записей в массиве персональных данных). Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи. Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

3.5. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.6. При использовании Оператором процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

3.7. Обезличивание персональных данных субъектов должно производиться Оператором перед внесением их в информационную систему.

3.8. В процессе обработки обезличенных данных Оператором, при необходимости, может проводиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

3.9. Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

3.10. Ответственным за проведение мероприятий по обезличиванию обрабатываемых персональных данных является лицо Оператора, ответственное за организацию обработки персональных данных.

3.11. Порядок обезличивания:

3.11.1. Руководители структурных подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения директору школы по обезличиванию персональных данных с обоснованием такой необходимости и указанием способа обезличивания.

3.11.2. Директор школы принимает решение о необходимости обезличивания персональных данных.

3.11.3. Администратор информационных систем персональных данных в школе совместно с ответственным за организацию обработки персональных данных осуществляют непосредственное обезличивание персональных данных.

IV. ПРОЦЕДУРЫ ОБЕЗЛИЧИВАНИЯ

4.1. 2.1. Процедура реализации метода введения идентификаторов

4.1.1. Каждому значению идентификатора должно соответствовать одно значение атрибута и каждому значению атрибута должно соответствовать одно значение идентификатора.

4.1.2. Таблицы соответствия (дополнительные данные) создаются для каждого атрибута персональных данных, значения которых заменяются идентификаторами.

4.1.3. При обезличивании персональные данные в исходном множестве заменяются идентификаторами согласно таблице соответствия. Деобезличивание достигается обратной заменой идентификаторов на значения персональных данных по таблице соответствия.

4.1.4. На этапе реализации процедуры обезличивания определяются следующие параметры:

4.1.4.1. перечень таблиц соответствия (перечень атрибутов, для которых происходит замена значений идентификаторами);

4.1.4.2. правила вычисления идентификаторов - наборов символов, однозначно соответствующих значениям атрибутов персональных данных субъекта;

4.1.4.3. объемы таблицы соответствия - количество строк таблицы соответствия, содержащих идентификатор и соответствующее ему значение.

4.1.5. В качестве атрибутов, значения которых заменяются идентификаторами, как правило, выбираются атрибуты, однозначно идентифицирующие субъекта персональных данных.

4.1.6. Количество идентификаторов и объем таблиц соответствия, как правило, равны исходному количеству субъектов персональных данных. Возможны случаи, когда идентификатор вычисляется в зависимости от значения соответствующего атрибута.

4.1.7. Таблицы соответствия должны быть доступны ограниченному числу сотрудников Оператора.

4.1.8. Программное обеспечение, реализующее процедуру, должно обеспечивать внесение изменений и поддержку актуальности таблиц соответствия.

4.2. Процедура реализации метода изменения состава или семантики

4.2.1. Процедура реализации метода должна содержать правила удаления либо замены значений персональных данных субъектов на новые значения, вычисляемые по заданным правилам.

4.2.2. При замене значений атрибутов на новые требуется устанавливать правила обратной замены, если это необходимо для деобезличивания.

4.2.3. На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

4.2.3.1. перечень атрибутов персональных данных, подлежащих удалению;

4.2.3.2. перечень атрибутов персональных данных, подлежащих замене на новые значения;

4.2.3.3. правила вычисления значений для замены (обратной замены) персональных данных субъектов.

4.2.4. Программная реализация процедуры должна обеспечить возможность внесения изменений и дополнений в состав обезличенных данных, динамическое вычисление значений для замены при занесении новых субъектов, проверку и поддержку актуальности данных.

4.3. Процедура реализации метода декомпозиции

4.3.1. Процедура реализации метода по заданному правилу (алгоритму) производит разделение исходного массива персональных данных на несколько частей, каждая из которых содержит заданный набор атрибутов всех субъектов. Сведения, содержащиеся в каждой части, не позволяют идентифицировать субъектов персональных данных.

4.3.2. Деобезличивание осуществляется по заданному набору связей (используются таблицы связей, являющиеся дополнительными данными) между раздельно хранимыми частями.

4.3.3. На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

4.3.3.1. перечень атрибутов, составляющих подмножества персональных данных;

4.3.3.2. таблицы связей между подмножествами персональных данных;

4.3.3.3. адреса хранения подмножеств персональных данных.

4.3.4. Правила разделения исходного массива данных определяются таким образом, чтобы каждая из раздельно хранимых частей не содержала сведений, позволяющих однозначно идентифицировать субъекта персональных данных.

4.3.5. Программная реализация процедуры должна обеспечивать

согласованное внесение изменений и дополнений во все подмножества и таблицы связей, поиск данных о субъекте во всех подмножествах, поддержку актуальности таблиц связей, проверку полноты данных (согласование подмножеств).

4.4. Процедура реализации метода перемешивания

4.4.1. Метод перемешивания реализуется путем перемешивания отдельных значений или групп значений атрибутов субъектов персональных данных между собой.

4.4.2. Перемешивание проводится по установленному правилу.

4.4.3. Деобезличивание достигается с использованием процедуры, обратной процедуре перемешивания.

4.4.4. Для реализации процедуры необходимо определить алгоритм перемешивания и его параметры.

4.4.5. На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

4.4.5.1. набор параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания);

4.4.5.2. значения параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания).

4.4.6. Выбор параметров перемешивания зависит от алгоритма перемешивания, требуемой стойкости к атакам, и объема обезличиваемых персональных данных.

4.4.7. Программная реализация процедуры должна обеспечивать возможность внесения изменений и дополнений в состав обезличенных данных, добавление новых пользователей, поддержку актуальности данных и возможность повторного перемешивания с новыми параметрами без предварительного деобезличивания.

V. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

5.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

5.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

5.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

5.3.1 парольной политики;

5.3.2 антивирусной политики;

5.3.3 правил работы со съемными носителями (если они используются);

5.3.4 правил резервного копирования;

5.3.5 правил доступа в помещения, где расположены элементы информационных систем.

5.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

5.4.1 правил хранения бумажных носителей;

5.4.2 правил доступа к ним и в помещения, где они хранятся.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный за обработку ПДн несёт персональную ответственность за соблюдение требований настоящих Правил в ИСПДн Оператора, за качество проводимых им работ по обезличиванию персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Ответственный за обработку ПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

6.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Оператора, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник Оператора, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Оператору (в соответствии с п.7 ст. 243 Трудового кодекса РФ).