КОМИТЕТ
РЕСПУБЛИКИ СЕВЕРНАЯ ОСЕТИЯ-АЛАНИЯ
ПО ЗАНЯТОСТИ НАСЕЛЕНИЯ

ПРИКАЗ

«11» 08 2022 г. № 100-р

г. Владикавказ

Об утверждении некоторых локальных актов в области защиты персональных данных в Комитете РСО-Алания по занятости населения

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, **п р и к а з ы в а ю:**

1. **УТВЕРДИТЬ** следующие локальные акты в области защиты персональных данных Комитета Республики Северная Осетия-Алания по занятости населения:

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Комитете РСО-Алания по занятости населения (Приложение 1);

Правила работы с обезличенными данными в случае обезличивания данных в Комитете РСО-Алания по занятости населения (Приложение 2).

Перечень мер, направленных на исключение несанкционированного доступа и обеспечивающих сохранность персональных данных в Комитете РСО-Алания по занятости населения (Приложение 3).

2. Козаевой И.Б. – ведущему советнику отдела организационной, кадровой работы и противодействия коррупции ознакомить с приказом касающихся лиц под роспись.

3. Контроль за исполнением настоящего приказа возложить на начальника отдела информационных технологий и автоматизации Амирову И.Л.

Председатель **А.А. Плаева**

Приложение 1

УТВЕРЖДАЮ
Председатель Комитета
РСО-Алания по занятости населения

А.А. Плаева

2022 г.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Комитете РСО-Алания по занятости населения

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Комитете РСО-Алания по занятости населения (далее - Правила) разработаны с учетом требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных Комитете РСО-Алания по занятости населения и действуют постоянно.

Исполнение данных Правил обязательно для всех работников Комитета, осуществляющих обработку персональных данных (далее - ПДн), как без использования средств автоматизации, так и в информационных системах обработки персональных данных (далее - ИСПДн).

2. Порядок проведения внутренних проверок

Внутренний контроль соответствия обработки персональных данных установленным требованиям организуется Оператором на основе проведения периодических проверок условий обработки ПДн.

Проверки осуществляются сотрудниками отдела информационных технологий и автоматизации.

Внутренние проверки также могут проводиться по необходимости и в соответствии с отдельным поручением председателя Комитета РСО-Алания по занятости населения.

Проверки осуществляются непосредственно на местах обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников Комитета РСО-Алания по занятости населения, допущенных к обработке персональных данных.

Результаты каждой проверки оформляются Протоколом проведения внутренней проверки, форма которого установлена в Приложением к настоящим Правилам.

При выявлении в ходе проверки нарушений в Протоколе делается запись о мероприятиях, необходимых для устранения нарушений, сроках исполнения и ответственных лицах.

Протоколы проверок хранятся в сейфе кабинета N 8. Начальник отдела ИТА обязан информировать председателя Комитета РСО-Алания по занятости населения по результатам всех проверок, в результате которых были выявлены нарушения, а также о мерах, которые необходимо принять для их устранения.

3. Содержание проверок внутреннего контроля

В процессе проверки соответствия обработки персональных данных без использования средств автоматизации требованиям к защите персональных данных должно быть установлено:

- порядок и условия хранения бумажных носителей, содержащих персональные данные обрабатываемые в Комитете;
- соблюдение правил доступа к бумажным носителям с персональными данными;
- условия доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными;
- наличие или отсутствие фактов несанкционированного доступа к персональным данным и необходимость принятия дополнительных мер по обеспечению безопасности ПДн.

При проведении проверки соответствия обработки персональных данных в ИСПДн Комитета требованиям к защите персональных данных должно быть установлено:

- соответствие используемых Пользователями полномочий параметрам доступа;
- соблюдение Пользователями ИСПДн правил парольной защиты;
- соблюдение Пользователями ИСПДн правил антивирусной защиты;
- соблюдение Пользователями ИСПДн правил работы со съемными носителями персональных данных;
- соблюдение порядка доступа в помещения Комитета, где расположены элементы ИСПДн;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- своевременность проведения мероприятий по уничтожению персональных данных;
- знание Пользователями ИСПДн своих действий во внештатных ситуациях;
- наличие или отсутствие фактов несанкционированного доступа к ИСПДн и необходимость принятия дополнительных мер по обеспечению безопасности ПДн;
- необходимость мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Приложение к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Комитете РСО-Алания по занятости населения

ПРОТОКОЛ
результатов проведения внутренней проверки условий обработки персональных данных в Комитете РСО-Алания по занятости населения

Настоящий Протокол составлен в том, что "__" _____ 20__ года в Комитете РСО-Алания по занятости населения проведена проверка

_____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями

_____

(название внутреннего локального акта)

В ходе проверки проверено:

_____

_____

Выявленные нарушения:

_____

_____

Меры по устранению нарушений:

_____

_____

Срок устранения нарушений: _____

Ответственный за исполнение _____

Подписи проверявших: _____

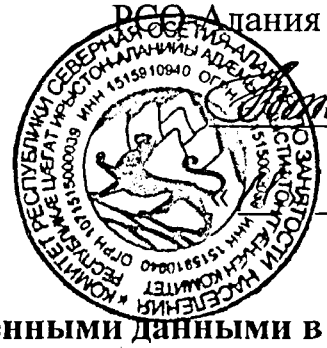
_____

_____

"__" _____ 20__ года

Приложение 2

УТВЕРЖДАЮ
Председатель Комитета
РСО-Алания по занятости населения



_____ А.А. Плаева

08 2022 г.

Правила работы с обезличенными данными в случае обезличивания персональных данных в Комитете РСО-Алания по занятости населения

1. Общие положения

1.1. Настоящие Правила работы с обезличенными данными в случае обезличивания персональных данных в Комитете РСО-Алания по занятости населения (далее - Правила) утверждены в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

1.2. Под обезличиванием персональных данных понимаются действия уполномоченных лиц Комитета РСО-Алания по занятости населения, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных, обрабатываемых у операторов, конкретному субъекту персональных данных.

1.3. Под уполномоченными лицами для целей настоящих Правил понимаются муниципальные служащие оператора, замещающие должности, которые содержатся в перечне должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

2. Условия обезличивания персональных данных

2.1. Обезличивание персональных данных может быть проведено в статистических целях и в целях предупреждения ущерба от разглашения персональных данных.

2.2. Обезличивание персональных данных может быть проведено по решению руководителя оператора (председателя Комитета) и лица, ответственного за организацию обработки персональных данных у оператора.

2.3. Могут быть использованы следующие способы обезличивания персональных данных при условии их дальнейшей обработки:

1) сокращение перечня обрабатываемых персональных данных;

2) замена части сведений идентификаторами;

3) понижение точности некоторых сведений в зависимости от цели обработки персональных данных;

4) обработка разных персональных данных в разных информационных системах;

5) иными способами, определяемыми оператором, исходя из целей обезличивания персональных данных.

2.4. Непосредственное обезличивание персональных данных и ответственность за осуществление таких действий несут уполномоченные лица.

3. Порядок работы с обезличенными данными

3.1. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

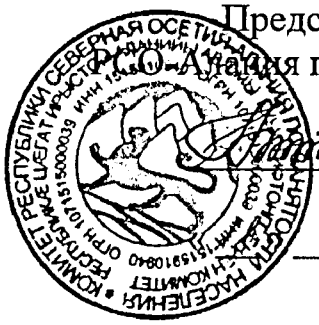
3.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение парольной политики, антивирусной политики, правил работы со съемными носителями (если они используются), правил резервного копирования, порядка доступа в помещения, где расположены информационные системы персональных данных.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил хранения бумажных носителей и правил доступа в помещения, где они хранятся.

Приложение 3

УТВЕРЖДАЮ
Председатель Комитета
РСО-Алания по занятости населения



_____ А.А. Плаева

08 2022 г.

Перечень мер, направленных на исключение несанкционированного доступа и обеспечивающих сохранность персональных данных в Комитете РСО-Алания по занятости населения

1. Комитет РСО-Алания по занятости населения (далее – Оператор) обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями 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 Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; нормативными правовыми актами, принятыми Федеральной службой по техническому и экспортному контролю.

2. При обработке персональных данных Оператор принимает необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Обеспечение безопасности персональных данных достигается, в частности, посредством:

определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработки моделей угроз;

применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

проведения оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

организации учета машинных носителей персональных данных;

обнаружения фактов несанкционированного доступа к персональным данным и принятия мер по их недопущению;

возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

контроля над принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

4. В целях обеспечения безопасности персональных данных, обрабатываемых без использования средств автоматизации, в отношении каждой категории персональных данных Оператором определяются места хранения персональных данных (материальных носителей) и устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. Оператором обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

5. В целях исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при обработке персональных данных в информационных системах, Оператор использует средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Используются технические и программные средства удовлетворяющие устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

6. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Классификация информационных систем персональных данных осуществляется Оператором в порядке, установленном законодательством Российской Федерации.

7. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8. Персональные данные, обрабатываемые в информационных системах, могут быть представлены для ознакомления:

должностным лицам Оператора, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;

уполномоченным лицам, осуществляющим обработку персональных данных по поручению Оператора на основании заключенного с ним договора;

уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

Должностные лица, доступ которым к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей, допускаются к соответствующим персональным данным на основании утвержденного Операторам списка.

9. При обнаружении нарушений порядка предоставления персональных данных Оператор приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

10. В целях реализации, эксплуатации, контроля и поддержания на должном уровне системы обеспечения информационной безопасности Оператором назначено должностное лицо, ответственное за организацию обработки Оператором персональных данных, за выполнение законодательных требований при их обработке, за обеспечение информационной безопасности Оператора.

11. Организован контролируемый доступ на территорию Оператора, круглосуточная охрана и видео-мониторинг контролируемой зоны.