Приложение 1
к приказу от 31.08.2018 № 16

муниципальное казенное учреждение
«Управление гражданской защиты»

ПОЛОЖЕНИЕ

об организации работы с персональными данными и гарантиях их защиты

г. Чусовой

2018 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика оператора

Настоящее Положение «Об организации работы с персональными данными и гарантиях их защиты" определяет политику юридического лица (оператора) - муниципального казенного учреждения «Управление гражданской защиты» (далее Управление ГЗ) в отношении обработки и защиты персональных данных.

Положение «Об организации работы с персональными данными и гарантиях их защиты" (далее - Положение) устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

Положение разработано в соответствии:

- с Конституцией РФ;
- гл. 14 Трудового кодекса Российской Федерации;
- Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных";
- Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации";
- Федеральным законом от 2 мая 2006 года N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации"
- Федеральным законом от 7 июля 2003 года N 126-ФЗ "О связи", Законом Российской Федерации от 27 декабря 1991 года N 2124-1 "О средствах массовой информации",
- Федеральным законом "О противодействии коррупции"
- Федеральным законом «О защите населения и территорий от ЧС природного и техногенного характера» от 21.12.1994 № 68-ФЗ;
- Федеральным законом «О гражданской обороне» от 12.02.1998 № 28-ФЗ
- Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
- Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».
- Приказом ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».
- Уставом муниципального казенного учреждения «Управление гражданской защиты», утвержденным постановлением администрации Чусовского муниципального района Пермского края от 04.10.2011 г. № 965
- Учебным пособием «Информационная безопасность для работников бюджетной сферы. Защита персональных данных» М.И. Шубинский ИТМО Национальный исследовательский университет г. Санкт-Петербург 2013 год

1.2. Цели Положения

Настоящее положение разработано в целях:

- регламентации порядка защиты и осуществления операций с персональными данными с учетом требований закона № 152-ФЗ и иных правовых актов, регулирующих использование персональных данных;
-осуществления Управлением ГЗ полномочий и видов деятельности в соответствии с Уставом, а также для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Управление ГЗ функций, полномочий и обязанностей;
- осуществления Управлением ГЗ административно-хозяйственной и управленческой деятельности;
- заключения с субъектом ПД любых договоров и их дальнейшего исполнения;
- ведение кадровой работы и организации учета работников;
- формирования отчетности и предоставление ее в государственные органы;
- привлечения и отбора кандидатов на вакантные должности;
- заключения и исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПД;

1.3. Действие Положения

Настоящее Положение является локальным правовым актом Управления ГЗ.

Действие настоящего Положения распространяется на все процессы обработки и защиты персональных данных и обязательно для соблюдения всеми сотрудниками, имеющими допуск к осуществлению сбора, использования и обработки информации составляющей персональные данные.

1.4. Порядок пересмотра Положения

Пересмотр настоящего Положения должен осуществляться:

- в случае изменения процессов обработки и защиты информации;
- при выявлении угроз безопасности информации и определении необходимости реализации дополнительных защитных мер;
- при изменении действующего законодательства в области защиты информации ограниченного доступа.

1.5. Основные понятия, используемые в настоящем Положении

В целях исполнения Федерального закона № 152-ФЗ «О защите персональных данных» в настоящем Положении используются следующие основные понятия:

*1) **персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (сотруднику или гражданину, обратившемуся за услугой – т.е. субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;*

*2) **оператор** - государственный орган, муниципальный орган, **юридическое** или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;*

*3) **обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;*

*4) **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в*

информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

*5) **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;*

*6) **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;*

*7) **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;*

*8) **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному человеку -субъекту персональных данных;*

*9) **информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;*

*10) **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;*

*11) **трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;*

*12) **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.*

1.6. Доступ к персональным данным

1.6.1. Сотрудники Управления ГЗ, которые в силу выполняемых служебных обязанностей постоянно работают с ПД, получают допуск к необходимым категориям ПД на срок выполнения ими соответствующих должностных обязанностей на основании перечня должностных лиц, допущенных к работе с ПД, утверждаемого приказом директора.

1.6.2. Списки должностных лиц, имеющих доступ к ПД должны поддерживаться в актуальном состоянии.

1.6.3. Сотрудникам Управления ГЗ предоставляется доступ к работе с ПД исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей по согласованию директора Управления ГЗ.

1.6.4. Доступ к ПД третьих лиц, не являющихся сотрудниками Управления ГЗ без согласия субъекта ПД, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с разрешения директора Управления ГЗ

1.6.5. В случае если сотруднику сторонней организации необходим доступ к ПД Управления ГЗ, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПД и обязанность сторонней организации и ее сотрудников по соблюдению требований действующего законодательства в области защиты ПД.

1.6.6. Передача личных сведений третьим лицам допускается только при получении согласия от лица, которому принадлежат ПД (от сотрудников, физических лиц, пользователей информационных и телекоммуникационных сетей интернета и иных). Согласие о предоставлении личных данных оформляется в любой, подтверждающей этот факт форме. (Приложение – образец уведомления и согласия о передаче ПД третьим лицам)

1.6.7. Сотрудники, занимающиеся обработкой ПД обязаны ознакомиться с соглашением об их неразглашении в соответствии с положениями 152-ФЗ и Трудового кодекса.

1.6.8. Доступ сотрудника Управления ГЗ к ПД прекращается с даты, прекращения с трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПД. В случае увольнения все носители, содержащие ПД, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

1.7. Способы обработки персональных данных

1.7.1. Управление ГЗ может самостоятельно выбирать способы обработки ПД в зависимости от целей такой обработки и собственных материально-технических возможностей.

1.7.2. Управление ГЗ обрабатывает ПД следующими способами:

Неавтоматизированная обработка ПД (на бумажных носителях);

Автоматизированная обработка (в ИСПД с использованием и без использования средств автоматизации), в том числе: с передачей и без передачи по локальной сети Управления ГЗ; с передачей и без передачи по сети Интернет;

Смешанная обработка ПД.

1.7.3. Работа с персональными данными в Управлении ГЗ производится с учетом направлений деятельности структурных подразделений в двух подсистемах:

- подсистема **Персональные данные сотрудников»**
- подсистема **Персональные данные субъектов»**

Доступ к персональным данным с закреплением полноты доступа и прав должностных лиц устанавливается приказом директора для каждой подсистемы отдельно.

2.УСЛОВИЯ И ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ

2.1. Цели обработки персональных данных сотрудников

Персональные данные сотрудников Управления ГЗ (в т.ч. граждан, претендующих на вакантные должности) обрабатываются **в целях** обеспечения работы с кадрами, в том числе в целях обучения и должностного роста, учета результатов исполнения сотрудниками должностных обязанностей, формирования кадрового резерва, оплаты труда, воинского учета, обеспечения сотрудникам и членам их семей установленных законодательством Российской Федерации гарантий и компенсаций.

2.2.Категории персональных данных сотрудников

В целях, указанных в пункте 2.1. настоящего Положения, обрабатываются следующие категории персональных данных сотрудников (в т.ч. граждан претендующих на вакантные должности):

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего приему на должность или работе в занимаемой должности;
- фотография;
- информация, содержащаяся в Трудовом договоре, дополнительных соглашениях к Трудовому договору;
- информация о наличии или отсутствии судимости;
- информация об оформленных допусках к государственной тайне;
- государственные награды, иные награды и знаки отличия;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения заработной платы;
- номер расчетного счета, реквизиты банка (для перечисления);
- иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1 настоящего Положения.

2.3. Биометрические персональные данные

2.3.1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПД) и которые используются для установления личности субъекта ПД, могут обрабатываться только при наличии согласия в письменной форме субъекта ПД, за исключением случаев, предусмотренных ч. 2 ст. 11 ФЗ № 152.

Биометрические данные содержатся:

- в документах воинского учета;
- дактилоскопических картах персонала Поисково-спасательного отряда;
- медицинских документах;

2.3.2. Обработка биометрических персональных данных и специальных категорий персональных данных сотрудников, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.1. настоящего Положения, в соответствии с пунктом 2 части 1 статьи 6, частью 2 статьи 11 и в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона "О персональных данных", а также положениями Федерального закона "О противодействии коррупции", Трудовым кодексом Российской

Федерации, в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Использование и хранение биометрических ПД вне информационных систем ПД могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

2.4. Порядок обработки персональных данных сотрудников

Обработка персональных данных сотрудников Управления ГЗ (в т.ч. граждан, претендующих на вакантные должности), в рамках целей указанных в п. 2.1. настоящего Положения **осуществляется без согласия указанных лиц**, в соответствии с пунктом 2 части 1 статьи 6 Федерального закона № 152-ФЗ "О персональных данных", Федерального закона "О противодействии коррупции", Трудовым кодексом Российской Федерации.

2.5. Условия обработки персональных данных, при которых согласие не требуется:

- для сбора информации, который регулируется федеральным законодательством;
- для отправления правосудия;
- для оказания государственных услуг;
- для исполнения трудового договора, (договора услуг - если субъект получает что-либо по сделке, либо поручается за сторону договора);
- если использование персональных сведений необходимо, чтобы защитить права субъекта, а оформить согласие на обработку персональных данных не представляется возможным;
- если использование необходимо, чтобы защитить права третьих лиц, либо это нужно для общественных целей (при условии, что не нарушаются права никаких иных физических лиц);
- в процессе журналисткой деятельности, в творчестве (при условии, что не ставятся по угрозу права иных физических лиц);
- для сбора статистики или проведения иных исследований (при этом информация о субъектах должна быть обезличена);
-если обрабатываются открытые данные (при условии, что доступными они стали на законном основании, а не посредством простого обнародования третьими лицами);
- при использовании данных, которые в Российской Федерации должны размещаться публично.

Во всех прочих случаях согласие субъекта на обработку персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом "О персональных данных".

2.6. Согласие на обработку ПДн

2.6.1. Субъект ПД самостоятельно принимает решение о предоставлении своих ПД и дает согласие на их обработку свободно, своей волей и в своих интересах. Согласие на обработку ПД должно быть конкретным, информированным и сознательным. Согласие на обработку ПД может быть дано как субъектом ПД так и его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ. В случае получения согласия на обработку ПД от представителя субъекта ПД полномочия данного представителя на дачу согласия от имени субъекта ПД проверяются Управлением ГЗ. (ст.9 закона)

2.6.2. Получение письменного согласия на обработку ПД осуществляется, при получении ПД от субъекта, путем оформления письменного согласия по форме, установленной в Управлении ГЗ. (Приложение -согласие на обработку ПД)
2.6.3. Обработка персональных данных сотрудников Управления ГЗ (в т.ч. граждан, претендующих на вакантные должности) осуществляется при условии получения согласия указанных лиц в следующих случаях:
- при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации;
- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.7. Обработка персональных данных в кадровом делопроизводстве и бухгалтерском учете

2.7.1 обработка персональных данных сотрудников Управления ГЗ (в т.ч. граждан, претендующих на вакантные должности), осуществляется сотрудниками, в обязанности которых входит ведение кадровой работы и бухгалтерского учета, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
2.7.2. сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем:
- получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в кадровое подразделение);
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадрового делопроизводства и бухгалтерской работы;
2.7.3. внесения персональных данных в информационные системы, используемые в кадровом делопроизводстве и бухгалтерском учете.
2.7.4. сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от сотрудников (в т.ч. граждан, претендующих на вакантные должности)
2.7.5. в случае возникновения необходимости получения персональных данных сотрудника у третьей стороны, должностным лицам следует известить об этом самого сотрудника заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных. (Приложение - уведомление и согласие субъекта ПД на получение ПД у третей стороны)
2.7.6. запрещается получать, обрабатывать и приобщать к личному делу сотрудника Управления ГЗ персональные данные, не предусмотренные пунктом 2.2. настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.
2.7.7. копии личных документов сотрудников могут храниться в личных делах и документах бухгалтерского учета только с письменного согласия самих сотрудников. (Приложение – Согласие на хранение копий личных документов)
2.7.8. сотрудник, отвечающий за работу с кадрами в Управлении ГЗ, осуществляющий сбор персональных данных непосредственно от сотрудников (в т.ч. граждан, претендующих на вакантные должности), обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.7.9. передача (распространение, предоставление) и использование персональных данных сотрудников Управления ГЗ в том числе граждан, претендующих на вакантные должности, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.
2.7.10. должностные лица обеспечивающие работу кадров и бухгалтерии обеспечивают сохранность персональных данных, принимают меры по их защите.
2.7.11. защита персональных данных сотрудников от неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

3.УСЛОВИЯ И ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЬЕКТОВ (физических лиц)

3.1. Обработка персональных данных субъектов (физических лиц)

3.1.1. Обработка персональных данных физических лиц (заявителей, граждан обратившихся за услугой, состоящих в договорных отношениях с Управлением ГЗ и т.д.) – **субъектов**, осуществляется в целях предоставления услуг и исполнения условий заключенных договоров, соглашений и функций в соответствии с видами деятельности по направлениям согласно полномочиям и Уставной деятельности Управления ГЗ.
3.1.2. Персональные данные физических лиц - субъектов, обратившихся в Управление ГЗ лично, а также направивших индивидуальные или коллективные письменные обращения (заявления, жалобы), обращения в форме электронного документа или посредством телефонной связи, обрабатываются для рассмотрения таких обращений, решения поставленных задач в рамках полномочий, оказания услуг и последующим уведомлением заявителей о результатах рассмотрения в случае поступления запросов.

3.2. Перечень подлежащих обработке персональных данных субъектов

Для рассмотрения обращений субъектов и выполнения условий договоров, заключаемых Управлением ГЗ в рамках действующих полномочий согласно Уставной деятельности по направлениям функционала структурных подразделений, подлежат обработке следующие персональные данные субъектов:
- фамилия, имя, отчество;
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- номер расчетного счета, реквизиты банка (для перечисления);
- информация, содержащаяся в документах установленного образца (в договорах, соглашениях, заявлениях, актах и др.), оформляемых в процессе деятельности;
- иные персональные данные, указанные заявителем в обращении, а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения от субъекта;
- персональные данные, находящиеся в общем доступе.

3.3. Условия обработки персональных данных субъектов

3.3.1. Обработка персональных данных субъектов, происходящая в связи с предоставлением услуг и исполнения функций в соответствии с видами деятельности по направлениям согласно Уставной деятельности Управления ГЗ, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6

Федерального закона "О персональных данных", Федеральным законом "О порядке рассмотрения обращений граждан Российской Федерации" и иными нормативными правовыми актами в установленной сфере деятельности.

3.3.2. Обработка персональных данных субъектов, осуществляемая структурными подразделениями Управления ГЗ, предоставляющими соответствующие услуги и (или) исполняющими определенные функции, включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных).

3.3.3. Прием ПД осуществляется непосредственно от субъектов персональных данных (заявителей) путем:

- получения оригиналов необходимых документов (заявление);
- заверения копий документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- внесения персональных данных в прикладные программные подсистемы;

3.3.4. Запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные при предоставлении услуг и исполнении функций в соответствии с видами деятельности по направлениям в случаях, не предусмотренных законодательством Российской Федерации.

3.3.5. При приеме персональных данных непосредственно от субъекта уполномоченное должностное лицо структурного подразделения Управления ГЗ, обязано разъяснить данному субъекту юридические последствия отказа предоставить персональные данные.

3.3.6. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Управлением ГЗ осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

3.4. Использование типовых форм документов

3.4.1. В структурных подразделениях Управления ГЗ обеспечиваются меры по обработке и защите ПД субъектов по направлениям деятельности.

3.4.2. Обработка персональных данных без использования средств автоматизации осуществляется в виде документов на бумажных носителях.

3.4.3. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.4.5. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

3.4.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных: заявления, акты, договоры, карточки, реестры, журналы и др. (далее - типовые формы), должны соблюдаться следующие условия:

- типовые формы документов должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора (Управления ГЗ), фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с

персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
3.4.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

4.ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Информационные системы обработки ПД в Управлении ГЗ

Обработка персональных данных в Управлении ГЗ осуществляется:
- через программно-аппаратный комплекс, предназначенный для приема, регистрации и обработки обращений в рамках «Системы 112»,
- через программу Table-Pro и систему оповещения «Побудка»;
- в информационной системе "1С: Предприятие 8",
- в «Единая информационная система в сфере закупок»,
- в «Площадка Сбербанк-АТС»
- на рабочих местах сотрудников в структурных подразделениях по направлениям деятельности;

4.2. Персональные данные в информационной системе "1С: Предприятие 8"

Информационная система "1С: Предприятие 8 и прикладные программные подсистемы "1С Бухгалтерия", содержат персональные данные сотрудников Управления ГЗ и физических лиц, являющихся стороной гражданско-правовых договоров, заключаемых Управлением ГЗ, и включает:
- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- место рождения субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- телефон субъекта персональных данных;
- ИНН субъекта персональных данных;
- табельный номер субъекта персональных данных;
- должность субъекта персональных данных;
- номер приказа и дату приема на работу (увольнения) субъекта персональных данных.

4.3. Обработка ПД в информационных системах кадрового делопроизводства и бухгалтерского учета

Обработка ПД в информационных системах кадрового делопроизводства и бухгалтерского учета в Управлении ГЗ предполагает обработку персональных данных сотрудников, предусмотренных пунктом 2.2 настоящего Положения:

4.3.1. При использовании цифровой информационной системы (предназначенной для автоматизированной обработки персональных данных), передача данных осуществляется по защищенным каналам связи, а также при задействовании средств криптозащиты.

4.3.2. При использовании информационной системы на основе бумажных носителей, передача данных осуществляется посредством перемещения или копирования содержимого данных носителей при участии сотрудников, имеющих доступ к соответствующей информационной системе.

4.3.3. Блокирование персональных данных в Управлении ГЗ осуществляется с учетом специфики конкретной информационной системы:

- при использовании цифровой информационной системы, блокирование данных осуществляется посредством закрытия доступа к файлам при задействовании средств криптозащиты.
- при использовании информационной системы на основе бумажных носителей, блокирование данных осуществляется посредством закрытия доступа к соответствующей ИС для определенных групп сотрудников, а также оснащенность рабочих мест соответствующим оборудованием (сейфами и другими системами хранения документов) огранивающим доступ.

4.3.4. Хранение персональных данных осуществляется с учетом специфики конкретной информационной системы

- при использовании цифровой ИС, хранение данных осуществляется на ПК на рабочих местах, а также на облачных серверах.
- при использовании ИС на основе бумажных носителей, хранение данных осуществляется в архиве кадровой службы и бухгалтерии.

4.4. Режимы внесения информации в информационные системы

Информация содержащая персональные данные может вноситься в информационные системы как в автоматическом режиме, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

4.5. Порядок доступа к информационной системе

Сотрудникам Управления ГЗ, имеющим право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе.

Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами.

4.6. При работе в информационных системах ПД запрещается:

Сотрудникам Управления ГЗ при работе в информационных системах содержащими персональные данные запрещается:

а) записывать значения кодов и паролей доступа к информационным системам персональных данных;

б) передавать коды и пароли доступа к информационным системам персональных данных другим лицам;

в) пользоваться в работе кодами и паролями других пользователей доступа к информационным системам персональных данных;

г) производить подбор кодов и паролей доступа к информационным системам персональных данных других пользователей;

д) записывать на электронные носители с персональными данными посторонние программы и данные;
е) копировать информацию с персональными данными на неучтенные электронные носители информации;
ж) выносить электронные носители с персональными данными за пределы Управления ГЗ;
з) покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств блокирования, доступа к персональному компьютеру;
и) приносить, самостоятельно устанавливать и эксплуатировать на персональном компьютере любые программные продукты, не принятые к эксплуатации;
к) открывать, разбирать, ремонтировать персональные компьютеры, вносить изменения в конструкцию, подключать нештатные блоки и устройства;
л) передавать информацию, содержащую персональные данные, подлежащие защите, по открытым каналам связи (факсимильная связь, электронная почта и иное), а также использовать сведения, содержащие персональные данные, подлежащие защите, в открытой переписке и при ведении переговоров по телефону.

5.ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Требования по защите ПД реализуемые в Управлении ГЗ

Управление ГЗ принимает правовые, организационные и технические меры, необходимые для выполнения предусмотренных законодательством обязанностей по защите ПД и обеспечению прав субъектов ПД, в частности:
- назначение лица ответственного за организацию обработки и защиты ПД;
- утверждение Положения определяющего политику в области ПД, а также издание локальных нормативных актов по вопросам обработки ПД, выявление и предотвращение нарушений законодательства РФ о ПД, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности ПД;
- организация внутреннего контроля процедур обработки ПД;
- оценка вреда, который может быть причинен субъектам ПД в случае нарушения требований законодательства, соотношение указанного вреда и мер, предпринимаемых Управлением ГЗ по его минимизации и соблюдению требований законодательства о ПД;
- применение сертифицированных технических и криптографических средств защиты ПД при обработке ПД в информационных системах.

5.2. Система защиты информации

Обеспечение защиты информации, составляющей персональные данные при ее обработке реализуется с помощью **системы защиты информации** (далее – СЗИ).

5.2.1. Задачами, решаемыми СЗИ, являются:
- предотвращение неправомерного доступа, копирования, предоставления или распространения информации, составляющей персональные данные, обрабатываемой в информационных системах (*обеспечение конфиденциальности информации*);
- исключение неправомерного уничтожения или модификации информации, составляющей персональные данные, обрабатываемой в информационных системах (*обеспечение целостности информации*);
- исключение неправомерного блокирования информации составляющей персональные данные, обрабатываемой в информационных системах (*обеспечение доступности информации*).

5.2.2. Объектами защиты являются:
- информация, составляющая персональные данные, содержащаяся в информационной системе;
- рабочие станции пользователей;
- мобильные технические средства (ноутбуки);
- машинные носители информации;
- системы связи и передачи данных;
- общесистемное, прикладное, специальное программное обеспечение;

5.2.3. Меры защиты информации от несанкционированного доступа и других неправомерных воздействий:
- идентификация и аутентификация субъектов и объектов доступа ;
- защита машинных носителей информации;
- регистрация событий безопасности
- антивирусная защита;
- обнаружение вторжений;
- контроль (анализ) защищенности информации;
- защита технических средств;

5.2.4. Для обеспечения защиты информации, содержащейся в информационных системах, применяются средства защиты, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.
5.2.5. Для защиты мобильных устройств (ноутбуков) применяются те же меры защиты, что и для стационарных рабочих станций пользователей.
5.2.6. Мероприятия по защите информации фиксируются в Журнале учета мероприятий по защите информации по форме согласно Приложению. (Приложение - Журнал учета мероприятий по защите информации.

5.3. Порядок использования технических средств и средств защиты информации

3.5.1. Подлежат резервному копированию используемые информационные системы, а так же прикладное программное обеспечение, предназначенное для работы с этими системами в случае, если они подвергаются модификации.
3.5.2. Резервное копирование должно осуществляться периодически на рабочих местах должностными лицами, имеющими соответствующий уровень допуска, путем записи на отчуждаемый носитель информации.
3.5.3. Запрещено бесконтрольное использование USB-флеш-накопителей и др. неучтенного оборудования для архивирования сведений.
3.5.4. Работа с Персональными данными в информационных системах допускается только при наличии антивирусной защиты.
3.5.5. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов либо полного восстановления системы с образа диска.
3.5.6. Работа с использованием неисправных технических средств запрещается.
3.5.7. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации.
3.5.8. При работе на ПК рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

5.4. Организация ответственным лицом мероприятий защиты ПД

Лицом, ответственным *за организацию работ с персональными данными, информационную безопасность и техническую защиту информации о персональных данных в Управлении ГЗ*, **организуется обеспечение комплекса мер защиты и**

безопасности персональных данных, обрабатываемых в информационных системах, и достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, принятием **следующих мер по обеспечению безопасности**:
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение 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;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- организация и контроль ведения учета материальных носителей персональных данных;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных;
- разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5.5. Обеспечение должностными лицами мер защиты ПД

5.5.1.Должностные лица, ответственные за обеспечение безопасности персональных данных на рабочих местах при их обработке в информационных системах персональных данных, **должны обеспечить**:
- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до лица ответственного за организацию работ с персональными данными, информационную безопасность и техническую защиту информации о персональных данных в Управлении ГЗ;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (защищенное резервное копирование);
- постоянный контроль за обеспечением уровня защищенности персональных данных на рабочих местах по своим направлениям деятельности;

- соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин.

6. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Сроки обработки и хранения персональных данных сотрудников и субъектов определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных сотрудников:
6.1.1. Персональные данные, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок), содержащиеся в личных делах сотрудников, в приказах о поощрениях, материальной помощи сотрудников, подлежат хранению в течение 75 лет.
6.1.2. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных командировках, о дисциплинарных взысканиях сотрудников, подлежат хранению в течение пяти лет с последующим уничтожением.
6.1.3. Персональные данные, содержащиеся в документах претендентов на вакантные должности, хранятся в кадровом подразделении в течение 3 лет со дня, после чего подлежат уничтожению.
6.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Управлении ГЗ, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.
6.3. Персональные данные граждан, обратившихся в Управление ГЗ лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет.
6.4. Персональные данные субъектов на бумажных носителях, обрабатываемые в Управлении ГЗ, хранятся в структурных подразделениях (у сотрудников), имеющих допуск к обработке соответствующих ПД и формируются по направлениям деятельности. Носители ПД не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПД должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПД осуществляется по возможности их восстановление.
6.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).
6.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.
6.7. Руководители структурных подразделений осуществляют контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях.
6.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных должен соответствовать сроку хранения бумажных оригиналов.

7. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В структурных подразделениях Управления ГЗ должен осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.
7.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается комиссионно. Состав комиссии утверждается директором Управления ГЗ. По итогам заседания составляются Протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии и утверждается директором Управления ГЗ.
7.3. Уничтожение документов содержащих персональные данные осуществляется путем сожжения или измельчения на спец. оборудовании, после утверждения Акта.
7.4. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

8. РАССМОТРЕНИЕ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

8.1. Сотрудники Управления ГЗ (в т.ч. граждане, претендующие на вакантные должности) и лица, состоящие с ними в родстве, а также граждане, персональные данные которых обрабатываются в Управлении ГЗ в связи с предоставлением услуг в соответствии с видами деятельности по направлениям, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:
8.1.1. подтверждение факта обработки персональных данных;
8.1.2. правовые основания и цели обработки персональных данных;
8.1.3. применяемые способы обработки персональных данных;
8.1.4. наименование и место нахождения Управления ГЗ, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании федерального закона;
8.1.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
8.1.6. сроки обработки персональных данных, в том числе сроки их хранения;
8.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
8.1.8. информацию о возможности трансграничной передаче данных;
8.1.9. наименование организации или фамилию, имя, отчество лица, осуществляющего обработку персональных данных по поручению Управления ГЗ, если обработка поручена или будет поручена такой организации или лицу;
8.1.10. иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.
8.2. Субъекты персональных данных, вправе требовать уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.3. Сведения должны быть предоставлены субъекту персональных данных оператором (Управлением ГЗ) в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
8.4. Сведения сообщаются субъекту персональных данных или его представителю, а также предоставляется возможность ознакомления с его персональными данными при обращении в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя.
Запрос должен содержать:
- номер документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Управлением ГЗ (документ, подтверждающий обращение заявителя или прием документов на оказание услуг соответствии видами деятельности), либо сведения, иным образом подтверждающие факт обработки персональных данных, подпись субъекта персональных данных или его представителя. Запрос может быть так же направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
8.5. В случае, если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
8.6. Субъект персональных данных вправе обратиться повторно или направить повторный запрос в целях получения сведений, указанных в подпунктах 8.1.1-8.1.10 пункта 8.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 8.5 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8.4 настоящего Положения, должен содержать обоснование направления повторного запроса.
8.7. Управление ГЗ вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.5 и 8.6 настоящего Положения. Такой отказ должен быть мотивированным.
8.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

9. ОБЯЗАННОСТИ ЛИЦА, ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ РАБОТ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ, ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ И ТЕХНИЧЕСКУЮ ЗАЩИТУ ИНФОРМАЦИИ

9.1. Лицо, ответственное за организацию работ с персональными данными, информационную безопасность и техническую защиту информации содержащей

персональные данные (далее - Ответственный за организацию работ и защиту ПД) назначается приказом директора Управления ГЗ.

9.2. Ответственный за организацию работ и защиту ПД в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

9.3. Ответственный за организацию работ и защиту ПД **обязан**:

9.3.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Управлении ГЗ, 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;

9.3.2. осуществлять внутренний контроль за соблюдением сотрудниками требований законодательства Российской Федерации в области обработки и защиты персональных данных;

9.3.3. доводить до сведения сотрудников положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

9.3.4. проводить инструктажи и занятия по изучению правовой базы по защите персональных данных с сотрудниками, имеющими доступ к персональным данным;

9.3.5. оказывать консультационную помощь персоналу по применению средств защиты персональных данных;

9.3.6. организовывать и контролировать прием и обработку обращений и запросов субъектов персональных данных или их представителей;

9.3.7. в случае нарушения требований к защите персональных данных, принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

9.4. Ответственный за организацию работ и защиту ПД **вправе:**

9.4.1. иметь доступ к информации, касающейся обработки персональных данных и включающей:

9.4.1.1. цели обработки персональных данных;

9.4.1.2. категории обрабатываемых персональных данных;

9.4.1.3. категории субъектов, персональные данные которых обрабатываются;

9.4.1.4. правовые основания обработки персональных данных;

9.4.1.5. перечень действий с персональными данными, общее описание используемых способов обработки персональных данных;

9.4.1.6. описание мер, предусмотренных статьями 18.1 и 19 Федерального закона "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

9.4.1.7. дату начала обработки персональных данных;

9.4.1.8. срок или условия прекращения обработки персональных данных;

9.4.1.9. сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

9.4.1.10. сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

9.4.2. привлекать иных сотрудников с возложением на них соответствующих обязанностей и закреплением ответственности по направлениям деятельности в структурных подразделениях к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Управлении ГЗ;

9.4.3. проводить регулярные внутренние проверки;

9.4.4. участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений Правил обработки персональных данных;

9.4.5.предлагать руководству мероприятия по совершенствованию работы по защите персональных данных;

9.4.6. составлять и предлагать на утверждение директору перечни должностных лиц и объемы их полномочий, которым разрешен доступ к персональным данным;

9.4.7. не допускать к работе с персональными данными лиц, не обладающих для этого соответствующими правами и допусками.

10. ОТВЕТСТВЕННОСТЬ

10.1. Виды штрафов

Согласно принятым поправкам к законам и КОАП Закон о персональных данных с 01.07.2017 года предусматривает следующие штрафы:

	Меры воздействия		
Нарушение	Для простых граждан	Для должностных лиц	Для предприятий
если производится сбор персональных данных в не предусмотренных законом случаях, либо выполняется обработка несовместимая с целями, указанными в законе	предупреждение либо штраф 1-3 тыс. руб.	штраф 5-10 тыс. руб.	штраф 30-50 тыс. руб.
Если у субъекта, получившего персональные данные, нет согласия на обработку персональных данных от их владельца, хотя оно обязательно должно быть получено	штраф 3-5 тыс. руб.	штраф 10-20 тыс. руб.	штраф 15-75 тыс. руб.
если оператор не опубликовал в открытом доступе документ, описывающий его политику по получению, обработке и хранению личных данных	штраф от 700 до 5 тыс. руб.	штраф 3-6 тыс. руб.	штраф для ИП 5-10 тыс. руб. штраф для организации 15-30 тыс. руб.
если оператор данных не предоставляет владельцу сведения о том, каким образом производится обработка его данных,	предупреждение либо штраф 1-2 тыс. руб.	предупреждение либо штраф 1-2 тыс. руб.	штраф для ИП 10-15тыс. руб. штраф для организации 25-40 тыс. руб.

10.2. Ответственность за нарушение порядка обработки и защиты информации

10.2.1. В силу ст. 90 ТК РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ и иными федеральными законами, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами. Виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 30 Трудового кодекса Российской Федерации.

10.2.2. Согласно статье 24 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении норм, регулирующих обработку персональных данных, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

10.2.3. К **административной ответственности** за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о сотрудниках и о гражданах (субъектах ПД) и за нарушение правил защиты информации могут привлекаться как само Управление ГЗ и его должностные лица, так и конкретные сотрудники, исполняющие соответствующие трудовые функции.

10.2.4. Лица, виновные в нарушении правил обработки или защиты информации, составляющей персональные данные, могут привлекаться к административной ответственности по следующим основаниям:

- неправомерный отказ в предоставлении сотруднику либо гражданину (субъекту ПД) собранных в установленном порядке документов, материалов, непосредственно затрагивающих его права и свободы, либо несвоевременное предоставление таких документом и материалов, не предоставление иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо недостоверной информации (ст. 5.39 КоАП РФ);

- нарушение установленного законом порядка сбора, хранения, использования или распространения информации содержащей персональные данные (ст. 13.11 КоАП РФ);

- нарушение правил защиты информации (ст. 13.12 КоАП РФ);

- разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет уголовную ответственность), лицом, получившим к ней доступ в связи с использованием служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

10.2.5. **Уголовная ответственность** за нарушение правил обработки информации, оставляющей персональные данные, может наступить в следующих случаях:

- неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ);

- создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273 УК РФ);

- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или повлекшее тяжкие последствия (ст. 274 УК РФ);

- незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан (ст. 137 УК РФ);

- неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ).

***