

Политика ФГУП «Госкорпорация по ОрВД» в области обработки и обеспечения безопасности персональных данных

1. Общие положения

1.1 Настоящая Политика в области обработки персональных данных в ФГУП «Госкорпорация по ОрВД» (далее – Политика) разработана на основании Конституции Российской Федерации, ст.18.1 Федерального закона № 152-ФЗ «О персональных данных», с учетом требований Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, международных договоров Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации в области персональных данных, и определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и категории обрабатываемых персональных данных, функции ФГУП «Госкорпорация по ОрВД» (далее – Предприятие) при обработке персональных данных, права субъектов персональных данных, а также реализуемые на Предприятии требования по защите персональных данных.

1.2 При разработке настоящей Политики учтены требования Концепции обеспечения информационной безопасности ФГУП «Госкорпорация по ОрВД», Политики информационной безопасности ФГУП «Госкорпорация по ОрВД» и Положения об обработке и защите персональных данных работников ФГУП «Госкорпорация по ОрВД».

Действие настоящей Политики распространяется на отношения, возникающие при обработке и обеспечении безопасности информации ограниченного доступа, относящейся в соответствии с законодательством Российской Федерации к персональным данным.

Настоящая Политика является общедоступным документом и опубликована на официальном сайте Предприятия.

Действие настоящей Политики не распространяется на отношения, возникающие при:

организации хранения, комплектования, учета и использования содержащих персональные данные документов, имеющих статус архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

2. Принципы обработки персональных данных

2.1 В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обработка персональных данных на Предприятии осуществляется на основе следующих принципов:

обеспечение законности целей, способов получения и обработки персональных данных;

обработка персональных данных должна быть ограничена достижением конкретных, заранее определенных и законных целей, а также полномочиями Предприятия;

соответствие объема и содержания обрабатываемых персональных данных, способов их обработки заявленным целям обработки;

обеспечение достоверности, точности персональных данных, их актуальности и достаточности для достижения целей обработки;

легитимность организационных и технических мер по обеспечению безопасности персональных данных;

недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

недопустимость обработки избыточных по отношению к целям сбора персональных данных;

недопустимость использования персональных данных в целях причинения имущественного и/или морального вреда субъектам персональных данных, затруднения реализации их прав и свобод;

обеспечение требуемого уровня знаний работников Предприятия в сфере обеспечения безопасности персональных данных при их обработке;

обеспечение поддержания на требуемом уровне и своевременного совершенствования системы защиты персональных данных;

3. Цели обработки персональных данных

3.1 С учетом состава обрабатываемых персональных данных и в соответствии с принципами их обработки, на Предприятии определены цели обработки персональных данных:

выполнение работодателем требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов ФГУП «Госкорпорация по ОрВД»;

осуществление прав и законных интересов Предприятия в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Предприятия, либо достижение общественно значимых целей;

осуществление функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Предприятие, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

подготовка, заключение, исполнение, изменение и расторжение трудовых договоров, которые являются основанием для возникновения или прекращения трудовых отношений между работодателем и работниками;

предоставление работникам Предприятия и членам их семей дополнительных гарантий и компенсаций, в том числе негосударственного пенсионного обеспечения, добровольного медицинского страхования,

медицинского обслуживания и других видов социального обеспечения;

защита жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

исполнение судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

содействие работникам в обучении и карьерном росте;

содействие в получении социальных льгот;

обеспечения пропускного и внутриобъектового режима на объектах Предприятия, организация прохода работников Предприятия, работников сторонних организаций и посетителей на территорию контролируемой зоны;

подготовка, заключение, сопровождение, исполнение, изменение и расторжение договоров гражданско-правового характера;

формирования справочных материалов для внутреннего информационного обеспечения деятельности Предприятия;

исполнение обязательств по договорам с контрагентами;

иные законные цели.

4. Категории субъектов, персональных данных

4.1 На Предприятии обрабатываются персональные данные следующих категорий субъектов персональных данных:

кандидаты на работу на Предприятии;

работники Предприятия и члены их семей (супруги и близкие родственники);

лица, имевшие ранее трудовые отношения с Предприятием;

лица, имеющие гражданско-правовой характер договорных отношений с Предприятием, или находящиеся на этапе преддоговорных или выполненных отношений подобного характера;

лица, проходящие практику (стажировку) на Предприятии;

контрагенты Предприятия, представленные индивидуальными предпринимателями, их руководителями, учредителями, работниками, представителями (действующими на основании доверенностей) и работниками юридических лиц, имеющих или имевших договорные отношения с Предприятием, либо желающих заключить договоры с Предприятием;

посетители Предприятия;

другие субъекты персональных данных, обработка персональных данных которых необходима Предприятию для реализации целей, указанных в разделе 3 Политики.

5. Категории обрабатываемых персональных данных

5.1 На Предприятии производится обработка общедоступных и иных категорий персональных данных, а также биометрических персональных данных, в

том числе – фотографий работников Предприятия с целью их идентификации при проходе на территорию контролируемой зоны Предприятия.

5.2 Не допускается обработка специальных категорий персональных данных:

- расовая принадлежность;
- политические взгляды;
- философские убеждения;
- интимная жизнь;
- национальная принадлежность;
- религиозные убеждения.

6. Организационная структура обработки и обеспечения безопасности персональных данных

6.1 Доступ к обрабатываемым на Предприятии персональным данным разрешен только работникам Предприятия, занимающим должности, при замещении которых предусмотрена обработка персональных данных.

6.2 В целях организации и контроля выполнения требований федерального законодательства Российской Федерации и иных нормативных документов в области обработки и обеспечения безопасности персональных данных, на Предприятии назначены должностные лица и органы, составляющие основу организационной структуры Предприятия в сфере обработки персональных данных:

- лицо, ответственное за организацию обработки персональных данных;
- лицо, ответственное за обеспечение безопасности персональных данных;
- комиссия по классификации информационных систем персональных данных;
- пользователи персональных данных.

7. Условия обработки персональных данных

7.1 Предприятие осуществляет сбор, хранение, обработку (запись, систематизацию, накопление, уточнение (обновление, изменение), извлечение, использование), передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

7.2 Сбор, хранение и обработка персональных данных работников Предприятия осуществляется с их письменного согласия. Предприятие без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом. Источники получения персональных данных:

- непосредственно от субъекта персональных данных;
- от третьей стороны, при необходимости исполнения договорных обязательств или исполнения требований федерального законодательства Российской Федерации.

7.3 Обработка персональных данных осуществляется следующими способами:
автоматизированная обработка персональных данных с передачей полученной

информации по информационно-телекоммуникационным сетям или без таковой;
неавтоматизированная обработка персональных данных;
смешанная обработка персональных данных.

7.4 Автоматизированная обработка персональных данных, содержащихся в информационных системах Предприятия, осуществляется в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

7.5 Неавтоматизированная обработка персональных данных организована в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687.

7.6 Предприятие вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также требования по защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7.7 Хранение и обработка персональных данных на Предприятии осуществляется в порядке, исключающем их утрату или незаконное использование, и в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.8 Основанием блокирования Предприятием персональных данных, относящихся к соответствующему субъекту персональных данных, является:

обращение или запрос субъекта персональных данных при условии подтверждения факта недостоверности, устаревания, неполноты персональных данных, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения;

обращение или запрос законного представителя субъекта персональных данных при условии подтверждения факта недостоверности, устаревания, неполноты персональных данных, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения;

обращение или запрос уполномоченного органа по защите прав субъектов

персональных данных при условии подтверждения факта недостоверности, устаревания, неполноты персональных данных, отсутствия необходимости в них для заявленной цели обработки, неправомерных действий с ними, незаконного их получения.

7.9 Основанием для прекращения обработки и уничтожения персональных данных, обрабатываемых на Предприятии, является:

достижение целей обработки персональных данных;

утрата необходимости в достижении целей обработки персональных данных;

истечение срока обработки (хранения) персональных данных, предусмотренного федеральным законодательством, договором или согласием субъекта персональных данных на обработку персональных данных. Хранение персональных данных после истечения указанного срока допускается только после их обезличивания;

отзыв субъектом персональных данных согласия на обработку своих персональных данных, за исключением случаев, когда обработка указанных персональных данных является обязательной в соответствии с законодательством Российской Федерации или договором;

выявление неправомерных действий с персональными данными и невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления;

истечение срока хранения персональных данных, установленного законодательством Российской Федерации и организационно-распорядительными документами Предприятия;

предписание уполномоченного органа по защите прав субъектов персональных данных, Прокуратуры или решение суда.

7.10 Предприятие не осуществляет:

обработку данных о судимости субъектов персональных данных;

принятие решений относительно субъектов персональных данных на основании исключительно автоматизированной обработки их персональных данных;

размещение персональных данных субъекта в общедоступных источниках без его предварительного согласия;

трансграничную передачу персональных данных (передачу персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

7.11 В целях внутреннего информационного обеспечения Предприятие может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством Российской Федерации, могут быть включены его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты и иные персональные данные, сообщаемые субъектом персональных данных.

8. Обеспечение безопасности персональных данных

8.1 Предприятие принимает все необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

8.2 В целях обеспечения безопасности персональных данных на Предприятии реализован комплекс мер, обоснованных по результатам определения угроз безопасности персональным данным и оценки вреда, который может быть причинен субъектам персональных данных:

8.2.1 При неавтоматизированной обработке персональных данных:

определен перечень лиц, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей;

определены места хранения персональных данных (материальных носителей) для каждой категории персональных данных и установлен перечень лиц, имеющих к ним доступ;

обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

обеспечен режим безопасности помещений, в которых осуществляется обработка персональных данных;

выполнены условия, обеспечивающие сохранность материальных носителей персональных данных и исключающие несанкционированный доступ к ним.

8.2.2 При автоматизированной обработке персональных данных:

определен требуемый уровень защищенности персональных данных при их обработке в информационных системах;

назначены лица, ответственные за организацию обработки и обеспечение безопасности персональных данных;

реализованы организационные и технические меры по обеспечению безопасности персональных данных в соответствии с установленным уровнем защищенности персональных данных;

применены сертифицированные средства защиты информации и антивирусной защиты;

введены в действие локальные нормативные акты и иные документы, определяющие порядок обработки и защиты персональных данных;

резервирования и восстановление персональных данных;

организовано обучение и проведение методической работы с работниками Предприятия, занимающими должности, связанные с обработкой персональных данных;

определены правила доступа к персональным данным, обрабатываемым в информационных системах, обеспечена регистрация и учет всех действий, совершаемых с персональными данными;

организован внутренний контроль соответствия обработки и обеспечения безопасности персональных данных организован учет и обеспечена сохранность машинных носителей персональных данных;

определен порядок требованиям законодательства Российской Федерации;

проведена аттестация информационных систем персональных данных на соответствие требованиям по защите информации;
организована оценка эффективности применяемых мер защиты.

9. Функции Предприятия при осуществлении обработки персональных данных

9.1 ФГУП «Госкорпорация по ОрВД» при осуществлении обработки персональных данных выполняет следующие функции:

принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Предприятия в области защиты персональных данных;

принимает организационные и технические меры по защите персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;

назначает лиц, ответственных за организацию обработки персональных данных;

издает локальные нормативные акты, определяющие политику, порядок обработки и защиты персональных данных на Предприятии;

осуществляет ознакомление работников Предприятия, осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации и локальных нормативных актов Предприятия, регламентирующих порядок обработки и обеспечение безопасности персональных данных, и обучение указанных работников;

публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации;

совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

10. Права субъектов персональных данных

10.1 Субъекты персональных данных имеют право на:

полную информацию об их персональных данных, обрабатываемых Предприятием;

доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законодательством Российской Федерации, а

также на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

отзыв согласия на обработку персональных данных;

принятие предусмотренных законом мер по защите своих прав;

обжалование действия или бездействия Предприятия, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

осуществление иных прав, предусмотренных законодательством Российской Федерации.

11. Контроль за выполнением требований по обработке и защите персональных данных

11.1. Внутренний контроль за соблюдением структурными подразделениями Предприятия законодательства Российской Федерации и локальных нормативных актов Предприятия в области обработки и защиты персональных данных, осуществляется в целях проверки соответствия процессов обработки персональных данных заявленным целям, выполнения требований по защите персональных данных, а также принятых мер, направленных на предотвращение нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

11.2. Проведение внутреннего контроля возложено на Комиссию ФГУП «Госкорпорация по ОрВД» в соответствии с «Регламентом обеспечения безопасности персональных данных» и осуществляется под руководством Дирекции по безопасности ФГУП «Госкорпорация по ОрВД».

12. Ответственность за нарушение норм, регулирующих обработку персональных данных

12.1. Предприятие несет ответственность за выполнение требований федерального законодательства Российской Федерации, определяющего порядок обработки и обеспечения безопасности персональных данных. Все работники Предприятия, осуществляющие обработку персональных данных, несут ответственность за соблюдение настоящей Политики и иных локальных актов Предприятия по вопросам обработки и обеспечения безопасности персональных данных.

12.2. Любой работник, которому стало известно о нарушении настоящей Политики или который подозревает о существовании такого нарушения, имеет право сообщить об этом лицу, ответственному за организацию обработки персональных данных, в соответствии с действующим на Предприятии порядком.

12.3. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов Предприятия в области обработки и защиты персональных данных в структурных подразделениях Предприятия, а также за обеспечение конфиденциальности и безопасности персональных данных в указанных подразделениях возлагается на их руководителей.

12.4. Любые нарушения настоящей Политики и иных локальных актов Предприятия по вопросам обработки и обеспечению безопасности персональных данных должны быть расследованы в соответствии с установленным на Предприятии порядком.

12.5. Лица, признанные виновными в нарушении установленного порядка обработки и обеспечения безопасности персональных данных, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством Российской Федерации.