

Утверждено
приказом управления социальной
защиты населения администрации
Белгородского района
от «15» 03 2017 г. № 54/10 пр.

Политика
управления социальной защиты населения
администрации Белгородского района
в отношении обработки персональных данных,
содержащихся в информационных системах персональных данных,
сведения о реализуемых требованиях к защите персональных данных

1. Введение

1.1. Настоящий документ (далее – Политика) устанавливает единый порядок обработки персональных данных с изложением целей, принципов, способов и условий обработки персональных данных, сведений о реализуемых требованиях к защите персональных данных в управлении социальной защиты населения администрации Белгородского района (далее – Учреждение). Политика разработана в соответствии с требованиями Федерального закона № 152-ФЗ от 27.06.2006 г. «О персональных данных», иных нормативно-правовых актов РФ, устанавливающих порядок обработки и защиты персональных данных. Политика является публичным документом.

1.2. Политика информационной безопасности Учреждения – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Учреждении.

Под Политикой понимается совокупность документированных управленческих решений, направленных на защиту информации и информационных ресурсов.

Политика относится к административным мерам обеспечения информационной безопасности и определяет стратегию Учреждения в области информационной безопасности.

1.3. В соответствии с Федеральным законом «О персональных данных» № 152-ФЗ от 27.06.2006 г. управление социальной защиты населения администрации Белгородского района является оператором персональных данных.

2. Цели обработки персональных данных

2.1. Целями обработки персональных данных (далее – ПДн) в Учреждении являются: защита информации Учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности; обеспечение функций по социальной поддержке и обслуживанию населения, предоставление мер социальной поддержки; назначение и выплата пособий и компенсаций; ведение единого государственного банка данных о детях, оставшихся без попечения родителей; учет оформленных и выданных удостоверений; ведение регистра получателей социальных услуг; учет данных о детях-сиротах, детях, оставшихся без попечения родителей, и лицах из

их числа, подлежащих обеспечению жильем и имеющих закрепленное жилое помещение; обеспечение исполнения обращений граждан РФ; ведение бухгалтерского и налогового учета, включая подготовку обязательной (регламентированной) отчетности; расчет заработной платы, передача электронной отчетности; ведение кадрового учета; реализация трудовых отношений с работниками,

2.2. Политика направлена на защиту информационных систем персональных данных от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

2.3. Стратегия обеспечения информационной безопасности заключается в использовании заранее отработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

3. Принципы и способы обработки персональных данных. Категории персональных данных.

3.1. Обработка персональных данных осуществляется на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.3. Способы обработки ПДн в Учреждении:

- автоматизированный, неавтоматизированный, смешанный, в том числе с передачей по информационно-телекоммуникационной сети.

3.4. Категории ПДн обрабатываемых в Учреждении: специальные, общедоступные и иные.

3.5. Состав обрабатываемых персональных данных определяется и утверждается перечнями персональных данных, обрабатываемых в информационных системах персональных данных Учреждения.

4. Условия обработки персональных данных в Учреждении

4.1. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных».

4.2. Обработка ПДн осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Обработка ПДн без согласия субъекта персональных данных осуществляется только в случаях, предусмотренных законодательством РФ.

4.3. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом соответствующего акта. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Учреждением определяются перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также указываются требования к защите обрабатываемых персональных данных,

4.4. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, не обязано получать согласие субъекта ПДн на обработку его персональных данных,

4.5. В случае если Учреждение поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

5. Конфиденциальность и требования Учреждения к защите персональных данных

5.1. Учреждения и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.2. Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами. При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу, ящике стола или сейфе.

5.3. Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с персональными данными для выполнения своих должностных обязанностей.

5.4. Допуск персонала к работе с защищаемыми информационными ресурсами Учреждения, конфиденциальной информацией Учреждения осуществляется только после его ознакомления с настоящей Политикой и инструкциями пользователей отдельных информационных систем.

5.5. Учреждение при обработке персональных данных обеспечивает принятие необходимых правовых, организационных и технических мер 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.

5.6. В целях защиты персональных данных Учреждение реализует требования к защите персональных данных при их обработке в информационных системах персональных данных, установленные Правительством РФ.

5.7. Сведения о предпринимаемых Учреждением мерах для защиты персональных данных являются информацией ограниченного доступа.

6. Права субъекта персональных данных

6.1. Учреждение при обработке ПДн обеспечивает необходимые условия для беспрепятственной реализации субъектом ПДн своих прав.

6.2. Права субъекта ПДн:

- на полную информацию о своих персональных данных и порядке их обработки;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством РФ;
- требование исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства;
- требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в судебных органах любые неправомерные действия или бездействие Учреждения при обработке и защите его персональных данных.

7. Обязанности Учреждения

7.1. В целях обеспечения прав и свобод человека и гражданина Учреждение при обработке персональных данных соблюдает следующие требования:

- обработка персональных данных гражданина осуществляется исключительно в целях оказания законных услуг;
- персональные данные гражданина получаются у него самого. Если персональные данные субъекта (гражданина), возможно, получить только у третьей стороны, то субъект уведомлен об этом заранее и от него должно быть получено письменное согласие, либо на иных законных основаниях. Работники Учреждения должны сообщить гражданину о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение;
- при наличии надлежащим образом оформленного запроса предоставлять гражданину доступ к его персональным данным;

- хранение и защита персональных данных гражданина от неправомерного их использования или утраты обеспечена Учреждением за счет его средств, в порядке, установленном законодательством;

- в случае достижения цели обработки персональных данных Учреждение обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий 30 дней, если это не противоречит законным основаниям обработки ПДн;

- в случае, если Учреждению необходимо последующее хранение персональных данных субъекта для осуществления обязательств, субъект должен быть об этом уведомлен и с него должно быть взято письменное согласие, за исключением случаев, оговоренных законодательством об архивном хранении личных сведений;

- в случае отзыва субъектом согласия на обработку своих персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 дней, если иное не предусмотрено соглашением между инспекцией и гражданином и не противоречит законодательству РФ.

8. Область действия Политики.

Регулирующие законодательные нормативные документы

8.1. Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

8.2. При организации и обеспечении работ по информационной безопасности сотрудники Учреждения должны руководствоваться следующими основополагающими законодательными нормативными документами:

- Доктрина информационной безопасности российской Федерации (утверждена Президентом Российской Федерации от 9 сентября 2000 года № Пр-1895);

- Закон Российской Федерации от 5 марта 1992 года № 2446-1 «О безопасности»;

- Глава 14. «Защита персональных данных работника» Гражданского кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ;

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

- Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации»;

- Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;

-Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.).

- Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;

- Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14 мая 2013 года N 28375)

- Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199);

- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие Приказом Гостехкомиссии России от 19 июня 2002 г. № 187).