УТВЕРЖДЕНА
приказом управления
государственного строительного
надзора Белгородской области
от «18» декабря 2020 года
№ 62-ОД

ПОЛИТИКА
управления государственного строительного надзора Белгородской области в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика «В отношении обработки персональных данных» (далее – Политика) разработана на основании ст. 24 Конституции РФ, главы 14 Трудового кодекса РФ, Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006, Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006, постановления Правительства РФ № 687 от 15.09.2008 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждений требований к защите персональных данных при их обработке в информационных системах персональных данных» и Гражданского кодекса РФ.

1.2. Настоящая Политика обработки персональных данных (далее – Политика) определяет порядок обработки персональных данных (приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета) и меры по обеспечению безопасности персональных данных в управлении государственного строительного надзора Белгородской области (далее – Управление) с целью обеспечения защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Категории субъектов персональных данных Управления:

– кандидаты на вакантные должности – физические лица, претендующие на замещение вакантных должностей Управление;

– государственные гражданские служащие – физические лица, проходящие в Управлении государственную гражданскую службу;

– работники – физические лица, связанные с Управлением трудовыми отношениями;

– контрагенты – физические лица, с которыми у Управления заключены договоры гражданско-правового характера;

– заявители – физические и юридические лица, направившие обращение в адрес Управления по вопросам, входящим в полномочия Управления;

– иные субъекты – физические лица, представляемые в Управление персональных данных в связи с выполнением Управлением иных функций, не противоречащих законодательству Российской Федерации и Положению об Управлении.

2. Основные понятия и состав персональных данных Субъектов

2.1. Для целей настоящей Политики используются следующие основные понятия:

1) **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), а также аналогичная информация об иных третьих лицах, полученная Управлением на законных основаниях от его контрагентов и иных третьих лиц в результате реализации полномочий. Персональные данные являются конфиденциальной информацией.

К персональным данным относятся (в том числе, но не ограничиваясь этим) следующие сведения и документы:

– паспортные данные;

– биографические сведения;

– сведения об образовании;

– сведения о специальности (профессии);

– сведения о занимаемой или ранее занимаемых должностях;

– место регистрации (пребывания);

– домашний телефон;

– состав семьи;

– подлинники и копии приказов по личному составу;

– другая информация, необходимая Управления в связи с реализацией полномочий, а также реализацией договорных отношений.

2) **обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

3) **конфиденциальность персональных данных** – обязательное для соблюдения назначенным должностным лицом Управления ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия Субъекта или наличия иного законного основания;

4) **распространение персональных данных** – действия, направленные на передачу Персональных данных определенному кругу лиц (предоставление персональных данных) или на ознакомление с персональными данными

неопределенного 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) **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

6) **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;

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

8) **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

9) **трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

10) **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

11) **информация** – сведения (сообщения, данные) независимо от формы их представления;

12) **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

2.2. Носителями персональных данных являются документы, содержащие сведения, перечисленные в п. 1 ч. 2.1. настоящей Политики.

3. Доступ к персональным данным Субъекта

3.1. Список должностей Управления, имеющих доступ к персональным данным, определяется отдельным документом, утверждаемым начальником Управления.

3.2. Передача Персональных данных третьим лицам возможна только с согласия Субъекта в письменной форме или без его согласия в случаях, предусмотренных законодательством РФ.

4. Сбор, обработка и хранение персональных данных

4.1. Обработка персональных данных может осуществляться исключительно в целях соблюдения нормативных правовых актов Российской Федерации, содействия Субъектам в трудоустройстве, обучении, продвижении по службе (работе), обеспечения личной безопасности Субъектов, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера, расчета и выплаты заработной платы, а также в иных целях при получении письменного согласия Субъекта.

4.2. Персональные данные следует получать непосредственно у Субъекта.

Если персональные данные возможно получить только у третьей стороны, Субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие, за исключением случаев, предусмотренных законодательством.

Управления должно сообщить Субъекту следующую информацию:

а) цель обработки персональных данных и ее правовое основание;

б) предполагаемые пользователи персональных данных;

в) права субъекта персональных данных;

г) источник получения персональных данных.

4.3. Персональные данные на бумажных носителях, обрабатываемые без использования средств автоматизации, хранятся в Управлении в запираемых помещениях, оборудованных охранно-пожарной сигнализацией под круглосуточной охраной.

4.5. Персональные данные могут также храниться в электронном виде в информационных системах Управления. В таком случае доступ к персональным данным должен быть технически возможен только специально уполномоченным лицам, упомянутым в пункте 3.1. При этом указанные лица должны иметь право получать только те персональные данные, которые необходимы им для выполнения конкретных функций.

Доступ к информационным системам, содержащим персональные данные, должен быть защищен паролями, а также разграничением доступа к различным подсистемам в зависимости от выполняемых должностных обязанностей.

5. Передача персональных данных Субъекта

5.1. При передаче персональных данных Управление должно соблюдать следующие требования:

- не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено законодательством;

- предупредить лиц, получающих персональные данные Субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц соблюдения правил обработки и хранения персональных данных. Лица, получающие персональные данные, обязаны

соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством РФ;

- разрешать доступ к персональным данным только специально уполномоченным лицам Учреждения.

6. Общедоступные источники персональных данных

6.1. В целях информационного обеспечения деятельности структурных подразделений Управления могут быть созданы общедоступные источники персональных данных (в том числе справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия Субъекта могут включаться его фамилия, имя, отчество, абонентский номер, сведения о занимаемой должности и иные персональные данные, предоставленные Субъектом.

6.2. Сведения о Субъекте должны быть в любое время исключены из общедоступных источников персональных данных по его требованию, а также в случаях, предусмотренных законодательством РФ.

7. Безопасность персональных данных

7.1. При обработке персональных данных, ответственное лицо обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

7.2. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии хранения, которая обеспечивает защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

7.3. В целях предупреждения нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечения безопасности информации в процессе управленческой и производственной деятельности Управления устанавливается комплекс мер по защите персональных данных. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой деятельности Управления.

Комплекс мер включает в себя:

7.3.1. Внутренняя защита

Регламентация доступа к конфиденциальным сведениям Управления, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий. Для защиты персональных данных Субъекта Управление обязано соблюдать следующие меры безопасности:

а) ограничивать и регламентировать состав государственных служащих и работников Управления, функциональные обязанности которых требуют доступа к персональным данным;

б) избирательно и обоснованно распределять документы и информацию между государственными служащими и работниками;

рационально размещать рабочие места, при котором исключается бесконтрольное использование конфиденциальной информации;

в) организовать необходимые условия в помещении для работы с конфиденциальными документами и базами данных;

г) регламентировать порядок уничтожения информации;

д) выявлять нарушения доступа к персональным данным;

е) проводить работы по предупреждению утраты сведений при работе с персональными данными;

ж) защищать персональные компьютеры паролями доступа.

7.3.2. Внешняя защита.

Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др. Под посторонним лицом понимается любое лицо, не имеющее санкционированного доступа к персональным данным, в том числе непосредственного отношения к деятельности Управления, посетители, работники других организаций и иные лица.

а) лица, не являющиеся работниками Управления, не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Управлении. В отдельных случаях возможно предоставление доступа к данной информации для третьих лиц, осуществляющих внедрение, сопровождение и аудит процессов в Управлении, при условии, что от них получено обязательство о неразглашении в письменной форме. Доступ к вышеуказанной информации возможен только после согласования с начальником (первым заместителем начальника) Управления.

б) для защиты персональных данных Субъектов необходимо соблюдать:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Управления;

- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

8. Обязанности Управления

8.1. При обработке персональных данных Управление обязано соблюдать следующие требования:

- при определении объема и содержания обрабатываемых персональных данных Управление должно действовать в соответствии с Конституцией РФ, действующим законодательством РФ и иными нормативными правовыми актами, закрепляющими полномочия Управления и порядок их реализации;
- защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Управлением за счет его средств в порядке, установленном действующим законодательством РФ;
- государственные гражданские служащие и работники Управления должны быть ознакомлены под роспись с документами Управления, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

9. Права и обязанности Субъекта в области защиты персональных данных

9.1 Субъект обязан:

- передавать Управлению достоверные, документированные персональные данные, состав которых установлен нормативно-правовыми актами РФ;
- своевременно сообщать Управлению об изменении своих персональных данных.

Обязанности Субъекта фиксируются в письменном виде в тексте Согласия на обработку персональных данных, которое он подписывает при приеме на государственную гражданскую службу (работу).

9.2. Субъект в целях обеспечения защиты персональных данных, хранящихся в Управлении, имеет право на:

а) свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством РФ;

б) исключение или исправление неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства РФ;

в) персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

г) требование об извещении Управлением всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях и дополнениях;

д) отзыв согласия на обработку персональных данных;

е) обжалование в суде любых неправомерных действий или бездействия Управления при обработке и защите его персональных данных.

ж) получение от Управления:

- сведений о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия может повлечь за собой обработка его персональных данных.

10. Ответственность за нарушение требований обработки и защиты персональных данных Субъекта

10.1. Защита прав Субъекта, установленных настоящей Политикой и законодательством Российской Федерации, осуществляется в целях пресечения неправомерного использования персональных данных, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

10.2. Государственные гражданские служащие (работники) Управления, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, персонально несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

11. Заключительное положение

11.1. Иные права и обязанности Управления как оператора персональных данных определяются законодательством Российской Федерации в области персональных данных.

11.2. Настоящая Политика обязательна для соблюдения всеми сотрудниками Управления.