**ПОЛОЖЕНИЕ**
**о порядке обработки и защиты персональных данных**
**в ООО «Компас»**

## 1. Общие положения

1.1. Положение о порядке обработки и защиты персональных данных (далее - Положение) в ООО «Компас» определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных у Оператора.

1.2. Настоящее Положение определяет действия ООО «Компас» как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Обработка персональных данных в ООО «Компас» (далее - Оператор) осуществляется в целях оказания услуг, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

1.5. Основные понятия, используемые в настоящем Положении:

1.5.1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному, или определяемому физическому лицу (далее – субъекту персональных данных).

1.5.2. Оператор персональных данных (оператор) – юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

1.5.3. Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;

– блокирование;
– удаление;
– уничтожение.

1.5.4. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.5.5. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.5.6. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.5.7. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.5.8. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.5.9. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.5.10. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5.11. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.6. Обработка персональных данных Оператором осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и действующим законодательством Российской Федерации в области персональных данных.

1.7. Перечень должностей Оператора, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утверждается приказом руководителем Оператора.

1.8. Деятельность по организации обработки и защиты персональных данных в соответствии с требованиями законодательства Российской Федерации о персональных данных осуществляет сотрудник Оператора, ответственный за организацию обработки персональных данных Оператором.

1.9. Деятельность по администрированию средств и механизмов защиты персональных данных осуществляет сотрудник Оператора, назначенный администратором информационной безопасности информационных систем Оператора.

1.10. Техническое обслуживание информационных систем персональных данных осуществляет сотрудник Оператора, назначенный администратором информационных систем Оператора.

1.11. Ответственный за организацию обработки персональных данных, администратор информационной безопасности информационных систем, и администраторы информационных систем назначаются приказом руководителя Оператора.

## 2. Условия и порядок обработки персональных данных

2.1. Персональные данные Оператором обрабатываются в следующих целях:

- ведения основного вида деятельности Оператора;
- выполнение Оператором своих договорных обязательств, ведение бухгалтерского учета, подготовка налоговой отчетности;
- выполнение норм Гражданского кодекса, регулирующих договорную работу, и исполнение договоров с контрагентами;

- выполнение функции налогового агента;
- обеспечения соблюдения законов и иных нормативных правовых актов;
- выполнение положений Трудового кодекса Российской Федерации, обязательств, предусмотренных трудовым договором между работодателем и работником;
- начисления заработной платы;
- исчисления и уплаты, предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- предоставления сведений в банк для открытия расчетного счета, оформления банковской карты и перечисления на нее заработной платы;
- предоставления сведений третьим лицам для прохождения обязательных медицинских осмотров и оформления полиса ДМС;
- предоставления налоговых вычетов;
- обеспечения личной безопасности работников;
- обеспечения безопасности условий труда;
- контроля количества и качества выполняемой работы;
- обеспечения сохранности имущества работодателя;
- представления работодателем расчетов по страховым взносам, расчетов по начисленным и уплаченным страховым взносам на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний, а также по расходам на выплату страхового обеспечения, сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ, а также статистической отчетности в Росстат;
- создания единого информационного пространства Оператора;
- содействия работникам в трудоустройстве, получении образования и продвижении по службе;
- выполнения обязательств перед Пользователем;
- проведения опросов и исследований общественного мнения в целях повышения качества услуг;
- предоставления Пользователю информации и услуг в соответствии с его запросами и предпочтениями;
- использования фамилии, имени, отчества, должности, номера рабочего телефона, адреса электронной почты, фотографии работника при его упоминании на сайте работодателя и/или общедоступных источниках;
- исполнение иных функций и полномочий, возложенных на Оператора положениями правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

2.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.3. Все персональные данные субъектов Оператор получает от них самих либо от их законных представителей.

2.4. Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных, кроме случаев, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральным законом № 152-ФЗ). Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

2.5. Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Допускается совмещение формы

согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

2.6. Персональные данные субъектов Оператором обрабатываются в структурных подразделениях в соответствии с исполняемыми функциями.

2.7. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные. Типовая форма разъяснения представлена в приложении 1 к настоящему Положению.

2.8. Доступ лиц к обработке персональных данных осуществляется в соответствии со списком, утвержденным приказом руководителя Оператора, и только после подписания обязательства о неразглашении персональных данных (Приложение 2 к настоящему Положению).

2.9. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие должно быть в письменной форме, в случаях, предусмотренных действующим законодательством (Приложения 3 - 6 к настоящему Положению).

2.10. Уполномоченные лица, допущенные к обработке персональных данных субъектов Оператора, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностной инструкцией уполномоченных лиц.

2.11. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться 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. Персональные данные при такой их обработке, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

2.12. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

2.13. Персональные данные подлежат уничтожению либо обезличиванию в следующих случаях:

– достижения целей обработки или в случае утраты необходимости в их достижении;

– отзыва согласия субъекта персональных данных на обработку персональных данных (форма отзыва согласия приведена в приложении 7 к настоящему Положению);

– представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

– выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных.

2.14. Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии со списком, утвержденным в порядке, определяемом Оператором.

2.15. В срок, не превышающий 7 дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, ответственный за обработку персональных данных вносит в них необходимые изменения, а также уведомляет субъекта о внесенных изменениях.

2.16. Уничтожение персональных данных осуществляется в срок, не превышающий 30 дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами Российской Федерации.

2.17. Уничтожение персональных данных осуществляется в срок, не превышающий 30 дней с момента отзыва согласия субъекта персональных данных на обработку персональных данных.

2.18. Уничтожение персональных данных осуществляется в срок, не превышающий 7 дней с момента представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

2.19. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных уничтожение персональных данных осуществляется в срок, не превышающий 10 дней с момента выявления неправомерной обработки персональных данных. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до уполномоченных руководителей Оператора. Оператора уведомляет субъекта персональных данных или его законного представителя об уничтожении персональных данных.

2.20. Уничтожение персональных данных осуществляется комиссией, с привлечением соответствующего руководителя структурного подразделения, являющимся ответственным за обработку уничтожаемых персональных данных.

2.21. Состав комиссии по уничтожению персональных данных утверждается руководителем Оператора.

2.22. Способ уничтожения материальных носителей персональных данных определяется комиссией/рабочей группой. Допускается применение следующих способов:

– сжигание;
– шредирование (измельчение);
– передача на специализированные полигоны (свалки);
– химическая обработка.

2.23. При этом составляется акт, подписываемый председателем комиссии, проводившей уничтожение материальных носителей персональных данных.

2.24. При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия/рабочая группа Оператора должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

2.25. Уничтожение полей баз данных Оператора, содержащих персональные данные субъекта, выполняется в случаях, установленных в пункте 2.12. по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

2.26. Уничтожение осуществляет комиссия/рабочая группа, в состав которой входит лицо, ответственное за техническое обслуживание автоматизированной системы персональных данных, с привлечением соответствующего руководителя структурного подразделения, являющимся ответственным за обработку уничтожаемых персональных данных.

2.27. Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях). При этом составляется акт, согласуемый лицом, ответственным за техническое обслуживание автоматизированных систем и руководителем структурного подразделения, являющимся ответственным за обработку уничтожаемых персональных данных.

2.28. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение

определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

2.29. При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных, допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была невозможна.

2.30. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

2.31. Обработка биометрических персональных данных (фотография, используемая для идентификации, отпечатки пальцев, изображение сетчатки глаза и т.д.), в соответствии со статьей 11 Федерального закона № 152-ФЗ, допускается при наличии согласия субъекта.

2.32. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

2.33. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Федеральном законе № 152-ФЗ.

2.34. Сотрудники должны быть ознакомлены под подпись с настоящим Положением и другими документами Оператора, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

## 3. Защита персональных данных

3.1. Защиту персональных данных субъектов от неправомерного их использования или утраты, Оператор обеспечивает за счет собственных средств в порядке, установленном законодательством Российской Федерации.

3.2. При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

3.3. Принятие необходимых организационных и технических мер по защите персональных данных осуществляется ответственным лицом за защиту информации и обеспечение безопасности персональных данных Оператором, администратором информационной безопасности Оператора.

3.4. Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии со следующими документами:

– постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности №149/7/2/6-432 от 31.03.2015;

– базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, от 15.02.2008;

– методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, от 14.02.2008;

– локальными актами Оператора, действующими в сфере обеспечения информационной безопасности.

3.5. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Оператора, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия 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;

– 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 Оператора, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

– контроль принимаемых мер по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

3.6. Ответственное лицо за защиту информации и обеспечение безопасности персональных данных Оператором, организует и контролирует ведение учета материальных носителей персональных данных и обеспечивает:

– своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных Оператором;

– 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;

– постоянный контроль обеспечения уровня защищенности персональных данных;

– знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– при обнаружении нарушений порядка представления персональных данных незамедлительное приостановление представления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

– 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.

3.7. Обмен персональными данными при их обработке в информационных системах персональных данных Оператора осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения сертифицированных программных и технических средств.

3.8. Доступ работников, допущенных к обработке персональных данных в информационной системе, предусматривает обязательное прохождение процедуры идентификации и аутентификации пользователя информационной системы.

3.9. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Оператора уполномоченными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

3.10. Защита персональных данных предусматривает ограничение к ним доступа.

3.11. Руководители структурных подразделений Оператора, осуществляющих обработку персональных данных:

– несут ответственность за организацию защиты персональных данных в подчиненном структурном подразделении;

– обеспечивают изучение подчинёнными сотрудниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

– обеспечивают режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении;

– организуют контроль доступа к персональным данным в соответствии с функциональными обязанностями сотрудников подразделения;

– организуют контроль доступа в помещения, в которых обрабатываются персональные данные.

3.12. Сотрудники, допущенные к персональным данным, дают письменное обязательство о неразглашении таких данных в установленном порядке.

## 4. Сроки обработки и хранения персональных данных

4.1. Сроки обработки и хранения персональных данных определяются в соответствии с законодательством Российской Федерации.

4.2. Сроки обработки и хранения персональных данных, представляемых субъектами персональных данных, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

4.3. Персональные данные граждан, обратившихся к Оператору лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет.

4.4. Персональные данные, представляемые субъектами на бумажном носителе, хранятся на бумажных носителях в соответствующих структурных подразделениях, к

полномочиям которых относится обработка персональных данных в соответствии с действующими нормативными актами.

4.5. 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).

4.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

4.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений.

4.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных Оператора, должен соответствовать сроку хранения бумажных оригиналов.

## 5. Правила работы с обезличенными персональными данными

5.1. Порядок обезличивания включает в себя замену идентифицирующей информации о субъекте (например: фамилию, имя и отчество) на произвольный код (далее – идентификатор).

5.2. Обезличивание должно проводиться таким образом, чтобы определить принадлежность персональных данных конкретному субъекту персональных данных было невозможно без использования дополнительной информации.

5.3. Если обезличенные персональные данные используются в целях продвижения товаров, работ, услуг на рынке, или в целях политической агитации, Оператор обязан получить согласие субъекта персональных данных на подобную обработку.

5.4. Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за организацию обработки персональных данных Оператором индивидуально для каждой информационной системы персональных данных.

## 6. Передача персональных данных третьим лицам

6.1. При обработке персональных данных субъекта должны соблюдаться следующие требования:

– не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта персональных данных, если иное не предусмотрено федеральными законами Российской Федерации;

– предупреждать 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 подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

6.2. При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Оператор запрашивает согласие субъекта в письменной форме.

## 7. Права субъектов персональных данных

7.1. В целях обеспечения своих интересов субъекты имеют право:

– получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ;

– требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона № 152-ФЗ. Субъект при отказе Оператором исключить или исправить персональные данные субъекта имеет право заявлять в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать в суд любые неправомерные действия или бездействие Оператора при обработке и защите персональных данных субъекта.

## 8. Порядок обработки обращений и запросов субъектов

8.1. При обращении либо письменном запросе субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Оператор руководствуется требованиями статей 14, 18 и 20 Федерального закона № 152-ФЗ;

8.2. Доступ субъекта персональных данных или его законного представителя к своим персональным данным Оператор предоставляет только под контролем ответственного за организацию обработки персональных Оператором.

8.3. Обращение субъекта персональных данных или его законного представителя фиксируются в журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

8.4. Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекта к персональным данным.

8.5. В случае, если данных предоставленных субъектом недостаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

8.6. Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает сотрудника (сотрудников) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения.

8.7. Сведения о наличии персональных данных Оператор предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

8.8. Сведения о наличии персональных данных должны быть предоставлены субъекту при ответе на запрос в течение тридцати дней от даты получения запроса субъекта персональных данных или его законного представителя.

## 9. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

9.1. Оценкой вреда, который может быть причинен субъектам персональных данных, в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

9.2. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав субъектов персональных данных или иным образом затрагивающие их права, свободы и законные интересы.

9.3. В целях недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам персональных данных при обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

9.4. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных Оператором утверждаются приказом руководителя Оператора.

## 10. Обязанности лиц, допущенных к обработке персональных данных

10.1. Лица, допущенные к работе с персональными данными, обязаны:

– знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Оператора по защите персональных данных;

– сохранять конфиденциальность персональных данных;

– обеспечивать сохранность закрепленных за ними носителей персональных данных;

– контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

– докладывать своему непосредственному руководителю структурного подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

## 11. Ответственность сотрудника за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности.

11.2. К данным лицам могут быть применены следующие дисциплинарные взыскания:

– замечание;

– выговор;

– увольнение.

11.3. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

11.4. Копия приказа о применении к сотруднику дисциплинарного взыскания с указанием оснований его применения вручается сотруднику под расписку в течение трех рабочих дней со дня издания приказа.

11.5. Если в течение года со дня применения дисциплинарного взыскания сотрудник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Оператор до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с сотрудника по собственной инициативе, по письменному заявлению сотрудника или по ходатайству его непосредственного руководителя.

## 12. Контроль обеспечения безопасности персональных данных

12.1. Целью контроля является соблюдение структурными подразделениями Оператора, эксплуатирующими информационные системы и обрабатывающими персональные данные без средств автоматизации, требований по обеспечению безопасности персональных данных.

12.2. Задачами контроля являются:

– установление фактического положения дел по обеспечению безопасности персональных данных при их обработке;

– выявление проблемных вопросов в организации обеспечения безопасности персональных данных;

– обеспечение соблюдения законодательства Российской Федерации в области персональных данных;

– выработка мер по оказанию методической и практической помощи структурным подразделениям Оператора, эксплуатирующим информационные системы и обрабатывающими персональные данные без средств автоматизации.

## 13. Порядок действий в случае запросов надзорных органов

13.1. В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Оператор сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с момента получения такого запроса.

13.2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением сотрудников Оператора.

13.3. В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.