**УТВЕРЖДАЮ**

**Генеральный директор ООО «Ромашка»**

 «\_\_\_» \_\_\_\_\_\_\_\_\_20\_\_\_г.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (расшифровка подписи)

 М.П.

ПОЛОЖЕНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

Название организации — далее «Организация», являясь работодателем (оператором), осуществляет работу с персональными данными работников Организации (субъекта персональных данных), руководствуясь соответствующими нормами Конституции РФ (Российской Федерации), Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также общепризнанными принципами и нормами международного права и международных договоров РФ, которые в соответствии с частью четвертой ст. 15 Конституции РФ являются составной частью российской правовой системы.

Так, в соответствии с частью первой ст. 23 Конституции РФ каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

1.1. Цель разработанного регламента.

1.1.1. Целью является защита персональных данных от несанкционированного доступа третьих лиц и организация приема, хранения, обработки и передачи персональных данных работников в соответствии с установленными законодательными требованиями.

1.2. Режим конфиденциальности.

1.2.1. Сбор, хранение, использование и распространение информации о частной жизни Работника без его письменного согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

1.2.2. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством РФ.

1.3. Порядок утверждения данных правил, ввода их в действие и внесения изменений.

Утверждаются генеральным директором Организации.

Вводятся в действие приказом по организации.

2. Понятие и состав персональных данных.

2.1. Понятие персональных данных

Персональные данные работника — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), необходимая работодателю в связи с трудовыми отношениями или полученная им на основании письменного согласия работника. Это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Если по совокупности сведений определить их принадлежность конкретному субъекту невозможно, то данные сведения не относятся к персональным данным.

Обработка персональных данных работника — 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.

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

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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

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

Представители работника - лица, выступающие в качестве законного представителя в соответствии с нормами гражданского и семейного законодательства.

3. Сбор, обработка и хранение персональных данных.

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные работника следует получить у него самого. Если персональные данные работника можно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.2. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ Работодатель вправе получать и обрабатывать данные о частной жизни Работника только с его письменного согласия.

Работодатель вправе обрабатывать персональные данные Работников только с их письменного согласия.

Письменное согласие Работника на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес Работника персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя Работника персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (*при получении согласия от представителя субъекта персональных данных);*

3) наименование или фамилию, имя, отчество и адрес Работодателя, получающего согласие Работника персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие Работника персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Работодателя, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Работодателем способов обработки персональных данных;

8) срок, в течение которого действует согласие Работника персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись Работника персональных данных.

Согласие Работника не требуется в случаях если:

* обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия Работодателя;
* обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
* обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Работника, если получение его согласия невозможно.

3.2. Состав работников, допущенных к обработке, передаче и хранению персональной информации.

3.2.1. Полный доступ: к обработке персональных данных работника, исходя из функциональных обязанностей должностных лиц, имеют полный доступ следующие работники:

* генеральный директор;
* главный бухгалтер;
* начальник юридического отдела;
* руководитель кадровой службы;
* системные администраторы;
* и другие при необходимости.

3.2.2. Ограниченный доступ: к обработке персональных данных работника, исходя из функциональных обязанностей должностных лиц, имеют ограниченный доступ следующие работники:

|  |  |
| --- | --- |
| Наименование должности | Персональные данные и перечень документов, к которым может быть допущен работник, а также цели, в которых данное должностное лицо имеет право обрабатывать данные сведения |
| Секретарь | — Паспортные данные работника (сведения о номере паспорта, дате, месте его выдачи) — для заказа билетов при отправлении работника в командировку и бронировании гостиницы; |
| — адрес места жительства — для отправки корреспонденции |
| — и т. д., указать подробно, исходя из специфики своей организации и особенностей распределения функций. |
| Бухгалтер по расчету заработной платы | — Сведения об иждивенцах — для произведения необходимых вычетов из заработной платы, установленных законодательно; |
| — ИНН, номер страхового свидетельства государственного пенсионного страхования, адрес места прописки — для оформления бухгалтерской, налоговой, статистической отчетности  |
| — и т. д., указать подробно, исходя из специфики своей организации и особенностей распределения функций. |
| Руководитель структурного подразделения, в котором работает работник | — Сведения о семейном положении, возрасте детей — для предоставления работнику гарантий, установленных законодательно, в частности для решения вопроса о возможности привлечения к работе сверхурочно, к работе в выходные и праздники, для привлечения к работе ночью, отправления в командировки; |
| — сведения о профессии, квалификации работника, о его опыте работы и имеющихся профессиональных навыках — для принятия решений о переводах, возложении дополнительных обязанностей; |
| — медицинские ограничения (группа инвалидности, условия, прописанные в карте реабилитации) — для соблюдения установленных для работника условий работы, решения вопроса о возможных переводах |
| — и т. д., указать подробно, исходя из специфики своей организации и особенностей распределения функций. |
| Продолжить список  |  |

3.3. Порядок обработки, передачи и хранения персональной информации.

3.3.1. В соответствии со ст.86 Трудового кодекса РФ в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

* обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении на службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
* ….

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право:

* на полную информацию об их персональных данных и обработке этих данных;
* на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
* на определение своих представителей для защиты своих персональных данных;
* на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
* на требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
* на требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
* на обжалование в суде любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

3.4. Ответственность за разглашение.

3.4.1. Все лица, непосредственно имеющие отношение к персональной базе данных, должны подписывать обязательство о неразглашении персональной информации работников.

3.4.2. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

3.4.3. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

3.4.4. Каждый работник Организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

3.4.5. Ответственность лиц, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, согласно действующему законодательству, может быть дисциплинарной, административной, гражданско-правовой или уголовной в соответствии с федеральными законами.

3.4.6. Должностные лица, допущенные к обработке персональных данных работника, в случае их разглашения могут быть уволены по инициативе работодателя по ст. 81 часть первая пункт 6 «в» Трудового кодекса РФ. То есть разглашение персональных данных работника, ставших известным должностным лицам в связи с исполнением должностных обязанностей, является грубым нарушением должностных обязанностей.

4. Доступ.

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным работника, имеют лица, указанные в п.3.2. данного положения. Другие работники Организации имеют доступ к персональным данным работника только с письменного согласия самого работника, субъекта данных.

4.1.2. По письменному заявлению работника работодатель обязан не позднее трех рабочих дней со дня подачи этого заявления выдать работнику копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказ об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться работнику безвозмездно.

4.2. Внешний доступ.

4.2.1. К числу лиц, допущенных к персональным данным работника, относятся организации (и соответственно должностные лица, данных организаций), осуществляющие контрольные и надзорные функции, а также другие лица, установленные федеральными законами, в частности:

* инспекции труда;
* прокуратура РФ;
* правоохранительные органы;
* налоговые инспекции;
* военкоматы;
* органы, осуществляющие миграционный учет иностранных граждан;
* органы ФСС РФ;
* органы Пенсионного фонда РФ
* и т. д.

4.2.3. Органы и должностные лица, указанные в п.4.2.1, имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством РФ.

4.2.4. Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае письменного разрешения работника.

4.2.5. Другие организации: сведения о работающем или уже уволенном работнике могут быть предоставлены другой организации только на основании письменного запроса, оформленного на бланке организации, с приложением копии нотариально заверенного заявления работника, содержащего согласие на передачу указанным лицам таких сведений, с полным указанием того, какие сведения могут быть переданы на основании данного согласия.

4.2.6. Родственники и члены семьи работника: персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника. В случае развода и отсутствия соглашения сторон об уплате алиментов справка о заработной плате работника может быть предоставлена в суд без его согласия, на основании письменного запроса и определения суда.

5. Защита персональных данных.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Общества.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в информационной системе персональных данных правила разграничения доступа к информации.

Этими субъектами могут быть:

* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

Под нарушителем понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах.

5.1. Внутренняя защита.

5.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

Для защиты персональных данных работников работодатель принимает следующие меры:

* ограничение и регламентация состава Работников, функциональные обязанности которых требуют конфиденциальных знаний;
* строгое избирательное и обоснованное распределение документов и информации между Работниками.
* рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;
* знание работниками требований нормативно - методических документов по защите информации и сохранении тайны. Для этого со всеми Работниками, допущенными к персональным данным, проводится при допуске и периодически соответствующий инструктаж и обучение;
* наличие необходимых условий, исключающих несанкционированный доступ в помещения для работы с конфиденциальными документами и базами данных;
* определение и регламентация состава Работников, имеющих право доступа (входа) в помещение, в котором находятся персональные данные на бумажных носителях и вычислительной технике.
* организация порядка уничтожения информации. Способ уничтожения определяется специальной комиссией;
* своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения. Для этого в организации создана постоянно действующая экспертная комиссия, в состав которой входят: *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.*
* воспитательная и разъяснительная работа с Работниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами. Данная обязанность возложена на руководителей структурных подразделений, в подчинении которых находятся Работники, допущенные к персональным данным.
* и т. д.

5.1.2. Защита персональных данных работника на электронных носителях: все папки, содержащие персональные данные работника, защищены паролем, который сообщается руководителю службы персонала и руководителю отдела информационных технологий.

5.1.3. Защита персональных данных на бумажных носителях: все документы, содержащие персональные данные работника, хранятся в кабинете руководителя службы персонала, помещении бухгалтерии Организации, в специально отведенном для этого месте, с применением специального оборудования (металлические несгораемые шкафы, сейфы).

5.1.4. Ключи от специального оборудования в рабочее время хранятся у начальников вышеуказанных подразделений без права передачи третьим лицам, на время их отсутствия ключи хранятся у лица, исполняющего обязанности руководителя подразделения.

**5.2. Внешняя защита.**

5.2.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося 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 непосредственного отношения к деятельности Организации, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в службе персонала.

5.2.2. Для защиты персональных данных работников работодатель предпринимает следующие меры:

* порядок приема, учета и контроля деятельности посетителей. Любой посетитель перемещается по территории Организации только в сопровождении лица, к которому он пришел;
* пропускной режим Организации. Каждое постороннее физическое лицо обязано зарегистрироваться на пункте охраны сообщив о себе следующие сведения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Данные сведения вносятся в журнал учета посетителей, ответственность за хранение которого несет \_\_\_\_\_\_\_\_\_\_\_\_;
* технические средства охраны, сигнализации. Ответственность за их бесперебойную работу лежит на \_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* порядок охраны территории, зданий, помещений, транспортных средств. Ответственность за охрану возлагается на \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* требования к защите информации при интервьюировании и собеседованиях. Контроль за соблюдением данного требования возложен на руководителя службы персонала.
* и т. д.

**6. Информационные системы**

6.1. Работодатель использует следующие информационные системы:

* **Информационная система,** **обрабатывающая биометрические персональные данные** (так как в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности Работника, на основании которых можно установить его личность и которые используются Работодателем для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных).
* **Информационная система, обрабатывающая общедоступные персональные данные** (так как в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных).
* **Информационная система, обрабатывающая персональные данные работников**. (так как в ней в ней обрабатываются персональные данные только работников).

6.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

6.3. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом, которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

6.4. Для обеспечения безопасности информационных систем Работодателем предпринимается следующая система защиты:

* Обеспечение безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.
* Назначение приказом ответственного лица за обеспечение безопасности;
* Обеспечение сохранностей носителей персональных данных, при помощи установления паролей и блокировок;
* Обеспечение средствами антивирусной защиты;
* Тестирование информационной системы на проникновения.

7. Заключительные положения.

7.1. Настоящее Положение по защите персональных данных работников вступает в силу с момента его утверждения генеральным директором и действует до введения нового Положения по защите персональных данных работников.

7.2. Ознакомление работников с условиями настоящего Положения производится под расписку в листе ознакомления, являющемся неотъемлемой частью настоящего Положения по защите персональных данных работников.

7.3. Подпись работника в листе ознакомления с Положением по защите персональных данных работников означает его согласие и обязательство исполнения.

Лист ознакомления:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | ФИО | Подпись | Дата ознакомления |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Положение по защите персональных данных состоит из \_\_\_\_\_ листов, включая \_\_\_\_ пронумерованных листов ознакомления.