

ПОЛИТИКА
в области обработки и защиты персональных данных в
информационных системах персональных данных
ООО «КВАЗАР»

1. Общие положения

1.1. Настоящая Политика в области обработки и защиты персональных данных в информационных системах персональных данных ООО «КВАЗАР» (далее – Политика).

- разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных (далее – ПДн) субъектов ПДн;
- раскрывает основные категории ПДн, обрабатываемых в ООО «КВАЗАР» (далее – Оператор), цели, способы и принципы обработки Оператором ПДн, права и обязанности Оператора при обработке ПДн, права субъектов ПДн, а также перечень мер, применяемых Оператором в целях обеспечения безопасности ПДн при их обработке;
- является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке ПДн.

2. Правовые основания и цели обработки персональных данных

2.1. Политика Оператора в области обработки ПДн определяется в соответствии со следующими нормативными правовыми актами Российской Федерации:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при обработке в информационных системах персональных данных».

2.2. Во исполнение настоящей Политики руководителем Оператора утверждены следующие локальные правовые акты:

- Приказ об организации работ по обеспечению безопасности персональных данных;
- перечень обрабатываемых персональных данных;
- перечень должностей, замещение которых предусматривает осуществление обработки персональных данных;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- типовое обязательство работника Оператора, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового

договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением трудовых обязанностей;

- типовая форма согласия на обработку персональных данных работника Оператора, иных субъектов персональных данных;

2.3. Цели обработки ПДн:

- исполнение положений нормативных правовых актов, указанных в пункте 2.1 настоящей Политики;

- проведение психофизиологического обследования;

- иные цели.

3. Источники получения персональных данных

3.1. Получение сведений о персональных данных осуществляется на основании документов и информации, представленных лично работниками Оператора в процессе трудовых отношений.

4. Основные принципы обработки, передачи и хранения персональных данных

4.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4.2. Оператор осуществляет обработку специальных категорий персональных данных, касающихся состояния здоровья, и биометрических категорий персональных данных.

4.3. Оператор не осуществляет трансграничную передачу персональных данных (передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

5. Меры по обеспечению безопасности персональных данных при их обработке

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

5.2. Обеспечение безопасности персональных данных достигается, в частности:

- назначением ответственного за организацию обработки ПДн;

- осуществлением внутреннего контроля соответствия обработки ПДн Федеральному закону Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам;

- ознакомлением работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, локальными актами в отношении обработки ПДн, и (или) обучением указанных работников;

- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите ПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн.

6. Организация парольной защиты

6.1. Личные пароли доступа к ИСПДн, первично назначаются пользователям Администратором ИБ при формировании персонального идентификатора, при этом имеют следующие требования:

- длина пароля должна быть не менее шести символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования ИСПДн, общепринятые сокращения и другие данные, которые могут быть подобраны путем анализа информации об ответственном исполнителе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 123456 и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4 позициях; – в числе символов пароля могут присутствовать латинские буквы в верхнем и нижнем регистрах, цифры;
- не использовать ранее использовавшиеся пароли.

6.2. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.п.);
- хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;
- сообщать посторонним лицам свои пароли.

7. Организация антивирусной защиты

7.1. К средствам антивирусной защиты относятся утилиты, программы и программные комплексы, предназначенные для обнаружения и уничтожения вредоносных программ, а также ликвидации последствий, от их воздействий.

7.2. Для постоянной защиты должны использоваться программные комплексы в корпоративном исполнении, состоящие из клиентских программ (модулей), устанавливаемых на каждом из объектов защиты, программ (модулей) централизованного администрирования, управления и обновления антивирусных баз и самих программ (модулей).

7.3. Основные антивирусные средства должны:

- быть официально приобретены, и использоваться согласно приобретенной лицензии (лицензиям);
- быть однородными по составу, т.е. должны быть выпущены одним производителем;
- обеспечивать возможность управления (администрирования, конфигурирования, удаленной установки, контроля работы, запуска заданий и т.п.) всеми клиентскими программами с единой консоли (панели) управления администратора;
- обеспечивать загрузку обновлений антивирусных баз и программного обеспечения;
- обеспечивать недоступность настроек клиентских программ, а также их отключения и деинсталляции для обычных пользователей;
- иметь возможность оперативного оповещения пользователей и должностных лиц, отвечающих за антивирусную защиту, обо всех случаях срабатывания антивирусной защиты;
- иметь в составе средство формирования отчетов.

8. Права субъектов персональных данных

8.1. Субъект ПДн имеет право на получение сведений об обработке его ПДн Оператором.

8.2. Субъект ПДн вправе требовать от Оператора уточнения, обрабатываемых Оператором ПДн субъекта ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.3. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с Федеральными законами Российской Федерации, в том числе если:

- обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;
- обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;
- обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

8.4. Для реализации своих прав и защиты законных интересов субъект ПДн имеет право обратиться к Оператору. Оператор рассматривает любые обращения и жалобы со стороны субъектов ПДн, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

8.5. Субъект ПДн вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов ПДн.

8.6. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

9. Сроки обработки (хранения) персональных данных

9.1. Течение срока обработки ПДн начинается с момента их получения Оператором.

9.2. Оператор осуществляет хранение ПДн в форме, позволяющей определить субъект ПДн, не дольше, чем того требуют цели их обработки.

9.3. ПДн работников Оператора, в том числе родственников работника, используются в течение трудовой деятельности в соответствии с трудовым договором, а также на протяжении установленного законодательством Российской Федерации срока хранения личного дела в архиве (75 лет).

10. Уточнение, блокирование и уничтожение персональных данных

10.1. Целью уточнения ПДн, в том числе обновления и изменения, является обеспечение достоверности, полноты и актуальности ПДн, обрабатываемых Оператором.

10.2. Уточнение ПДн осуществляется Оператором по собственной инициативе, по требованию субъекта ПДн или его представителя, по требованию уполномоченного органа по защите прав субъектов ПДн в случаях, когда установлено, что ПДн являются неполными, устаревшими, недостоверными.

10.3. Целью блокирования ПДн является временное прекращение обработки ПДн до момента устранения обстоятельств, послуживших основанием для блокирования ПДн.

10.4. Блокирование ПДн осуществляется Оператором по требованию субъекта ПДн или его представителя, а также по требованию уполномоченного органа по защите прав субъектов ПДн в случае выявления недостоверных ПДн или неправомерных действий с ними.

10.5. Уничтожение ПДн осуществляется Оператором:

- по достижении цели обработки ПДн;
- в случае утраты необходимости в достижении целей обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн;
- по требованию субъекта ПДн или уполномоченного органа по защите прав субъектов ПДн в случае выявления фактов совершения администрацией района неправомерных действий с ПДн, когда устранить соответствующие нарушения не представляется возможным.

10.6. При уничтожении материальных носителей ПДн составляется акт об уничтожении носителей, содержащих ПДн.

11. Заключительные положения

11.1. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПДн, но не чаще одного раза в три года.

11.2. Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности ПДн при обработке в ИСПДн.

11.3. Ответственность должностных лиц Оператора, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.