

УТВЕРЖДАЮ

Генеральный директор

ООО «Интер-Прайм»

А.С. Куренкова

«06» октября 2014 г.



Политика по обеспечению безопасности персональных данных в ООО «Интер-Прайм»

1. Назначение документа

Документ «Политика обеспечения безопасности персональных данных» (далее Политика) ООО «Интер-Прайм» (далее Компания) регулирует отношения, связанные с защитой персональных данных физических лиц при их сборе, хранении, обработке, осуществляемых Компанией.

2. Основные понятия

Персональные данные (ПДн) - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие сбор, хранение, обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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;

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Обработка персональных данных

- 3.1. Компания является Оператором по отношению к лицам, состоящим с Компанией в трудовых отношениях. Компания может становиться Оператором персональных данных иных субъектов персональных данных в результате своей деятельности.
- 3.2. Порядок обращения с персональными данными урегулирован в Компании Положениями о защите персональных данных и иными локальными нормативными актами.
- 3.3. Будучи Оператором, Компания в установленных законодательством случаях и порядке, исполняет обязательство по уведомлению уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных.
- 3.4. Состав персональных данных, обрабатываемых Компанией, цели их обработки определены в Перечнях персональных данных, обрабатываемых в Компании.
- 3.5. В Компании определены и документально зафиксированы списки лиц, осуществляющих обработку персональных данных в ИСПДн или имеющих доступ к персональным данным с целью исполнения своих должностных обязанностей.
- 3.6. Использование персональных данных возможно только в соответствии с целями обработки персональных данных.
- 3.7. Обработка персональных данных в Компании производится без применения средств автоматизации с соблюдением правил, предусмотренных для обработки данных без использования средств автоматизации (Положение, утв. Постановлением Правительства РФ от 15.09.2008 N 687). Персональные данные обособлены от иной информации путем фиксации их на отдельных материальных носителях.
- 3.8. Обработка и передача персональных данных в Компании осуществляется с согласия субъектов персональных данных за исключением случаев, установленных федеральным Законом.
- 3.9. В случае обработки персональных данных по поручению третьих лиц, либо при передаче права обработки персональных данных третьим лицам, в условия договора Компанией включается обязанность сторон обеспечения конфиденциальности персональных данных и безопасности персональных данных при их обработке, либо дополнительно заключается соглашение о конфиденциальности.
- 3.10. При достижении целей обработки персональных данных, Компания обязуется незамедлительно прекратить обработку персональных данных, вернуть их по принадлежности, либо уничтожить соответствующие персональные данные в сроки, установленные законодательством, если иное не предусмотрено федеральными законами, и отправить уведомление об их уничтожении.

- 3.11. В Компании определен и документально зафиксирован порядок уничтожения персональных данных.

4. Обработка запросов по персональным данным

- 4.1. Компания обязуется в установленные законом сроки реагировать на запросы субъектов персональных данных (или их законных представителей) и Уполномоченных органов по защите прав субъекта персональных данных.
- 4.2. В Компании существует единый, документально зафиксированный порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных и порядок обработки запросов по персональным данным Уполномоченного органа по защите прав субъекта персональных данных.

5. Защита персональных данных

- 5.1. Защита персональных данных — комплекс мер технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к субъекту персональных данных.
- 5.2. Для построения целостной системы безопасности персональных данных в Компании определены основные цели и задачи защиты персональных данных. Главная цель защиты персональных данных - обеспечение конституционных прав граждан по сохранению личной тайны и конфиденциальности персональных данных, имеющих в информационных системах Компании. Задачами защиты персональных данных являются прогнозирование, своевременное выявление и устранение угроз носителям персональных данных.
- 5.3. Обеспечение безопасности персональных данных осуществляется организационными и инженерно-техническими мерами (в том числе установленными арендодателем), использованием шифровальных (криптографических) средств защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и иных неправомерных действий.

6. Требования к обеспечению безопасности персональных данных в информационных системах персональных данных

- 6.1. Безопасность персональных данных в ИСПДн обеспечивается комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации, подобранным в зависимости от класса ИСПДн и оборудования, установленного в соответствии с локальным нормативным актом «Политика стандартизации автоматизированных рабочих мест».
- 6.2. Комплекс мер по обеспечению безопасности персональных данных в ИСПДн предусматривает, в том числе:
- защиту относящейся к персональным данным информации от искажения, фальсификации, переадресации, несанкционированного уничтожения;

- доступ сотрудника Компании только к тем ресурсам ИСПДн, которые необходимы ему для исполнения должностных обязанностей;
 - контроль (мониторинг) обработки персональных данных;
 - работу в ИСПДн только авторизованных пользователей;
 - контроль, направленный на исключение возможности совершения злоумышленных действий;
 - восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники.
- 6.3. На всех сотрудников Компании, в том числе и сотрудников, осуществляющих обработку персональных данных в ИСПДн, наложено обязательство соблюдения регламента по информационной безопасности.
- 6.4. На всех автоматизированных рабочих местах и серверах, применяются сертифицированные средства антивирусной защиты.
- 6.5. Передача персональных данных по линиям связи между подразделениями организации, с одной стороны, и внешними организациями, с другой стороны, осуществляется с использованием сертифицированных СКЗИ или иных защитных механизмов, применение которых определяется лицом, ответственным за обеспечение безопасности персональных данных.
- 6.6. Администрирование систем защиты информации, применяемых в ИСПДн, осуществляется квалифицированными специалистами, прошедшими обучение и имеющими опыт работы с ними.

7. Управление инцидентами

- 7.1. Сотрудники обязаны уведомлять обо всех инцидентах, связанных с обработкой персональных данных.
- 7.2. Каждый выявленный инцидент рассматривается в отдельном порядке, при участии руководителя Компании, администратора информационной безопасности и сотрудника, ответственного за обработку персональных данных лица.

8. Распределение ответственности

- 8.1. Ответственность за выполнение сотрудниками требований настоящей Политики возлагается непосредственно на сотрудников и руководителей подразделения, в котором они работают. Контроль исполнения данной Политики возлагается на руководителей структурных подразделений Компании.