ПОЛИТИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика определяет порядок обеспечения безопасности персональных данных, обрабатываемых Индивидуальным предпринимателем Гардюшиной Екатериной Игоревной, ИНН 501811725860 (далее - Оператор), и меры по недопущению несанкционированного доступа, утраты, модификации, раскрытия, распространения, а также иных неправомерных действий.

1.2. Политика разработана в целях выполнения требований законодательства Российской Федерации о персональных данных, обеспечения конфиденциальности и безопасности информации, а также соблюдения прав и свобод субъектов персональных данных.

2. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Законность и справедливость обеспечения безопасности.

2.2. Предотвращение угроз: своевременное выявление, предупреждение и минимизация рисков нарушения безопасности персональных данных.

2.3. Соответствие принимаемых мер характеру, объему и категории обрабатываемых персональных данных.

2.4. Ответственность: персональная ответственность лиц за соблюдение режима конфиденциальности, допущенных к персональным данным.

3. УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Угрозами считаются:

3.1.1. несанкционированный (в том числе случайный) доступ к персональным данным;

3.1.2. утрата, модификация, блокировка, копирование, распространение персональным данных без правовых оснований;

3.1.3. утечка персональных данных через сети связи или физические носители;

3.1.4. действия вредоносных программ.

3.2. Анализ угроз проводится регулярно. Результаты анализа используются для актуализации мер защиты.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Организационные меры:

4.1.1. Назначение самого Оператора ответственным за организацию обработки персональных данных.

4.1.2. Разграничение доступа к персональным данным по ролям и полномочиям (если применимо);

4.1.3. Обучение персонала требованиям защиты персональных данных (если применимо);

4.1.4. Регламентация доступа к персональным данным в локальных нормативных актах;

4.1.5. Контроль соблюдения правил безопасности и проведение внутренних проверок.

4.2. Технические меры:

4.2.1. Ограничение физического доступа к техническим средствам обработки персональных данных;

4.2.2. Резервное копирование и хранение данных на защищённых носителях;

4.2.3. Использование межсетевых экранов, антивирусной защиты и криптографических средств (при передаче персональных данных через открытые каналы связи) (если применимо);

4.2.4. Регистрация и аудит действий пользователей с персональными данными.

4.3. Правовые меры:

4.3.1. Уведомление Роскомнадзора о начале обработки персональных данных;

4.3.2. Ведение учета инцидентов и уведомление субъектов персональных данных в случае утечки.

5. УРОВНИ ЗАЩИЩЁННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Уровень защищённости определяется на основании актуальных угроз и категорий персональных данных в соответствии с классификацией, установленной ФСТЭК России.

5.2. Применяемый уровень защиты — базовый, в зависимости от характера данных и каналов обработки.

6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

6.1. В случае обнаружения инцидента (утечки, взлома, несанкционированного доступа и др.):

6.1.1. незамедлительно проводится локализация и минимизация последствий;

6.1.2. фиксируются технические и организационные параметры инцидента;

6.1.3. по возможности уведомляются субъекты персональных данных и Роскомнадзор.

7. ОТВЕТСТВЕННОСТЬ

7.1. Все имеющие доступ к персональным данным, обрабатываемым в ходе деятельности Оператора, обязаны соблюдать требования настоящей Политики.

7.1.2. Оператор не несет ответственности за причинённый ущерб субъектам персональных данных в случае, если утечка или иное нарушение конфиденциальности персональных данных произошло не по вине Оператора, в том числе:

7.1.2.1. в результате действий (бездействия) самого субъекта персональных данных, повлекших раскрытие его данных третьим лицам;

7.1.2.2. вследствие неправомерных действий третьих лиц, направленных на взлом технических средств Оператора, если Оператор предпринял достаточные меры защиты, установленные законодательством Российской Федерации;

7.1.2.3. в случаях наступления форс-мажорных обстоятельств, повлекших нарушение функционирования информационных систем (стихийные бедствия, аварии, перебои в электроснабжении, военные действия и т.д.);

7.1.2.4. при использовании субъектом персональных данных незащищённых каналов связи или программного обеспечения, способствующего утечке данных.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящая Политика подлежит пересмотру в случае изменений законодательства, условий обработки персональных данных, выявления новых угроз или технических изменений.

8.2. Политика опубликована на сайте https://bgfinance.ru и доступна для всех пользователей.