Положение о защите персональных данных

1. Общие положения.

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Гражданским кодексом, Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами, действующими на территории России.

1.2. Настоящее Положение определяет порядок обеспечения безопасности персональных данных, обрабатываемых Обществом с ограниченной ответственностью «Профобразование», (далее — «Оператор»), и меры по недопущению несанкционированного доступа, утраты, модификации, раскрытия, распространения, а также иных неправомерных действий и гарантии конфиденциальности предоставленных сведений.

1.3. Цель настоящего Положения – защита персональных данных, обрабатываемых Оператором в целях деятельности, от несанкционированного доступа и разглашения. Предоставляемые Оператору персональные данные являются конфиденциальной, строго охраняемой информацией.

1.4. Для целей настоящего Положения используются следующие термины и определения:

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

1.6. Оператор – юридическое лицо, которое самостоятельно или совместно с другими лицами организует и осуществляет обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, и действия, совершаемые с персональными данными;

1.7. Защита персональных данных – комплекс правовых, организационных и технических мер, применяемый для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных;

1.8. Распространение персональных данных - действия, направленные на раскрытие персо**нальн**ых данных неопределенному кругу лиц;

2. Основные принципы обеспечения безопасности ваших данных

2.1. Принципы. Минимизация объема — главный принцип, которого мы неукоснительно придерживаемся при обработке персональных данных: мы не собираем их, не храним и не обрабатываем иным образом, если этого действительно не требуется.

Мы также руководствуемся установленными действующим законодательством РФ принципами обработки персональных данных, включая следующие:

- Законность и справедливость обработки персональных данных;
- Обработка персональных данных только в соответствии с конкретными, заранее определенными и законными целями;
- Недопущение объединения баз персональных данных, обработка которых осуществляется в несовместимых целях;
- Точность, достаточность, актуальность и достоверность персональных данных (насколько это зависит от нас*).

** Компания не проверяет достоверность предоставленных персональных данных и дееспособность лица, их предоставившего. При передаче нам персональных данных Вы гарантируете, что они являются достоверными, актуальными и не нарушают законодательство Российской Федерации.*

2.2. Применение такого комплекса мер защиты, который позволяет обеспечить предотвращение угроз по неправомерному или случайному доступу к персональным данным, их уничтожения, изменения, блокирования, копирования, предоставления и распространения.

2.3. Превентивность мер защиты, достигаемая путем своевременное выявление, предупреждение и минимизация рисков нарушения безопасности персональных данных.

2.4. Ответственность Оператора за соблюдение конфиденциальности и безопасности хранения персональных данных.

3. Сведения о защите персональных данных

Все предоставляемые вами персональные данные конфиденциальны по умолчанию. Защита персональных данных, обрабатываемых Компанией, обеспечивается правовыми, организационными и техническими мерами, необходимыми и достаточными для обеспечения требований законодательства Российской Федерации в области защиты персональных данных:

- Организационные меры:

- Назначение Оператором отдельных ответственных лиц за доступ, хранение и обеспечение безопасности персональных данных посредством издания локальных нормативных актов (приказов о назначении);
- Определение актуальных угроз безопасности персональных данных при их обработке и разработка мер, мероприятий по защите персональных данных;
- Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
- Регламентация доступа к персональным данным в локальных нормативных актах;
- Осуществление внутреннего контроля и аудита.

● Технические меры:
- Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- Установление правил доступа к персональным данным, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными, в специальном журнале учета;
- Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- Оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений.

● Правовые меры:
- Уведомление Роскомнадзора о начале обработки персональных данных;
- Ведение учета инцидентов и уведомление субъектов персональных данных в случае несанкционированного или случайного распространения персональных данных.

4. Угрозы безопасности персональных данных, их категории

4.1. В целях настоящего Положения угрозами безопасности персональных данных считаются:

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

● противоправные действия, влияющие на целостность и структурность персональных данных, а именно: утрата, модификация, блокировка, копирование, распространение персональным данных;

● техническая неисправность, связанная с неконтролируемым воздействием на доступность персональных данных (утечка) через сети связи или физические носители;

● действия вредоносных программ.

● Противоправные действия сотрудников ООО «Профобразование», направленные на нарушение режима безопасности хранения персональных данных.

● С целью профилактики предотвращения вышеуказанных угроз и их недопущения проводится регулярный анализ и проверка работоспособности всего комплекса защиты персональных данных.

5. Уровень защиты ваших персональных данных при их обработке

5.1. Уровень защищённости определяется на основании актуальных угроз и категорий персональных данных в соответствии с классификацией, установленной Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5.2. Применяемый уровень защиты — 2-й уровень защищенности согласно классификации, установленной Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6. Какие действия предпринимаются Компанией в случае нарушения безопасности персональных данных

6.1. В случае обнаружения нарушений в режиме безопасности персональных данных Оператор:
6.2. Незамедлительно проводит устранение источника и последствий, приведших к нарушению режима безопасности;
6.3. Оператором проводится внутренняя проверка для установления причин и ответственных лиц за нарушение режима безопасности;
6.4. Уведомляются субъекты персональных данных и Роскомнадзор о нарушении режима безопасности и возможности его восстановления, предпринятых действиях и результатах внутренней проверки.

7. Ответственность Компании

7.1. Все ответственные лица, имеющие доступ к персональным данным, обрабатываемым в ходе деятельности Оператора, обязаны соблюдать требования настоящего Положения.
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;
7.1.2.5. Работники Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8. Заключительные положения

Настоящее Положение расположено в открытом доступе на сайте: https://vkr-smart.ru.

Общество с ограниченной ответственностью «Профобразование»
ИНН: 6455057001
ОГРН: 1126455002520
Юридический адрес: 410033, САРАТОВСКАЯ ОБЛАСТЬ, Г.О. ГОРОД САРАТОВ, Г САРАТОВ, УЛ ХАБАРОВСКАЯ, Д. 25, КВ. 159
Контактные данные: e-mail: office@profspo.ru, телефон: 8-800-511-14-70