Общество с ограниченной
ответственностью
«АльфаПласт»
(ООО «АльфаПласт»)

УТВЕРЖДАЮ
Генеральный директор
ООО «АльфаПласт»
_____
Ю.В. Пятова
10.01.2022

ПОЛОЖЕНИЕ

10.01.2022 № 1
о защите персональных данных пользователей веб-сайта

г.Санкт-Петербург

1. Общие положения

1.1. Положение о защите персональных данных пользователей веб-сайта ООО «АльфаПласт» (далее – Оператор) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных пользователей веб-сайта ООО «АльфаПласт» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- под персональными данными (далее – ПД) понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- под угрозами безопасности ПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- под уровнем защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются Генеральным директором ООО «АльфаПласт» и вводятся приказом. Все сотрудники, имеющие доступ к персональным данным пользователей веб-сайта, должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу с 10.01.2022.

2. Защита персональных данных

2.1. Оператор принимает следующие меры по защите ПД:

2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением сотрудниками требований к защите ПД.

2.1.2. Разработка политики в отношении обработки ПД.

2.1.3. Установление правил доступа к ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД.

2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их служебными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.

2.1.8. Обнаружение фактов несанкционированного доступа к ПД.

2.1.9. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.1.10. Обучение сотрудников, непосредственно осуществляющих обработку ПД, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Оператора в отношении обработки ПД, локальным актам по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля и аудита.

2.1.12. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных.

2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах сотрудников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищенности персональных данных.

2.3.1. Первый уровень защищенности. Если оператор отнес информационную систему к первому типу угрозы или если тип угрозы второй, но оператор обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета сотрудников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и оператор обрабатывает специальные категории ПД сотрудников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы оператор обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы оператор обрабатывает общие ПД сотрудников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы оператор обрабатывает специальные категории ПД сотрудников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы оператор обрабатывает биометрические ПД, или при третьем типе угрозы оператор обрабатывает общие ПД более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы оператор обрабатывает только общие ПД сотрудников или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных оператор:

- обеспечивает режим безопасности помещений, в которых размещается информационная система;
- обеспечивает сохранность носителей информации;
- утверждает перечень сотрудников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, оператор назначает ответственного за обеспечение безопасности ПД в информационной системе.

2.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, оператор ограничивает доступ к электронному журналу сообщений, за исключением сотрудников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4—2.6 настоящего Положения, оператор:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий сотрудников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов оператора.

2.8. В целях защиты ПД на бумажных носителях оператор:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД;

•хранит документы, содержащие ПД в шкафах, запирающихся на ключ;

•хранит документы с персональными данными пользователей веб-сайта в сейфе.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД пользователей веб-сайта, оформляются, ведутся и хранятся только уполномоченными сотрудниками оператора.

2.10. Сотрудники оператора, допущенные к ПД пользователей веб-сайта, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД сотрудников не допускаются.

2.11. Допуск к документам, содержащим ПД пользователей веб-сайта, внутри организации осуществляется на основании Регламента допуска сотрудников к обработке персональных данных пользователей веб-сайта.

2.12. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия пользователя веб-сайта на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.13. Передача информации, содержащей сведения о ПД пользователей веб-сайта, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

3. Гарантии конфиденциальности персональных данных

3.1. Все сотрудники организации, осуществляющие обработку ПД пользователей веб-сайта, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.

3.2. Пользователь веб-сайта вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД пользователей веб-сайта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

Генеральный директор Ю.В. Пятова

10.01.2022