ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ ОСТРИШКО ЕЛЕНА ЮРЬЕВНА
644012, Омская обл., г. Омск, ул. Малиновского 18/2, цокольный этаж
ОГРНИП 325554300037460, ИНН 550112037269
Телефон: +7 (904) 827-01-18, Электронная почта: eostrishko@yandex.ru

Утверждаю
Индивидуальный предприниматель
Остришко Е.Ю.

_____
(Остришко Е.Ю.)

18.12.2025 г.

Положение
О защите персональных данных

1. **Общие положения**

1.1. Положение о защите персональных данных (далее- Положение) разработано Индивидуальным предпринимателем Остришко Еленой Юрьевной ОГРН ИП 325554300037460 (далее - Оператор персональных данных или Оператор) 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 клиентов, контрагентов, их представителей, участников мероприятий, а также пользователей Интернет - площадки (Профиль, сообщество «Варенье» внутри платформы VK (ВКонтакте) https://vk.com/varenie55omsk).

1.3. В целях 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. Положение утверждается Оператором.

2. **Защита ПД**

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 Оператором 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 в информационную систему в соответствии с обязанностями лиц, имеющих доступ.
2.1.5. Встроенные в операционные системы средства защиты с регулярно обновляемыми базами.
2.1.6. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный доступ к ним.
2.1.7. Обнаружение фактов несанкционированного доступа к ПД.
2.1.8. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
2.1.9. Изучение лицами, непосредственно осуществляющими обработку ПД, положений законодательства РФ о персональных данных, в том числе требований к защите персональных данных, документов, определяющих Политику в отношении обработки ПД, локальных актов по вопросам обработки персональных данных.
2.1.10. Осуществление внутреннего контроля и аудита.
2.1.11. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

3. Угрозы безопасности персональных данных

3.1. В зависимости от наличия потенциальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных выделяются следующие типы угроз:
3.1.1. Угрозы первого типа — наличие в системном программном обеспечении функциональных возможностей, не заявленных производителем и способных привести к нарушению безопасности персональных данных.
3.1.2. Угрозы второго типа — наличие потенциальных угроз, связанных с прикладным программным обеспечением.
3.1.3. Угрозы третьего типа — отсутствие угроз, связанных с системным и прикладным программным обеспечением.
3.2. В соответствии с утверждённой Моделью угроз безопасности персональных данных для Оператора актуален третий тип угроз.

4. Уровни защищённости персональных данных

4.1. В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 устанавливаются четыре уровня защищённости персональных данных.
4.2. **Первый уровень защищённости** применяется при первом типе угроз либо при обработке специальных категорий персональных данных более чем 100 000 субъектов.
4.3. **Второй уровень защищённост**и применяется при втором типе угроз либо при обработке специальных категорий персональных данных либо персональных данных более чем 100 000 субъектов.
4.4. **Третий уровень защищённости** применяется при:

- втором типе угроз и обработке общих персональных данных менее чем 100 000 субъектов, либо
- третьем типе угроз и обработке специальных категорий персональных данных.

4.5. Четвёртый уровень защищённости применяется при третьем типе угроз, если Оператор обрабатывает только общие персональные данные субъектов персональных данных в количестве менее 100 000.

4.6. Установленный уровень защищённости

4.6.1. Оператор:

- не обрабатывает специальные категории персональных данных;
- не обрабатывает биометрические персональные данные в целях идентификации;
- не имеет работников в штате;
- обрабатывает персональные данные клиентов, контрагентов и пользователей сайта в количестве менее 100 000 субъектов;
- использует информационные системы (CRM, 1С, электронные таблицы Excel), не содержащие угроз первого и второго типа.

4.6.2. В соответствии с утверждённой Моделью угроз безопасности персональных данных информационные системы Оператора отнесены к четвёртому уровню защищённости персональных данных.

4.7. Меры защиты при 4 уровне защищённости

При четвёртом уровне защищённости персональных данных Оператор:

- обеспечивает режим безопасности помещений, в которых размещаются материальные носители персональных данных;
- обеспечивает сохранность материальных и электронных носителей персональных данных;
- утверждает перечень лиц, допущенных к обработке персональных данных;
- использует средства защиты информации, прошедшие оценку соответствия требованиям законодательства Российской Федерации.

4.8. Защита персональных данных на бумажных носителях

В целях защиты персональных данных на бумажных носителях Оператор:

- приказом назначает ответственное лицо за обработку персональных данных;
- ограничивает доступ в помещения хранения документов;
- обеспечивает хранение документов в шкафах, запирающихся на ключ.

4.9. Лица, допущенные к обработке персональных данных, подписывают обязательства о неразглашении персональных данных.

4.10. Оператор использует средства электронной подписи, содержащие средства криптографической защиты информации, применяемые для подписания электронных документов в соответствии с требованиями законодательства Российской Федерации. (Использование указанных средств не является обязательным требованием для обеспечения 4 уровня защищённости персональных данных и осуществляется в пределах функциональных возможностей применяемых программных средств).

5. Гарантии конфиденциальности персональных данных

5.1. Все лица, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Политикой Оператора по обработке персональных данных требованиями законодательства РФ.
5.2. Субъект персональных данных вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.
5.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.