

АО «Империя вкуса»	Вид документа	ЛНА
	Номер документа	ЛНА/П-5/2022
	Статус	Версия 1.0
	Дата ввода в действие	01.09.2022
	Страница	Стр. 1 из 10

УТВЕРЖДАЮ
Генеральный директор
АО «Империя вкуса»



подпись

Е.А. Сергеева

«31» августа 2022 г.

ПОЛОЖЕНИЕ

О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

АКЦИОНЕРНОГО ОБЩЕСТВА «ИМПЕРИЯ ВКУСА»

г. Брянск, 2022 год

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус:	Версия 1.0	Страница	стр. 2 из 10

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. ОСНОВНЫЕ ПОНЯТИЯ, ТЕРМИНЫ, СОКРАЩЕНИЯ	3
3. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....	3
4. ГАРАНТИИ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	5
5. МЕСТО ХРАНЕНИЯ ДОКУМЕНТА	5

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус:	Версия 1.0	Страница	стр. 3 из 10

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о защите персональных данных (далее - Положение) Акционерного общества «Империя вкуса» (далее - Предприятие) 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 Российской Федерации.

1.2. Цель настоящего Положения – защита персональных данных работников Предприятия от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.3. Изменения и дополнения к настоящему Положению разрабатываются и утверждаются Работодателем в установленном порядке. Все работники Предприятия должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

2. ОСНОВНЫЕ ПОНЯТИЯ, ТЕРМИНЫ, СОКРАЩЕНИЯ

№ п/п	Термин	Определение
1.	Предприятие, Работодатель	Акционерное общество «Империя вкуса».
2.	Директор	Генеральный директор АО «Империя вкуса».
3.	Работник	Физическое лицо, вступившее в трудовые отношения с Работодателем на основании трудового договора и на иных основаниях, предусмотренных ст. 16 Трудового кодекса РФ.
4.	РФ	Российская Федерация.
5.	Персональные данные (ПД)	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
6.	Угрозы безопасности ПД	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.
7.	Уровень защищенности ПД	комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

3. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Работодатель принимает следующие меры по защите ПД:

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

3.1.2. Разработка политики в отношении обработки ПД.

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус:	Версия 1.0	Страница	стр. 4 из 10

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

3.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

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

3.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

3.1.7. Соблюдение условий, обеспечивающих сохранность ПД и исключаящих несанкционированный к ним доступ.

3.1.8. Обнаружение фактов несанкционированного доступа к ПД.

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

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

3.1.11. Осуществление внутреннего контроля и аудита.

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

3.2. Угрозы защищенности ПД.

3.2.1. 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 ПД.

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

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

3.3. Уровни защищенности персональных данных.

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

3.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории ПД работников 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 работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

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

3.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД работников или менее чем 100 тыс. физических лиц.

3.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещает информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус:	Версия 1.0	Страница	стр. 5 из 10

требованиям закона в области обеспечения безопасности информации.

3.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 3.4 настоящего Положения, Работодатель назначает ответственного за обеспечение безопасности ПД в информационной системе.

3.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 3.4, 3.5 настоящего Положения, Работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

3.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 3.4-3.6 настоящего Положения, работодатель:

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

3.8. В целях защиты ПД на бумажных носителях работодатель:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников;
- хранит документы, содержащие ПД работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе.

3.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только работником, назначенным ответственным за обработку ПД.

3.10. Работники, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных (Приложение № 1). В противном случае до обработки ПД работников не допускаются.

3.11. Допуск к документам, содержащим ПД работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

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

3.13. Передача информации, содержащей сведения о ПД работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4. ГАРАНТИИ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.

4.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

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

5. МЕСТО ХРАНЕНИЯ ДОКУМЕНТА

5.1. Оригинал Положения хранится по месту регистрации Работодателя.

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус:	Версия 1.0	Страница	стр. 6 из 10

Место хранения файлов

№	Название приложения	Формат
1.	Положение о защите персональных данных АО «Империя вкуса»	MS Word, Adobe Reader, а также на бумажном носителе

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус:	Версия 1.0	Страница	стр. 7 из 10

Приложение № 1

ОБЯЗАТЕЛЬСТВО
о неразглашении сведений,
составляющих персональные данные работников

Я, _____

(фамилия, имя, отчество)

в качестве работника АО «Империя вкуса» в период исполнения работы по трудовому договору

ОБЯЗУЮСЬ:

1. Выполнять требования приказов, инструкций и положений по обеспечению сохранности персональных данных работников.
2. Пресекать действия других лиц, которые могут привести к разглашению персональных данных работников.
3. Не использовать сведения о персональных данных работников в свою личную пользу.
4. Использовать в своей работе лишь те персональные данные работников, которые действительно необходимы для полноценного выполнения должностных обязанностей.
5. При составлении документов, включающих персональные данные работников, ограничиваться минимальными, действительно необходимыми в документе сведениями; определять количество экземпляров документов в строгом соответствии с действительной служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения.
6. При уходе с работы или выходе из помещения на срок более 20 минут документы, содержащие персональные данные работников, запирать в сейф (если нет сейфа, то в специально отведенные места для сохранения конфиденциальных документов - ящик рабочего стола, хранилище документов и т.п.), а также запирать дверь помещения, если в нем не осталось других работников;
7. Документы, содержащие персональные данные работников во время работы располагать так, что бы исключить возможность ознакомления с ними других лиц, в том числе допущенных к подобным сведениям, но не имеющих к ним прямого отношения;
8. В случае попытки посторонних лиц получить сведения о персональных данных работников, немедленно сообщить Генеральному директору.
9. Об утрате или недостатке документов, содержащих персональные данные работников немедленно сообщать Генеральному директору;
10. Отказывать в предоставлении персональных данных кому бы-то ни было без письменного разрешения работодателя или уполномоченного им лица;
11. В случае увольнения все носители персональных данных работников (бумажные, электронные документы), которые находились в моем распоряжении в связи с выполнением служебных обязанностей во время работы в организации, сдать в архив.

Мне разъяснены требования локальных нормативных актов АО «Империя вкуса» вопросам обеспечения сохранности сведений, содержащих персональные данные работников.

Номер документа	ЛНА-5/2022	Дата ввода в действие	01.09.2022
Статус	Версия 1.0	Страница	стр. 8 из 10

Мне известно, что нарушение указанных требований может повлечь за собой уголовную, административную, гражданско-правовую, дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

(должность)

(подпись)

(расшифровка подписи)

«__» _____ 20__ г.

Один экземпляр обязательства получил «__» _____ 20__ г.

(подпись)

