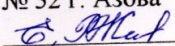



СОГЛАСОВАНО:  
Председатель первичной  
профсоюзной организации МБДОУ  
№ 32 г. Азова  
  
25.07.2022

Жердева Е. В.



С. В. ВОЛОСНЫХ  
Заведующий МБДОУ № 32 г. Азова  
  
Приказ № 53 от 25.07.2022

• Дополнительное соглашение №1  
к Политике по обработке персональных данных  
и реализации требований к защите персональных данных  
муниципального бюджетного дошкольного образовательного  
учреждения детский сад №32 г. Азова

В соответствии с Федеральным законом от 14.07.2022 № 266-ФЗ «О внесении изменений в  
ФЗ «О персональных данных»

Политику по обработке персональных данных и реализации требований к защите  
персональных данных от 11.01.2016 года изложить в следующей редакции:

**ПОЛИТИКА**  
по обработке персональных данных и реализации  
требований к защите персональных данных  
МБДОУ №32 г. Азова

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. В целях гарантирования выполнения норм федерального законодательства в полном объеме МБДОУ № 32 г. Азова (далее – Оператор) считает своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая политика в области обработки и защиты персональных данных в МБДОУ № 32 г. Азова (далее – Политика) характеризуется следующими признаками:

1.2.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных субъектов персональных данных.

1.2.2. Раскрывает основные категории персональных данных, обрабатываемых оператором, цели, способы и принципы обработки оператором персональных данных, права и обязанности оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых оператором в целях обеспечения безопасности персональных данных при их обработке.

1.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности оператора при обработке персональных данных.

**2. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ**

Наименование: Муниципальное бюджетное дошкольное образовательное учреждение детский сад № 32 г. Азова.

ИНН: 6140018778

Фактический адрес: 346782, Ростовская область, г. Азов, ул. Комсомольская 7

Тел. 8 (86342)4-03-80

Сведения об Операторе внесены в Реестр операторов, осуществляющих обработку персональных данных (регистрационный номер 10-0096672, дата записи 15.03.2010. дата начала обработки 10.03.2010).

### 3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Политика Оператора в области обработки персональных данных определяется следующими нормативными правовыми актами:

- Конституцией Российской Федерации.
- Трудовым кодексом Российской Федерации.
- Гражданским кодексом Российской Федерации.
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».
- Федеральным законом от 14.07.2022 № 266-ФЗ «О внесении изменений в ФЗ «О персональных данных»
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
- Постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
  - Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Федеральным законом от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации»
- Приказом Министерства Здравоохранения Российской Федерации от 3 июля 2000 г. N 241 «Об утверждении медицинской карты ребенка для образовательных учреждений».

3.2. Во исполнение настоящей Политики руководящим органом Оператора утверждены следующие локальные нормативные правовые акты:

- Положение о защите персональных данных. (Приложение 1)
- Порядок обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные. (Приложение 2)
  - Типовая форма согласия на обработку персональных данных работников МБДОУ №32 г. Азова. (Приложение 3)
  - Типовая форма согласия на обработку персональных данных воспитанников МБДОУ №32 г. Азова и их родителей (законных представителей). (Приложение 4)
  - Должностная инструкция ответственного за организацию обработки и обеспечения безопасности персональных данных (Приложение 5)

### 4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Персональные данные работника используются для целей, связанных с выполнением работником трудовых функций.

4.2. Работодатель для этой цели запрашивает у работника общие персональные данные: фамилию, имя, отчество, дату, месяц и год рождения, место рождения, адрес, семейное положение, образование, профессию; специальные категории персональных данных: состояние здоровья, сведения о судимости; биометрические персональные данные: фото в бумажном и электронном виде.

4.3. Персональные данные воспитанников и их родителей (законных представителей)

используются для целей, связанных с образовательной деятельностью по образовательным программам дошкольного образования.

4.3. Оператор для этой цели запрашивает общие персональные данные: фамилию, имя, отчество, дату, месяц и год рождения, место рождения, адрес.

4.5. Персональные данные, представленные работником, персональные данные воспитанников и родителей воспитанников (законных представителей), обрабатываются автоматизированным и без использования средств автоматизации способами. Оператор не принимает, не снимает и не хранит копии личных документов. Документы, которые предъявляются оператору для хранения в оригинале (справки, медицинские заключения и т. д.), хранятся в личном деле работника в течение 50 лет после расторжения с работником трудового договора.

4.6. После истечения срока нормативного хранения документов, которые содержат персональные данные, документы подлежат уничтожению. Для этого работодатель создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению. После чего документы измельчаются в шредере. Персональные данные работников в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация.

## 5. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИСТОЧНИКИ ИХ ПОЛУЧЕНИЯ

5.1. В информационных системах персональных данных оператора обрабатываются следующие категории персональных данных:

- Персональные данные работников МБДОУ №32 г. Азова.
- Персональные данные воспитанников МБДОУ №32 г. Азова и их родителей (законных представителей).
- Персональные данные родителей воспитанников (законных представителей).

5.2. К персональным данным Субъекта, которые обрабатывает МБДОУ № 32 г. Азова относятся:

- фамилия имя отчество;
- адрес места жительства;
- паспортные данные;
- данные свидетельства о рождении;
- контактный телефон;
- данные страхового свидетельства, ИНН;
- данные о трудовой деятельности;
- семейное положение;
- образование;
- информация о наличии судимости для сотрудников;
- данные о состоянии здоровья;
- иная необходимая информация, которую субъект добровольно сообщают о себе для получения услуг предоставляемых МБДОУ, если ее обработка не запрещена законом.

## 6. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ, ПЕРЕДАЧИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст.5 Федерального закона 152-ФЗ «О персональных данных».

6.2. Оператор не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

6.3. Оператор не выполняет обработку специальных категорий персональных данных, (за исключением ограниченных сведений, касающихся состояния здоровья работника, воспитанников и их родителей (законных представителей)).

6.4. Оператор не производит трансграничную (на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

6.5. Оператором созданы общедоступные источники персональных данных (сайт). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, должность, фотографии и награды с мероприятий), включаются в такие источники только с письменного согласия субъекта персональных данных.

## 7. СВЕДЕНИЯ О ТРЕТЬИХ ЛИЦАХ, УЧАСТВУЮЩИХ В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

- Финансовому управлению г. Азова;
- Пенсионному фонду РФ;
- Федеральной налоговой службе РФ;
- ОАО «Сбербанк России»;
- Управлению социальной защиты населения Администрации г. Азова;
- Министерству образования и науки Ростовской области;
- Лицензирующим и/или контролирующим органам государственной власти и местного самоуправления.

## 8. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

8.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- Назначением ответственных за организацию обработки персональных данных;
- Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных ФЗ от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, локальным актам;
- Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников;
- Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- Учетом носителей персональных данных;
- Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

## 9. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

9.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

9.4. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, урегулирует спорные и конфликтные ситуации в досудебном порядке.

9.5. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

9.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

## 10. КОНТАКТНАЯ ИНФОРМАЦИЯ

10.1. Ответственным за организацию обработки и обеспечения безопасности персональных данных в МБДОУ № 32 г. Азова назначен главный бухгалтер Эбингер Г.В.

10.2. Уполномоченным органом по защите прав субъектов персональных данных является федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Управление Роскомнадзора по Ростовской области. Адрес: 344029, г. Ростов-на-Дону, ул. Металлургическая, 113/46 Тел.: (863) 223-79-49 E-mail: rsockanc61@rkn.gov.ru Руководитель Управления: Сидорцов Игорь Николаевич Сайт: 61.rkn.gov.ru

## 11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящая Политика является внутренним документом Оператора, общедоступной и подлежит размещению на официальном сайте Оператора.

11.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

11.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных Оператора.

11.4. Ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.

## Приложение 1

### ПОЛОЖЕНИЕ

о защите персональных данных

#### 1. Общие положения

1.1. Положение о защите персональных данных МБДОУ №32 г. Азова (далее – Работодатель) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ, Федеральным законом от 14.07.2022 № 266-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных работников МБДОУ №32 г. Азова 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 Заведующим МБДОУ №32 г. Азова и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение вступает в силу с 01.09.2022.

## **2. Защита персональных данных**

2.1. Работодатель 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 работниками 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 производственными 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 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.

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 работников.

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 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.

2.3.2. 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.

2.3.3. 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.

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

2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, 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, работодатель 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, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, 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, 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.

2.8. 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 в отделе кадров.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только заведующей и работниками бухгалтерии.

2.10. Работники бухгалтерии, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.

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

2.12. 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.

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

### **3. Гарантии конфиденциальности персональных данных**

- 3.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.
- 3.2. Работник 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 работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

## Приложение 2

### Порядок обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

#### 1. Общие положения

1.1. Порядок обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – Инструкция) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 (в ред. от 23.09.2005) «Об утверждении перечня сведений конфиденциального характера», постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации.

1.2. Настоящая Инструкция устанавливает в муниципальном бюджетном дошкольном образовательном учреждении детский сад №32 г.Азова (далее – Учреждение) порядок работы с документами – носителями конфиденциальной информации, содержащей персональные данные, в целях:

- предотвращения неконтролируемого распространения конфиденциальной информации, содержащей персональные данные в результате ее разглашения должностным лицом, имеющим доступ к информации, содержащей персональные данные, или получения несанкционированного доступа к конфиденциальной информации;
- предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;
- предотвращения утраты, несанкционированного уничтожения или сбоев в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные, обеспечение полноты, целостности, достоверности такой информации;
- соблюдения правового режима использования информации, содержащей персональные данные;
- обеспечения возможности обработки и использования персональных данных Учреждением и должностными лицами, имеющими соответствующие полномочия.

1.3. Обработка персональных данных осуществляется в Учреждении с согласия субъекта персональных данных. Согласие субъекта на обработку его персональных данных не требуется в следующих случаях:

- если персональные данные являются общедоступными;
- когда персональные данные относятся к состоянию здоровья субъекта и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия субъекта невозможно;



- если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработки персональных данных по требованию уполномоченных на то государственных органов в случаях, предусмотренных федеральным законом;
- когда обработка персональных данных осуществляется в целях исполнения обращения, запроса самого субъекта персональных данных, трудового или иного договора с ним;
  - обработки адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
  - обработки данных, включающих в себя только фамилии, имена и отчества;
- обработки персональных данных без использования средств автоматизации.

1.4. В целях обеспечения сохранности и конфиденциальности информации, содержащей персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками Учреждения, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

1.5. Режим конфиденциальности персональных данных отменяется в случаях обезличивания этих данных, в отношении персональных данных, ставших общедоступными, или по истечении 50-летнего срока их хранения, если иное не предусмотрено законом.

1.6. В Учреждении должностными лицами, имеющими доступ к информации, содержащей персональные данные, формируются и ведутся перечни персональных данных с указанием регламентирующих документов, мест хранения и лиц, ответственных за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, не допускается.

## **2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации**

2.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна вестись таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

2.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.4. Материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах.

2.5. Должностным лицам, работающим с персональными данными, запрещается разглашать информацию, содержащую персональные данные, устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью.

2.6. Не допускается формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные.

2.7. Передача персональных данных допускается только в случаях, установленных действующим законодательством Российской Федерации и действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению вышестоящих должностных лиц.

2.8. Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи (телефон, телефакс, электронная почта и т.п.) без письменного согласия субъекта персональных данных, за исключением случаев, установленных действующим законодательством Российской Федерации.

2.9. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах запроса или опубликованных в общедоступных источниках.

2.10. В Учреждении обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели, обработки которых заведомо несовместимы. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.11. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия: а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных; б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных; в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных; г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели, обработки которых заведомо несовместимы.

2.12. При ведении журналов (реестров, книг), содержащих персональные данные, должны соблюдаться следующие условия: а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Учреждения, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о внесении изменений в персональные данные субъекта; б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается; в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза.

2.13. Лица, имеющие отношение к работе с персональными данными, в работе должны руководствоваться формой Журнала учета обращений субъектов персональных данных о выполнении законных прав (Приложение 1), при обработке персональных данных в Учреждении. Для ведения Журнала учета обращений субъектов персональных данных о выполнении законных прав, при обработке персональных данных в Учреждении назначается лицо, ответственное за ведение и хранение Журнала учета обращений субъектов персональных данных о выполнении законных прав. Журнал учета обращений субъектов персональных данных о выполнении законных прав, при обработке персональных данных в Учреждении должен быть пронумерован, прошнурован и скреплен подписью заведующего Учреждением. Хранение Журнала учета обращений субъектов персональных данных о выполнении законных прав, при обработке персональных данных в Учреждении должно исключать несанкционированный доступ к нему.

2.14. Для обработки различных категорий персональных данных, осуществляемых без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.15. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, но с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

2.16. Лица, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией.

2.17. Лица, осуществляющие обработку и(или) хранение персональных данных в Учреждении, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную действующим законодательством Российской Федерации ответственность.

### **3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации**

3.1. Безопасность персональных данных при их обработке в автоматизированных информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.2. Допуск должностных лиц к обработке персональных данных в автоматизированной информационной системе осуществляется на основании соответствующих разрешительных документов и ключей доступа (паролей).

3.3. Размещение автоматизированных информационных систем, специальное оборудование и организация с их использованием работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в соответствующих помещениях посторонних лиц.

3.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа или под чужими, а равно общими (одинаковыми) паролями, не допускается.

3.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, не допускается.

3.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с действующим законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.7. При обработке персональных данных в информационной системе пользователями должно быть обеспечено: – использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей; – недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование; – постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; – недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.8. При обработке персональных данных в автоматизированной информационной системе ответственными лицами должны обеспечиваться:

- непрерывное обучение лиц, использующих средства защиты информации, применяемые в автоматизированных информационных системах, правилами работы с ними;
- учет лиц, допущенных к работе с персональными данными в автоматизированной информационной системе, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за обеспечением соблюдения условий за использованием средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных;
- иные требования по защите персональных данных, установленных инструкциями Учреждения по их использованию и эксплуатации.

3.9. Особенности обеспечения безопасности информации и конфиденциальности персональных данных, связанные с использованием конкретных автоматизированных информационных систем, определяются локальными нормативными документами Учреждения. Локальные акты регламентируют порядок использования указанных информационных систем, а также эксплуатационной и инструктивной документацией, касающейся технических средств обработки персональных данных в рамках конкретной автоматизированной информационной системы.

#### **4. Порядок учета, хранения и обращения со съемными носителями персональных данных (их твердыми копиями), а также их утилизации**

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.2. Учет съемных носителей, содержащий персональные данные должен производиться по форме, установленной Приложением 2.

4.3. Не допускается: – хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;

– вынос съемных носителей с персональными данными из служебных помещений для работы с ними на дому и т.д.

4.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов имеющих гриф «ДСП» (для служебного пользования). Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения заведующего Учреждением.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся на них сведений немедленно ставится в известность заведующий Учреждением. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

4.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется соответствующей комиссией, состав которой утверждается приказом заведующего Учреждением. По результатам уничтожения носителей составляется акт по форме, установленной Приложением 3.

**Приложение 1**  
к порядку обеспечения конфиденциальности при  
обращении с информацией, содержащей персональные  
данные

Муниципальное бюджетное дошкольное образовательное учреждение детский сад №32 г. Азова  
Дело № \_\_\_\_\_

ЖУРНАЛ учета обращений субъектов персональных данных  
о выполнении их законных прав, при обработке персональных данных

начат \_\_\_\_\_

окончен \_\_\_\_\_

Хранить 50 лет

На \_\_\_\_\_ листах

№ п/п	Сведения о запрашивающем лице	Содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи /отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

**Приложение 2**  
к порядку обеспечения конфиденциальности при обращении  
с информацией, содержащей персональные данные

Муниципальное бюджетное дошкольное образовательное учреждение детский сад №32 г. Азова  
Дело № \_\_\_\_\_

ЖУРНАЛ учета приема и передачи ключевого носителя (ЭЦП)

начат \_\_\_\_\_ окончен \_\_\_\_\_ Хранить 5 лет

На \_\_\_\_\_ листах

№ п/п	Тип носителя ЭЦП Идентификатор ЭЦП	Дата и время передачи носителя	ФИО лица, принявшего носитель	Подпись ответственного лица	Примечание	Должность и ФИО ответственного за хранение Подпись
1	2	3	4	5	6	7

\* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

**Приложение 3**  
к порядку обеспечения конфиденциальности при обращении  
с информацией, содержащей персональные данные

АКТ уничтожения съемных носителей персональных данных

Комиссия, образованная приказом заведующего от «\_\_\_» \_\_\_\_\_ 20\_\_\_ г. № \_\_\_\_\_,  
в составе: председателя - \_\_\_\_\_ ФИО, должность  
членов - \_\_\_\_\_

\_\_\_\_\_ ФИО, должности  
провела отбор съемных носителей персональных данных, не подлежащих дальнейшему  
хранению:

№ п/п \_\_\_\_\_

Дата \_\_\_\_\_

Учетный номер съемного носителя Пояснения \_\_\_\_\_

Всего съемных носителей \_\_\_\_\_  
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на  
устройстве гарантированного уничтожения информации (механического уничтожения, сжигания  
и т.п.). Перечисленные съемные носители уничтожены путем

\_\_\_\_\_ (разрезания, демонтажа и т.п.),

\_\_\_\_\_ измельчены и сданы для уничтожения предприятию по утилизации вторичного  
сырья \_\_\_\_\_

(Наименование предприятия по утилизации )

Дата \_\_\_\_\_

Председатель комиссии \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_  
Подпись Фамилия И.О. Дата

Члены комиссии \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_  
Подпись Фамилия И.О. Дата

\_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_  
Подпись Фамилия И.О. Дата

\_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_  
Подпись Фамилия И.О. Дата

### Приложение 3

#### Согласие на обработку персональных данных работника

Я, \_\_\_\_\_  
проживающий по адресу: \_\_\_\_\_,  
паспорт серии \_\_\_\_\_, № \_\_\_\_\_, выданный «\_\_\_» \_\_\_\_\_ года,  
выдан \_\_\_\_\_

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю  
свое согласие муниципальному бюджетному дошкольному образовательному учреждению  
детскому саду № 32 г. Азова на обработку персональных данных (включая получение от меня  
и/или от любых третьих лиц, с учетом требований действующего законодательства РФ, моих  
персональных данных) и подтверждаю, что, давая такое согласие, я действую по своей воле и в  
своих интересах.

Даю свое согласие на обработку следующих персональных данных:

фамилия, имя, отчество, дата рождения, пол, реквизиты документа удостоверяющего  
личность, уровень образования и реквизиты документа об образовании, гражданство, место  
рождения, адрес регистрации, контактные телефоны, сведения о языках, изучаемых в школе,  
специальность; ИНН, номер пенсионного удостоверения, приказы связанные с  
профессиональной деятельностью, номер банковского счета для перечисления финансовых  
средств, наличие и уровень льгот, отношение к воинской обязанности, реквизиты документа о  
воинской обязанности, реквизиты диплома, иные сведения, содержащиеся в «личном деле» в  
кадровой службе.

Настоящее согласие дается до истечения сроков хранения соответствующей информации  
или документов, содержащих вышеуказанную информацию, определяемых в соответствии с

законодательством РФ, после чего может быть отозвано путем направления мною соответствующего письменного заявления не менее чем за 2 (два) месяца до момента отзыва согласия.

Настоящее согласие предоставляется на осуществление работодателем любых действий в отношении моих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокирование, уничтожение Персональных данных.

« \_\_\_\_ » \_\_\_\_\_ года

\_\_\_\_\_ (подпись представителя)

\_\_\_\_\_ (расшифровка подписи)

#### Приложение 4

Заведующему МБДОУ №32 г. Азова  
Волосных С.В.

от \_\_\_\_\_

паспорт: серия \_\_\_\_\_ № \_\_\_\_\_

выдан \_\_\_\_\_

дата выдачи: \_\_\_\_\_

код подразделения: \_\_\_\_\_

зарегистрированной по адресу: \_\_\_\_\_

### Согласие на обработку персональных данных воспитанников

Я, \_\_\_\_\_, даю согласие на сбор, систематизацию, накопление, хранение, уточнение, использование, обезличивание, блокирование, уничтожение и передачу моих персональных данных и персональных данных

\_\_\_\_\_ (Фамилия Имя Отчество полностью ребенка)

родителем (законным представителем) которого я являюсь в органы местного самоуправления, а также организации, участвующие в процессе предоставления муниципальной услуги, третьими лицами, заключившим договоры (соглашения) о едином информационном пространстве, а также производить обмен персональными данными, содержащимися в настоящем заявлении о документах, прилагаемых к нему, а именно совершение действий, предусмотренных статьями 6, 9 и 10 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных». Подтверждаю, что, давая такое согласие я действую по своей воле и в своем интересе. Настоящее согласие может быть отозвано в письменной форме.

\_\_\_\_\_ (дата)

\_\_\_\_\_ (подпись)

\_\_\_\_\_ (расшифровка подписи)

#### Приложение 5

Должностная инструкция  
ответственного за организацию обработки и обеспечения безопасности персональных данных

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая должностная инструкция определяет обязанности, права и ответственность ответственного за обработку персональных данных.

1.2. Решение о назначении на должность и об освобождении от должности принимается заведующим.

1.3. На должность ответственного за обработку персональных данных назначается лицо, имеющее высшее профессиональное образование и стаж работы в области обработки персональных данных не менее трех лет.

1.4. Ответственный за обработку персональных данных в своей деятельности руководствуется:

- действующими нормативными документами по вопросам выполняемой работы;
- уставом организации, локальными нормативными актами организации;
- настоящей должностной инструкцией.

1.5. Ответственный за обработку персональных данных должен знать:

- руководящие материалы по организации труда и управления производством;
- трудовое законодательство;
- документы, определяющие политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- методы применения правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- меры осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных;
- порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим федеральным законом;
- алгоритм ознакомления работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;
- организацию труда и управления;
- методы учета кадров;
- порядок разработки нормативных материалов для защиты персональных данных;
- передовой отечественный и зарубежный опыт в области обработки персональных данных.

1.6. Ответственный за обработку персональных данных подчиняется заведующему.

1.7. На время отсутствия ответственного за обработку персональных данных (отпуск, болезнь и пр.) его обязанности исполняет лицо, назначенное в установленном порядке.

## 2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Ответственный за обработку персональных данных обязан:

2.1. Организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

2.2. Организовывать и осуществлять внутренний контроль за соблюдением уполномоченными на обработку персональных данных требований законодательства РФ в области персональных данных, в том числе требований к защите персональных данных.

2.3. Организовывать доведение до сведения уполномоченных на обработку персональных данных положений законодательства РФ в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.4. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов.



- 2.5. В случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.
- 2.6. Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных.
- 2.7. Доводить до сведения работников оператора положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.
- 2.8. Блокировать неправомерно обрабатываемые персональные данные, прекращать обработку персональных данных в соответствии с законодательством РФ.
- 2.9. Уведомлять субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных.
- 2.10. Проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства РФ о персональных данных, соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством РФ в области обработки и защиты персональных данных.
- 2.11. Участвовать в рассмотрении проектов решений по вопросам своей компетенции.

### 3. ПРАВА

Ответственный за обработку персональных данных имеет право:

- 3.1. Знакомиться с проектами решений руководства организации, касающимися его деятельности.
- 3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией.
- 3.3. Получать от руководителя, специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей.
- 3.4. Требовать от заведующего учреждения оказания содействия в исполнении своих должностных обязанностей и прав.

### 4. ОТВЕТСТВЕННОСТЬ

Ответственный за обработку персональных данных несет ответственность:

- 4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, – в пределах, определенных действующим трудовым законодательством РФ.
- 4.2. За нарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством РФ.
- 4.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством РФ.

### 5. ПОРЯДОК ПЕРЕСМОТРА ДОЛЖНОСТНОЙ ИНСТРУКЦИИ

- 5.1. Должностная инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в пять лет.
- 5.2. С приказом о внесении изменений (дополнений) в должностную инструкцию знакомятся под подпись все работники организации, на которых распространяется действие этой инструкции.

**ДОКУМЕНТ ПОДПИСАН  
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

**СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП**

Сертификат 603332450510203670830559428146817986133868575787

Владелец Волосных Светлана Владимировна

Действителен с 15.03.2022 по 15.03.2023