

Муниципальное бюджетное дошкольное образовательное учреждение  
Детский сад № 34 «Лукоморье»

ПРИКАЗ

От 05.02.2025г.

№ 20

**О назначении ответственных за  
организацию работы по выполнению  
требований, предусмотренных  
Федеральным законом от 27 июля 2006 года  
№ 152 «О персональных данных»**

В соответствии с Трудовым кодексом Российской Федерации, Федеральными законами от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями от 31.07.2023г., от 27.07.2006г. № 152-ФЗ «О персональных данных» с изменениями от 06.02.2023г., Федеральным законом №273-ФЗ от 29.12.2012г. «Об образовании в Российской Федерации» с изменениями от 04.08.2023г., Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022г. № 179 «Об утверждении требований к подтверждению уничтожения персональных данных»,

**ПРИКАЗЫВАЮ:**

1. За организацию и внедрение мероприятий по выполнению требований Федерального закона «О персональных данных» (ч.1 ст.22), за обработку и обеспечение безопасности персональных данных при их обработке с применением средств автоматизации и бумажных носителей, назначить ответственным лицом ведущего документоведа Муниципального бюджетного дошкольного образовательного учреждения Детский сад № 34 «Лукоморье» Дерюшеву Людмилу Ольбертовну.
2. Организовать Дерюшевой Л.О. мероприятия по сбору, хранению и обработке персональных данных в соответствии с требованиями законодательства РФ.
3. Доводить до сведения работников МБДОУ Д/с № 34 «Лукоморье» нормативно-правовые акты по вопросам обработки персональных данных, требований к защите персональных данных.
4. В случае отсутствия Дерюшевой Л.О. по уважительным причинам (больничный лист, отпуск и проч.) замещающей её назначить документоведа Аношкину Светлану Григорьевну.
5. Ознакомить Дерюшеву Л.О. и Аношкину С.Г. с должностной инструкцией ответственного за обработку персональных данных под роспись. (Приложение 1).




6. Ознакомить Дерюшеву Л.О. и Аношкину С.Г. с Памяткой пользователю по информационной безопасности (Приложение 2).
7. Администратору официального сайта МБДОУ Д/с № 34 «Лукоморье» Голдобиной Марие Владимировне проверить сайт на соответствие норм законодательства:
  - правовые основания сбора данных (ч.1 ст. 6 Закона № 152-ФЗ);
  - правовые основания распространения ПД (ст. 10.1 Закона № 152-ФЗ);
  - правовые основания трансграничной передачи ПД (ст. 12 Закона № 152-ФЗ);
  - размещение политики (ч.2 ст. 18.1 Закона № 152-ФЗ);
  - локализация баз данных (ч.5 ст. 18 Закона № 152-ФЗ).
8. В своей работе при обработке персональных данных руководствоваться Положением об обработке персональных данных работников МБДОУ Д/с № 34 «Лукоморье», утверждённого приказом заведующего № 1 от 09.01.2024г.
9. Контроль за исполнением данного приказа возлагаю на себя.

Заведующий:



В.В.Неустроева

С приказом ознакомлены:

	Дерюшева Л.О. « 05 » 02 2025г.
	Аношкина С.Г. « 05 » 02 2025г.
	Голдобина М.В. « 05 » 02 2025г.

**Должностная инструкция  
ответственного за организацию обработки персональных данных в  
Муниципальном бюджетном дошкольном образовательном учреждении  
Детский сад № 34 «Лукоморье»**

**1. Общие положения**

1.1. Нормативной базой, регламентирующей положения настоящей Инструкции, является статья 24 Конституции Российской Федерации, глава 14 Трудового кодекса Российской Федерации, статья 137 Уголовного кодекса Российской Федерации.

1.2. К персональным данным, гражданина, работника относятся:

1.2.1. сведения об образовании;

1.2.2. сведения о предыдущем месте работы, опыте работы и занимаемой должности;

1.2.3. сведения о составе семьи и наличии иждивенцев;

1.2.4. сведения о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законом);

1.2.5. сведения об отношении к воинской обязанности;

**2. Порядок обработки персональных данных работника**

2.1. При обработке персональных данных гражданина, работника, то есть их получении, хранении, комбинировании, передаче или любом другом использовании персональных данных работника, специалисты по обработке персональных данных обязаны соблюдать следующие общие требования:

2.1.1. Обрабатывать персональные данные гражданина, работника может исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия гражданам, работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности граждан, работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2.1.2. Все персональные данные гражданина, работника следует получать у него самого. Если персональные данные гражданина, работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;

2.1.3. Специалист по обработке персональных данных не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев непосредственно связанных с вопросами трудовых

отношений с письменного согласия работника, а также случаев предусмотренных федеральным законом;

2.1.4. Персональную ответственность за соблюдение настоящей Инструкции, а также контроль за её соблюдением возложен всех специалистов по обработке персональных данных.

2.1.5. Все специалисты по обработке персональных данных должны быть ознакомлены с настоящей Инструкцией под расписку.

### **3. Хранение персональных данных работников**

3.1. Хранение документов, содержащих персональные данные гражданина, работник осуществляет в несгораемых шкафах (сейфах), ключи от которых находятся у специалистов по обработке персональных данных, а в его отсутствие у лица его замещающего.

### **4. Передача персональных данных работника**

4.1. При передаче персональных данных гражданина, работника специалист по обработке персональных данных должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные гражданина, работника третьей стороне без письменного согласия гражданина, работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина, работника, а также в случаях, установленных федеральным законом, а также не сообщать соответствующие сведения в коммерческих целях без письменного согласия гражданина, работника;

4.1.2. При передаче персональных данных работников предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

4.1.3. Специалисту по обработке персональных данных разрешается доступ только к тем персональным данным граждан, работников, которые необходимы для выполнения им его должностных обязанностей;

4.1.4. Специалист по обработке персональных данных не имеет права запрашивать информацию о состоянии здоровья гражданина, работника, за исключением тех сведений, которые предусмотрены федеральным законодательством.

### **5. Ответственность**

5.1. Лица, виновные в нарушении норм, регулирующих получение, обработку персональных данных гражданина, работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

С инструкцией ознакомлен:

Вруцкий Александр  
должность

Документовед  
должность

А  
подпись

А  
подпись

Александр С. С.  
расшифровка подписи

Александр С. С.  
расшифровка подписи

## Памятка о неразглашении персональных данных

1. Не допускать обработку персональных данных граждан без получения Согласия на обработку персональных данных за исключением случаев, установленных законодательством Российской Федерации, когда такое согласие не требуется.
2. Специалист обязан соблюдать конфиденциальность персональных данных, обеспечивать сохранность персональных данных при их обработке. Обращаться только те персональные данные, к которым получен доступ в силу исполнения должностных обязанностей.
3. Запрещается использовать сведения, содержащие персональные данные, в неслужебных целях. Запрещается снимать копии с документов и других носителей информации, содержащих персональные данные, без служебной необходимости.
4. В случае публикации в сети Интернет персональных данных гражданина необходимо брать отдельное Согласие на обработку персональных данных, разрешенных для распространения.
5. Не пересылать персональные данные по незащищенным каналам связи в открытом виде (электронной почте, мессенджерам).
6. Не выкладывать персональные данные в облачные сервисы (Яндекс Диск, Облако Mail.ru, Google Диск и др.)
7. Не создавать формы анкет (опросов), где могут обрабатываться персональные данные в сети Интернет с помощью Яндекс Форм, Google Форм и иные.
8. Передавать персональные данные на бумажном носителе в запечатанном конверте, исключающем несанкционированный просмотр сведений посторонними лицами, из рук в руки. Персональные данные в электронном виде передавать только на учетных съемных машинных носителях информации.
9. Исключать несанкционированный доступ посторонних лиц в помещения, где обрабатываются и хранятся персональные данные. В случае ухода ответственных сотрудников помещения должны закрываться на ключ.
10. Не оставлять без присмотра документы, содержащие персональные данные на столе в рабочее время, по окончании рабочего дня убирать их в надежно запираемые на ключ хранилища (тумбочки, шкафы).
11. При обработке персональных данных в составе информационной системы мониторы рабочих станций должны быть повернуты задней стороной к дверям и окнам, либо должны использоваться шторы, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.
12. Лицо, получившее доступ к персональным данным, обязано не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта.
13. При достижении цели обработки персональных данных или истечения сроков хранения персональных данных необходимо уничтожить путем измельчения бумагорезательных машин (шредера).

# Памятка пользователю по информационной безопасности

## Ответственность

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Ответственность за нарушения законодательства в области персональных данных установлена ст. 13.11 Кодекса Российской Федерации об административных правонарушениях.

За обработку персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработку персональных данных, несовместимую с целями сбора персональных данных предусмотрен:

на граждан административный штраф в размере от двух тысяч до шести тысяч рублей;

на должностных лиц - от десяти тысяч до двадцати тысяч рублей;

на юридических лиц - от шестидесяти тысяч до ста тысяч рублей.

Важно:

**не допускать использование персональных данных, к которым у пользователя информационной системы имеется доступ, в личных и иных не связанных с целями обработки целях;**

**не совершать действий, которые приведут к передаче персональных третьим лицам или доступу к таким сведениям со стороны третьих лиц.**

За утечку персональных данных (с 30.05.2025) предусмотрены следующие административные составы:

Нарушение	Физлица	Должностные лица	Компании
Утечка персданных 1 000 — 10 000 чел.	Первичное — 100 — 200 тыс. руб. Повторное — 400 — 600 тыс. руб.	Первичное — 200 — 400 тыс. руб. Повторное — 800 тыс. руб. — 1,2 млн руб.	Первичное — 3 — 5 млн руб. Повторное — от 1% до 3% совокупного размера годовой выручки

Утечка персданных 10 000 — 100 000 чел.	Первичное — 200 — 300 тыс. руб. Повторное — 400 — 600 тыс. руб.	Первичное — 300 — 500 тыс. руб. Повторное — 800 тыс. руб. — 1,2 млн руб.	Первичное — 5 — 10 млн руб. Повторное — от 1% до 3% совокупного размера годовой выручки
Утечка персданных более 100 000 чел.	Первичное — 300 — 400 тыс. руб. Повторное — 400 — 600 тыс. руб.	Первичное — 400 — 600 тыс. руб. Повторное — 800 тыс. руб. — 1,2 млн руб.	Первичное — 10 — 15 млн руб.
Утечка персданных спецкатегорий	Первичное — 300 — 400 тыс. руб. Повторное — 500 — 800 тыс. руб.	Первичное — 1 — 1,4 млн руб. Повторное — 1 — 2 млн руб.	Повторное — от 1% до 3% совокупного размера годовой выручки
Утечка биометрических персданных	Первичное — 400 — 500 тыс. руб. Повторное — 500 — 800 тыс. руб.	Первичное — 1,3 — 1,5 млн руб. Повторное — 1 — 2 млн руб.	Первичное — 15 — 20 млн руб. Повторное — от 1% до 3% совокупного размера годовой выручки

## Парольная защита

- Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам и не храните записанный пароль в общедоступных местах.
- Не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним.
- Не используйте пароль доступа в локальную сеть, систему электронного документооборота Управления в других программах и на сайтах, где требуется регистрация;
  - Смена паролей осуществляется не реже одного раза в 30 дней. Критерии сложности паролей пользователей определены администратором безопасности и должны соответствовать парольной политике. Использовать «стойкие» пароли от 7 символов, с использованием букв различного регистра и цифр, не использовать в качестве ответов на контрольные вопросы (и в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию; не сохранять пароли в формах веб-страниц.

## Антивирусная защита

- Своевременно обновлять и не отключать антивирусное программное обеспечение.
- Обязательно проверяйте на наличие вирусов все внешние носители информации (дискеты, диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений и т.п.)
- Во всех случаях возможного проявления действий вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно. Незамедлительно сообщите ответственному за антивирусный контроль и оцените с ним возможные пути заражения и распространения данного вируса.

## Интернет и электронная почта

- Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.
- Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.
- Не передавайте по электронной почте Ваши пароли.
- Соблюдайте режим конфиденциальности персональных данных.
- Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете.
- Если электронный адрес отправителя вам не знаком или выглядит «странно», не открывать прикрепленные файлы.

## Прочее

- Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение;
- Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.
- При временном оставлении рабочего места в течение рабочего дня в обязательном порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».



## Правила работы с персональными данными

**Персональные данные** - любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (далее - субъект персональных данных).

Контактные данные и реквизиты юридического лица, а также иные сведения, по которым можно его определить, не подпадают под понятие персональных данных.

**К персональным данным относятся сведения:**

- Фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных.
- Различные **идентификаторы** личности (номер паспорта, СНИЛС, ИНН, номер водительского удостоверения, реквизиты банковской карты, IP-адрес, адрес электронной почты, номер телефона) и т.д.

**Оператором персональных данных** является любое лицо, которое их обрабатывает или совершает с ними любые другие действия. К ним относятся:

1. физические лица;
2. индивидуальные предприниматели;
3. организации, как коммерческие, так и некоммерческие;
4. органы власти – государственной или муниципальной – в лице соответствующих учреждений и должностных лиц.

Обработку персональных данных оператором требуется производить с соблюдением ряда **обязательных правил:**

1. Производить обработку персональных данных в строгом соответствии с требованиями действующего законодательства.
2. Перед началом обработки персональных данных необходимо уведомить об этом органы Роскомнадзора (за исключением отдельных случаев) (ч. 1 ст. 22 Закона о персональных данных).
3. Персональные данные обрабатываются исключительно с согласия субъекта персональных данных. Согласие в установленных законодательством случаях требуется получить в письменной форме со включением в документы ряда обязательных положений (например, ФИО, реквизиты документа, удостоверяющего личность субъекта персональных данных, цель, с которой персональные данные обрабатываются, перечень обрабатываемых персональных данных, срок выдачи согласия, способы отзыва).
4. Сбор и обработка персональных данных производятся со строго определенной целью, что должно определять объем обрабатываемых персональных данных. Запрещается обрабатывать персональные данные без определенной цели либо те персональные данные, которые не требуются для достижения обозначенной цели.
5. Следить за актуальностью персональных данных, при их изменении вносить в процессе обработки необходимые сведения.

6. Поручение оператором обрабатывать персональные данные иным лицам допускается в случае, если такое право установлено законом или договором.

7. Соблюдать конфиденциальность при работе с персональными данными. Не допускать их передачу третьим лицам без согласия субъекта персональных данных. Исключение составляют случаи, предусмотренные законом.

8. При необходимости необходимо производить обезличивание персональных данных.

9. Обеспечить при работе с персональными данными их безопасность, исключаящую несанкционированный доступ к ним третьих лиц.

10. Назначить ответственных лиц, отвечающих за обработку, хранение и защиты персональных данных в организации.

11. Разработать и утвердить локальные нормативные акты (далее – ЛНА), которыми регулируются вопросы обработки персональных данных (положения, политика, правила и т.п.). Ознакомить с указанными ЛНА сотрудников, которые обрабатывают персональные данные. Провести обучение сотрудников по работе с персональными данными, регулярно проводить переобучение, доводя до сотрудников изменения, происходящие в законодательстве, регулирующем работу с персональными данными.

12. Своевременно выявлять и устранять нарушения, допускаемые в процессе работы с персональными данными.