

# Порядок обработки и обеспечения безопасности персональных данных в ООО «Д-СЛУХ»

## 1. Общие положения.

1. Целью «Порядка о порядке обработки и обеспечения безопасности персональных данных в ООО «Д-СЛУХ»» (далее – Порядок) определяет процессы обработки персональных данных, осуществляемые в ООО «Д-СЛУХ» (далее – Компания) включая:
  - цели обработки персональных данных;
  - объёмы обрабатываемых персональных данных
  - субъекты, персональные данные которых обрабатываются
  - виды обрабатываемых персональных данных;
  - основания обработки персональных данных;
  - лица, осуществляющие обработку ПДн.
2. Настоящий Порядок описывает мероприятия, выполняемые Компанией в целях:
  - соблюдения требований законодательства Российской Федерации в области обработки и защиты персональных данных, а также органов власти, имеющих отношение к регулированию области обработки и защиты персональных данных, Роскомнадзор, ФСБ России, ФСТЭК России;
  - обеспечения безопасности обрабатываемых персональных данных;
  - соблюдения законных прав субъектов персональных данных.
3. Порядок разработан с учётом законодательных актов, приведённых в разделе «Нормативные ссылки».

## 2. Термины и определения.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу (субъекту ПДн);

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

**Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

**Информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;

**Работник, ответственный за обеспечение безопасности ПДн** – работник, назначаемый приказом Генерального директора Компании и несущий ответственность за выполнение процедур, связанных с обеспечением безопасности обрабатываемых ПДн.

### 3. Принятые сокращения.

**ПДн** – персональные данные;

**ИСПДн** – информационная система персональных данных;

**ИБ** – информационная безопасность;

**152-ФЗ** – Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

**ФСБ** – Федеральная служба безопасности;

**ФСТЭК** – Федеральная служба по техническому и экспортному контролю;

**Роскомнадзор** – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

**КоАП РФ** – Кодекс Российской Федерации об административных нарушениях;

**УК РФ** – Уголовный кодекс Российской Федерации;

### 4. Нормативные ссылки.

При разработке настоящего Порядка использованы следующие законодательные акты:

1. Федеральный закон от 27 июля 2006 года и № 152-ФЗ «О персональных данных» (с допол-нениями и изменениями);
2. Постановление Правительства от 01 ноября 2012 года РФ №1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
3. Постановление Правительства от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»;
4. Постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
5. «Кодекс РФ об административных правонарушениях» от 30 декабря 2001 г. № 195-ФЗ (с изменениями и дополнениями);
6. «Уголовный кодекс РФ» от 13 июня 1996 г. № 63-ФЗ (с изменениями и дополнениями).

### 5. Основные правила.

1. Компания является оператором ПДн.
2. Обработка ПДн в Компании осуществляется, как с использованием средств автоматизации, так и без их применения.
3. Виды обрабатываемых ПДн, субъекты, которым принадлежат обрабатываемые ПДн, а также цели обработки ПДн, приведены в Приложении 1 к настоящему Порядку.
4. При обработке ПДн Компания руководствуется принципами:
  - обеспечения законности целей и способов обработки ПДн;
  - соответствия целей обработки ПДн целям, заранее определённым и заявленным при сборе ПДн;
  - соответствия объема и характера обрабатываемых ПДн, а также способов обработки ПДн целям обработки ПДн;
  - отсутствия избыточных ПДн по отношению к заявленным при сборе ПДн целям;

- использования отдельных баз данных ИСПДн для несовместных целей обработки ПДн.
5. Компания не осуществляет обработку специальных категорий ПДн.
  6. Компания не осуществляет обработку биометрических ПДн.
  7. Компания осуществляет трансграничную передачу ПДн

## 6. Основания обработки ПДн.

1. Компания осуществляет обработку ПДн на основании:
  - требований Федеральных законов, в которых установлена цель обработки ПДн, условия получения ПДн и круг субъектов, ПДн которых подлежат обработке, а также определены полномочия оператора;
  - согласия субъекта на обработку его ПДн (в роли субъекта ПДн выступают клиенты Компании).
2. Полный перечень целей и оснований обработки ПДн приведены в Приложении 2 к настоящему Порядку.
3. Доказательством получения согласия субъекта ПДн на обработку его данных являются согласие субъекта на обработку его ПДн, представленное в форме, предусмотренной действующим законодательством.

## 7. Порядок обработки персональных данных.

1. Обработка персональных данных в Компании должна осуществляться с учетом следующих требований:
  - Обработка персональных данных субъекта ПДн должна осуществляться с соблюдением требований Федерального закона 152-ФЗ «О защите персональных данных», а также требований постановления Правительства от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и иных нормативных правовых актов.
  - При определении объема и содержания обрабатываемых персональных данных субъекта ПДн Компания обязана руководствоваться Конституцией Российской Федерации и иными Федеральными законами.
  - Персональные данные следует получать у самого субъекта ПДн. Если персональные данные субъекта ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Компания должна сообщить субъекту ПДн о целях обработки ПДн, о правовом основании, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение. Компания освобождается от обязанности предоставлять субъекту ПДн перечисленные сведения, в случаях, если субъект ПДн уведомлен об осуществлении обработки его персональных данных Компанией, персональные данные получены Компанией на основании Федерального закона или в связи с исполнением договора, стороной которого является субъект ПДн, персональные данные являются общедоступными или получены из общедоступного источника.
  - Компания не имеет права получать и обрабатывать персональные данные субъекта ПДн о его политических, религиозных, иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами договорных отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны Компанией только с его письменного согласия.
  - Компания не имеет право получать и обрабатывать персональные данные субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Федеральным законом.
  - Компания не имеет право запрашивать информацию о состоянии здоровья субъекта ПДн, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.
2. Работники структурных подразделений Компании, указанных в Приложении 3 к настоящему Порядку, осуществляют обработку персональных данных субъектов ПДн в объемах и целях, предусмотренных законодательством Российской Федерации и нормативными документами Компании, а также

обеспечивают их защиту от неправомерного использования, утраты и несанкционированного уничтожения.

3. При принятии решений, затрагивающих интересы субъекта ПДн, Компания не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронного получения, в том числе на цифровых носителях, кроме согласия субъекта ПДн в письменной форме.
4. Защита персональных данных субъектов ПДн от неправомерного их использования или утраты обеспечивается Компанией за счёт собственных средств и в порядке, установленном действующим законодательством РФ в области защиты персональных данных.
5. При обработке персональных данных принимаются организационные и технические меры по обеспечению их конфиденциальности в соответствии с действующим законодательством РФ в области защиты персональных данных.
6. Персональные данные хранятся:
  - в электронном виде (на серверах, входящих в состав ИСПДн) с соблюдением всех требований по их конфиденциальности (информационной безопасности);
  - на бумажных носителях, в запираемых шкафах и несгораемых сейфах соответствующих подразделений Компании с соблюдением их конфиденциальности.

## **8. Передача персональных данных Субъектов ПДн третьим лицам.**

1. Компания вправе поручить обработку персональных данных третьему лицу с согласия субъекта персональных данных, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Компании, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные действующим законодательством РФ в области защиты персональных данных.
2. При передаче персональных данных субъекта ПДн Компания обязана соблюдать следующие требования:
  - не сообщать персональные данные субъектов ПДн третьей стороне без согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными Федеральными законами;
  - предупредить лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъектов ПДн, обязаны соблюдать режим секретности (конфиденциальности).
3. предупредить лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъектов ПДн, обязаны соблюдать режим секретности (конфиденциальности).
4. Компания несёт ответственность перед субъектом ПДн за действия третьего лица, осуществляющего обработку ПДн по поручению Компании. В свою очередь, указанное третье лицо несёт ответственность перед Компанией.

## **9. Организация доступа к персональным данным.**

1. Защита персональных данных в Компании предусматривает ограничение к ним доступа.
2. Доступ к персональным данным разрешается только работникам структурных подразделений Компании, указанным в Приложении 3 к настоящему Порядку. При этом указанные лица имеют право получать только те ПДн, которые необходимы для выполнения конкретных функций, и в целях, для которых они сообщены.
3. Доступ представителей государственных органов к ПДн регламентируется действующим законодательством Российской Федерации.

## **10. Обязанности лиц, допущенных к обработке персональных данных.**

1. Лица, допущенные к работе с персональными данными, обязаны:
  - соблюдать требования по защите ПДн установленные в Компании;
  - обеспечивать сохранность закреплённого массива носителей с персональными данными, исключать возможность ознакомления с ними третьих лиц;
2. Порядок хранения персональных данных определяются внутренними нормативными документами Компании.

## **11. Соблюдение прав субъектов персональных данных.**

1. Субъект ПДн вправе требовать от Компании уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
2. В случае соответствующего обращения субъекта ПДн Компания:
  - осуществляет идентификацию субъекта ПДн;
  - устанавливает факт обработки персональных данных субъекта ПДн;
  - предоставляет субъекту ПДн возможность ознакомления с полной информацией о его персональных данных, обрабатываемых в Компании;
  - вносит изменения, уничтожает или блокирует ПДн субъекта при предоставлении им сведений, подтверждающих, что обрабатываемые ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного Федерального закона;
  - извещает всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн обо всех произведённых в них исключениях, исправлениях или дополнениях;
  - уведомляет субъекта ПДн о результатах запрашиваемых субъектом действий.

## **12. Защита персональных данных.**

1. Компания обеспечивает конфиденциальность ПДн при их обработке.

## **13. Контроль и надзор за обработкой персональных данных.**

1. Порядок взаимодействия Компании с органами, уполномоченными осуществлять контроль и надзор за обработкой персональных данных, определен внутренними нормативными документами Компании.

## **14. Ответственность.**

1. Компания несёт ответственность:
  - за нарушение требований законодательства РФ по обработке и защите ПДн;
  - за нарушение конфиденциальности обрабатываемых ПДн;
  - за нарушение требований регулирующих организаций по обработке и защите ПДн.
2. Работник Компании, в соответствии со своими полномочиями владеющий информацией о клиентах Компании, получающий и использующий её, несет ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
3. Работник Компании, получающий для работы конфиденциальный документ, несёт ответственность за сохранность носителя и конфиденциальность полученной информации.
4. Работник, виновный в нарушении норм, регулирующих получение, обработку и защиту персональных данных, может быть привлечен к ответственности.

## ПЕРЕЧЕНЬ обрабатываемых персональных данных

Субъект	Обрабатываемые ПДн	Источник получения	Цель обработки(порядковый номер по «Перечню целей обработки пер
Клиент			
	<ol style="list-style-type: none"> <li>1. Фамилия, Имя; Отчество</li> <li>2. Дата рождения;</li> <li>3. Адресные данные;</li> <li>4. Информация о заказах;</li> <li>5. Адрес электронной почты;</li> <li>6. Контактный телефон.</li> <li>7. Паспортные данные (серия, номер, кем и когда выдан)</li> </ol>	Субъект ПДн;	1

## ПЕРЕЧЕНЬ целей обработки персональных данных в ООО «Д-СЛУХ»

№ п/п	Цели обработки
1	<ol style="list-style-type: none"> <li>1. Информирование клиентов Компании о новых акциях;</li> <li>2. Заключение договора розничной купли-продажи;</li> <li>3. Анализ базы данных клиентов для маркетинговых целей;</li> </ol>

## ПЕРЕЧЕНЬ подразделений, допущенных к обработке ПДн

№ п/п	Структурное подразделение
1	<ol style="list-style-type: none"> <li>1. Бухгалтерия;</li> <li>2. Департамент УП;</li> </ol>
2	<ol style="list-style-type: none"> <li>1. Аналитическая группа;</li> <li>2. служба по работе с клиентами;</li> <li>3. Отдел маркетинга.</li> <li>4. Работники склада на участках формирования и отгрузки;</li> <li>5. Работники службы доставки;</li> <li>6. Отдел ассортимента.</li> </ol>
3	<ol style="list-style-type: none"> <li>1. Супервайзеры коллцентра;</li> <li>2. Операторы коллцентра;</li> <li>3. Руководители направлений.</li> </ol>