

«09» сентября 2015 г.

Сбор ПДн сотрудников происходит от самих субъектов, без письменного согласия, при трудоустройстве.

Сотрудник несет персональную ответственность за достоверность предоставленных данных и последующее доведение до сведения Учреждения изменений своих ПДн.

ПДн сотрудников обрабатываются с использованием средств автоматизации в ИСПДн и без использования средств автоматизации.

9. Обработка ПДн потребителей

Сбор ПДн потребителей происходит от представителей потребителей с письменного согласия.

ПДн потребителей обрабатываются с использованием средств автоматизации в ИСПДн и без использования средств автоматизации.

10. Обработка ПДн родителей

Сбор ПДн родителей происходит от самого субъекта с письменного согласия.

ПДн родителей обрабатываются с использованием средств автоматизации в ИСПДн и без использования средств автоматизации.

11. Обработка ПДн заявителей

Сбор ПДн заявителей происходит от самого субъекта с письменного согласия.

ПДн заявителей обрабатываются с использованием средств автоматизации в ИСПДн и без использования средств автоматизации.

12. Доступ к ПДн

Доступ к ПДн имеют только штатные сотрудники Учреждения, в соответствии с утвержденными списками.

Сотрудники Учреждения, имеющие доступ к ПДн наделены минимально необходимыми полномочиями для выполнения своих должностных обязанностей.

Каждый сотрудник Учреждения имеет право доступа к своим ПДн.

Физические лица, чьи ПДн обрабатываются в Учреждения, имеют право доступа к своим ПДн по запросу.

13. Передача ПДн

ПДн сотрудников Учреждения могут передаваться в: ФСС, УФНС, ПФР, отделение банка для начисления заработной платы.

ПДн потребителей периодически передаются в формате обезличенных отчетов в управление культуры и туризма администрации г.Владимира.

14. Основные нормы безопасности ПДн при распределении полномочий доступа

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

Каждый сотрудник Учреждения, имеющий отношение к ПДн, должен быть наделен минимальными полномочиями обработки ПДн, необходимыми для выполнения своих обязанностей.

Каждый сотрудник Учреждения, имеющий отношение к ПДн, обязан знать и выполнять установленные нормы безопасности ПДн.

15. Нормы безопасности при обработке ПДн

При обработке ПДн на бумажных носителях необходимо соблюдать следующие меры безопасности:

- бумажные носители, находящиеся в работе, не должны оставаться без присмотра сотрудника, работающего с ними;
- передача бумажных носителей между подразделениями Учреждения возможна только тем сотрудникам, которые имеют санкционированный доступ к ним, в соответствии со списками таких сотрудников;
- хранение бумажных носителей должно осуществляться в местах, не доступных посторонним лицам, а также сотрудникам Учреждения, не имеющим санкционированного доступа к ним;
- в отношении каждого вида бумажных носителей должны быть определены сроки хранения и методы уничтожения;
- при передаче бумажных носителей на долгосрочное хранение в архив, к ним применяются нормы безопасности, установленные владельцем архива.

При обработке ПДн в ИСПДн необходимо соблюдать следующие меры безопасности:

- каждый сотрудник Учреждения, обрабатывающий ПДн в ИСПДн, должен иметь свою учетную запись и пароль к ней;
- сотрудникам запрещается передавать пароли на учетные записи между собой и кому либо вообще;
- каждый сотрудник при обнаружении компрометации своего пароля должен незамедлительно сообщить об этом ответственному за организацию обработки ПДн, в части обеспечения внутреннего контроля за выполнением сотрудниками мер и правил обеспечения безопасности ПДн, ведение учета средств защиты информации, поддержание технической составляющей системы защиты ПДн;
- каждое автоматизированное рабочее место ИСПДн должно быть оснащено сертифицированными средствами защиты в программном или программно-аппаратном исполнении;
- защита ИСПДн должна быть комплексной и охватывать все возможные каналы утечки ПДн (угрозы техногенного характера, стихийные бедствия, несанкционированный доступ разного рода, воздействия из внешних сетей и т.д.);
- необходимо соблюдение организационных мероприятий при защите ИСПДн в целом и отдельных элементов. К организационным мероприятиям относятся: контроль со стороны сотрудников, работающих в ИСПДн, за нахождением в кабинете посторонних лиц, а также сотрудников не имеющих санкционированного доступа к ПДн, просмотр ПДн с экрана монитора, доступ к автоматизированному рабочему месту, работа с ПДн;
- при обработке критичных ПДн, необходима аттестация ИСПДн.

16. Нормы безопасности при передаче ПДн

Передача ПДн по телефону, факсу запрещена.

Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Учреждения и в том объеме, который позволяет не разглашать излишний объем персональных сведений о носителях ПДн.

Предоставление ПДн в другие организации без письменного запроса, или при превышении их компетенции, действий вне рамок законодательных актов, запрещено.

При передаче по открытым каналам связи (например, Интернет, в том числе и по электронной почте) должны использоваться сертифицированные криптографические средства защиты.

13. Сотрудники Учреждения, имеющие доступ к ПДн несут персональную ответственность за сохранение конфиденциальности, целостности вверенных им ПДн и исполнение настоящего Положения.

Лица, виновные в нарушении установленных норм, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательными актами.

Контроль за исполнением Положения осуществляет ответственный за организацию обработки ПДн.