Приложение № 1

к приказу от 10.01.2022 г. № 2 - од

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных в краевом государственном бюджетном учреждении «Ачинский психоневрологический интернат»

1.Общие положения

1.1. Положение по организации и проведению работ по обеспечению безопасности персональных данных в краевом государственном бюджетном учреждении социального обслуживания «Ачинский психоневрологический интернат» (далее - Положение) устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием и без использования средств автоматизации.

1.2. Настоящее Положение разработано в соответствии со ст.19 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. В Положении используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 N 152-ФЗ.

2.Обеспечению безопасности персональных данных

2.1 Основные условия обработки персональных данных

2.1.1. Обработка персональных данных осуществляется после получения согласия субъекта персональных данных, составленного по типовой форме.

2.1.2. Оператором организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных является краевое государственное бюджетное учреждение социального обслуживания «Ачинский психоневрологический интернат».

2.1.3. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения,

изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.1.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке с использованием средств автоматизации оператором назначается лицо, ответственное за обеспечение безопасности персональных данных.

2.1.5. Доступ к персональным данным имеют работники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей утвержденных приказом директора Учреждения.

2.1.6. Уполномоченные на обработку персональных данных работники Учреждения, в обязательном порядке под роспись знакомятся с локальными актами Учреждения по обработке и защите персональных данных и подписывают Соглашение о неразглашении персональных данных.

2.1.7. Оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Оператор или иное получившее доступ к персональным данным лицо обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

2.1.8. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условие договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

2.1.9. Ответственность за безопасность персональных данных возлагается на лиц, допущенных к их обработке.

2.2. Обеспечение безопасности перед началом обработки персональных данных

2.2.1. Перед началом обработки персональных данных необходимо изучить настоящую Инструкцию.

2.2.2. Перед началом обработки персональных данных необходимо убедиться в том, что:

- в помещении, в котором ведется работа с персональными данными, отсутствуют посторонние лица;
- носители персональных данных не повреждены;
- к персональным данным не был осуществлен несанкционированный доступ;
- персональные данные не повреждены;
- технические средства автоматизированной обработки и защиты персональных данных находятся в исправном состоянии.

2.3. Обеспечение безопасности во время обработки персональных данных

2.3.1. Во время обработки персональных данных необходимо обеспечить:

-недопущения воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование;

- недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;

- постоянный контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- недопущение несанкционированного доступа к персональным данным;

- конфиденциальность персональных данных.

2.4. Обеспечение безопасности в экстремальных ситуациях

2.4.1. При модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.

2.4.2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.

2.4.3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.

2.4.4. В случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести проверку и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

2.4.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора Учреждения и произвести проверку по возникшей ситуации.

2.5. Обеспечение безопасности при завершении обработки персональных данных

2.5.1. После завершения сеанса обработки персональных данных необходимо обеспечить:

- исключение возможности несанкционированного проникновения или нахождения в помещении, в котором размещены средства автоматизированной обработки и ведется работа с персональными данными;

- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;

- фиксацию всех случаев нарушения данной инструкции в журнале.

3. Порядок обработки персональных данных субъектов персональных данных, осуществляемой с использованием средств автоматизации, содержание персональных данных

3.1. Порядок обработки персональных данных с использованием средств автоматизации:

1. Обработка персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями действующего законодательства.

2. При эксплуатации автоматизированных систем необходимо соблюдать требования:

1) разработка и принятие локальных нормативных актов, регулирующих защиту персональных данных;

2) использованием лицензированных антивирусных программ, не допускающих несанкционированный вход в локальную сеть Учреждения;

3) к работе допускаются только лица, назначенные приказом директора Учреждения;

4) на ПЭВМ, дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, устанавливаются пароли;

5) на период обработки защищаемой информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации;

3.2. Обработка персональных данных в Учреждении осуществляется:

а) в системе бухгалтерского учета и отчетности «Wins», включающей:

фамилию, имя, отчество субъекта персональных данных;

дату рождения субъекта персональных данных;

место рождения субъекта персональных данных;

серию и номер основного документа, удостоверяющего личность субъекта персональных данных, дату выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

ИНН субъекта персональных данных;

табельный номер субъекта персональных данных;

должность субъекта персональных данных;

номер приказа и дату приема на работу (увольнения) субъекта персональных данных;

номер страхового свидетельства государственного пенсионного страхования субъекта персональных данных.

3.3. Обработанные персональные данные (работников учреждения), содержащиеся в бухгалтерской отчетности передаются в ПФР, ФНС по сети Интернет с использованием программы "СбиС+ Электронная отчетность". Вся передаваемая информация закрыта от несанкционированного доступа средствами криптографической защиты информации.

Содержание персональных данных передаваемых в:

а) Пенсионный фонд России, включает:

фамилию, имя, отчество субъекта персональных данных;

дату рождения субъекта персональных данных;

серию и номер основного документа, удостоверяющего личность субъекта персональных данных;

сведения о дате выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

ИНН субъекта персональных данных;

номер страхового свидетельства государственного пенсионного страхования субъекта персональных данных;

сведения о заработной плате, доходах.

б) ФНС № 4 по Красноярскому краю сведений по налогу на доходы физических лиц, включающей:

фамилию, имя, отчество субъекта персональных данных;

дату рождения субъекта персональных данных;

серию и номер основного документа, удостоверяющего личность субъекта персональных данных;

сведения о дате выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

ИНН субъекта персональных данных;

сведения о заработной плате, доходах.

3.4. Персональные данные могут быть представлены для ознакомления:

а) работникам, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;

б) уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

3.5. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

3.6. Уполномоченными на обработку персональных данных работниками Учреждения при обработке персональных данных с использованием средств автоматизации должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

3.7. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

3.8. Доступ пользователей к данным в информационных системах осуществляется с применением индивидуальных логинов и паролей.

3.9. Уполномоченными на обработку персональных данных работниками Учреждения, ответственными за обеспечение безопасности персональных данных при их обработке с использованием средств автоматизации, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства;

б) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) постоянный контроль за обеспечением уровня защищенности персональных данных;

д) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных до выявления причин нарушений и устранения этих причин;

з) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

3.10. В случае выявления нарушений порядка обработки персональных данных при автоматизированной обработке уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

4. Порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации

4.1. Фиксация персональных данных при неавтоматизированной обработке может осуществляться на бумажных и других материальных носителях (далее материальные носители).

4.2. Обработка персональных данных без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющим к ним доступ;
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целя;
- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

4.2. Обеспечение безопасности персональных данных при неавтоматизированной обработке:

- все документы (материальные носители) содержащие персональные данные, должны храниться в служебных помещениях в закрытых для визуального просмотра, запираемых сейфах, шкафах, столах. Ключи от сейфов, шкафов, столов хранятся лично у уполномоченных на обработку ПДн работников учреждения;

- помещение Учреждения в ночное время, выходные и праздничные дни охраняется физической охраной, кнопкой вызова вневедомственной охраны;

- в рабочее время, документы (материальные носители), содержащие ПДН, не должны находиться на столах работников дольше времени необходимого на их обработку, Во время обработки документы, содержащие ПДн, по возможности размещаются таким образом, чтобы с них отсутствовала возможность просмотра информации посторонними лицами;

- в отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные;

- при уходе в отпуск, во время служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные лицу, на которое приказом директора Учреждения будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому работнику, имеющему доступ к персональным данным по указанию директора Учреждения.

- в конце рабочего дня все документы, содержащие персональные данные, помещаются в шкафы, обеспечивающие защиту от несанкционированного доступа. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются путем разрывания, предотвращающего возможность их восстановления.

4.3. При использовании типовых форм документов, характер информации в 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, критерии субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

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 согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными, не имел возможности доступа к персональным данным иных лиц, содержащимся в указанной типовой форме;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.4. Уничтожение или обезличивание персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

4.5. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

4.6. Перечни персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а так же в связи с оказанием социальных услуг указаны в Положении об обработке и защите персональных данных получателей социальных услуг в краевом государственном бюджетном учреждении социального обслуживания «Ачинский психоневрологический интернат».

5. Заключительные положения

5.1. Проверка и пересмотр настоящего Положения осуществляются в следующих случаях:

- при пересмотре требований обеспечения безопасности персональных данных;
- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности персональных данных;
- по требованию уполномоченных органов, наделенных функциями контроля в области защиты персональных данных.

5.2. Обязанность за своевременную корректировку настоящего Положения возлагается на ответственного за организацию обработки персональных данных в Учреждении.