

**Положение по обеспечению безопасности персональных данных  
при их обработке в информационных системах персональных данных  
(далее- ИСПДн)**

**1. Общие положения**

1.1. Целью настоящего Положения является обеспечение безопасности объектов информационной системы оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.2. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.3. В Положении определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн оператора. Назначение ответственного за организацию обработки персональных данных.

1.4. Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с законодательством. Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

1.5. Государственное бюджетное учреждение «Центр социального обслуживания граждан пожилого возраста и инвалидов Вачского муниципального округа» (далее – Учреждение) обеспечивает неограниченный доступ к документу, определяющему его Положение в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных, путем размещения на официальном сайте.

**2. Основные понятия и правила обработки персональных данных:**

2.1. Для реализации Положения используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

3) 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;

4) 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;

5) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

8) 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;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационными технологиями и техническими средствами;

11) конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

12) субъект - гражданин Российской Федерации и иностранный гражданин, постоянно и временно проживающий на территории Нижегородской области, а также гражданин, состоящий в трудовых отношениях с оператором в соответствии с законодательством.

2.2. Обработка ПДн оператором осуществляется в соответствии с :

1. Федеральным законом Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных»;
2. Указом Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
3. Постановлением Правительства Российской Федерации от 21.03.2012 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»;
4. Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

#### 2.3 Область действий:

Требования настоящего Положения распространяются на всех сотрудников.

#### 2.4. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- перечня персональных данных, подлежащих защите;
- модели угроз безопасности персональных данных;
- разграничение прав доступа к обрабатываемым персональным данным;

#### 2.5. Цели обработки ПДн Учреждением:

- 1) ведение учета обратившихся граждан за предоставлением социальных услуг;
- 2) формирование системы учета и отчетности и иных информационных ресурсов в сфере социальной защиты населения в Российской Федерации;

#### 2.6. Категории ПДн, обрабатываемых в ИСПДН:

граждане Российской Федерации и иностранные граждане, постоянно и временно проживающие на территории Нижегородской области.

По критериям:

- фамилия, имя, отчество;
- место, год и дата рождения;
- адрес по прописке;
- паспортные данные (серия, номер паспорта, кем и когда выдан);-
- адрес проживания (реальный);
- телефонный номер (домашний, рабочий, мобильный);
- состав семьи (муж/жена, дети);
- данные о льготных документах;
- степень инвалидности;

2.7. Обработка ПДн осуществляется путем смешанной обработки ПДн с использованием информационной системы ПДн. Полученные в ходе обработки информации данные передаются:

- 1) по защищенным каналам связи или на внешних носителях информации для обмена информацией конфиденциального характера между управлениями и Министерством социальной политики Нижегородской области;
- 2) по каналам факсимильной связи для приема и передачи служебной информации;
- 3) по сети общего пользования «Интернет» только статистические и отчетные данные;

## 2.8. Сроки или условия прекращения обработки ПДн.

Основанием для прекращения обработки ПДн является: прекращение деятельности оператора, изменение действующего законодательства Российской Федерации, другие предусмотренные законодательством Российской Федерации и Нижегородской области основания.

### **3. Правила рассмотрения запросов субъектов ПДн или их представителей:**

3.1. Субъект ПДн имеет право на получение сведений, касающихся обработки его ПДн. Сведения предоставляются субъекту ПДн или его представителю Учреждения при обращении либо при получении запроса субъекта ПДн или его представителя. Субъект ПДн вправе требовать от Учреждения уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.2. Запрос, направленный в форме электронного документа должен быть подписан электронной подписью в соответствии с законодательством Российской Федерации. Запросы, не отвечающие указанным требованиям не подлежат обработке, в соответствии с федеральным законодательством.

3.3. Сведения должны быть предоставлены субъекту ПДн Учреждения в доступной форме. В них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

3.4. Субъект персональных данных вправе требовать от оператора 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.

3.5. Сведения, предоставляются субъекту персональных данных или его представителю оператором в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.6. Оператор предоставляет сведения, указанные в части 7 федерального закона №152-ФЗ субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

3.7. Субъект Пд в праве повторно обратиться к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 федерального закона №152-ФЗ, а также в целях ознакомления с обрабатываемыми Пд до истечения срока, указанного в части 4 федерального закона №152-ФЗ, в случае, если такие сведения и (или) обрабатываемые Пд не были предоставлены ему для ознакомления в полном объеме по результатам

рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 федерального закона №152-ФЗ, должен содержать обоснование направления повторного запроса.

3.7. Субъект персональных данных может отозвать согласие на обработку персональных данных путем направления письменного заявления на имя директора ГБУ «ЦСОГПВИИ Вачского муниципального округа»;

3.8. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

3.9. Субъект персональных данных может обратиться с жалобой в уполномоченный федеральный орган исполнительной власти по защите прав субъектов персональных данных или в суд в том случае, если полагает, что обработка его персональных данных осуществляется с нарушением требований законодательства или иным образом нарушает его права и свободы.

#### **4. Правила работы с обезличенными ПДн :**

Под обезличиванием ПДн понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Хранение персональных данных в ГБУ «ЦСОГПВИИ Вачского муниципального округа» осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в их достижении.

Обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона № 152-ФЗ, при условии обязательного обезличивания персональных данных;

Обработка Пд , полученных в результате обезличивания Пд , осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте РФ- городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» и Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в РФ.

Обезличивание ПДн Учреждением при обработке ПДн с использованием средств автоматизации может осуществляться с целью выполнения требований по предоставлению отчетности по результатам деятельности в соответствии с нормативными документами органов государственной власти и оператором, а также в связи с достижением целей обработки ПДн.

## **5. Перечень информационных систем ПДн.**

Наименование информационных систем, баз данных, реестров, регистров, номенклатур дел.

Категория содержащейся информации (для открытого доступа/ограниченного доступа):

1. Информационная система Комплекс «Соцпомощь»/ для ограниченного доступа
2. Информационная система социальной защиты населения Нижегородской помощи (АИС «СЗН НО») / для ограниченного доступа
3. Автоматизированный электронный сервис «Учет мероприятий по выполнению индивидуальных программ реабилитации инвалидов/ для ограниченного доступа.
4. Система автоматизации бухгалтерского и кадрового учета/для ограниченного доступа.

## **6. Пользователи ИСПДн**

6.1. В Положении Учреждения в отношении обработки и информационной безопасности ПДн определены основные категории пользователей. На основании этих данных производится типизация пользователей ИСПДн, определен их уровень доступа и возможности.

6.2. В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора безопасности;
- Пользователи АРМ;

6.3. Администратор безопасности обладает:

- правами Администратора БД;
- имеет доступ к средствам защиты информации.

6.4. Администратор безопасности уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;

6.5. Пользователь ИСПДн:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

## **7. Обязательство о неразглашении ПДн, непосредственно осуществляющего обработку ПДн.:**

7.1. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку по своей воле для своих интересов и сознательно. Согласие на обработку ПДн должно быть конкретным.

Согласие на обработку ПДн может быть отозвано субъектом ПДн.

7.2. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя:

- 1) фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа,

- удостоверяющего его личность, сведения о дате выдачи указанного документа и наименование выдавшего органа;
- 2) фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и наименование выдавшего органа, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
  - 3) наименование учреждения, получающего согласие субъекта ПДн;
  - 4) цель обработки ПДн;
  - 5) перечень ПДн, на обработку, которых дается согласие субъекта ПДн в соответствии с законодательством;
  - 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
  - 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных.
  - 8) срок, в течении которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
  - 9) подпись субъекта ПДн.

## **8. Требования к персоналу по обеспечению защиты ПДн:**

8.1. Все сотрудники Учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

8.2. При вступлении в должность нового сотрудника, допущенного к работе с персональными данными обрабатываемыми в информационной системе, ответственный за проведение первичного инструктажа обязан организовать его ознакомление с программой первичного инструктажа и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

8.3. Сотрудник должен быть ознакомлен с настоящим Положением и принятыми процедурами работы с элементами ИСПДн и СЗПДн.

8.4. Сотрудники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

8.5. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

8.6. При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

8.7. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, доступом по паролю, если не используются более сильные средства защиты.

8.8. Сотрудники должны быть проинформированы ответственным по обеспечению безопасности ПДн в ИСПДн об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятую политику и процедуры безопасности ПДн.

8.9. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководителю или лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

### **9. Порядок доступа в помещения, в которых ведется обработка ПДн:**

Запретить допуск посторонних лиц в кабинеты, в которых расположены технические средства ИСПДн, во время обработки персональных данных. В случае приема в кабинетах посторонних лиц обработка персональных данных должна производиться таким образом, чтобы исключить просмотр посторонними лицами текстовой и графической видовой информации отображаемой устройствами отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

### **10. Правовые, организационные и технические меры для обеспечения установленных уровней защищенности ПДн.**

10.1. Приказом директора ГБУ «ЦСОГПВИИ Вачского района» назначен ответственный работник:

- за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных (администратором безопасности);

- за организацию обработки ПДн (Администратор БД).

10.2. Для каждого структурного подразделения предусмотрены следующие организационные и технические меры для обеспечения установленных уровней защищенности ПДн:

1) Заключены обязательства о неразглашении ПДн с сотрудниками, осуществляющими обработку ПДн.

3) Определен перечень должностей работников, имеющих доступ к персональным данным в ИСПДн и осуществляющих их обработку в Учреждении (Приложение ).

10.3 Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,



предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

10.4. Обеспечение безопасности персональных данных достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 5) учетом машинных носителей персональных данных;
- 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы Пд и по его реагированию на компьютерные инциденты в них; (в ред. Федерального закона от 30.12.2020 №515-ФЗ)
- 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

## **11. Особенности обработки Пд, разрешенных субъектом Пд для рассмотрения**

1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2. В случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, предусмотренного настоящей статьей, обязанность предоставить доказательства законности последующего распространения или иной обработки таких

персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

3. В случае, если персональные данные оказались раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку.

4. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения.

5. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные частью 9 ст.10.1 федерального закона №152-ФЗ, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии с частью 9 ст.10.1 федерального закона №152-ФЗ, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

1) непосредственно;

2) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

7. Правила использования информационной системы уполномоченного органа по защите прав субъектов персональных данных, в том числе порядок взаимодействия субъекта персональных данных с оператором, определяются уполномоченным органом по защите прав субъектов персональных данных.

8. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

9. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в

установлении субъектом персональных данных запретов и условий, предусмотренных настоящей статьей, не допускается.

10. Оператор обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

11. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

12. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

13. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, указанного в части 12 настоящего раздела.

14. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений настоящей статьи или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

15. Выше указанные требования не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

## **11. Обработка ПДн без использования средств автоматизации (неавтоматизированная обработка ПДн):**

11.1. ПДн при их обработке, осуществляемой без использования средств, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

11.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:

- 1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры, журналы и др.);
- 2) обработка ПДн, осуществляется таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей).
- 3) необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.
- 4) при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

## **12. Принятые сокращения:**

ПДн – персональные данные;

ИСПДн – информационные системы персональных данных;

СЗПДн – система защиты персональных данных;

УБПДн – угрозы безопасности персональных данных;

БД – база данных;

НСД – настройка системы данных