Приложение № 4 к Приказу от 26.08.2025г. № 70-5 ОД «Об утверждении Перечня лиц, имеющих доступ к персональным данным, обрабатываемым в ОГБУСО «Шебертинский ДСО»

Правила доступа к персональным данным, обрабатываемым в ОГБУСО «Шебертинский ДСО»

1. Общие положения

1.1. Настоящие правила определяют порядок предоставления прав доступа в персональным данным, обрабатываемым в ОГБУСО «Шебертинский ДСО»
1.2. Настоящие правила разработали в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Федеральный закон № 152-ФЗ), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждения требований к защите персональных данных при их обработке в информационных системах персональных данных».
1.3. Основные понятия и термиты, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.
1.4. Перечень персональных данных, обрабатываемых в информационных системах, а также перечень информационных систем утверждаются приказом директора Учреждения.
1.5. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.
1.6. Управление Системой защиты осуществляет системный администратор информационных систем, назначаемый директором Учреждения.
1.7. Ответственными за выполнение требований данного документа u реализацию указанных в нем процедур являются ответственный за организацию обработки персональных данных и Администратор безопасности информационных систем персональных данных.
1.8. Лица, допущенные к персональным данным, должны ознакомиться с настоящими правилами под роспись.

2. Организация доступа к персональным данным

2.1. Перечень должностей, которым предоставляется доступ к персональным данным, обрабатываемым в информационных системах, для выполнения ими трудовых и служебных обязанностей (далее — лица, допущенные к персональным данным) утверждается приказом Директора ОГБУСО «Шебертинский ДСО»
2.2. На основании и в соответствии с утвержденным перечнем лиц, допущенных к персональным данным, системный администратор информационных систем разрабатывает таблицу разграничения доступа к персональным данным.
2.3. Системный администратор информационных систем на основания таблицы доступа предоставляет пользователям доступ к персональным данным, проверяет на его автоматизированном рабочем месте (далее — АРМ) заданные возможности доступа и впадает персональный идентификатор.

3. Общий порядок оформления заявок на предоставление, изменение, прекращение прав доступа

3.1. *Порядок оформления заявок для сотрудников.*

Оформление заявки на предоставление, изменение или прекращение прав доступа к персональным данные (далее — Заявка) может производиться следующими способами:

– в виде служебной записки;

- в виде электронной заявки по электронной почте.

Заявка в обязательном порядке содержит:
– фамилию, имя, отчество и должность работника, оформившего Заявку;
– фамилию, имя, отчество и должность работника, которому необходимо предоставить/изменить/прекратить доступ.

Кроме того, в общем случае, Заявка содержит:
– перечень либо категорию персональных данных, к которым необходимо предоставить/изменить/прекратить доступ:
– перечень информационных систем персональных данных с указанием полномочий в рамках этих систем;
– цели и основание для оформления доступа;
— дополнительные сведения при необходимости;
– комментарии.

Если Заявка оформляется в виде служебной записки, то работник, оформивший ее, проставляет свою подпись. Служебные записка на предоставление доступа передаются лично Администратору безопасности информационных систем персональных данных (далее — Администратор безопасности ИСПДн).

При необходимости Заявка предварительно согласуется с ответственным за организацию обработки персональных данных. Любой согласующий Заявку может потребовать уточнения указанной в Заявке информации и при необходимости внести коррективы.

Администратор безопасности информационных систем персональных данных настраивает (организует предоставление) доступ работнику в соответствии с Заявкой. После завершения настройки (организации предоставления) доступа работнику. Администратор безопасности информационных систем персональных данных уведомляет об этом работника, оформившего Заявку. Уведомление может быть в форме электронного письма или телефонного звонка.

3.2. Порядок оформления заявок для третьих лиц

В случае, если доступ к персональным данным необходимо предоставить третьим лицам, которые являются обработчиками персональных данных, то оформления заявки не требуется. Вместо процесса оформления заявки права доступа обговариваются при заключении договора и/или подписания Соглашения об обеспечении безопасности персональных данных, переданных на обработку (далее — Соглашение).

4. Предоставление прав доступа к персональным данным

Общие требования для предоставления прав доступа работникам к персональным данным осуществляются в соответствии с нормами, изложенными в Положении об обработке и защите персональных данных.

Право доступа к персональным данным имеют должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, которым доступ к такой информации предусмотрен Федеральными законами.

Право доступа к персональным ,данным имеют должностные лица ОГБУСО «Шебертинский ДСО», которым доступ к такой информации предусмотрен Федеральными законами и (и/или) локальными актами Учреждения.

Доступ к персональным данным субъектов персональных данных осуществляется на основании направленного оператору запроса.

При работе с документами, связанными с предоставлением персональных данных, должен обеспечиваться режим ограниченного доступа к соответствующим документам.

4.1. *Предоставление прав доступа к персональным данным на постоянной основе для работников*

Основаниями для оформление работнику прав доступа к персональным данным на постоянной основе являются следующие случаи:

– поступление нового работника в штат Оператора
– перевод работника внутри Оператора из другого подразделения на должность, где для выполнения трудовых обязанностей необходим доступ к персональным данным.

Непосредственный руководитель работника оформляет Заявку, в которой указываются:

– фамилия, имя, отчество и должность работника, которому предоставляется доступ;
– перечень, либо категория персональных данных, к которым предоставляется доступ;
– перечень ИСПДн с указанием полномочий в рамках этих систем.

Администратор безопасности ИСПДн организует настройку прав доступа работнику в соответствии с Заявкой в течение срока, не превышавшего трех рабочих дней.

4.2. Предоставление прав доступа к персональным данным па постоянной основе для третьих лиц

Основаниями для оформление третьему лицу прав доступа к персональным данным на постоянной основе являются следующие случаи:

– определенные условия, заложенные в договоре с третьим лицом, в связи с исполнением которых, третьему лицу нужен доступ к персональным данным на Постоянной основе;
– определенные условия, заложенные в договоре с третьим лицом, и для исполнения которых третьему лицу нужен доступ к персональным данным на постоянной основе.

Лицо, ответственное за заключение договора и/или подписание Соглашения, уведомляет Администратора безопасности ИСПДн через направление Заявки, содержащей следующую информацию:

– наименование и ИНН третьего лица, которому предоставляется доступ;
– перечень либо категория персональных данных, к которым предоставляется доступ;
- перечень ИСПДн с указанием полномочий в рамках этих систем.

Администратор безопасности ИСПДн организует настройку прав доступа третьему лицу в соответствии е Заявкой в течение срока, не превышающего пяти рабочих дней.

4.2. *Предоставление работникам разового доступа к персональным данным*

Основанием для оформления разового доступа к персональным данным работнику является выполнение служебного задания, в рамках которого работнику требуется доступ к персональным данным.

Непосредственный руководитель работника оформляет Заявку на предоставление разового доступа работника к персональным данным. В заявке указываются:

- перечень персональных данных, к которым предоставляется доступ;
- перечень ИСПДн с указанием полномочий в рамках этих систем;
- перечень документов, к которым необходим доступ;
- цели и основание для оформления разового доступа;
- время, на которое оформляется доступ.

Руководитель работника передает Заявку для согласования ответственному за организацию обработки персональных данных. Срок рассмотрения Заявки ответственным за организацию обработки персональных данных не должен превышать одного рабочего дня.

После согласования Заявки ответственный за организацию обработки персональных данных передает ее на исполнение Администратору безопасности ИСПДн.

В случае если работник выполнил свои задачи, раньше заявленного срока он должен проинформировать об этом своего непосредственного руководителя.

Руководитель работника оформляет заявку на прекращение доступа работнику.

4.3. *Предоставление третьим лицам разового доступа к персональным данным*

Основанием для оформление разового доступа к ПДн третьем лицам является выполнение ими срочных работ или услуг по договору с Оператором, в рамках которых третьему лицу требуется доступ к ПДн.

Непосредственный руководитель работника оформляет Заявку на предоставление разового доступа работника к ПДн. В заявке указываются:

- наименование и ИНН третьего лица, которому предоставляется доступ;
- перечень ПДн, к которым предоставляется доступ;
- перечень ИСПДн с указанием полномочий в рамках этих систем;
- перечень документов, к которым необходим доступ;
- цели и основания для оформления разового доступа;
- время, на которое оформляется доступ.

Лицо, ответственное за заключение договора с третьим лицом на оказание срочных работ или услуг, передает Заявку для согласования ответственному за организацию обработки персональных данных. Срок рассмотрения Заявки ответственным за организацию обработки персональных данных не должен превышать трех рабочих дней.

После согласования Заявки ответственным за организацию обработки персональных данных передает ее на исполнение Администратору безопасности ИСПДн.

В случае если третье лицо выполнило свои задачи, раньте заявленного срока он должен проинформировать лицо, ответственное за заключение договора с данным третьим лицом на оказание срочных работ или услуг. Лицо, ответственное за заключение договора с данным третьим лицом на оказание срочные работ или у слуг, оформляет Заявку на прекращение доступа третьему лицу.

5. Обязанности лиц, допущенных к п ерсональным данным.

5.1. *Обязанности лиц, допущенных к персональным данным*

– соблюдать конфиденциальность персональных данных;
– обеспечивать безопасность персональных данных при обработке в соответствии с Федеральным законом № 152-ФЗ;
– не делать неучтенных копий на бумажных и электронных носителях;
– не оставлять включенными АРМ с предоставленными правами доступа, после окончания работы (в перерывах) не оставлять материалы с конфиденциальной информацией на рабочих столах. Покидая рабочее место, пользователь обязан убрать документы и электронные носители с конфиденциальной информацией в закрываемые на замок шкафы (сейфы);
– при работе с документами, содержащими персональные данные, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;
– не выносить документы и иные материалы с персональными данными из служебных посещений, предназначенных для работы с ними;
– не вносить изменения в настройку средств защиты информации;
– немедленно сообщать лицу, ответственному за организацию обработки персональных данных, об утрате, утечке или искажении персональных данных, об обнаружении неучтенных материалов с указанной информацией;
– не допускать действий, способных повлечь утечку персональных данных;
– предъявлять для проверки лицам, наделенным необходимыми полномочиями в соответствии с законодательством Российской Федерации, числящиеся и имеющиеся в наличии документы касающиеся персональных данных только по согласованию с директором Учреждения.

6. Пересмотр н изменение прав доступа к персональным данным

6.1. *Пересмотр и изменение прав доступа работников к п*ерсональным *данным при отсутствии изменений в процессах обработки персональных данных:*

Основаниями для пересмотра прав являются:

– перевод работника на должность, в рамках подразделения, где для выполнения служебных (трудовых) обязанностей работнику требуется расширить или сократить права доступа к ПДн;

– служебная необходимость, в рамках которой работнику требуется разовое расширение
– проведение в отношении работника служебного расследования, в рамках которого работнику сокращают права доступа к ПДн.

Непосредственный руководитель работника пересматривает права всходя из оснований, представляемых выше, и принимает решение о целесообразности изменить права доступа работнику к ПДв.

Если руководитель принимает решение, что работнику необходимо изменить права доступа к ПДн, он оформляет Заявку, в которой указываются:

- основание для изменения доступа работника к ПДн;
– перечень ПДн, к которым предоставляется или сокращается доступ;
– перечень ИСПДн, с указанием расширения или сокращения полномочий в рамках этих систем;
– перечень документов, к которым изменяется доступ.

Руководитель работника должен оформить Заявку не позднее одного рабочего дна с момента появления такой служебной необходимости.

Руководитель работника направляет Заявку ответственному за обработку ПДн. Срок рассмотрения Заявки ответственным за обработку ПДн не должен превышать одного рабочего дня.

После согласования ответственный за организацию обработки персональных данных передает Заявку Администратору безопасности ИСПДн на исполнение. Срок рассмотрения Звявки не должен превышать одного рабочего дня.

Администратор безопасности ИСПДн, получив Заявку от ответственного за организацию обработки персональных данных, в срок, не превышающий трех рабочих дней, организует изменение в правах доступа согласно указанным в Заявке изменениям.

6.2. *Пересмотр и изменение прав доступа третьих лиц к персональным данным при отсутствии изменений в процессах обработки персональных данных*

Основаниями для пересмотра прав являются:

- экстренные условия в плане выполнения договорных работ или услуг с оператором, для исполнения которых необходимо расширение доступа к ПДн;
- нарушение третьем лицом договорные отношения на оказание работ или услуг с оператором, влекущих за собой разрыв договорных отношений;

Лицо, ответственное за заключение договора и/или подписания соглашения, пересматривает права исходя из оснований, представленных выше, и принимает решение о целесообразности изменить права доступа третьему лицу к ПДн.

Если руководитель принимает решение, что третьему ляду необходимо изменить права доступа к ПДн, он оформляет Заявку, в которой указываются:

– основание для изменения доступа работника к ЦДн;
- перечень ПДн, к которым предоставляется или сокращается доступ;
– перечень ИСПДн, с указанием расширения или сокращения полномочий в рамках этих систем;
– перечень документов, к которым изменяется доступ.

Лицо, ответственное за заключение договора и/или подписания Соглашения, должно оформить Заявку не позднее одного рабочего дня с момента появления такой необходимости.

Лицо, ответственное за заключение договора и/или подписания Соглашения, направляет Заявку ответственному за организацию обработки персональных данных. Срок рассмотрения Заявки ответственным за организацию обработки персональных данных не должен превышать одного рабочего дня.

После согласования ответственным за обработку ПДн передает Заявку Администратору безопасности ИСПДн на исполнение. Срок рассмотрения Заявки не должен превышать одного рабочего дня.

Администратор безопасности ИСПДн, получив Заявку от ответственного за обработку ПДн,

в срок, не превышающий трех рабочих дней, организует изменение в правах доступа согласно указанным в Заявке изменениям.

7 . Прекращение прав доступа к персональным данным

7.1. Прекращении прав доступа работников к персональным данным

Основаниями для прекращения прав доступа являются:
– перевод работника в другое структурное подразделение;
- достижение заявленных целей, для которых предоставлялся разовый доступ к персональным данным;
– прекращение трудовых отношений с работником.

Непосредственный руководитель работника, которому более не требуется доступ к персональным данным, оформляет Заявку, которая содержит:
- основание для прекращения доступа;
- перечень ресурсов, к которым прекращается доступ.

Заявка должна быть подготовлена не позднее одного рабочего дня, с момента возникновения основания для прекращения доступа.

Заявка направляется непосредственно Администратору безопасности ИСЦДн. Срок исполнения заявки не должен превышать одного рабочего дня.

Администратор безопасности ИСПДн организует прекращение доступа указанному работнику.

В случае, когда доступ прекращается из-за перевода работника в другое подразделение, новый непосредственный руководитель работника при необходимости предоставляет работнику права доступа к ПДн руководствуется разделом 6.1 данного документа.

7.2. Прекращение прав доступа третьих лиц к персональный данным

Основанием для прекращения прав доступа являются:
- достижение заявленных целей, для которых предоставлялся разовый доступ к персональным данным;
— прекращение договорных отношений с третьим лицом.

Лицо, ответственные за заключение договора и/или подписания Соглашения с третьим лицом, оформляет Заявку, которая содержит:
– основание для прекращения доступа;
– перечень ресурсов, к которым прекращается доступ.

Заявка должна быть подготовлена не позднее одного рабочего дня, с момента возникновения основания для прекращения доступа.

Заявка направляется непосредственно Администратору безопасности ИСПДн. Срок исполнения заявки не должен превышать одного рабочего дня.

Администратор безопасности ИСПДн организует прекращение доступа указанному работнику.

8. Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в следующих случаях:
– при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти Российской Федерации;
– по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;
- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;
– по результатам расследования инцидентов информационной безопасности, связанных с

обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

Ответственным за пересмотр настоящих Правил является Администратор безопасности ИСПДн.

Внесение изменений производится на основании соответствующего приказа Директора Учреждения.

9. Ответственность лиц, допущенных к персональным данным

9.1. Лица, виновные в нарушении требований настоящих правил и иных документов, регламентирующих вопросы защиты персональных данных, несут ответственность в соответствии с действующим законодательством Российской Федерации.

9.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.3. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несет дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

9.5. За неисполнение или ненадлежащее выполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

9.6. Должностные лица, в обязанности которых входит ведение персональных данных сотрудника, обязанных обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов либо иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информация — влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

9.7. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

9.8. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Учреждения, что влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде замечания, выговора, увольнения. Сотрудник Учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения своими действиями ущерба Учреждению (в соответствии с п.7 ст. 243 ТК РФ).

9.9 В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

9.10. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушение неприкосновенность частной жизни), предусмотрено ответственность в соответствии со статьей 137 Уголовного кодекса РФ.

Приложение № 5 к Приказу от 26.08.2025г.
№ 70-5 ОД «Об утверждении
Перечня лиц, имеющих доступ к
персональным данным,
обрабатываемым в ОГБУСО
«Шебертинский ДСО»

Обязательство о неразглашении персональных данных

_____

паспорт серии , номер , выданный « » 20 г.,

_____ ,

занимаемая должность _____

областного государственного бюджетного учреждения социального облуживания «Шебертинский ДСО», предупрежден(а), что на период исполнения должностных обязанностей в соответствии с нормами закона от 27.07.2006 № 152-ФЗ «О персональных данных», Положением об обработке и защите персональных данных работников ОГБУСО «Шебертинский ДСО», приказом «Об утверждении перечня лиц, имеющих, доступ к персональным данным работников ОГБУСО «Шебертинский ДСО», трудовым договором, должностной инструкцией мне будет предоставлен доступ к персональным данным
ОГБУСО «Шебертинский ДСО»

Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой, накоплением, хранением и т.д. персональных данных физически лиц.

Настоящим добровольно принимаю на себя обязательства:

1. Хранить в тайне известные мне конфиденциальные сведения, информировать руководителя учреждения о фактах нарушения порядка обращения с конфиденциальными сведениями, о ставших мне известными попытках несанкционированного доступа к информации.
2. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. Не использовать конфиденциальные сведения с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений, соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранности информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих служебных обязанностей.
5. После прекращения права на доступ к конфиденциальным сведениям не разглашать и не передавать третьим лицам неизвестные мне конфиденциальные сведения.

Я понимаю, что разглашение такого рода информации может нанести ущерб физическим лицам, как прямой, так и косвенный.

Я подтверждаю, что не имею права разглашать сведения:
анкетные и биографические данные; сведения об образовании; сведения о трудовом и общем стаже; сведения о составе семьи; паспортные данные; сведения о воинском учете; сведения о заработной плате сотрудника; сведения о социальных льготах; специальность; занимаемая должность; наличие судимостей; адрес места жительства; домашний телефон; место работы или учебы членов семьи и родственников; характер взаимоотношений в семье; содержание трудового договора; состав декларируемых сведений о наличии материальных ценностей; содержание декларации, подаваемой в налоговую инспекцию; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников: основания к приказам по личному составу; дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации; копии ответов, направляемые в органы статистики.

В связи с этим даю обязательство при работе (сборе, обработке, накоплении, хранении и т.д.) с персональными данными физических лиц соблюдать все описанные Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации› и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной конфиденциальной информации касающейся персональных данных физических лиц, или их утраты я несу ответственность в соответствии с действующим законодательством РФ (ст. 90 ТК РФ):

в случае разглашения сведений, являющихся конфиденциальной информацией, Работник обязан в полном объеме возместить понесенные в результате такого разглашения Учреждением убытки;

- в случае разглашения Работник может быть привлечен к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

Настоящее Соглашение действует бессрочно. Прекращение отношений по трудовому договору не является основанием для прекращения обязательств Сторон по настоящему соглашению.

Настоящее Соглашение составлено на двух страницах, на одном листе, в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному для каждой Стороны

(дата)	(подпись)	(расшифровка подписи)