МИНИСТЕРСТВО ТРУДА И
СОЦИАЛЬНОГО РАЗВИТИЯ ПЕРМСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ ПЕРМСКОГО КРАЯ
«СОЛИКАМСКИЙ ДОМ-ИНТЕРНАТ
ДЛЯ ПРЕСТАРЕЛЫХ И ИНВАЛИДОВ»

ПРИКАЗ

№ 01-05-109 от «05» августа 2026г.

Об утверждении политики в отношение обработки и защиты персональных данных

В целях исполнения Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику в отношении обработки и защиты персональных данных (приложение №1 к настоящему приказу).
2. Секретарю руководителя Л.Ю.Вотяковой ознакомить заместителей директоров (по направлениям), руководителей филиалов Учреждения с настоящим приказом в течение 5-ти дне й, с даты издания приказа.
3. Заместителям директоров (по направлениям), руководителям филиалов Учреждения ознакомить с локальным нормативным актом «Политика в отношении обработки и защиты персональных данных» всех сотрудников, в выполнении трудовых функций которых входит забор, использование и распространение (размещение) персональных данных, как в отношении сотрудников учреждения, так и в отношении получателей социальных услуг.
4. Системному администратору Ю.В. Ивашову обеспечить опубликование настоящего приказа на сайте Учреждения.
5. Контроль исполнения настоящего приказа оставляю за собой.

Директор Л.Б.Серегина

приложение №1 к приказу от
05.08.2026 года №01-05-109

МИНИСТЕРСТВО ТРУДА И
СОЦИАЛЬНОГО РАЗВИТИЯ
ПЕРМСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ ПЕРМСКОГО КРАЯ
«СОЛИКАМСКИЙ ДОМ-ИНТЕРНАТ
ДЛЯ ПРЕСТАРЕЛЫХ И ИНВАЛИДОВ»

УТВЕРЖДАЮ:
Директор
ГБУ ПК «Соликамский ДИПИ»
_____ Л.Б.Серегина

ПОЛИТИКА
в отношении обработки и защиты персональных данных

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является локальным правовым актом Государственного бюджетного учреждения Пермского края «Соликамский дом-интернат для престарелых и инвалидов» (далее - Учреждение), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Государственное бюджетное учреждение Пермского края «Соликамский дом-интернат для престарелых и инвалидов».

1.2. Политика направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Учреждением участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Учреждение становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние документы Учреждения распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних документах прямо не упоминаются, но фактически участвуют в правоотношениях с Учреждением.

2. Основания обработки и состав персональных данных, обрабатываемых в Учреждении

2.1. Обработка ПДн в Учреждении осуществляется в связи с выполнением законодательно возложенных на Учреждение полномочий и функций, определяемых Уставом ГБУ ПК «Соликамский дом-интернат для престарелых и инвалидов», кроме того в Учреждении осуществляется обработка ПДн, связанная с приемом на работу, реализацией трудовых отношений, формированием кадрового резерва.

2.2. ПДн получаются и обрабатываются Учреждением на основании федеральных законов и принятых в соответствии с ними нормативными правовыми актами, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.
2.3. В рамках осуществления функции организации предоставления государственной социальной и иной социальной помощи, мер социальной поддержки населению в соответствии с законодательством Российской Федерации, Пермской области, Пермского края - лица, имеющие право на получение мер государственной социальной помощи и поддержки, ПДн обрабатываются Учреждением:
1) при предоставлении мер социальной помощи и поддержки;
2) при учете фактов предоставления мер социальной помощи и поддержки.
2.4. В рамках осуществления функции в области содействия занятости населения ПДн обрабатываются Учреждением:
1) при реализации в Пермском крае единой государственной политики в области содействия занятости населения.
2.5. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Учреждение выступает в качестве работодателя, для обеспечения кадровой работы ПДн обрабатываются Учреждением в целях:
- реализации трудовых отношений;
- противодействия коррупции;
- формирования кадрового резерва.
2.6. Учреждением обрабатываются следующие специальные категории ПДн.
2.6.2. Для лиц, имеющих право на получение мер социальной помощи и поддержки, а также получателей государственных услуг в сфере занятости населения:
- сведения о состоянии здоровья;
- сведения о судимости.
2.6.3. Для граждан, претендующих на замещение должностей в Учреждении:
- сведения о состоянии здоровья (медицинское заключение по установленной форме);
- информация о наличии или отсутствии судимости.
Запрещается получать, обрабатывать и приобщать к личному делу работника персональные данные - касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.
2.7. Учреждением обрабатываются биометрические ПДн для следующих категорий субъектов Пдн:
2.7.2. Для лиц, перечисленных в п. 2.5 настоящей Политики: - фотография.
2.8. Обработка иных специальных категорий персональных данных, а также биометрических персональных данных Учреждением не ведется.
2.9. В целях исполнения возложенных на Учреждение функций Учреждение в установленном порядке вправе поручить обработку ПДн третьим лицам. В договоры с лицами, которым Учреждение поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные Законом о ПДн и Политикой правила обработки ПДн.
2.10. Учреждение предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим в соответствии с федеральным законом право на получение соответствующих ПДн.
2.11. В Учреждении не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в

Учреждении, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Учреждением ПДн уничтожаются или обезличиваются.

2.12. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки.

Учреждение принимает необходимые меры по удалению или уточнению не полных или не точных ПДн.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Учреждение руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения (далее - ИС), и других имеющихся в Учреждении систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на должностных лиц Учреждения в пределах их обязанностей, связанных с обработкой и защитой ПДн;

7) минимизация прав доступа: доступ к ПДн предоставляется должностным лицам только в объеме, необходимом для выполнения их должностных обязанностей;

8) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию должностных лиц, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Учреждения до заключения договоров;

9) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

10) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Учреждении ПДн имеют лица, уполномоченные приказом Учреждения, а также лица, чьи ПДн подлежат обработке.

4.2. Доступ должностных лиц к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних документов Учреждения. Допуск должностных лиц к обработке ПДн осуществляется согласно перечню типовых полномочий (ролей пользователей), утверждаемых приказом Учреждения. Соответствующие полномочия (роль пользователя) вносятся в должностные обязанности указанных должностных лиц. Допущенные к обработке ПДн должностные лица под роспись знакомятся с документами Учреждения, устанавливающими порядок обработки ПНд, включая документы, устанавливающие права и обязанности конкретных должностных лиц.

4.3. Факты получения доступа и обработки ПДн регистрируются, в том числе с использованием средств обеспечения информационной безопасности. Информация о фактах обработки ПДн хранится в Учреждении в течение трех лет. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Учреждением, осуществляется в соответствии с Законом о ПДн и определяется внутренними документами Учреждения.

5. Реализация Политики

5.1. Учреждение принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в Учреждении несет должностное лицо Учреждения, назначаемое приказом Учреждения.

Ответственный за организацию обработки ПДн в Учреждении, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Учреждении требований нормативных правовых актов и внутренних документов Учреждения в области обработки и защиты ПДн;

2) доводить до сведения должностных лиц Учреждения о положениях нормативных правовых актов и внутренних документов Учреждения в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. В Учреждении реализуется комплекс правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку внутренних документов Учреждения по вопросам обработки и защиты ПДн, контроль за исполнением в Учреждении требований нормативных правовых актов и внутренних документов Учреждения в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

2) оформление письменных обязательств должностных лиц о неразглашении ПДн;

3) доведение до сведения должностных лиц информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

4) обеспечение наличия в положениях о структурных подразделениях Учреждения и должностных обязанностях требований по соблюдению установленного порядка обработки и защиты ПДн;
5) разработку и введение в действие внутренних документов Учреждения по обеспечению информационной безопасности;
6) ознакомление должностных лиц с положениями нормативных правовых актов и внутренних документов Учреждения в области обработки и защиты ПДн и (или) организация обучения их правилам обработки и защиты ПДн;
8) проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:
а) физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;
б) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;
9) регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Учреждения, так и при взаимодействии с контрагентами Учреждения, государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;
10) установление правил доступа на объекты, в помещения, применение в этих целях систем охраны и управления доступом;
11) формирование участков (виртуальные локальные компьютерные сети) администрирования безопасности, мониторинга и аудита, управления доступом к защищаемым ресурсам;
12) организацию технического оснащения объектов в соответствии с существующими требованиями к информационной безопасности;
13) формирование условий и технологических процессов обработки, хранения и передачи информации в Учреждении (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних документов Учреждения в области обработки и защиты ПДн;
14) установление полномочий пользователей и форм представления информации пользователям;
15) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;
16) организацию необходимых мероприятий с должностными лицами, а также собеседование с лицами, претендующими на работу в Учреждение, изучение их биографии и проверку предоставляемых сведений; обучение должностных лиц требованиям информационной безопасности;
17) осуществление контроля эффективности организационных мер защиты;
18) разработку защитных технических решений:
19) применение программно-технических мер защиты;
5.10. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в

квартал проходят актуализацию. Должностные лица проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нештатных ситуациях.

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПДн реализуются в Учреждении в следующих направлениях:

1) предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

2) предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

3) защита от вредоносных программ;

4) обеспечение безопасного межсетевого взаимодействия;

5) обнаружение вторжений и компьютерных атак;

6) осуществление контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

1) реализацию разрешительной системы допуска пользователей к информационным ресурсам ИС и связанным с их использованием работам, документам;

2) разграничение доступа пользователей и обслуживающих специалистов к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

3) регистрацию действий пользователей и обслуживающих специалистов, контроль несанкционированного доступа и действий пользователей и обслуживающих специалистов, а также третьих лиц;

4) использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

5) предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям информации, в том числе на наличие компьютерных вирусов;

6) ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

7) размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

8) организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

9) учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

10) резервирование технических средств, дублирование массивов и носителей информации;

11) реализацию требований по безопасному межсетевому взаимодействию ИС;

12) использование защищенных каналов связи, защиту информации при ее передаче по каналам связи;

16) активный аудит безопасности ИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

17) анализ защищенности ИС с применением специализированных программных средств (сканеров безопасности);

18) централизованное управление системой защиты ПДн в ИС.

6.3. С целью поддержания состояния защиты ПДн на надлежащем уровне в Учреждении осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.
Внутренний контроль включает:
1) мониторинг состояния технических и программных средств;
2) контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн, требований договоров).
6.4. В целях осуществления внутреннего контроля в Учреждении проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Учреждении либо комиссией, образуемой по приказу Учреждения.
6.5. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается директору Учреждения.