Приложение 4
УТВЕРЖДЕНО
приказом И.о.директора
ЛОГБУ «Приозерский
КЦСОН»
от 09.09.2020 г. № 114

**Правила**
**обработки персональных данных**

## I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данные Правила разработаны с целью защиты интересов Ленинградского областного государственного бюджетного учреждения «Приозерский комплексный центр социального обслуживания населения» ЛОГБУ «Приозерский КЦСОН» и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

1.2. Данные Правила предназначены для использования всеми работниками ЛОГБУ «Приозерский КЦСОН», допущенными к работе с персональными данными.

1.3. Работники ЛОГБУ «Приозерский КЦСОН», доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных

## II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.2. **Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.3. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

2.4. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах,

архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.5. **Контролируемая зона (КЗ)** – это пространство (территория, здание, часть здания, кабинеты), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

2.6. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.7. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.8. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.9. **Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.10. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.11. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.12. **Субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных

2.13. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

## III. ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3.1. При обработке персональных данных на бумажных носителях, съёмных машинных носителях (флеш - носителях, дисках, и т.п.), компьютерах и других технических средствах, работники ЛОГБУ «Приозерский КЦСОН» обязаны следить как за сохранностью самих бумажных документов, съёмных машинных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно, не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Запрещается хранение или оставление бумажных документов и съёмных машинных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных машинных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.3. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные машинные носители.

3.4. Запрещается использовать для передачи персональных данных съёмные машинные носители, не учтённые в Журнале учета съемных носителей информации.

3.5. Запрещается выносить документы, съёмные машинные носители или переносные компьютеры, содержащие персональные данные, за пределы помещений контролируемой зоны ЛОГБУ «Приозерский КЦСОН», если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение директора ЛОГБУ «Приозерский КЦСОН» или ответственного за организацию обработки персональных данных.

3.6. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в шредерах).

3.7. Большие объёмы бумажных документов с персональными данными, съёмные машинные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

3.8. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

3.9. Запрещается установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети, самовольное изменение сетевых адресов, самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удаленными сетевыми настройками. Использование технологии беспроводного доступа без разрешения ответственного за обеспечение безопасности в информационных системах.

3.10. Для работы с персональными данными разрешается использовать только автоматизированные рабочие места, указанные в Перечне автоматизированных рабочих мест информационных систем, при это для обработки персональных данных можно использовать только программное обеспечение, указанное в Перечне программного обеспечения обрабатывающего персональные данные.

3.11. Запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

3.12. Запрещается в нерабочее время или за пределами помещений ЛОГБУ «Приозерский КЦСОН» упоминать в разговоре с кем-либо, включая любых работников ЛОГБУ «Приозерский КЦСОН», сведения, содержащие персональные данные.

3.13. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных в информационных системах, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

## IV. ПОРЯДОК ДОСТУПА ЛИЦ В ПОМЕЩЕНИЯ

4.1. При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

4.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений и определяет порядок пропуска работников ЛОГБУ «Приозерский КЦСОН» и иных третьих лиц в помещения.

4.3. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителя структурного подразделения.

4.4. Не допускается нахождение работников ЛОГБУ «Приозерский КЦСОН» в помещениях контролируемой зоны в нерабочее для них время без согласования с руководством и без служебной записки. В нерабочее время, в случае служебной необходимости могут задержаться на рабочих местах только при наличии служебной записки, подписанной руководителем структурного подразделения. В служебной записке указывается (Ф.И.О. работника, № кабинета и время окончания работы, при работе нескольких человек указывается ответственное лицо). Служебная записка предоставляется ответственному за организацию обработки персональных данных. В случае неотложных заданий, поступивших после окончания рабочего дня, порядок допуска в помещения контролируемой зоны ЛОГБУ «Приозерский КЦСОН» осуществляется аналогичным образом, по личному разрешению ответственного за организацию обработки персональных данных до начала неотложных работ.

4.5. В случаях, не терпящих отлагательства (пожар, авария систем тепло-, водоснабжения и т.п.), когда находящимся в помещении оборудованию, материальным ценностям и документации грозит опасность уничтожения или вывода из строя, работник оповещает пожарную охрану (аварийную службу), вызывает руководителя подразделения или работника, ответственного за помещение. Помещение вскрывается до прибытия указанных лиц, и принимаются меры к тушению пожара (ликвидации аварии), эвакуации ценностей, имущества и документации. Около эвакуируемых ценностей, имущества и документации выставляется временный пост охраны. Акт о вскрытии помещения составляется после окончания работ, связанных с ликвидацией происшествия.

4.6. Нахождение посетителей допускается только в рабочее время в присутствии работников, имеющих допуск к персональным данным.

4.7. В помещения ИС пропускаются:

4.7.1. беспрепятственно – директор ЛОГБУ «Приозерский КЦСОН» и работники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

4.7.2. при наличии служебного удостоверения, с разрешения директора ЛОГБУ «Приозерский КЦСОН» или руководителя структурного подразделения, в сопровождении ответственного за организацию обработки персональных данных или руководителя структурного подразделения - работники контролирующих органов, работники пожарных и аварийных служб, работники полиции;

4.7.3. ограниченно - работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

4.8. Посетители пропускаются в помещения ИС ЛОГБУ «Приозерский КЦСОН» в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

4.9. В помещениях, в которых происходит обработка персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4.10. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных директором или руководителями структурных подразделений ЛОГБУ «Приозерский КЦСОН».

4.11. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за организацию обработки персональных данных или руководителя структурного подразделения.

4.12. Контроль за допуском в помещения контролируемой зоны в рабочее время возлагается на руководителей подразделений, за которыми закреплены данные помещения. В нерабочее время, выходные и нерабочие праздничные дни охрана помещений контролируемой зоны обеспечивается средствами охранной сигнализации, а в случае их неисправности выставлением поста охраны.

4.13. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ.

4.14. Руководители структурных подразделений, либо работники, уполномоченные хранить ключи от сейфов и помещений должны вести Журнал учета ключей от сейфов и помещений.

4.15. Контроль за допуском в помещения контролируемой зоны в рабочее время возлагается на руководителей подразделений, за которыми закреплены данные помещения. В нерабочее время, выходные и нерабочие праздничные дни охрана помещений контролируемой зоны обеспечивается средствами охранной сигнализации, а в случае их неисправности выставлением поста охраны.

4.16. Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц.

4.17. Окна помещений, в которых ведётся обработка персональных данных, должны быть оборудованы шторами или жалюзи.

4.18. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

4.19. Уборка помещений ИС должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

4.20. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

## V. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

5.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования личного пароля, разглашённого владельцем учётной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа пользователь ИСПДн обязан:

5.2.1. прекратить несанкционированный доступ к персональным данным;

5.2.2. доложить директору ЛОГБУ «Приозерский КЦСОН» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки ПДн о факте несанкционированного доступа.

## VI. ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОМУ УКРЕПЛЕНИЮ

6.1. Руководители структурных подразделений обеспечивают обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями:

6.1.1. Двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек.

6.1.2. Оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности.

6.1.3. Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

6.1.4. Стекла в рамах должны быть надежно закреплены в пазах.

6.1.5. Рамы указанных оконных проемов должны оборудоваться запорными устройствами.

## VII. ОТВЕТСТВЕННОСТЬ

7.1. Работники ЛОГБУ «Приозерский КЦСОН», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную,

административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

7.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, 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) ЛОГБУ «Приозерский КЦСОН», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник ЛОГБУ «Приозерский КЦСОН», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ЛОГБУ «Приозерский КЦСОН» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

7.2.1. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

7.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

7.4. Директор ЛОГБУ «Приозерский КЦСОН» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.