

Утверждаю
Директор ГАУ СО «Энгельсский дом-интернат для престарелых и инвалидов»
С.В. Сафошкин
« 20 » 2014 г.

ПОРЯДОК

доступа сотрудников ГАУ СО «Энгельсский дом-интернат для престарелых и инвалидов» в помещения, в которых ведется обработка персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Порядок доступа сотрудников ГАУ СО «Энгельсский дом-интернат для престарелых и инвалидов» (далее - Учреждение) в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», в целях обеспечения защиты конфиденциальной информации, обрабатываемой в Учреждении, и исключения фактов неконтролируемого пребывания в них посторонних лиц. Настоящим документом определяются границы контролируемой зоны, порядок доступа в неё работников и посетителей, а также правила обработки и хранения документов, содержащих персональные данные, и материальных носителей персональных данных.

Порядок устанавливает единые требования к обеспечению сохранности технических средств и персональных данных.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Неавтоматизированная обработка персональных данных – обработка персональных данных без использования средств вычислительной техники.

Технические средства – серверные станции, персональные компьютеры и ноутбуки, настроенные на доступ к программному обеспечению, хранящему и обрабатывающему персональные данные сотрудников и контрагентов.

Контролируемая зона (КЗ) – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

Постоянная контролируемая зона – это зона, границы которой устанавливаются на длительный срок.

Временная контролируемая зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера.

3. ГРАНИЦЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

3.1. Граница контролируемой зоны, в которой ведётся обработка персональных данных с использованием средств автоматизации и без таковых утверждаются приказом Директора Учреждения.

К контролируемой зоне в Учреждении относят помещения, расположенные по адресам:

- Саратовская область, город Энгельс, ул. Санаторная д.3;
- Саратовская область, город Энгельс, ул. Санаторная дом 3а;
- Саратовская область, Энгельсский район, с. Квасниковка, ул. Колхозная д.85.

3.2. Контроль доступа на территорию контролируемой зоны объектов Учреждения осуществляется сотрудниками Учреждения в соответствии с внутренними должностными инструкциями.

3.3. При необходимости, в целях обеспечения защиты конфиденциальной информации за пределами постоянной контролируемой зоны и обеспечения санкционированного (контролируемого) пребывания в ней посторонних лиц, в Учреждении может быть организована временная контролируемая зона.

Границы временной контролируемой зоны определяются, исходя из целей планируемого мероприятия, на основании принятых нормативных документов и выполнения режимных мер.

4. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

4.1. В целях обеспечения сохранности технических средств и материальных носителей помещения, в которых осуществляется обработка персональных данных, оборудованы пожарной сигнализацией, а также прочными дверями с механическими замками.

Ключи от замков находятся на ответственном хранении у сотрудника охраны, уполномоченного хранить ключи от замков всех помещений, и передаются ответственным лицам, осуществляющим обработку данных в помещении под роспись в журнале приема-передачи ключей.

4.2. Сотрудникам отделов, не работающим непосредственно в данном помещении, доступ в него разрешен только в присутствии сотрудников отдела, работающих в данном помещении.

4.3. В случае, если в течение рабочего дня сотрудник отдела уходит из помещения (не остается других сотрудников этого отдела), он обязан проследить, чтобы в помещении не было посторонних лиц (в том числе сотрудников других отделов) и закрыть помещение на замок.

4.4. По окончании рабочего дня помещения, в которых осуществляется обработка персональных данных, запираются, ключи от них сдаются сотрудникам охраны. По окончании рабочего дня сотрудник охраны осуществляет охрану помещений.

4.5. Нахождение клиентов (посторонних лиц) в помещениях, где осуществляется обработка персональных данных, допускается только в присутствии сотрудников отдела,

непосредственно работающих в данном помещении, с соблюдением установленных правил ограничения доступа к обрабатываемой информации.

5. ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

5.1. Закрытие помещений, в которых осуществляется обработка персональных данных, производится ответственными работниками по окончании рабочего времени, проведении в нём (при необходимости) влажной уборки и осмотра его в целях выявления и устранения возможных нарушений (не выключенное оборудование, неубранные документы, незапертые хранилища, окна и т.п.), в том числе правил противопожарной безопасности (отключение электрических приборов, освещения и т.п.).

5.2. После осмотра помещения, выявления и устранения возможных недостатков, ответственный сотрудник закрывает помещение

С указанного момента помещение считается принятым под охрану.

5.3. В случаях, если за период рабочего времени произошли изменения, вследствие которых может потребоваться изменение характера охраны, ответственный работник сообщает об этом дежурному сотруднику службы охраны.

В случае значительных изменений в режиме охраны производится корректировка руководящих документов.

5.4. Вскрытие помещений, в которых осуществляется обработка персональных данных, производится ответственными лицами, указанными в списке дежурного сотрудника службы охраны, имеющими допуск в охраняемые помещения.

5.5. При входе в помещения, в которых осуществляется обработка персональных данных, ответственный работник производит внешний осмотр на предмет выявления возможных видимых недостатков (отсутствие техники, оборудования) и нарушений (повреждение целостности дверей и т.п.). При отсутствии признаков нарушения целостности охраняемого объекта или причинения ущерба объект считается снятым с охраны.

5.6. В случае обнаружения повреждения (нарушения целостности) внешней двери помещения, в котором осуществляется обработка персональных данных, или при обнаружении попытки проникновения в него ответственный работник незамедлительно сообщает о случившемся руководителю или лицу, его замещающему, после чего должностное лицо принимает необходимые меры по локализации нарушения:

- вызывает сотрудников полиции по номеру 02 или мобильному 112 для принятия мер реагирования;
- в течение двенадцати часов с момента выявления факта нанесения ущерба организует проведение инвентаризации имущества и подтверждение размера ущерба соответствующими документами бухгалтерского учета с расчетом его стоимости;
- обеспечивает сохранность пострадавшего имущества в том виде, в каком оно находилось после нанесения ущерба.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ УСТАНОВЛЕННОГО ПОРЯДКА

6.1. Контроль выполнения требований настоящего Порядка возлагается на начальников отделов, являющихся пользователями информационной системы персональных данных, а также отдельные лиц, имеющих право доступа в охраняемые помещения.

6.2. Работник, нарушивший требования данного Порядка, может быть привлечен к дисциплинарной или правовой ответственности в соответствии с законодательством РФ и трудовым договором, если проступок не содержит состава преступления.

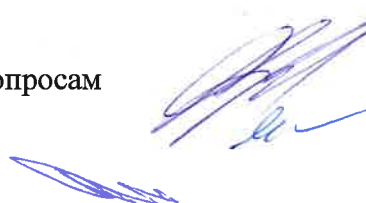
Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Согласовано:

Зам. директора по общим вопросам

Начальник ОК

Юрисконсульт



Ф.Б. Аллахвердиев

Е.Ю. Голубкина

О.Л. Ринглер