Утверждаю:
Директор ГБОУ РШИ с. Камышла

"28" сентября 2023 г. № 323

_____/Садриев З.Г./
(подпись / Ф.И.О.)

М.П

РЕГЛАМЕНТ
РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

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

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 Федеральным законом «О персональных данных».

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.

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. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. **Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных. Специальная информационная система – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент определяет единый и обязательный порядок проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, в ГБОУ РШИ с. Камышла (далее – Оператор, Организация).

3. ПРОВЕДЕНИЕ ВНУТРЕННЕГО РАССЛЕДОВАНИЯ ИНЦИДЕНТА

Проведение внутреннего расследования и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов: – нарушение конфиденциальности, целостности, доступности персональных данных; – выявление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных; – халатность и несоблюдение требований по обеспечению безопасности персональных данных; – несоблюдение условий хранения носителей персональных данных; – использование средств защиты информации, которые могут привести к

нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных. Задачами внутреннего расследования являются: – установление обстоятельств нарушения, в том числе времени, места и способа его совершения; – установление лиц, непосредственно виновных в данном нарушении; – выявление причин и условий, способствовавших нарушению. Проведение внутреннего расследования возлагается приказом руководителя на комиссию в области персональных данных (далее – Комиссия). Комиссия должна приступить к работе по расследованию не позднее следующего дня после даты выявления нарушения. Общая продолжительность внутреннего расследования не должна превышать 72 часов с момента выявления нарушения или инцидента в области персональных данных.

4. ПРАВА И ОБЯЗАННОСТИ КОМИССИИ

Права и обязанности Комиссии: – опрос работников, допустивших нарушение конфиденциальности информации, а также лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента в области персональных данных; – проведение осмотров объектов и предметов, которые могут иметь отношение к факту нарушения; – привлечение (с разрешения соответствующего руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования. Работник, в отношении которого проводится расследование, должен быть ознакомлен с приказом руководителя о проведении расследования. Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (актами, справками и т. п.). Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии (не менее чем за двумя подписями). В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения руководителя Оператора. Для организованного и оперативного проведения внутреннего расследования Администратор безопасности разрабатывает версии причин и составляет план проведения необходимых мероприятий по каждой из этих версий. В ходе расследования могут выдвигаться и отрабатываться дополнительные версии, в этом случае план действий уточняется. Одновременно с проведением внутреннего расследования, руководитель Оператора может поручить Комиссии определить актуальность утраченной (разглашенной) конфиденциальной информации, оценить вред, который возможно был причинен субъектам

персональных данных в случае нарушения Федерального закона "О персональных данных", а также определить (подсчитать) ущерб (убытки) по расследуемому факту. В отдельных случаях такая оценка может быть осуществлена специализированной организацией.

5. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ РАССЛЕДОВАНИЯ

По окончании внутреннего расследования Комиссия представляет руководителю Оператора заключение, в котором излагаются: – основания и время проведения расследования; – проделанная работа (кратко); – время, место и обстоятельства факта нарушения; – причины и условия совершения нарушения; – виновные лица и степень их вины; – наличие умысла в действиях виновных лиц; – степень вреда, который был причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных" – предложения по возмещению ущерба; – предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия; – рекомендации по исключению подобных нарушений; – другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т.д.). К заключению прилагаются: – письменные объяснения лиц, которых опрашивали члены Комиссии; – акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.; – другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба (убытков), оценке вреда. Заключение должно быть подписано всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде). Заключение по результатам расследования подлежит утверждению руководителя Оператора. Работник, в отношении которого проводится расследование, или его уполномоченный представитель, имеют право знакомиться с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов. Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с заключением по результатам расследования. Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом. При наличии в действиях лица признаков административного правонарушения или уголовного преступления руководитель обязан обращаться в правоохранительные органы для привлечения виновного к ответственности в соответствии с законодательством Российской Федерации. 5 В соответствии с Трудовым кодексом возмещение ущерба проводится независимо от привлечения работника к дисциплинарной, административной или уголовной

ответственности за действия или бездействие, которыми причинен ущерб работодателю. При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности. Первый экземпляр заключения с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дело о внутренних расследованиях вносится в номенклатуру дел Оператора.