«СОГЛАСОВАНО»
Председатель ПК
ГБОУ НШ «Гармония»
_____Л.М.Каткасова
«01» марта 2023г.

«УТВЕРЖДАЮ»
Директор
ГБОУ НШ «Гармония»
_____В.И. Шишкина
«01» марта 2023г.

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

в ГБОУ НШ «Гармония» п.г.т. Безенчук

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в государственном бюджетном общеобразовательном учреждении Самарской области начальной школе «Гармония» п.г.т. Безенчук муниципального района Безенчукский Самарской области (далее – ГБОУ), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании положений законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения», приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"», приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных», приказа Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

1.3. Для обработки ПДн, необходимых для предоставления государственных и муниципальных услуг ГБОУ, используется информационная система персональных данных

ЭП
C=RU, O="ГБОУ НШ ""Гармония"" п.г.т. Безенчук", CN=Директор - Шишкина В.И., E=garmoniya_nsds_bzn@samara.edu.ru
008d6da80728a89db9
2023.03.30 11:30:17+04'00'

(далее – ИСПДн) АИС «Е-услуги. Образование», АИС «АСУРСО», предназначенные для осуществления работы с данными воспитанников, учащихся, их законных представителей.

1.4. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в ГБОУ в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн «Сотрудники предприятия», ИСПДн «Кластер», АИС «АСУРСО», АИС «Кадры в образовании».

1.5. Пользователем ИСПДн (далее – Пользователь) является сотрудник – Ответственный за обработку персональных данных, использованных в ИСПДн (далее - Ответственный), участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн ГБОУ проводятся в следующих целях:

1.6.1 проверка выполнения требований организационно-распорядительной документации по защите информации в ГБОУ и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.6.2 оценка уровня осведомленности и знаний работников ГБОУ в области обработки и защиты персональных данных;

1.6.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Ответственным периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в ГБОУ.

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности. Решение о проведении внеплановых контрольных мероприятий по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению руководителя ГБОУ.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий ответственный за обработку ПДн, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1 Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБОУ (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии Ответственного за обработку персональных данных,

5.2. Ответственный за обработку ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет ответственного по ИБ, всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в ГБОУ.
- Соблюдение Порядка доступа в помещения, где ведется обработка персональных данных.
- Порядок и условия применения средств защиты информации.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.