РЕКОМЕНДОВАНЫ К ПРИНЯТИЮ
Общим собранием работников
Муниципального бюджетного
общеобразовательного учреждения «Средняя
общеобразовательная школа № 20»
(протокол от 09.03.2023 №2)

УТВЕРЖДЕНО
приказом Муниципального бюджетного
общеобразовательного учреждения «Средняя
общеобразовательная школа № 20»
от 20.03.2023 № 46-Д

Мнение Родительского комитета учтено

(протокол от 20.03.2023 № 3)

Мнение Совета учащихся учтено

(протокол от 20.03.2023 №3)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00D9ACBB53214C8A0C152A4A29DB2CFFEF
Владелец: Фуртова Галина Александровна
Действителен: с 01.11.2022 до 25.01.2024

Изменения в Положение об обработке персональных данных в МБОУ «СОШ №20»

1. Положение об обработке персональных данных в МБОУ «СОШ № 20» дополнить следующими разделами:

XIV. ТРЕБОВАНИЯ К ПОДТВЕРЖДЕНИЮ УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. В случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

14.2. В случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, содержащимся в пунктах 14.3. и 14.4., и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

14.3. Акт об уничтожении персональных данных должен содержать:

а) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес оператора;

б) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению оператора (если обработка была поручена такому (таким) лицу (лицам);

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

14.4. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в подпункте "г" пункта 14.3.

14.5. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

14.6. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 14.5. недостающие сведения вносятся в акт об уничтожении персональных данных.

14.7. В случае если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, установленным пунктами 14.3 и 14.4 и выгрузка из журнала, соответствующая требованиям, установленным пунктом 14.5.

14.8. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

XV. ПОРЯДОК И УСЛОВИЯ ВЗАИМОДЕЙСТВИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ С ОПЕРАТОРАМИ В РАМКАХ ВЕДЕНИЯ РЕЕСТРА УЧЕТА ИНЦЕДЕНТОВ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

15.1. Взаимодействие Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в целях учета в реестре учета инцидентов в области персональных данных информации о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных,

осуществляется в форме направления операторами в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомления о таких фактах (далее - уведомление), содержащего:

- информацию о произошедшем инциденте (далее - первичное уведомление);
- информацию о результатах внутреннего расследования выявленного инцидента (далее - дополнительное уведомление).

15.2. Первичное уведомление должно содержать:

15.2.1. Сведения:

о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее - скомпрометированная база данных), количество содержащихся в ней записей. Дополнительно оператор может представить информацию об актуальности скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);

о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);

о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда, проведенной в соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона "О персональных данных");

о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых оператором организационных и технических мер по устранению последствий инцидента в соответствии со статьями 18.1, 19 Федерального закона "О персональных данных");

о лице, уполномоченном оператором на взаимодействие с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, по вопросам, связанным с выявленным инцидентом.

15.2.2. Данные оператора, направившего уведомление:

фамилию, имя и отчество (при наличии) гражданина, индивидуального предпринимателя;

полное и сокращенное (при наличии) наименование юридического лица;

идентификационный номер налогоплательщика юридического лица, индивидуального предпринимателя, физического лица;

адрес регистрации по месту жительства (пребывания) физического лица, индивидуального предпринимателя;

адрес юридического лица в пределах места нахождения юридического лица;

адрес электронной почты (при наличии) для направления информации, предусмотренной пунктом 8 настоящего Порядка.

15.2.3. Иные сведения и материалы, находящиеся в распоряжении оператора, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии).

15.3. Дополнительное уведомление должно содержать сведения:

о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов персональных данных, и вреде, нанесенном правам субъектов персональных данных, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении оператора о проведении внутреннего расследования с указанием его реквизитов);

о лицах, действия которых стали причиной выявленного инцидента (при наличии) (фамилия, имя, отчество (при наличии) должностного лица оператора с указанием должности (если причиной инцидента стали действия сотрудника оператора), фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия посторонних лиц) и иные сведения о выявленном инциденте, имеющиеся в распоряжении оператора).

15.4. В случае если оператор на момент направления первичного уведомления располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

15.5. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа.

15.6. Уведомление в виде документа на бумажном носителе направляется по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

15.7. Уведомление в форме электронного документа направляется оператором посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети "Интернет" (далее - Портал персональных данных), после прохождения процедуры идентификации и аутентификации посредством федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее - ЕСИА) и подписывается электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

15.8. Оператору с момента поступления уведомления в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также номер и ключ уведомления.

15.9. При направлении дополнительного уведомления посредством Портала персональных данных оператор должен указать номер и ключ уведомления, полученного в соответствии с пунктом 8 настоящего Порядка.

15.10. В случае направления оператором неполных или некорректных сведений Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, не позднее трех рабочих дней со дня получения первичного или дополнительного уведомления направляет запрос оператору о представлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений.

15.11. Недостающие сведения и (или) пояснения относительно некорректности представленных в уведомлении сведений предоставляются оператором в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение трех рабочих дней со дня получения запроса, указанного в пункте 10 настоящего Порядка, одним из способов, предусмотренных пунктом 5 настоящего Порядка.

15.12. В случае если по истечении сроков, установленных пунктом 2 части 3.1 статьи 21 Федерального закона "О персональных данных", дополнительное уведомление в адрес Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций не поступило, Федеральной службой по надзору в сфере связи,

информационных технологий и массовых коммуникаций оператору направляется требование о необходимости представить сведения о результатах внутреннего расследования выявленного инцидента (далее - требование о предоставлении сведений).

15.13. Ответ на требование о предоставлении сведений направляется оператором Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение одного рабочего дня со дня получения такого требования одним из способов, предусмотренных пунктом 5 настоящего Порядка.

15.14. В случае если Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций выявлен факт неправомерного распространения скомпрометированной базы данных, содержание которой указывает на ее принадлежность к конкретному оператору, такому оператору Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций направляется требование о необходимости представить уведомление (далее - требование о предоставлении уведомления).

15.15. Оператор, которому направлено требование о предоставлении уведомления, направляет его в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в сроки, установленные частью 3.1 статьи 21 Федерального закона "О персональных данных».

15.16. В случае неподтверждения оператором факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, и (или) неустановления принадлежности скомпрометированной базы данных, содержащей персональные данные, указанному оператору при выявлении такого инцидента Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций или иным заинтересованным лицом, оператором направляется уведомление, предусмотренное частью 3.1 статьи 21 Федерального закона "О персональных данных".

В указанном случае к дополнительному уведомлению оператором прикладывается акт о проведенном внутреннем расследовании, подтверждающий отсутствие факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, и (или) неустановления принадлежности скомпрометированной базы данных, содержащей персональные данные, соответствующему оператору в деятельности такого оператора.

15.17. В случае установления оператором, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, содержащихся в базе данных, характеристики которых полностью соответствуют ранее скомпрометированной базе данных, оператором направляется уведомление, предусмотренное частью 3.1 статьи 21 Федерального закона "О персональных данных".

В указанном случае при направлении уведомления оператором указывается дата и номер ранее направленного уведомления, содержащего сведения, предусмотренные частью 3.1 статьи 21 Федерального закона "О персональных данных", о ранее скомпрометированной базе данных, содержащей персональные данные.

Директор Г. А. Фуртова