



Администрация Комсомольского муниципального района
Хабаровского края

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ

ПРИКАЗ

18.11.2015 № 825

г. Комсомольск-на-Амуре

Об утверждении правил осуществления
внутреннего контроля соответствия обработки
персональных данных требованиям к защите
персональных данных в управлении образования

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"

ПРИКАЗЫВАЮ:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении образования.

2. Контроль за исполнением данного приказа возложить на Болдыреву Ольгу Сергеевну-главного специалиста, юриста управления образования.

И.о. начальника
управления образования

В.А. Павленко

УТВЕРЖДЕНЫ

приказом

управления образования

от 18.11.15 № 825

Правила

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении образованием

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении образованием (далее - Правила) устанавливаются процедуры (основания, порядок и формы) проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", постановлением Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", постановлением Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами", и другими нормативными правовыми актами.

3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

5. В целях осуществления внутреннего контроля соответствия обработки персональных данных организовывается проведение проверок условий обработки персональных данных.

6. Проверки условий обработки персональных данных могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях управления образования в которых ведется обработка персональных данных

7. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок, утвержденным приказом управления образования.

8. План проведения проверок разрабатывается лицом, ответственным за организацию обработки персональных данных в управлении образования.

9. Внеплановые проверки проводятся на основании поступившего в управление на имя начальника письменного заявления физического лица (субъекта персональных данных) о нарушениях правил обработки персональных данных.

10. В течение трех рабочих дней с момента поступления в управление заявления о нарушениях правил обработки персональных данных принимается решение о проведении внеплановой проверки, которое оформляется приказом управления.

11. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента выхода приказа.

12. При проведении проверок условий обработки персональных данных порядок обработки персональных данных и его соответствие требованиям обработки персональных данных, установленным в управлении должен быть полностью, объективно и всесторонне исследован, а именно:

- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;
- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;
- отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер; мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности персональных данных.

13. В случае выявления фактов:

- несоблюдения установленного порядка обработки персональных данных; несоблюдения условий хранения носителей персональных данных;
- использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциаль-

ность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

- нарушения заданного уровня безопасности персональных данных (конфиденциальность/целостность/доступность);
- в обязательном порядке устанавливаются причины нарушения обработки персональных данных и наличие (отсутствие) вины.

14. Комиссия по персональным данным имеет право:

- запрашивать у сотрудников управления информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

15. В процессе проведения внутреннего контроля (проверок) соответствия обработки персональных данных требованиям к защите персональных данных разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.

16. В случаях выявления нарушений обработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.

17. Плановая проверка должна быть завершена не позднее чем через месяц со дня ее назначения. Заключение о результатах проведенной проверки и принятых по устранению выявленных нарушений мерах, а также мерах, необходимых для устранения нарушений, направляется начальнику за подписью председателя комиссии по персональным данным.

18. Устранение выявленных нарушений проводится не позднее 30 дней с момента завершения проверки.

19. В отношении персональных данных, ставших известными Комиссии по персональным данным в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.
