Муниципальное бюджетное дошкольное образовательное учреждение

Детский сад «Светлячок»

Председатель ПК
Филиала МБДОУ Д/с
«Светлячок»
_____ Н. П. Стаценко

УТВЕРЖДАЮ
Заведующий
МБДОУ Д/с «Светлячок»
_____ И.В. Ильина

Приказ № 5 от 14.01.2019г

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ Д/с «Светлячок»

1. Настоящие правила устанавливают процедуры проведения в МБДОУ Д/с «Светлячок» (далее – ДОУ) внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законодательством о персональных данных.
2. Настоящие Правила разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 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».
3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере защиты персональных данных.
4. Тематика внутреннего контроля.
4.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:
- соответствие полномочий пользователя матрице доступа;
- соблюдение пользователями информационных систем персональных данных парольной политики;
- соблюдение пользователями информационных систем персональных данных антивирусной политики;
- соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;

- соблюдение ответственными за криптографические средства защиты информации правил работы с ними;
- соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- соблюдение порядка работы со средствами защиты информации;
- знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

4.2. Тематика проверок обработки персональных данных без использования средств автоматизации:
- хранение бумажных носителей с персональными данными;
- доступ к бумажным носителям с персональными данными;
- доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

5. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в МБДОУ Д/с «Светлячок» организуется проведение проверок условий обработки персональных данных.

6. Проверки условий обработки персональных данных на соответствие требованиям к защите персональных данных, установленных в ДОУ (далее - проверки) осуществляются ответственным за организацию обработки персональных данных (либо комиссией, образуемой для проведения проверки).

7. Проверки могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях ДОУ, в которых ведется обработка персональных данных.

8. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок, утвержденным приказом ДОУ, но не реже 1 раза в год.

9. План проведения проверок разрабатывается лицом, ответственным за организацию обработки персональных данных в ДОУ.

10. Внеплановые проверки проводятся на основании поступившего в ДОУ письменного заявления физического лица (субъекта персональных данных) о нарушениях правил обработки персональных данных.

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

12. Проведение внеплановой проверки организуется в течение 10 рабочих дней с момента подписания приказа ДОУ о проведении внеплановой проверки.

13. При проведении проверок должен быть полностью, объективно и всесторонне исследован порядок обработки персональных данных и его соответствие требованиям обработки персональных данных, установленным в ДОУ, 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.

14. В случае выявления фактов: несоблюдения установленных правил обработки персональных данных; несоблюдения условий хранения носителей персональных данных; использования 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; нарушения заданного уровня безопасности персональных данных - в обязательном порядке устанавливаются причины нарушения обработки персональных данных и наличие (отсутствие) вины.

15. Лицо, проводящее проверку, имеет право:
- запрашивать у сотрудников ДОУ 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 руководителю ДОУ предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить руководителю ДОУ предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

16. В процессе проведения внутреннего контроля (проверок) соответствия обработки персональных данных требованиям к защите персональных данных разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.
17. В случаях выявления нарушений обработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.
18. Плановая проверка должна быть завершена не позднее чем через месяц со дня её начала.
19. Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении к настоящим Правилам.
20. При выявлении в ходе проверки нарушений, ответственным за организацию обработки персональных данных в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения. Устранение выявленных нарушений проводится не позднее 30 дней со дня подписания Протокола, если в нем не определено иное, о чем письменно сообщается ответственному за организацию обработки персональных данных.
21. Протоколы хранятся у ответственного за организацию обработки персональных данных в течение текущего года.
22. Заключение о результатах проведенной проверки и принятых по устранению выявленных нарушений мерах, а также мерах, необходимых для устранения нарушений, направляется ответственным за организацию обработки персональных данных руководителю ДОУ.
23. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться их конфиденциальность.

Приложение
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ Д/с «Светлячок»

Форма Протокола
проведения внутренней проверки условий обработки персональных данных в МБДОУ Д/с «Светлячок»

Настоящий Протокол составлен в том, что __. __.20__ ответственным за организацию обработки персональных данных / комиссией по внутреннему контролю проведена проверка _____.

тема проверки

Проверка осуществлялась в соответствии с требованиями _____
_____

название документа

В ходе проверки проверено:

_____

_____

_____

_____

_____

Выявленные нарушения:

_____

_____
_____
_____
_____
_____

Меры по устранению нарушений:

_____
_____
_____
_____
_____
_____

Срок устранения нарушений: _____.

_____	_____	_____
(должность ответственного)	(подпись)	(Ф.И.О.)

либо

Председатель комиссии

_____		
(должность)	_____	_____
	(подпись)	(Ф.И.О.)

Члены комиссии:

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)
_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)