	Длъжност	Фамилия	Подпис	Дата
Изготвил	Домакин - касиер	Николова		11.01.2019 г.
Изготвил	Учител ЦДО	Пенчева		11.01.2019 г.
Изготвил	Старши учител прогимназиален етап	Теберова		11.01.2019 г.
Утвърдил	Директор	Петрова-Динева		11.01.2019 г.

В сила от: 11.01.2019 г.	Подлежи на периодична проверка: Да ☒ Срок на периодична проверка: 1 година Не ☐ Срок на действие до: …….…… /дата/	Отговорно лице за документа: …… Даниела Николова Касиер-домакин 11.01.2019 г.

ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА РИСКА ЗА СИГУРНОСТТА НА ДАННИТЕ В ОУ „СВ. СВ.КИРИЛ И МЕТОДИЙ“, С. ДЪБОВО

СТРАНИЦИ: 11 **ПРИЛОЖЕНИЯ: 3**

РАЗРАБОТЕНА: на основание чл. 32, § 2 от Регламент (ЕС) 2016/ 679.

11.01.2019 г.

РЕГИСТРАЦИЯ НА ИЗВЪРШЕНИТЕ ИЗМЕНЕНИЯ В ДОКУМЕНТА

№ и Дата на изменение	**Основание за изменението**	**Изменени, отменени и добавени страници**	**Отговорно лице** /длъжност, фамилия, подпис и дата/

РЕГИСТРАЦИЯ НА ПРОВЕРКИТЕ

№ и дата на проверката	**Заключение**	**Продължен срока на действие до:**	**Отговорно лице** /длъжност, фамилия, подпис и дата/

	Длъжност	Фамилия	Подпис	Дата
Изготвил	Домакин - касиер	Николова		11.01.2019 г.
Изготвил	Учител ЦДО	Пенчева		11.01.2019 г.
Изготвил	Старши учител прогимназиален етап	Теберова		11.01.2019 г.
Утвърдил	Директор	Петрова-Динева		11.01.2019 г.

В сила от: 11.01.2019 г.	Подлежи на периодична проверка: Да ☒ Срок на периодична проверка: 1 година Не ☐ Срок на действие до: …….……. /дата/	Отговорно лице за документа: …… Даниела Николова Касиер-домакин 11.01.2019 г.

С Ъ Д Ъ Р Ж А Н И Е **Стр.**

1. ПРЕДМЕТ И ЦЕЛ НА ОЦЕНКАТА

Настоящата политика внедрява рамката за извършване оценка на риска относно планираните и извършваните дейности по обработка на лични данни на субекти данни от ОУ „Св. св. Кирил и Методий", с. Дъбово като администратор на лични данни, съгласно изискванията на ОРЗД и другите разпоредби за защита на данните на равнище ЕС или национално законодателство.

Същата има за цел да извлече и предложи подходящи мерки за защита на изложените на опасност лични данни, с които да бъдат овладени идентифицираните рискове, а в случай на установен висок риск – да предложи извършване на оценка на въздействието като по този начин се създаде и запази една стойностна политика на ОУ „Св. св. Кирил и Методий", с. Дъбово по отношение на защитата на данните, съгласно изискванията на Регламент (ЕС) 2016/ 679.

2. ТЕРМИНИ И ОПРЕДЕЛЕНИЯ

РИСК – вероятност за влияние на неопределеността върху постигането на целите, както в положителна, така и в отрицателна насока или и в двете, като създава или води до възможност или заплаха.

ЕЛЕМЕНТИ НА РИСКА – вероятността за възникване на риска и тежестта на последиците, които ще настъпят, ако това се случи.

ИЗТОЧНИК НА РИСК – елемент, който самостоятелно или заедно с други, представлява потенциал за възникване на риск.

СЪБИТИЕ – възникване или изменение на дадена конкретна съвкупност от обстоятелства (може да бъде източник на риск).

ОЦЕНКА НА РИСКА – процес на идентифициране на риска, анализ на риска и преценка на риска.

ИДЕНТИФИЦИРАНЕ НА РИСКА – процес на идентифициране, разпознаване и описване на рисковете, които могат да подпомогнат или да попречат на организацията да постигне целите си.

АНАЛИЗ НА РИСКА – включва подробно отчитане на неопределеностите, източниците на риск, последствията, вероятностите, събитията, сценариите, мерките за контрол и тяхната ефикасност.

ПРЕЦЕНКА НА РИСКА - взимане на решение, относно значимостта на риска на база на анализа на риска и установените критерии за риска.

ВЪЗДЕЙСТВИЕ ВЪРХУ РИСКА – формулиране и предлагане на подходящи мерки за въздействие върху риска с цел неговото овладяване и избор на такива.

ПЛАН ЗА ВЪВЕЖДАНЕ НА ПОДХОДЯЩИ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННА МЕРКИ ЗА ЗАЩИТА – приетите мерки, срокове и отговорни лица за предотвратяване, намаляване, ограничаване и контрол на риска и начини на контрол на изпълнението на тези мерки.

3. ОБХВАТ И ПОДХОД ЗА ИЗВЪРШВАНЕ НА ОЦЕНКАТА

3.1. Обхват на оценката.

Оценката на риска обхваща: всички вътрешни и външни фактори, които могат да породят риск за сигурността на данните и по специално тези, които са свързани с обработването на личните данни, по специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработвани по друг начин лични данни. Същите се идентифицират и оценяват по отношение на всички налични потоци от информация в рамките, на които се обработват лични данни в зависимост от прилаганите към тях дейности по обработка, както и по отношение на планираните дейности по обработка.

Съгласно изискванията на чл. 32, § 2 от Регламент (ЕС) 2016/679 се оценяват рисковете, които оказват отрицателно влияние върху защитата на данните. Целта е да се оценят и ограничат при източника на възникване рисковете, които представляват заплаха за сигурността на данните, до едно приемливо ниво за организацията. Предложените от оценителите мерки за защита се съобразяват с променящите се обстоятелства с цел подобряване на съществуващото положение като същите следва да бъдат подходящи с оглед разглеждания риск, ефективни по отношение на разходите, изчерпателни и разумни.

3.2. Подход за извършване на оценката.

Рисковете трябва да се бъдат определени на ниво конкретна обработка или дейност с цел поддържането на едно приемливо за организацията ниво на риск при планиране на дейността на ОУ „Св. св. Кирил и Методий”, с. Дъбово за една календарна година като по този начин се осигури гаранция за ефективен анализ на риска.

За оценка на риска за сигурността на личните данни, които обработва или планира да обработва ОУ „Св. св. Кирил и Методий”, с. Дъбово като администратор, ще бъде използван интеративен подход, тъй като същия осигурява възможност да се задълбочи и детайлизира оценката на риска, което дава гаранция, че високите рискове ще бъдат подходящо оценени,

съгласно изискванията на чл. 35 от Регламент (ЕС) 2016/679. Същият е илюстриран в Приложение 3 към настоящата политика.

4. ОЦЕНКА НА РИСКА

4.1. Събиране на необходимата информация.

Нормативна уредба – нормативни изисквания, насоки и становища относно сигурността на данните:

- Регламент (ЕС) 2016/ 679 (в сила от 24 май 2016 г., прилага се от 25.05.2018 г.)
- Регламент (ЕС) № 611/2013 (в сила от 25 август 2013 г.)
- Конвенция № 108 за защита на лицата при автоматизирана обработка на лични данни от 28.01.1981 г.
- Закон за защита на личните данни (Обн., ДВ, бр. 1 от 4 януари 2002 г.)
- Закон за електронното управление (Обн., ДВ, бр. 46 от 12 юни 2007 г.)
- Закон за електронния документ и електронните удостоверителни услуги (Обн., ДВ, бр. 34 от 06 април 2001 г.)
- Закон за достъп до обществена информация (Обн., ДВ, бр. 55 от 07 юли 2000 г.)
- Закон за училищното и предучилищното образование (Обн., ДВ, бр. 79 от 13 септември 2015 г.)
- Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование (Обн., ДВ, бр. 66 от 23 август 2016 г.)
- Насоките относно оценката на въздействието върху защитата на данните и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент (ЕС) 2016/ 679 на Работната група по чл. 29
- Становище с Рег. № П-5375/2017 от 30.04.2018 г. на КЗЛД по въпроси, касаещи въвеждането на видеонаблюдение в детските заведения (детски ясли и детски градини), както и в училищата
- Становище на КЗЛД с рег. № НДМСПО-17-916/1.11.2018 г. от 21.12.2018 г. относно монтиране на входно-изходни камери за лицево разпознаване, свързани с електронния дневник на училище "Д.И.Б.", гр. П.
- Становище 06/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО

4.2. Идентифициране на опасностите

№	РИСК	ИЗТОЧНИК НА РИСК / СЪБИТИЕ/
1	2	3
1.	Унищожаване	**Преднамерени действия на служител, отговорен за поддържане на съответния регистър по смисъла на ОРЗД**
		Изгаряне на техническия носителя на регистъра при липса на възможност за възстановяване на информацията
		Изгаряне на техническия носител на информацията с възможност за възстановяване на информацията
		Хакване или злонамерен софтуер
2.	Загуба	**Случайно загубване на техническия носител на регистъра, поради нерегламентирано изнасяне на данни от организацията**
		Случайно загубване на техническия носител на регистъра, поради регламентирано изнасяне на данни от организацията
3.	Промяна	**Преднамерено действие на служител, отговорен за поддържане на регистъра**
		Действие на служител, осъществил нерегламентиран достъп до регистъра
		Хакване или злонамерен софтуер
4.	Неправомерно разкриване	**Преднамерено действие на служител, отговорен за поддържането на регистъра**
		Преднамерено действия на служител, осъществил нерегламентиран достъп до регистъра
		Хакване или злонамерен софтуер
		Загубване на техническия носител на регистъра от служител
		Неправилен начин за третиране на документите, съдържащи данни, които подлежат на унищожаване/ заличаване

		и/или изтриване
5.	Неправомерен достъп	**Преднамерено умишлено действие на служител, отговорен за поддържането на регистъра**
		Служител, осъществил нерегламентиран достъп до регистъра
		Случайно осъществяване на достъп до данни, които са разположени на бюрото на служител, приемащ външни лица
		Случайно осъществяване на достъп до данни от външно лице или друг служител, посредством отворен регистър на работния плот на компютъра на служител
		Загубване на техническия носител на регистъра от служител
		Хакване или злонамерен софтуер
		Неправилен начин за третиране на документите, съдържащи данни, които подлежат на унищожаване/ заличаване и/или изтриване

4.3. Анализ на риска.

Анализа на риска за сигурността на данните включва подробно отчитане на източниците на риска, събитията, последствията, вероятността, мерките за контрол и тяхната ефективност, като се взима предвид и броя на засегнатите субекти по отношение на всяка конкретна обработка/ дейност, установени в организацията на ОУ „Св. св. Кирил и Методий”, с. Дъбово, съгласно извършената инвентаризация на потоците от информация в рамките, на които се обработват лични данни, както и по отношение на всяка планирана нова дейност по обработка.

Методика за оценка на риска

За всеки идентифициран източник на риск свързан с обработката на лични данни след анализ на елементите формиращи източника на риск и видовете дейности по обработка, които се планират или извършват спрямо всеки регистър – настоящ или съществуващ, се определят източниците на риск и изложените на риска регистри.

Значимостта на риска се оценява като се определя вероятността източника на риска да стане реално събитие, броя на засегнатите субекти и възможния обхват на последствията върху субектите на данни при отчитане характера на обработваните данни в рамките на регистъра. Използвания метод за оценка на риска е Матрица с предварително зададени стойности, като са определени елементите на риска - вероятност (В); брой засегнати субекти (Б); последици (вреда) (П):

	Вероятност за реализация на източника на риск (събитието)	Малко			Средна			Голяма		
	Последици	**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
Брой на засегнатите субекти	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Елементите на риска се определят по следния начин:

Вероятност (В)	Характеристика
Малка	Възможни са рискови ситуации, но са въведени подходящи технически и организационни мерки и се спазват, персонала е обучен и е с подходяща квалификация
Средна	Недостатъчна квалификация на персонала и/или пропуски във взетите мерки за контрол на риска
Голяма	Неквалифициран и необучен персонал и/или няма взети мерки и не се контролира източника на опасност.

Брой засегнати субекти (Б)	Стойност
Незначителен (по-малко от 10 лица)	0
Нисък (от 11 до 1 000 лица)	1
Висок (от 1001 до 10 000 лица)	2
Много висок (от 10 0001 до 100 000 лица)	3
Изключително висок (повече от 1 000 000 лица)	4

Тежестта на вредата (последицата) **(П)** се преценява съобразно характера на съдържащите се лични данни в регистъра, подлежащи на защита, и обхвата на възможните последици за субектите на данни.

Последствия (П)	Характеристика
Ниски	В случаите, когато нарушението на сигурността на личните данни би довело до необосновано навлизане в личния живот на субектите на данни и/или би застрашило неприкосновеността им
Средни	В случаите, когато нарушението на сигурността на личните данни би могло да доведе до засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философки, политически или синдикални цели, здравословно състояние, сексуалния живот или човешкия геном
Високи	В случаите, когато нарушението на сигурността на личните данни би могло да доведе до възникване на значителни вреди или кражба на самоличност или трайни здравословни увреждания или смърт

Стойността на риска се определя от цифрата посочена в пресечната клетка след определяне на реда отговарящ на броя субекти, както и на вероятността и последствията или

ако за броя на засегнатите субекти е определена стойност 3, за вероятност „висока“ и за последствия „ниски“, тогава в пресечната клетка на реда на броя засегнати субекти, вероятността и последствията намираме стойност на риска 5.

Класацията на риска се извършва по следната скала:

- Нисък риск – 0 - 2
- Среден риск – 3 - 5
- Висок риск – 6 – 8

Допустимост на **Р**иска за сигурността на данните:

Стойност на риска	Степен	Риск (Р)
0-2	**1**	Допустим – неголям риск, необходимо е внимание
3-5	**2**	Умерен - неголям риск, необходими са технически и организационни мерки за защита
6-8	**3**	Висок - необходими е оценка на въздействието

Крайният резултат, от оценката на риска установява допустимостта на установения риск и необходимостта от прилагане на мерки за неговото предотвратяване/ намаляване до едно приемливо за организацията ниво (превантивни и/или коригиращи) или извършване на оценка на въздействието върху сигурността на данните.

Вземане на решение за планиране и прилагане на мерки:

- При степен 1 - Приемлив, не са необходими мерки;
- При степен 2 - Необходимо внимание, предлагат се превантивни и/или коригиращи мерки;
- При степен 3 – Извършва се оценка на въздействието върху сигурността на данните;

Забележка!

Ако не са спазени законовите изисквания по отношение на регистъра, рискът е неприемлив! – Проверката се прави с Карта за оценка на съответствието с нормативните изисквания по ОРЗД.

4.4. Планиране на действия за елиминиране или намаляване на риска

Решение за предприемане на действия (мерки) по отстраняване или намаляване на риска се вземат в зависимост от оценената стойност (степен) на риск и възможностите на организацията,

като е допустимо един риск да бъде ограничаван с няколко мерки и обратното една мярка да въздейства върху няколко риска.

Възможните предложения за решения за въздействие върху риска (мерки) могат да бъдат такива, които водят до:

- избягване на риска чрез решение да не се започва или продължава дейността по обработка, за която е налице риска;
- редуциране на риска;
- прехвърляне на риска;
- запазване на риска въз основа на аргументирано решение.

Препоръчаните от оценителите мерки се внасят за запознаване и обсъждане с Директора на ОУ „Св. св. Кирил и Методий”, с. Дъбово и на база проведеното обсъждане се изготвя Плана за въвеждане на подходящи технически и организационни мерки за защита.

Сроковете за изпълнение на планираните мероприятия за елиминиране или ограничаване на риска и отговорниците, се определят от Директора на ОУ „Св. св. Кирил и Методий”, с. Дъбово след разглеждане и приемане Плана за въвеждане на подходящи технически и организационни мерки за защита.

4.5. Документиране и съхранение на оценката на риска. Условия за преразглеждане. Приложения.

4.5.1. Документиране и съхранение

Документацията по оценката на риска включва настоящата политика, Процедурата за оценка на риска и всички образци на документи към нея, включително и резултатите от оценката с предложените и одобрени мерки за въздействие със сроковете за тяхното изпълнение, както и Процедура за оценка на риска на етапа на проектирането и всички образци към нея, включително и резултатите от оценката с предложените и одобрени мерки за въздействие със сроковете за тяхното изпълнение. Тя се съхранява в папка като част от класьор „Лични данни“ на ОУ „Св. св. Кирил и Методий”, с. Дъбово със срок за съхранение постоянен. Контролирани копия се предоставят на отговорните лица за изпълнението на планираните мерки.

4.5.2. Условия за преразглеждане

Оценката на риска се преразглежда веднъж годишно по нареждане на Директора на ОУ „Св. св. Кирил и Методий”, с. Дъбово.

В случай, че в този период се установи:

- промяна, която може да окаже влияние върху риска;
- промяна в нормативната уредба;
- че оценката е направена при данни и информация, станали невалидни или неподходящи;
- че има условия оценката да бъде подобрена;
- че прилаганите мерки са неефективни или неадекватни;
- по предписание на контролни органи

оценката на риска се преразглежда по нареждане на Директора на ОУ „Св. св. Кирил и Методий”, с. Дъбово преди изтичане на едногодишния срок.

4.5.3. Приложения

- Процедура за извършване на оценка на риска за сигурността на данните в ОУ „Св. св. Кирил и Методий”, с. Дъбово (Приложение 1)
- Процедура за извършване на оценка на риска за сигурността на данните на етапа на проектирането в ОУ „Св. св. Кирил и Методий”, с. Дъбово (Приложение 2)
- Подход за оценка на риска (Приложение 3)