ОЦЕНКА НА РИСКА

ЗА СИГУРНОСТТА НА ДАННИТЕ,

СЪГЛАСНО ИЗИСКВАНИЯТА НА

РЕГЛАМЕНТ (ЕС) 2016/ 679

Основно училище „Св. св. Кирил и Методий“,
с. Дъбово

2019 г.

ОСНОВНО УЧИЛИЩЕ „СВ.СВ. КИРИЛ И МЕТОДИЙ”

🖂 С. ДЪБОВО, ОБЩ. МЪГЛИЖ УЛ. СЛАВЯНСКА № 36 Б ТЕЛ: 04333/23-61 E-MAIL: OUDABOVO@ABV.BG

Идентифициране на източниците на риск за установените регистри, съгласно видовете дейности по обработка, прилагани към тях, в ОУ «Св. Св. Кирил и Методий», с. Дъбово

В ОУ «Св. св. Кирил и Методий», с. Дъбово се обучават ученици от 7 до 14-годишна възраст. В процеса по осигуряване на обучение учебното заведение обработва техните данни, данни на техните родители, лични лекари и др., както и данни на своите работници/ служители, изпълнители по договор и т.н.

След извършена инвентаризация на потоците на информация в рамките, на които се обработват лични данни, е установен обхвата на наличните регистри по смисъла на ОРЗД в ОУ «Св. св. Кирил и Методий», с. Дъбово.

Източниците на риск за регистрите

№	Регистър	Източници на риск
1.		
2.		
3.		
	…	

Източници на информация

- Политика за управление на риска за сигурността на данните в ОУ «Св. св. Кирил и Методий», с. Дъбово
- Заповед № 182/ 14.11.2018 г. за утвърждаване на наличните регистри в организацията
- Резултатите от Процедурата за първоначален вътрешен анализ на оценка на съответствието с изискванията на Регламент (ЕС) 2016/ 679 на установените в организацията регистри
- Листи от проведени интервюта за установяване на прилаганите технически и организационни мерки за защита към установените регистри

Оценката на риска за сигурността на данните е извършена при спазване на Политиката за управление на риска за сигурността на данните в ОУ «Св. св. Кирил и Методий», с. Дъбово по следната методика:

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)	Малка			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, философски, 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.

Оценката на риска за сигурността на данните е представена в оценителен лист за всеки регистър, съгласно образеца към Процедурата за извършване на оценка на риска за сигурността на данните в ОУ «Св. св. Кирил и Методий», с. Дъбово като в него са отразени и предложените мерки за въздействие при спазване на следните приоритети:

1.) За рисковете от трета степен следва да бъде извършена ОВЗД като те следва да бъдат напълно избегнати или редуцирани до едно приемливо за организацията ниво чрез прилагане на мерки за сигурност, които намаляват както тежестта им, така и тяхната вероятност. Към тях следва да бъдат приложени мерки, както за предотвратяване, така и за защита (действия, предприети по време на нарушението на сигурността) и възстановяване.
2.) Към рисковете с висока тежест, но с малка вероятност за настъпване от средна степен следва да се прилагат мерки за сигурност, които намаляват тежестта на последиците или вероятността за настъпването им, като приоритет следва да имат превантивните мерки (тези за предотвратяване).
3.) Към рисковете с ниска тежест на последствията, но голяма вероятност за настъпване от средна степен следва да се прилагат мерки за сигурност, които намаляват тяхната вероятност. Следва да се наблегне и на мерки за възстановяване.
4.) Към рисковете от първа степен не следва да се прилагам мерки за защита към настоящия момент, тъй като третирането на другите рискове може да окаже положително влияние и върху тях, затова те ще бъдат третирани на по-късен етап, освен ако по отношение на тях не е налице несъответствие със законовите изисквания (тогава е необходимо прилагането на мерки за въздействие в зависимост от установеното несъответствие).

Допустимостта на риска е установена, съгласно критериите, установени в Политиката за управление на риска за сигурността на данните в ОУ «Св. св. Кирил и Методий», с. Дъбово.

Приложени са оценителни листи за всеки регистър.