

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

2021 – 2022 година

ПОЛИТИКА
ЗА
ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

2021 – 2022 ГОДИНА

1. ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Администратор	**ОУ „Св. Иван Рилски**
Адрес	**с. Кошарица ул."23-ти септември" № 36**
E-mail	**kosarica@abv.bg**
Телефон	**0556 6 10 97**

Раздел I.

Цел

1. Настоящият документ предоставя общ преглед на изискванията за защита на данните и насочва към по-подробни указания, ако е необходимо.

2. Въпроси относно политиката могат да бъдат отправяни на e-mail адрес на образователната институция: ОУ“ Св. Иван Рилски“, с. Кошарица.

Раздел II.

Основания

3. Общият регламент за защита на данните (ОРЗД), който е директно приложим в законодателството на България и може да е/е допълнен чрез Закона за защита на личните данните (ЗЗЛД) и други нормативни актове, установява рамка от права и задължения, предназначени да защитават личните данни. В настоящата политика към тях се реферира като "законодателство за защита на данните".

4. Принципите са следните:

- 4.1. Личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин.
- 4.2. Личните данни, събирани за конкретни, изрично указани и легитимни цели, не се обработват по-нататък по начин, несъвместим с тези цели.
- 4.3. Личните данни следва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“).
- 4.4. Личните данни следва да са точни и при необходимост да бъдат поддържани в актуален вид („точност“).
- 4.5. Личните данни следва да са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни („ограничение на съхранението“).
- 4.6. Прилагат се подходящи технически или организационни мерки срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане („цялостност и поверителност“).

5. ОРЗД задава определени права на субектите на данни, свързани с техните лични данни, които са:

- право на достъп;
- право на коригиране;
- право на изтриване (при определени обстоятелства) – правото „да бъдеш забравен“;
- правото за ограничаване на обработването;
- право на преносимост (при определени обстоятелства);
- правото за възражение, включително срещу директен маркетинг;
- правото да се изисква човешка намеса с оглед на автоматизирани процеси, включително профилиране.

6. Условията, при които личните данни могат да бъдат прехвърлени в страни извън Европейското икономическо пространство, са определени в ОРЗД. Те включват адекватност, подходящи гаранции, обвързващи корпоративни договори и изрично съгласие, наред с другите.

7. Дефиниране на „лични данни“ и „специални категории лични данни“ (чувствителни данни), съгласно ОРЗД:

- „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната,

психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

- „специални категории лични данни“ са лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице;

8. Всяка обработка на лични данни следва да почива на поне едно законово основание, съгласно ОРЗД. Възможните основания са (чл. 6 от ОРЗД): договор, законово задължение, жизненоважни интерес, обществен интерес, легитимен интерес и съгласие. Данните за специалните категории изискват по-специално законово основание (чл. 9 от ОРЗД). Тази законова основа се посочва в Регистър на дейностите по обработването. Служител, който не е сигурен какво правно основание се отнася до личните данни, които възнамерява да обработва, трябва да потърси съвет от Длъжностното лице по защита на личните данни.

Раздел III.

Политика и насоки

9. ОУ“ Св. Иван Рилски“, с. Кошарица се ангажира с политика за защита на правата и свободите на лицата по отношение на обработката на техните лични данни.

10. Настоящата Политика и допълнителните насоки към нея, се отнасят за всички лични данни, обработвани за целите на институцията, независимо от това къде и как се съхраняват.

Раздел IV.

Приложение на политиката

11. ОУ“ Св. Иван Рилски“, с. Кошарица обработва лична информация за служители, ученици, родители, и други, определени като субекти на данни в законодателството за защита на данните. Тези данни трябва да се обработват само в съответствие със законодателството за защита на данните, което е и цел на настоящата политика.

12. Всяко нарушение на тази Политика може да доведе до това институцията като администратор на данни (и в някои случаи физическите лица, работещи за нея) да наруши законодателството за защита на данните и да носи отговорност за последиците от такова нарушение.

13. Ръководителите в институцията отговарят за това тя да спазва законодателството за защита на данните. Всички служители трябва да са прочели и разбрали тази политика преди да имат достъп до лични на данни, обработвани от институцията. Отговорност на всички ползватели на лични данни в институцията е да гарантира сигурността на личните данни. Личните данни не трябва да се разкриват на никое неупълномощено лице под каквато и да е форма, случайно или по друг начин.

14. Всяко нарушение или неспазване на настоящата Политика, особено всяко преднамерено разкриване на лични данни на неупълномощена страна, може да доведе до дисциплинарни или други подходящи действия.

15. Институцията периодично проверява спазването на законодателството за защита на данните и политиката и при необходимост актуализира своите насоки в тази област.

16. Всеки неоторизиран достъп до или разкриване на лични данни или други нарушения на сигурността на данните трябва да бъде докладван съгласно Инструкция за действие при пробив в сигурността на личните данни веднага след установяването им или при наличието на основателно подозрение за настъпило нарушение.

17. Заместник-директорът по учебната дейност, отговаря за това всички служители в институцията да бъдат информирани за задълженията си съгласно законодателството за защита на данните, включително тяхното обучение и инструктаж. Съвети и подкрепа във връзка със законодателството за защита на данните се предоставят от определения служител за защита на личните данни (СЗД) или назначеното длъжностно лице за защита на личните данни (ДЗЛД).

18. ДЗЛД докладва на ръководството на институцията (директор).

Раздел V.

Достъп до данни

19. Правото на достъп от страна на субектите на данни следва да се реализира в определен срок от 30 дни. Поради това от съществено значение е предоставяне на исканията за достъп до данни към СЗД/ДЛЗД във възможно най-кратък срок след тяхното получаване, независимо от това, по какъв начин точно е постъпило искането в институцията и до кого е било подадено.

Раздел VI.

Съхраняване на данни

20. Личните данни се съхраняват само за времето, необходимо за извършване на обработката, за която са събрани. Това важи както за електронни, така и за не електронни лични данни. Това се разпростира също така и върху резервните копия и копията, направени на преносими носители.

Раздел VII.

Трансфер на данни 2

1. Всеки трансфер на данни, включително използването на облачни услуги, извън ЕИП следва да бъде предварително съгласуван със СЗД/ДЛЗД с оглед изискването в ОРЗД за предприемането на определени мерки.

Раздел VIII.

Регистър на дейностите по обработването

22. Регистърът на дейностите по обработването се използва, за да се отговори на изискванията за съхранение на данни в законодателството за защита на данните (Приложение I).

23. Отговарящите за отделните организационни и оперативни дейности, които формират целите на обработваната информация, осигурят създаването и поддържането на актуалността на информацията в регистъра.

24. Всяка година те извършват преглед на актуалността.

25. ДЗЛД гарантира, че притежателите на информационни активи получават подходяща помощ за поддържане на регистъра.

Раздел IX.

Технически и организационни мерки за защита на данните

26. Институцията въвежда подходящи технически и организационни мерки (ТОМ), за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с ОРЗД, като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица.

27. Техническите и организационните мерки следва да допринесат за защита на данните на етапа на проектирането и по подразбиране. Същите са посочени в Инструкция за техническите и организационни мерки на институцията във връзка с обработването на лични данни.

28. В техническите и организационните мерки институцията изрично предвижда минимално необходимите реквизити при сключване на споразумения с обработващи данни, така че да се постигне ниво на защита не по-ниско от прилаганото от самата институция.

Раздел X.

Съответствие, свеждане до знание и дисциплинарни процедури

29. Нарушаването на поверителността на личните данни е и нарушение на законодателството за защита на данните и може да доведе до наказателен или граждански иск срещу институцията. Следователно всички обработващи лични данни в институцията трябва да се придържат към политиката за защита на личните данни и политиките, които допринасят за нейното изпълнение.

30. Всички настоящи служители и други упълномощени потребители биват информирани за наличието на тази политика и наличието на съпътстващи политики, процедури, инструкции и насоки.

31. Всички служители подписват Декларация за поверителност (Приложение II).

32. Всяко нарушение на сигурността ще бъде разгледано в съответствие с правила на институцията и съответните дисциплинарни политики.

Приложения

№	Наименование на приложението
1.	**Приложение I: 1. Регистър на дейности по обработване на лични данни (администратор) 2. Регистър на категории дейности по обработването (обобщаващ)**
2.	**Приложение II 1. Регистър на лицата, обработващи лични данни 2. Списък на лица, които обработват лични данни**
3.	**Приложение II: Декларация за поверителност на данните**