

# ОСНОВНО УЧИЛИЩЕ „ОТЕЦ ПАИСИЙ“,с. БАТОВО

УТВЪРДИЛ:  
ДИРЕКТОР ОУ  
ВАНЯ КОСТОВА



## ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ

## **I. ОБЩИ ПОЛОЖЕНИЯ**

**Чл. 1.** Настоящите вътрешни правила са изготвени в съответствие със Закона за защита на личните данни и Регламент (ЕС) 2016/679 и имат за цел да регламентират:

- механизмите на водене, поддържане и защита на лични данни в ОУ „Отец Паисий“ като администратор и обработващ лични данни във връзка с осъществяването на образователната си дейност;
- задълженията на оправомощените лица, обработващи лични данни и тяхната отговорност при неизпълнение на тези задължения;
- необходимите технически и организационни мерки за защита личните данни от неправомерно обработване;

## **II. ОБРАБОТВАНЕ И СЪХРАНЯВАНЕ НА ЛИЧНИ ДАННИ.**

**Чл. 2.** (1) Личните данни се събират и съхраняват в Регистър с оглед законосъобразно:

- обработване на данни за целите на дейността на училището;
- администриране на трудовите правоотношения със служители в училището;
- уреждане на всички други правоотношения с контрагенти и партньори на училището;

(2) Регистърът събира и съхранява лични данни на: учениците, служителите, кандидати за работа, контрагенти, както и други физически лица, с които училището влиза в отношения при осъществяването на правомощията и дейността си, с цел изпълнение на задълженията си по българското и европейското законодателство.

**Чл. 3.** (1) Регистърът за лични данни съдържа данни относно физическата идентичност на лицата – образование, трудова дейност, медицински данни и други лични данни необходими за дейността на училището.

(2) Начини на водене на регистъра за лични данни в училище:

1. На хартиен носител:

- личните данни са в писмена (документална) форма подадени на оправомощеното лице, обработващо лични данни, на основание нормативно задължение;
- съхраняване на личните данни в шкафове с достъп само за служители оторизирани за обработване на лични данни, помещаващи се в специални помещения снабдени със СОТ;

## 2. На технически (електронен) носител:

- личните данни се съхраняват на външен електронен носител или специално подготвен за тази цел компютър, разположени в помещения с контролиран достъп;
- достъп до личните данни на електронен носител имат само обработващите лични данни;

**Чл. 4.** Задълженията на лицата, обработващи данните в регистъра включват набиране, обработване, актуализация и съхраняване на лични данни. Със заповед на директора се определя длъжностно лице по защита на личните данни в училището.

**Чл. 5.** (1) Актуализация на лични данни е допълнение или изменение на съществуваща информация в регистъра. Актуализация се извършва:

- по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице непълнота или промяна в тях и удостовери това с документ;
- по инициатива на обработващия лични данни - при наличие на документ, даващ основание за актуализация;

**Чл. 6.** Архивиране на личните данни на технически носител (външни електронни носители, сървъри) се извършва периодично от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид. Документите в хартиен вид се съхраняват в специално помещение, определено за архив и снабдено със СОТ.

## III. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ

**Чл. 7.** (1) Правилата за защита при обработване на лични данни регламентират техническите мерки за:

- ограничаване достъпа до информационни носители на лични данни на неоторизирани лица;
- предотвратяване на неоторизирано добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни - контрол по съхраняването;
- гарантиране, че лицата, които са оторизирани да ползват система за обработка на данни и имат достъп само до данните, включени в обхвата на техния достъп;
- осигуряване възможност за последваща проверка и установяване какви

лични данни са въведени в системите за обработка на данни, кога и от кого са въведени данните;

- предотвратяване на неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или пренасяне на носители на данни;
- поддържане на архивен софтуер, който може да възстановява информация в случаи на прекъсване на функционирането;
- осигуряване правилното функциониране на системата, докладване при поява на грешки във функциите с цел обезпечаване на съхранените данни;

(2) Служителите, обработващи лични данни, вземат мерки за гарантиране на надеждността при обработване, като осъществяват техническа и организационна защита на личните данни.

(3) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(4) При внедряване на нов програмен продукт за обработване на лични данни се извършва предварителна проверка на възможностите на продукта с оглед спазване изискванията на ЗЗЛД и Регламент (ЕС) 2016/679 и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(5) Освен на обработващите лични данни, правомерен достъп имат и директора на училището или посочен, назначен или упълномощен от него служител, както и заместник-директорите, класните ръководители, техническият секретар с оглед изпълнение на трудовите им задължения.

**Чл. 8.** (1) Никое трето лице няма право на достъп до регистъра с лични данни, освен ако е изисквано по надлежен път от органи на надзора или на съдебната власт. Достъпът на тези органи до личните данни на лицата е правомерен.

(2) Не се изисква съгласие на лицето, ако обработването на техните лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни.

(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до

трудовете досиета на персонала.

**Чл. 9.** За неизпълнение на задълженията, вменени на съответните оправомощени лица в тези правила по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган — предвиденото в ЗЗЛД административно наказание.

#### **IV. ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ**

**Чл. 10.** (1) Заетите по трудови и граждански правоотношения, както и физическите лица имат право на достъп до личните си данни, за което подават писмено заявление до обработващия лични данни, в това число и по електронен път - лично или чрез упълномощено лице.

(2) Заявлението, което се завежда във входящия регистър за кореспонденция на училището, съдържа име на лицето и други данни, които го идентифицират – ЕГН, длъжност, месторабота, описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес на кореспонденцията и пълномощно, ако заявлението се подава от упълномощено лице.

(3) Достъп до данните на лицето се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице или упълномощено от него такова;
4. предоставяне на копие от исканата информация;

(4) При подаване на искане за осигуряване на достъп, представляващият администратора разглежда заявлението за достъп или разпорежда на обработващия лични данни да осигури искания от лицето достъп в предпочитаната от заявителя форма.

(5) Срокът за разглеждане на заявлението и произнасяне по него е 14-дневен от деня на подаване на искането, съответно 30-дневен, когато е необходимо повече време за събиране на личните данни на лицето с оглед възможни затруднения в дейността на администратора.

(6) Решението се съобщава писмено на заявителя лично срещу подпис или по пощата с обратна разписка. Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение. Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмото орган и срок.

## **V. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

§ 1. За всички неуредени в настоящите вътрешни правила въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни и действащото приложимо законодателство на Република България.