СУ "ДИМИТЪР ТАЛЕВ" – ГРАД ДОБРИЧ

ул. "Ген. Георги Попов" № 16; тел.: 690 390
e-mail: *dtalev@mail.bg*; web: http://www.sou-dtalev.info

Утвърждавам:
Директор: Весела Панчева

ВЪТРЕШНИ ПРАВИЛА
ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ В СРЕДНО УЧИЛИЩЕ „ДИМИТЪР ТАЛЕВ" ГРАД ДОБРИЧ

I. ОБЩИ ПОЛОЖЕНИЯ

1. С тези вътрешни правила се урежда организацията и вътрешния ред на Средно училище „Димитър Талев", като администратор на лични данни, както и нивото на технически и организационни мерки при обработване на лични данни и допустимия вид защита.
2. Настоящите правила се издават на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД).
3. Администраторът предоставя достъп до обработваните от него лични данни на физическите лица и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

II. ЦЕЛИ И ОБХВАТ НА ПРАВИЛАТА

1. Настоящите Правила регламентират:

- механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни в Средно училище „Димитър Талев" с цел гарантиране на неприкосновеността на личността и личния живот;
- задълженията на Администратора, лицата обработващи лични данни, длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;
- видовете регистри и механизмите за тяхното водене, поддържане и защита на съхраняваните лични данни;
- необходимите технически и организационни мерки за адекватна защита на личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни). Тя включва:
  - ✓ Физическа защита;
  - ✓ Персонална защита;
  - ✓ Документална защита;
  - ✓ Защита на автоматизирани информационни системи и/или мрежи;
- процедури за докладване, управляване и реагиране при инциденти. Организацията и реда за упражняване на контрол при обработването на лични данни от служителите на СУ „Димитър Талев".

2. СУ „Димитър Талев" обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им.
3. Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.
4. Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на СУ „Димитър Талев" и/или нормалното му функциониране.
5. Събирането, обработването и съхраняването на лични данни в регистрите на СУ „Димитър Талев" се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразено с посочените мерки за защита и нивото на въздействие на съответния регистър.
6. За обработването на лични данни извън необходимите за изпълнение на нормативно установено задължение на администратора, физическите лица, чиито лични данни се обработват, подписват декларация за съгласие. ***Приложение № 12-17***

6.1. Предоставя информация за ученици и родители (*съгласно чл.13 от ОРЗД*) ***Приложение № 18***

7. Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

7.1. Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на СУ „Димитър Талев".

7.2. Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение

на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.
8. Документите и преписките, по които работата е приключила, се архивират.
8.1. Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.
8.2. Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд по действащата Номенклатура на делата на СУ „Димитър Талев“.
8.3. Документите на електронен носител се съхраняват на специализирани компютърни системи.
8.4. Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица.
9. При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на прекия си ръководител, който от своя страна е длъжен, своевременно да информира ръководството на СУ „Димитър Талев“.
10. Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е било докладвано, последствията от него и мерките за отстраняването му.
11. След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от СУ „Димитър Талев“ регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни. При промени в структурата на училището, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.
12. В случаите, когато се налага унищожаване на носител на лични данни, СУ „Димитър Талев“ прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване и злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване/изгаряне.
12.1. Унищожаване се осъществява от служителя, отговорен за архива на СУ „Димитър Талев“
13. Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство и след тяхното легитимиране.
13.1. Информацията може да бъде предоставена под формата на:
- устна справка;
- писмена справка;
- преглед на данните от самото лице;
- предоставяне на исканата информация на технически и/или електронен носител.

14. Правилата са задължителни за всички лица имащи достъп до личните данни, обработвани за нуждите на администратора.

III. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

1. Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.
2. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.
3. При оценката на въздействието администраторът отчита характера на обработваните лични данни, както следва:
- ✓ систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение и др.
- ✓ данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;
- ✓ лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;
- ✓ лични данни в широкомащабни регистри на лични данни;
- ✓ данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

IV. НИВА НА ВЪЗДЕЙСТВИЕ

1. Определят се следните нива на въздействие:

✓ „Изключително високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

✓ „Високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

✓ „Средно” – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от 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, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

✓ Ниско” – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

2. Администраторът извършва оценка на въздействие за всички поддържани регистри .

3. Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

4. Най-високото ниво на въздействие, определено по всеки от критериите определя нивото на въздействие на съответния регистър.

5. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

6. Нивата на защита са според нива на въздействие - ниско, средно, високо и изключително високо.

V. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ В СРЕДНО УЧИЛИЩЕ „ДИМИТЪР ТАЛЕВ“ ГРАД ДОБРИЧ И ТЯХНОТО УПРАВЛЕНИЕ:

1. Поддържаните от СУ „Димитър Талев“ регистри са:

- Обучаеми - ***Приложение № 1***
- Родители - ***Приложение № 2***
- Персонал - ***Приложение № 3***
- Пропускателен режим - ***Приложение № 4***
- Видеонаблюдение - ***Приложение № 5***

Заповеди на директора за определяне на длъжностите - ***Приложение № 6***

2. В **регистър „Обучаеми“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „обучаеми“, обучавани в СУ „Димитър Талев“.

2.1. Общо описание на регистър „Обучаеми“

- Регистърът съдържа следните категории лични данни:
  - ✓ физическата идентичност –име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка;
  - ✓ културна идентичност – интереси и хоби;
  - ✓ социална идентичност – образование;
  - ✓ семейна идентичност – родствени връзки;
  - ✓ лични данни, които се отнасят до здравето.

2.2. Технологично описание на регистър „Обучаеми“:

- носители на данни:
  - ✓ на хартиен носител. Информацията за всеки ученик, се записва предвидените за това регистри със задължителни реквизити съгласно законите и Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.
  - ✓ на технически носител: Личните данни се въвеждат в специализирана Информационна система за администрацията на СУ „Д. Талев“. Базата данни се намира на твърдия диск на изолирани компютри.
- срок на съхранение: съгласно нормативната уредба в СУ „Димитър Талев“;

2.3. Определяне на длъжностите:

Обработващи лични данни на регистър „Обучаеми“ са: зам.-директори, ЗАС, класни ръководители, касиер - домакин и РН ИКТ .

Оператор на лични данни на регистър „Обучаеми“ са всички педагогически специалисти. Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

2.4. Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- поверителност – ниско ниво;
- цялостност – ниско ниво;
- наличност – ниско ниво;
- общо за регистъра – ниско ниво.

2.5. Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните

им задължения (на база заключващи системи). Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.
Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.
Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.
2.6. СУ „Димитър Талев“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:
- защита при аварии, независещи от училището – предприемат се конкретни действия в зависимост от конкретната ситуация;
- защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
- защита от наводнения – предприемат се действия по ограничаване на разпространението, както и се изпомпва водата или загребва със собствени подръчни средства.

2.7. Достъп до регистър „Обучаеми“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.
Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.
2.8. Лични данни на обучаемите се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно действащата номенклатура на делата на база нормативната уредба със сроковете за тяхното съхранение.
2.9. След постигане целите по предходната алинея личните данни на обучаемите се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.
3. В **регистър „Родители“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.
3.1. Общо описание на регистър „Родители“.
- Регистърът съдържа следните групи данни:
  - ✓ физическата идентичност – име, ЕГН, адрес, телефони за връзка и месторабота;
  - ✓ икономическа идентичност – финансово състояние;
  - ✓ социална идентичност – образование, трудова дейност;
  - ✓ семейна идентичност – семейно положение и родствени връзки.

3.2. Технологично описание на регистър„Родители“: - носители на данни:
- На хартиен носител: Данните се набират в писмена (документална) форма и се класират в папки. Папките се съхраняват в заключващи се помещения на операторите на лични данни. Информацията се записва предвидените за това регистри със задължителни реквизити съгласно законите и Наредба № 8 от 11.08.2016г. за информацията и документите за системата на предучилищното и училищното образование.
- На технически носител: Личните данни се въвеждат в специализирана Информационна система за администрацията на СУ „Димитър Талев“. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно нормативната уредба в СУ „Д. Талев“ със срокове на съхранение;

3.3. Определяне на длъжностите:
Обработващи лични данни на регистър „Родители“ са: ЗД, ЗАС, класни ръководители, касиер – домакин.
Оператор на лични данни на регистър „Родители“ е целия педагогически персонал. Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.
3.4. Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
- поверителност – ниско ниво;
- цялостност – ниско ниво;
- наличност – ниско ниво;
- общо за регистъра – ниско ниво.

3.5. Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли,

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Защитата на електронните данни от неправомерен достъп се осъществява посредством
поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

3.6. СУ „Д. Талев“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

- защита при аварии, независещи от училището – предприемат се конкретни действия в зависимост от конкретната ситуация;
- защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомване на съответните органи ;
- защита от наводнения – предприемат се действия по ограничаване на разпространението, както и се изпомпва водата или загребва със собствени подръчни средства.

3.7. Достъп до регистър „Родители“ имат и държавните органи – МОН, РИО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

3.8. Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за съхранение в СУ „Д. Талев“

3.9. След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

4. В **регистър „Персонал“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

4.1. Общо описание на регистър „Персонал“

- Регистърът съдържа следните групи данни:
  - ✓ физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение,
  - ✓ телефони за връзка и банкови сметки;
  - ✓ психологическа идентичност – документи относно психическото здраве;
  - ✓ социална идентичност - образование и трудова дейност;
  - ✓ семейна идентичност - семейно положение и родствени връзки;
  - ✓ лични данни, които се отнасят до здравето;
  - ✓ други - лични данни относно гражданско-правния статус на лицата.
- Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право. Предназначението на събираните данни в регистъра е свързано с:
  - ✓ Индивидуализиране на трудовите правоотношения;
  - ✓ Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
  - ✓ Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.
  - ✓ Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

4.2. Технологично описание на регистър „Персонал“:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на операторите на лични данни .
- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма , счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно нормативната уредба със срокове на съхранение в СУ „Д. Талев“.

4.3. Определяне на длъжностите:

- Обработващи лични данни на регистър „Персонал“ са: ЗДАСД, гл.счетоводител, ЗАС
- Оператор на лични данни на регистър „Персонал“ е ЗДУД , касиер - домакин

4.4. Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- поверителност – ниско ниво;
- цялостност – ниско ниво;

- наличност – ниско ниво;
- общо за регистъра – ниско ниво.

4.5. Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Трудовите досиета на персонала не се изнасят извън сградата на училището. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър (Автоматизираната обработка на данните в СУ „Д. Талев“ се осъществява посредством счетоводна програма TERESA).

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

4.6. СУ „Димитър Талев“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

- защита при аварии, независещи от училището – предприемат се конкретни действия в зависимост от конкретната ситуация;
- защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
- защита от наводнения – предприемат се действия по ограничаване на разпространението както и се изпомпва водата или загребва със собствени подръчни средства.

4.7. Достъп до регистър „Персонал“ имат и държавните органи – НАП, НОИ, МОН,РУО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

4.8. Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в училище.

4.9. След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

5. В **регистър „Пропускателен режим“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.

5.1. Общо описание на регистър „Пропускателен режим“

- Регистърът съдържа следните групи данни - физическата идентичност: име по лична карта.

5.2. Технологично описание на регистър „Пропускателен режим“: Данните се набират в писмена форма в дневник.

5.3. Определяне на длъжностите:

Оператори на лични данни на регистър „Пропускателен режим“ са охранителите.

5.4. Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- поверителност – ниско ниво;
- цялостност – ниско ниво;
- наличност – ниско ниво;
- общо за регистъра – ниско ниво.

5.5. Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

5.6. Действия за защита при аварии, произшествия и бедствия: длъжностното лице изнася дневника при евакуация.

5.7. Достъп до регистър „Пропускателен режим“: Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

5.8. Лични данни се съхраняват до осъществяване на целите, за които се обработват (до приключване на дневника).

5.9. След приключване на дневника, същият се унищожава физически, чрез нарязване или изгаряне.

5.10. Източниците, от които се събират данните, са: от физическите лица.

5.11. Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на УЧЕБНОТО ЗАВЕДЕНИЕ.

6. В **регистър „Видеонаблюдение“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

6.1. Общо описание на регистър „Видеонаблюдение“:

Категориите физически лица, за които се обработват лични данни, са посетители, обучаеми, преподаватели и служители в сградите на СУ „Димитър Талев“.

Регистърът съдържа следните групи данни - физическата идентичност на лицето – видеообраз.

6.2. Технологично описание на регистър „Видеонаблюдение“: Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите в сградата на училището.

6.3. Определяне на длъжностите:

- Оператори на лични данни на регистър „Видеонаблюдение“ са ЗДАСД, РН ИКТ, охранители.

6.4. Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- поверителност – ниско ниво;
- цялостност – ниско ниво;
- наличност – ниско ниво;
- общо за регистъра – ниско ниво.

6.5. Организационни мерки за физическа защита – определени са помещенията, в които ще се обработват лични данни (офис „Охрана“; 302-РН ИКТ; 207-ЗД АСД), като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

6.6. Категориите лица, на които личните данни могат да бъдат разкривани са: физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

6.7. Лични данни се съхраняват в паметта за срок до 1 месец. При необходимост записите могат да бъдат свалени на външен носител.

6.8. След постигане целите личните данни се унищожават физически, чрез изтриване.

6.9. Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на СУ „Димитър Талев“.

6.10. На входовете на сградата се поставят информационни табла за уведомяване гражданите, че при влизане и излизане от сградата подлежат на проверка и за използването на технически средства за наблюдение и контрол съгласно ЗЧОД.

7. Подробно описание на регистрите, включително категории физически лица, за които се обработват лични данни, групи обработвани данни, източници и средства за събирането им, форма за водене на регистъра, ред за съхраняване и унищожаване на информационни носители, служители, обработващи лични данни, техническите ресурси, прилагани за обработване на данните в електронните регистри и други се съдържа в Приложенията, неразделна част от настоящите Вътрешни правила.

8. Създаването на нови регистри и извършването на промени се извършва със заповед на Директора на Администратора.

IV. ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

1. Права и задължения на лицата, обработващи лични данни

1.2. За обезпечаване на адекватна защита на регистрите с лични данни администраторът определя **лице по защита на личните данни.**

- Лицето по защита на личните данни има следните правомощия:
  - ✓ осигурява организация по водене на регистрите и мерки за гарантиране на адекватна защита;
  - ✓ следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;
  - ✓ осъществява контрол по спазване на изискванията по защита на регистрите;
  - ✓ специфицира техническите ресурси, прилагани за обработване на личните данни;
  - ✓ подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите;
  - ✓ в случай на установяване на нарушение на сигурността на личните данни, лицето по защита на личните данни уведомява в спешен порядък администратора на лични данни. Настъпилото събитие поражда задължение за администратора на лични данни в рамките на 72 часа от установяване на нарушението незабавно да уведоми КЗЛД за нарушаване сигурността на личните данни в училище;
  - ✓ поддържа връзка с Комисията за защита на личните данни (КЗЛД) относно предприетите мерки и средства за защита на регистрите;
  - ✓ контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
  - ✓ периодично информира персонала по въпросите на защитата на личните данни;

✓ следи за спазване на организационните процедури за обработване на личните данни и провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

➢ С цел недопускането на неправомерен достъп, както и всички други незаконни форми на обработване на личните данни, администраторът организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

1.3. Служителите на СУ „Димитър Талев“ са длъжни:

✓ да обработват лични данни законосъобразно и добросъвестно;

✓ да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

✓ да актуализират регистрите на личните данни (при необходимост);

✓ да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

✓ да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

✓ да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

1.4. За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

1.5. Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

2. Мерки по осигуряване на защита на личните данни

2.1. Физическа защита в СУ „Димитър Талев“ се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни. *СОТ; охрана*

➢ Основните приложими организационни мерки за физическа защита включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

✓ Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения.

✓ Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения. *Кът за общуване.*

✓ Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

✓ Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

✓ Като зони с контролиран достъп се определят всички помещения на територията на СУ „Димитър Талев“, в които се събират, обработват и съхраняват лични данни.

✓ Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

➢ Основните приложими технически мерки в СУ„Д. Талев“ включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

2.2. Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

➢ Основните мерки на персоналната защита са:

✓ познаване на нормативната уредба в областта на защитата на личните данни;

✓ познаване на политиката и ръководствата за защита на личните данни;

✓ знания за опасностите за личните данни, обработвани от администратора;

- ✓ споделяне на критична информация между персонала (идентификатори, пароли за достъп и т.н.);
- ✓ съгласие за поемане на задължение за неразпространение на личните данни;

➢ Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

2.3. Лицата могат да започнат да обработват лични данни след запознаване със:

➢ нормативната уредба в областта на защитата на личните данни;
➢ политиката и ръководствата за защита на личните данни;
➢ опасностите за личните данни, обработвани от администратора.

2.4. Основните приложими мерки за документална защита на личните данни са:

➢ Определяне на регистрите, които ще се поддържат на хартиен носител,
➢ Определяне на условията за обработване на лични данни.
➢ Регламентиране на достъпа до регистрите.
➢ Определяне на срокове за съхранение
➢ Процедури за унищожаване.

2.5. Защитата на автоматизираните информационни системи и/или мрежи в СУ „Димитър Талев“ включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

➢ Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

- ✓ Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на СУ „Димитър Талев“. Прилагането на тази мярка е с цел да се регламентират нива на достъп;
- ✓ Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;
- ✓ Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от избрано за целта лице.
- ✓ Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)
- ✓ Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на УЧЕБНОТО ЗАВЕДЕНИЕ.
- ✓ Данните, които вече не са необходими за целите на СУ „Димитър Талев“ и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ чрез нарязване, изгаряне или постоянно заличаване от електронните средства.

3. Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка

3.1. Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола. С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на период от 6 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват, включително и чрез изтриване на акаунта.

3.2. Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява възможности за архивиране и възстановяване на данните и работното състояние на средата. При необходимост от ремонт на компютърната техника, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

3.3. СУ „Димитър Талев“ се използва единствено софтуер с уредени авторски права.

3.3.1. На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.

3.3.2. При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

3.4. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

V. Ред за упражняване на правата, свързани със защитата на лични данни *Приложения № 7-11*

1. За упражняване на правата си, свързани със защитата на личните данни, всеки субект на данни подава подписано Искане за упражняване на правата за защита на личните данни (чл.12-21 от ОРЗД *(Общ регламент на Европейския съюз*) или Уведомление за оттегляне на съгласие за обработване на лични данни от субекта на лични данни (чл.7, ал.3 от ОРЗД) до УЧЕБНОТО ЗАВЕДЕНИЕ.

1.1. Искането задължително съдържа следната информация:
- ✓ име, адрес на съответното физическо лице;
- ✓ описание на искането;
- ✓ предпочитана форма за комуникация и действия по чл. 15-21 от Регламент (ЕС) 2016/679;
- ✓ подпис, дата на подаване и адрес за кореспонденция.

1.2. Към искането се прилага пълномощното, ако същото се подава от упълномощено лице.
1.3. Исканията за упражняване правата за защита на лични данни и Уведомлението за оттегляне на съгласие за обработване на лични данни се подават по някой от следните начини:
- ➢ По електронен път на имейл адреса на длъжностното лице по защита на личните данни, *(имейла е dtalev@mail.bg)* по реда на Закона за електронния документ и електронните удостоверителни услуги;
- ➢ На място, в СУ „Димитър Талев“ на адрес : *гр. Добрич; ул. „Ген. Г. Попов“ 16*
- ➢ Писмено чрез куриер или пощенски служби до адреса на СУ „Димитър Талев“, училището може да изиска да извърши допълнителни действия по идентификация на лицето.

1.4. Искането може да бъде отправено лично или от пълномощник с нотариално заверено пълномощно.
1.5. Искането се подава до Директора на СУ „Димитър Талев“
1.6. Администраторът, получил искането за упражняване на индивидуални права на субектите на данни, своевременно в срок от **48 часа** информира всички звена, които обработват лични данни за лицето, както и съответните длъжностни лица по защита на лични данни.
1.7. Всяко звено прави справка за наличните данни в нейните регистри и информационни масиви и предприема съответните мерки съобразно искането на субекта на данни.
1.8. Администраторът на данни съдейства за упражняването на правата на субекта на данните и не отказва да предприеме действия по тях, освен ако не е в състояние да идентифицира субекта на данните.
1.9. Когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искане за упражняване на права, администраторът може да поиска предоставянето на допълнителна информация за потвърждаване на самоличността му.
1.10. За личните данни на заявителя се извършва служебна проверка за наличност във всички регистри и масиви на електронен и хартиен носител, с които училището работи.
2. При подадено Искане за упражняване на права по защита на лични данни СУ „Димитър Талев“ предоставя информация относно предприетите действия в срок от един месец от получаването му. При необходимост, този срок може да бъде удължен с още два месеца, като се вземе предвид сложността и броя на исканията от определено лице. СУ „Димитър Талев“ информира субекта на данните за всяко удължаване в срок от един месец от получаване на искането, като посочва и причините за удължаването.
2.1. По отношение на правото на достъп до личните данни, СУ „Димитър Талев“ потвърждава дали се обработват лични данни за субекта и съответно предоставя необходимата информация. Училището може да откаже да отговори на искането за достъп в случаите, когато заявлението за достъп е явно неоснователно или прекомерно, особено поради своята повтаряемост.
2.2. Изискват се документи за самоличност, а в случай на упълномощаване – и документът за упълномощаването. СУ „Димитър Талев“ предоставя лични данни само ако е извършена идентификация на лицето, вкл. проверени пълномощия. СУ „Димитър Талев“ не е задължена да отговаря на искане, в случай че не е в състояние да идентифицира субекта на данни или неговите пълномощия.
2.3. СУ „Димитър Талев“ може да поиска предоставяне на допълнителна информация, необходима за потвърждаване на самоличността и пълномощията на субекта на данни, когато са налице основателни опасения във връзка със самоличността на физическото лице, което подава искане.
2.4. Субектът на данни има право по всяко време да оттегли дадено съгласие за обработване на личните данни без заплащане на каквито и да е такси.
3. За всяко изтриване на лични данни се издава нарочна заповед на администратора на данни, съставя се комисия и се съставя надлежен протокол за унищожаването. ***Приложение №19.*** Всеки служител и ръководител на звено, който е в притежание на документи, съдържащи лични данни е отговорен за сигурното им унищожаване.
3.1. Когато унищожаването на данни е в резултат на искане на субект на данни, то получава копие от протокола за унищожаване по електронен път или на посочен пощенски адрес.
3.2. Физически лица, субекти на данни, които са недоволни от действията на съответните длъжностни лица в могат да отправят писмена жалба до Директора на училището и до КЗЛД. ***Приложение № 20***

X. ОТГОВОРНОСТ

1. За неизпълнение на задълженията, вменени на съответните оправомощени лица по 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, ако такава отговорност се предвижда по закон.

2. За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в СУ „Д. Талев“, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.
3. Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на администратора на лични данни, на виновните лица се търси имуществена отговорност по Кодекса на труда .
4. За всички неуредени случаи се прилагат разпоредбите на Регламент 2016/679, ЗЗЛД и разпорежданията на Директора на образователната институция- администратор на лични данни.

Настоящите правила са утвърдени със заповед № РД 03 - 107/14.10.2019 г.
на Директора на СУ „Д.Талев“/, както и прилежащите към тях приложения.