

Утвърдил:
Галина Котленска – Директор
ДГ „Буратино“ Суворово

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ДЕТСКА ГРАДИНА „БУРАТИНО“ СУВОРОВО

2018

I. Общи положения

Чл. 1. (1) Детска градина „Буратино“ наричано по-долу **УЧЕБНО ЗАВЕДЕНИЕ** е юридическо лице със седалище ул. "Снежанка" №9, гр. Суворово, обл. Варна, с основен предмет на дейност образование и образователни услуги.

(2) **УЧЕБНОТО ЗАВЕДЕНИЕ** обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им.

Чл. 2. Настоящите правила уреждат организацията на обработване и защитата на лични данни на педагогическите специалисти, служителите, обучаемите, посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на **УЧЕБНОТО ЗАВЕДЕНИЕ**.

Чл. 3 **УЧЕБНОТО ЗАВЕДЕНИЕ** организира и предприема мерки, за защита на личните данни от случайно или незаконно унищожаване, от неправилен достъп, от изменение или разпространение както и от други незаконни форми на обработване. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 4. (1) **УЧЕБНОТО ЗАВЕДЕНИЕ** прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и/или мрежи;

Чл. 5. (1) 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.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на **УЧЕБНОТО ЗАВЕДЕНИЕ** и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на **УЧЕБНОТО ЗАВЕДЕНИЕ** 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.

Чл. 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.

Чл. 7. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на УЧЕБНОТО ЗАВЕДЕНИЕ.

(3) 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.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 8. (1) Документите и преписките, по които работата е приключила, се архивират.

(2) 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.

(3) 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.

(4) Документите на електронен носител се съхраняват на специализирани компютърни системи.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица.

Чл. 9. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 10. (1) При регистриране на неправилен 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 УЧЕБНОТО ЗАВЕДЕНИЕ.

(2) 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.

Чл. 11. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, УЧЕБНОТО ЗАВЕДЕНИЕ може да определи друго ниво на защита за регистъра.

Чл. 12. (1) След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от УЧЕБНОТО ЗАВЕДЕНИЕ 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 УЧЕБНОТО ЗАВЕДЕНИЕ, 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.

(2) В случаите, когато се налага унищожаване на носител на лични данни, **УЧЕБНОТО ЗАВЕДЕНИЕ** прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните 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.

(3) Унищожаване се осъществява от служителя, отговорен за архива на **УЧЕБНОТО ЗАВЕДЕНИЕ**.

Чл. 13. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство и след тяхното легитимиране.

(2) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

II. Мерки по осигуряване на защита на личните данни

Чл. 14. (1) Физическа защита в **УЧЕБНОТО ЗАВЕДЕНИЕ** 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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 ангажменти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(6) 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.

(7) Като зони с контролиран достъп се определят всички помещения на територията на УЧЕБНОТО ЗАВЕДЕНИЕ, в които се събират, обработват и съхраняват лични данни.

(8) 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.

(9) Основните приложими технически мерки за физическа защита в УЧЕБНОТО ЗАВЕДЕНИЕ включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Чл. 14. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на политиката и ръководствата за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
5. съгласие за поемане на задължение за неразпространение на личните данни;

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

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

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

Чл. 16. (1). Основните приложими мерки за документална защита на личните данни са:

1. Определяне на регистрите, които ще се поддържат на хартиен носител: на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на УЧЕБНОТО ЗАВЕДЕНИЕ;
2. Определяне на условията за обработване на лични данни: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на

УЧЕБНОТО ЗАВЕДЕНИЕ, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

3. Регламентиране на достъпа до регистрите: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители.

4. Определяне на срокове за съхранение: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.

5. Процедури за унищожаване: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на УЧЕБНОТО ЗАВЕДЕНИЕ, се унищожават по подходящ и сигурен начин чрез изгаряне, нарязване, електронно изтриване и други подходящи за целта методи.

6. За всяко унищожаване на лични данни, което не е пряко свързано с изпълнение на законовите задължения и/или нормалната дейност на УЧЕБНОТО ЗАВЕДЕНИЕ, се документира.

Чл. 17. (1) Защитата на автоматизирани информационни системи и/или мрежи в УЧЕБНОТО ЗАВЕДЕНИЕ 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.

(2) Основните мерки за защита на автоматизирани информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

1. Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на УЧЕБНОТО ЗАВЕДЕНИЕ. Прилагането на тази мярка е с цел да се регламентират нива на достъп;

2. 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;

3. 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.

4. Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, паметни ленти и други носители на информация, еднократно записваеми носители и др.)

5. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на УЧЕБНОТО ЗАВЕДЕНИЕ.

6. Данните, които вече не са необходими за целите на УЧЕБНОТО ЗАВЕДЕНИЕ и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ чрез нарязване, изгаряне или постоянно заличаване от електронните средства.

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

Чл. 18. (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.

(5) 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).

Чл. 19. (1) 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.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 20. (1) В УЧЕБНОТО ЗАВЕДЕНИЕ се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.

(3) 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.

Чл. 21. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

IV. Поддържани регистри и тяхното управление

Чл. 22. Поддържаните от УЧЕБНОТО ЗАВЕДЕНИЕ регистри с лични данни са:

1. Обучаеми
2. Родители
3. Персонал
4. Пропускателен режим
5. Видеонаблюдение

Чл. 23. (1) В регистър „Обучаеми“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица „обучаеми“, обучавани в УЧЕБНОТО ЗАВЕДЕНИЕ.

(2) Общо описание на регистър „Обучаеми“

Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка;
2. културна идентичност: интереси и хоби;
3. социална идентичност – образование;
4. семейна идентичност - родствени връзки;
5. лични данни, които се отнасят до здравето.

(3) 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 УЧЕБНОТО ЗАВЕДЕНИЕ. Базата данни се намира на твърдия диск на изолирани компютри.

- срок на съхранение: съгласно нормативната уредба в УЧЕБНОТО ЗАВЕДЕНИЕ със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Обучаеми“ са учителите по групи, Директора, касиера събиращ таксите, медицински сестри

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.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

(6) 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). 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, 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.

(7) УЧЕБНОТО ЗАВЕДЕНИЕ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

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

Достъп до регистър „Обучаеми“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните закони и подзаконовни 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.

(9) Лични данни на обучаемите се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно нормативната уредба със сроковете за тяхното съхранение.

(10) След постигане целите по предходната алинея личните данни на обучаемите се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 24. (1) В регистър „Родители“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.

(2) Общо описание на регистър „Родители“ Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, телефони за връзка и месторабота;
2. икономическа идентичност – финансово състояние;
3. социална идентичност – образование, трудова дейност;
4. семейна идентичност – семейно положение и родствени връзки.

(3) 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 11.08.2016 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 УЧЕБНОТО ЗАВЕДЕНИЕ. Базата данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно нормативната уредба в УЧЕБНОТО ЗАВЕДЕНИЕ със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Родители“ са: учители, медицински сестри, Директор, ЗАС

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.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

(6) 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). 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.

(7) УЧЕБНОТО ЗАВЕДЕНИЕ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от УЧЕБНОТО ЗАВЕДЕНИЕ – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи ;

3. защита от наводнения – предприемат се действия по ограничаване на разпространението, както и се изпомпва водата или загребва със собствени подръчни средства.

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

(9) 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 УЧЕБНОТО ЗАВЕДЕНИЕ

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

Чл. 25. (1) 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.

(2) Общо описание на регистър „Персонал“

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;
2. психологическа идентичност – документи относно психическото здраве;
3. социална идентичност - образование и трудова дейност;
4. семейна идентичност - семейно положение и родствени връзки;
5. лични данни, които се отнасят до здравето;
6. 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:

1. Индивидуализиране на трудовите правоотношения;

2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

3. 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.

4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(3) 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 УЧЕБНОТО ЗАВЕДЕНИЕ.

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Персонал“ са: ЗАС, касиер, Директор

Оператор на лични данни на регистър „Персонал“ е ЗАС

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност – ниско ниво;

2. цялостност – ниско ниво;

3. наличност – ниско ниво;

4. общо за регистъра – ниско ниво.

(6) 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). 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, 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. Трудовите досиета на персонала не се изнасят извън сградата на УЧЕБНОТО ЗАВЕДЕНИЕ. 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.

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.

(7) УЧЕБНОТО ЗАВЕДЕНИЕ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

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

(8) 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.

(9) 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 УЧЕБНОТО ЗАВЕДЕНИЕ

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

Чл. 26. (1) 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 УЧЕБНОТО ЗАВЕДЕНИЕ.

(2) Общо описание на регистър „Пропускателен режим“

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

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

(4) Определяне на длъжностите:

Обработващ лични данни на регистър „Пропускателен режим“ е портиерът. Оператор на лични данни на регистър „Пропускателен режим“ е ЗАС

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

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

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

(8) 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.

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

(10) След приключване на дневника, същият се унищожава физически, чрез нарязване или изгаряне.

(11) Източниците, от които се събират данните, са: от физическите лица.

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

Чл. 27. (1) В регистър „Видеонаблюдение“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Общо описание на регистър „Видеонаблюдение“:

Категориите физически лица, за които се обработват лични данни, са посетители, обучаеми, преподаватели и служители в сградите на УЧЕБНОТО ЗАВЕДЕНИЕ.

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

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

(4) Определяне на длъжностите:

Оператори на лични данни на регистър „Видеонаблюдение“ са Директора

- (5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:
1. поверителност – ниско ниво;
 2. цялостност – ниско ниво;
 3. наличност – ниско ниво;
 4. общо за регистъра – ниско ниво.
- (6) 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.
- (7) 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.
- (8) Лични данни се съхраняват в паметта за срок от 1 седмица. При необходимост записите могат да бъдат свалени на външен носител.
- (9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.
- (10) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на УЧЕБНОТО ЗАВЕДЕНИЕ.
- (11) На входовете на сградата се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка и за използването на технически средства за наблюдение и контрол съгласно ЗЧОД.

V. Права и задължения на лицата, обработващи лични данни

Чл. 28. (1) Лице по защита на личните данни е Директорът на УЧЕБНОТО ЗАВЕДЕНИЕ.

- (2) Лицето по защита на личните данни има следните правомощия:
1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
 2. следи за спазването на конкретните мерки за защита и контрол на достъпа, съобразно, спецификата на водените регистри;
 3. осъществява контрол по спазване на изискванията за защита на регистрите;
 4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
 5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрацията на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл. 29. Служителите на УЧЕБНОТО ЗАВЕДЕНИЕ са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. 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;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. 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.
6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 33. (1) За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

(2) 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.

VI. Ред за упражняване на правата, свързани със защитата на лични данни

Чл. 34. (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) 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.

(2) Искането задължително съдържа следната информация:

1. име, адрес на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за комуникация и действия по чл. 15-21 от Регламент (ЕС) 2016/679;

4. подпис, дата на подаване и адрес за кореспонденция.

(3) Към искането се прилага пълномощното, ако същото се подава от упълномощено лице.

(4) Исканията за упражняване на правата за защита на лични данни и Уведомлението за оттегляне на съгласие за обработване на лични данни се подават по някой от следните начини:

1. По електронен път на имейл адреса на длъжностното лице по защита на личните данни, което е определено от съответния администратор в структурата на УЧЕБНОТО ЗАВЕДЕНИЕ имейл meti_1987@abv.bg по реда на Закона за електронния документ и електронните удостоверителни услуги;

2. На място, в УЧЕБНОТО ЗАВЕДЕНИЕ на адрес : „Снежанка „№9, гр. Суворово, обл. Варна

3. Писмено чрез куриер или пощенски служби до адреса на УЧЕБНОТО ЗАВЕДЕНИЕ, като УЧЕБНОТО ЗАВЕДЕНИЕ може да изиска да извърши допълнителни действия по идентификация на лицето.

(5) Искането може да бъде отправено лично или от пълномощник с нотариално заверено пълномощно.

(6) Искането се подава на УЧЕБНОТО ЗАВЕДЕНИЕ

(7) 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.

(8) Всяко звено прави справка за наличните данни в нейните регистри и информационни масиви и предприема съответните мерки съобразно искането на субекта на данни.

(9) 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.

(10) 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.

(11) За личните данни на заявителя се извършва служебна проверка за наличност във всички регистри и масиви на електронен и хартиен носител, с които УЧЕБНОТО ЗАВЕДЕНИЕ работи.

Чл. 35. (1) При подадено Искане за упражняване на права по защита на лични данни УЧЕБНОТО ЗАВЕДЕНИЕ 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. УЧЕБНОТО ЗАВЕДЕНИЕ информира субекта на данните за всяко удължаване в срок от един месец от получаване на искането, като посочва и причините за удължаването.

(2) По отношение на правото на достъп до личните данни, УЧЕБНОТО ЗАВЕДЕНИЕ потвърждава дали се обработват лични данни за субекта и съответно предоставя необходимата информация. УЧЕБНОТО ЗАВЕДЕНИЕ може да откаже да отговори на искането за достъп в случаите, когато заявлението за достъп е явно неоснователно или прекомерно, особено поради своята повтаряемост.

Чл. 36. (1) Изискват се документи за самоличност, а в случай на упълномощаване – и документът за упълномощаването. УЧЕБНОТО ЗАВЕДЕНИЕ предоставя лични данни само ако е извършена идентификация на лицето, вкл. проверени пълномощия. УЧЕБНОТО ЗАВЕДЕНИЕ не е задължена да отговаря на искане, в случай че не е в състояние да идентифицира субекта на данни или неговите пълномощия.

(2) УЧЕБНОТО ЗАВЕДЕНИЕ 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.

(3) 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.

Чл. 37. (1) За всяко изтриване на лични данни се издава нарочна заповед на администратора на данни, съставя се комисия и се съставя надлежен протокол за унищожаването. Всеки служител и ръководител на звено, който е в притежание на документи, съдържащи лични данни е отговорен за сигурното им унищожаване.

(2) 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) Физически лица, субекти на данни, които са недоволни от действията на съответните длъжностни лица в УЧЕБНОТО ЗАВЕДЕНИЕ могат да отправят писмена жалба до Директора на УЧЕБНОТО ЗАВЕДЕНИЕ.

Преходни и заключителни разпоредби

§ 1. По смисъла на настоящите вътрешни правила:

„Лични данни“ са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

„Администратор“ е физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, който сам или съвместно с друг определя целите и средствата за обработване на личните данни.

„Администратор на лични данни“ е УЧЕБНОТО ЗАВЕДЕНИЕ

„Ниво на защита“ е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.

„Обработване на лични данни“ е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране,

употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

„Обработващ лични данни“ е лице, което обработва лични данни от името на администратора на лични данни.

„Оператор на лични данни“ е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на УЧЕБНОТО ЗАВЕДЕНИЕ.

„Оценка на въздействие“ 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.

„Поверителност“ е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

„Предоставяне на лични данни“ са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

„Регистър на лични данни“ е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.

„Съгласие на физическото лице“ е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява, те да бъдат обработвани.

„Трето лице“ е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.

§2. Всички служители на УЧЕБНОТО ЗАВЕДЕНИЕ са длъжни срещу подпис да се запознаят с инструкцията и да я спазват.

§3. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и действащото приложимо законодателство на Р България.

ПРИЛОЖЕНИЕ № 1

**ОЦЕНКА НА НИВОТО НА ВЪЗДЕЙСТВИЕ НА РЕГИСТРИТЕ
В ДЕТСКА ГРАДИНА „БУРАТИНО“ СУВОРОВО**

Име на регистър	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	цялостност	наличност	общо за регистъра
Обучаеми	ниско	ниско	ниско	ниско
Родители	ниско	ниско	ниско	ниско
Персонал	ниско	ниско	ниско	ниско
Пропусквателен режим	ниско	ниско	ниско	ниско
Видеонаблюдение	ниско	ниско	ниско	ниско

ПРИЛОЖЕНИЕ № 2

ДО:

УВЕДОМЛЕНИЕ
ЗА ОТТЕГЛЯНЕ НА СЪГЛАСИЕ ЗА ОБРАБОТВАНЕ НА
ЛИЧНИ ДАННИ ОТ СУБЕКТА НА ЛИЧНИ ДАННИ (ЧЛ. 7, АЛ. 3 ОТ ОРЗД)

ОТ:
(три имена и ЕГН)

в качеството ми на субект на лични данни според чл. 4 от ОРЗД

Уважаема/и госпожо/господин,

в качеството Ви на администратор на мои лични данни,
като се има предвид, че:

- съм предоставил/а съгласието си за обработване на следните лични данни:
.....
....., по следния начин:
..... (посочва се по какъв начин е дадено съгласието - на
хартиен носител, по електронен път и т.н.), във връзка със следната цел:
.....

С НАСТОЯЩОТО ВИ УВЕДОМЯВАМ, ЧЕ:

- Оттеглям съгласието си личните ми данни, посочени в тази декларация, да бъдат събирани и обработвани за посочената в тази декларация цел.
- Декларирам, че оттеглям своето съгласие за обработване на лични данни свободно, изрично и относно всички лични данни, съгласно собствената си воля и убеждение.
- Запознат/а съм, че имам право на възражения и жалби пред Комисия за защита на личните данни, която е надзорен орган в Република България, в случай, че администраторът продължи обработването на личните ми данни след оттеглянето на съгласието с настоящото уведомление.

Изразявам предпочитанието си комуникацията с мен във връзка с изпълнението на настоящото искане да бъде извършвана по следните начини:

- ☐ на следния телефонен номер:
.....
- ☐ на следния имейл адрес:
.....
- ☐ чрез конвенционална кореспонденция с използването на сигурен куриер до адрес:
.....
.....

Личните данни, които се обработват за попълването на настоящото искане ще бъдат използвани само за идентификация на субекта на данни с цел осигуряване на неприкосновеност на личните му данни, осигуряване на правата му по настоящата заявка и според ОРЗД. Данните ще се съхраняват за осигуряване на легитимния интерес на администратора за проверки от КЗЛД до по-късната от двете дати – пет години след обработване на искането или датата на изтриване на личните данни на субекта, когато се обработват на други основания.

Дата:

Подпис:

Получено от:

ПРИЛОЖЕНИЕ № 3

ДО:
.....

ИСКАНЕ
ЗА УПРАЖНЯВАНЕ НА ПРАВА НА СУБЕКТ НА ЛИЧНИ ДАННИ
(чл. 12-21 ОТ ОРЗД)

ОТ:
.....

(три имена и ЕГН)
в качеството ми на субект на лични данни според чл. 4 от ОРЗД

Уважаема/и госпожо/господин,

в качеството Ви на администратор на мои лични данни,
с настоящото Ви уведомявам, че желая да упражня правата си на субект на лични данни
(чл. 12-21 от ОРЗД), както следва:

(В следващата таблица се поставя отметка пред правата, които лицето желае да упражни и се попълва съответната
необходима информация, а ненужните редове се зачертават. За обслужване на искането е желателно да предоставите в
максимална степен поисканата информация, като задължително следва да предоставите поне три имена, ЕГН и да
посочите начин за комуникация.)

☐	Искане за достъп до личните ми данни (чл. 15 ОРЗД)
Известно е ми е, че следните ми лични данни са свързани със следните операции по обработване в администратора. и са ми необходими за следната цел:	
☐	Искане за достъп до лични данни с цел установяване на наличие, точност и актуалност
Моля да ми бъде предоставен достъп до съхраняваните от Вас мои лични данни за установяване на наличие, точност и актуалност на данните. Декларирам, че ☐ не ми е известно личните ми данни да са обработвани от администратора. ☐ ми е известно, че личните ми данни са обработвани от администратора във връзка със следните операции.	
☐	Искане за коригиране на личните ми данни (чл. 16 ОРЗД)

Известно ми е и се уверих, че следните ми лични данни
.....
свързани със следните операции по обработване в администратора.

и са неточни и непълни.

Моля в законовия срок данните ми да бъдат коригирани, както следва:

☐ **Искане за изтриване на личните ми данни (чл. 17 ОЗРД)**

с настоящата декларация заявявам, че желая свързаните с мен лични данни да бъдат изтрети без ненужно забавяне, по следната причина*:

Моля да се уведомят всички администратори и обработващи личните ми данни, че съм поискал изтриване на личните ми данни, включително на всички връзки, копия или реплики на тези лични данни.

**Причината трябва да бъде от възможните по чл. 17 от Общия регламент: (i) личните данни повече не са необходими за целите, за които са били събрани; (ii) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването; (iii) субектът на данните възразява срещу обработването „за изпълнението на задача от обществен интерес или при упражняването на официални правомощия; (iv) субектът на данните възразява срещу обработването „за целите на легитимните интереси на администратора или на трета страна“ и няма законни основания за обработването, които да имат преимущество; (v) субектът на данните възразява срещу обработването за целите на директния маркетинг; (vi) личните данни са били обработвани незаконосъобразно; (vii) личните данни са били събрани във връзка с предлагането на услуги на и за деца.*

☐ **Искане за ограничаване обработването на лични данни (чл. 18 ОЗРД)**

Известно ми е и съм информиран, че следните ми лични данни
.....
са свързани със следните операции по обработване в администратора.

с настоящата молба Ви информирам, че желая обработването на личните ми данни да бъде ограничено по следната причина**:

Моля всички засегнати трети страни да бъдат уведомени за ограничаването на обработването на личните данни.

*** Субектът на данните има право да изиска от администратора ограничаване на обработването, когато се прилага едно от следното: а) точността на личните данни се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността на личните данни; б) обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрети, а изисква вместо това ограничаване на използването им; в) администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции; г) субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.*

☐ **Възражение срещу обработване на лични данни (чл. 21 ОЗРД)**

Известно ми е и съм информиран, че следните ми лични данни
.....
са свързани със следните операции по обработване в администратора.

с настоящото възразявам срещу обработването на личните ми данни поради следната причина.

☐	Искане за използване на право за преносимост на личните данни (чл. 20 ОЗРД)
Известно ми е и съм информиран, че следните ми лични данни са свързани със следните операции по обработване в администратора. , като обработването на данните е основано на съгласие или на договорно задължение и обработването се извършва по автоматизиран начин. С настоящото моля електронно копие на описаните по-горе мои лични данни да бъде прехвърлено до следния администратор на лични данни / на мене, по следния начин , като се използва следния защитен електронен адрес: или по куриер на следния адрес	

Допълнителна информация:

.....

.....

.....

Изразявам предпочитанието си комуникацията с мен във връзка с изпълнението на настоящото искане да бъде извършвана по следните начини:

- ☐ на следния телефонен номер:
- ☐ на следния имейл адрес:
.
- ☐ чрез конвенционална кореспонденция с използването на сигурен куриер до адрес:
.
.

Личните данни, които се обработват за попълването на настоящото искане ще бъдат използвани само за идентификация на субекта на данни с цел осигуряване на неприкосновеност на личните му данни, осигуряване на правата му по настоящата заявка и според ОРЗД. Данните ще се съхраняват за осигуряване на легитимния интерес на администратора за проверки от КЗЛД до по-късната от двете дати – пет години след обработване на искането или датата на изтриване на личните данни на субекта, когато се обработват на други основания.

Дата:

Подпис:

Получено от:

ДЕКЛАРАЦИЯ ЗА ИНФОРМИРАНО СЪГЛАСИЕ

Настоящата декларация цели да гарантира спазването на правата на детето и родителите/настойниците/попечителите му по време на мероприятия свързани с дейността на ДГ „Буратино“ Суворово

С цел гарантиране правото на мнение на децата (чл.12 от Конвенцията на ООН за правата на детето), моля обсъдете това с детето си и попълнете декларацията.

Информацията, която предоставяте, ще се счита за строго конфиденциална.

Адресът, който посочвате, е за целите на кореспонденция с Вас и ще бъде използван за изпращане на информация и награди.

Долуподписаният/ата

.....
/име, презиме, фамилия на декларатора/

родител/настойник

на.....

/име, презиме, фамилия на детето/

на.....

/име, презиме, фамилия на детето/

на.....

/име, презиме, фамилия на детето/

Основна информация за родителя/настойника/попечителя:

Адрес:

Телефон (мобилен телефон):

E-mail адрес:

Декларирам, че съм запознат/а и давам съгласието си за следното:

Декларирам, че съм запознат/а и давам съгласието си за следното:

Снимки, видео и аудио записи на детето/децата ми и на мен, заснети във връзка със събития, кампании и инициативи на ДГ „Буратино“, да бъдат публикувани в интернет сайта на детската градина и фейсбук страници, както и да бъдат използвани в печатни и видео материали, свързани с дейността на учебното заведение.

С настоящата декларация декларирам съгласие за съхранение и обработка на личните ми данни при спазване на разпоредбите на Закона за защита на личните данни.

Запознат/а съм с правото на достъп и на коригиране на събраните данни.

Запознат/а съм с целта и средствата на обработка на личните ми данни.

Запознат/а съм с доброволния характер на предоставянето на данните.

Място и дата:

Декларатор:

/подпис/

Длъжностно лице по защита на данните

1. Какво представлява т.нар. длъжностно лице по защита на данните?

Новият регламент за защита на личните данни въвежда фигурата на т.нар. длъжностно лице по защита на данните. Това е служител на администратор на лични данни или външно за организацията на администратора физическо лице, натоварено с консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията на администратора и повишаването на осведомеността и обучението на персонала.

2. За първи път ли се въвежда длъжността „лице по защита на личните данни“ в България?

В България и до сега съществуваше правна възможност за назначаване на лице по защита на личните данни, която произтичаше от разпоредбата на чл. 18 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни. За първи път обаче определянето на такова длъжностно лице произтича от акт със сила на закон и става задължително в изрично определени в Регламента случаи.

3. Всички администратори ли ще трябва задължително да имат длъжностно лице по защита на личните данни?

Не. Регламентът предвижда длъжностно лице по защита на личните данни да имат само определени категории администратори, а именно:

- Публични органи или структури, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- Администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и систематично мащабно наблюдение на субектите на данни;
- Администратори, чиито основни дейности се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

4. Има ли възможност едно лице по защита на данните да отговаря за няколко структури?

Да, Регламентът предвижда такава възможност, при условие че администраторът е обществен орган или структура. В тези случаи при определянето на служителя следва да се отчита организационната структура и размер на администраторите. Група предприятия също могат да определят едно длъжностно лице по защита на данните, което да работи за тях, като изискването е всяко от предприятията да има лесен и свободен достъп до това лице.

5. На какви изисквания трябва да отговаря даден служител, за да бъде назначен или определен за лице по защита на личните данни?

Регламентът изисква лицето по защита на личните данни да притежава задълбочени експертни познания в областта на законодателството и практиката на защитата на личните данни.

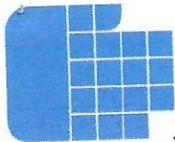
6. Какви функции ще изпълнява лицето по защита на личните данни?

Лицето по защита на личните данни има набор от задължения, сред които:

- Да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на нормативните актове за защита на личните данни;
- Да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;
- При поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;
- Да си сътрудничи с надзорния орган;
- Да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация и по целесъобразност да се консултира по всякакви други въпроси.

ИЗВАДКИ ОТ СТАНОВИЩА НА КЗЛД ПО ПОВОД ВИДЕОНАБЛЮДЕНИЕ В УЧИЛИЩА И ДЕТСКИ ГРАДИНИ

- ✓ Устройството и дейността на детските ясли се регламентира с разпоредбите на Наредба № 26 от 2008 г. за устройството и дейността на детските ясли и детските кухни и здравните изисквания към тях. Изискванията към детските градини се регламентират с разпоредбите на Правилника за прилагане на Закона за народната просвета и Наредба № 3 от 2007 г. за здравните изисквания към детските градини. Към настоящия момент разпоредбите на горепосочените подзаконови нормативни актове не регламентират осъществяване на видеонаблюдение в детските ясли и градини.
- ✓ Допустимо е постоянното видеонаблюдение в общите помещения и дворните пространства, което да гарантира безопасността на децата и учениците при игри, занимания и в свободното им време. Такова наблюдение е допустимо единствено да бъде приложено за местата на заниманията, ако са отделени от местата за сън и почивка, и в общите части на сградата.
- ✓ С оглед на защита на правата на децата и учениците е недопустимо извършването на видеонаблюдение в помещения за сън, в санитарните помещения, в помещенията за почивка и лична хигиена на децата, тъй като с наличните устройства в тези помещения не се дава право на децата на уединение и запазване на личното им достойнство, както и представлява нарушение на правото на неприкосновеност на личността.
- ✓ Допустимо е извършването на видеонаблюдение в общите помещения и дворните пространства, което да гарантира безопасността на децата и учениците при игри, занимания и в свободното им време. Такова наблюдение е допустимо единствено да бъде приложено за местата на заниманията, ако са отделени от местата за сън и почивка, и в общите части на сградата.
- ✓ Безспорно е, че всяко лице има право на достъп до отнасящи се до него лични данни, включително до видеозаписи. Когато при осъществяване на правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, както е в случая, администраторът на лични данни е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него, като за целта трябва да предприеме съответните технически мерки за заличаване/маскиране на образите на другите лица обект на видеонаблюдението. При липса на такава възможност достъп до видеозаписите може да бъде предоставен само със съгласието на всички лица – обект на видеонаблюдението, с оглед защита на правата им по ЗЗЛД.



СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Рег. № П – 5375/2017 г.
гр. София, 30.04.2018 г.

ОТНОСНО: Искане с вх. № П-5375/2017 год. от Председателя на Държавна агенция за закрила на детето, по въпроси, касаещи въвеждането на видеонаблюдение в детските заведения (детски ясли и детски градини), както и в училищата.

Комисията за защита на личните данни (КЗЛД, Комисията) в състав: членове: Цанко Цолов, Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 28.03.2018 г., разгледа преписка с вх. № П-5375/2017 г. от Председателя на Държавна агенция за закрила на детето (ДАЗД), в което посочва, че в ДАЗД е постъпило писмо с вх. № 04-22-11/29.06.2017г., от г-жа Светлана Йорданова - зам.-министър на здравеопазването, с молба за изразяване на становище, относно въвеждането на видеонаблюдение в детските заведения /детски ясли и детски градини/ и дали това ще доведе до нарушаване правата на децата.

Председателят на ДАЗД моли, във връзка с компетентността си, КЗЛД да изрази становище по темата.

В искането се посочва, че за Държавната агенция за закрила на детето е от първостепенна важност правата на всяко дете в Р. България да са гарантирани и защитени и вярва, че ползотворното сътрудничество между институциите ще осигури в пълна степен правата и интересите на децата.

Към искането е приложено копие на писмо с вх. № 04-22-11/29.06.2017г. и отговор от ДАЗД до Министерството на здравеопазването.

В писмото си Заместник-министъра на здравеопазването, отбелязва, че в последно време в различните медии е огласен и коментиран въпросът с видеонаблюдението на децата в детските заведения, с цел подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детските заведения. В тази връзка в Министерството на здравеопазването са постъпили редица писма от родители и медицински специалисти с въпроси по дискутираната тема.

Във връзка с горното на вниманието и на КЗЛД е изпратено и копие от отворено писмо от колектива на 31 детска ясла в гр. София, с молба за изразяване на становище, предвид

компетентността на ДАЗД, дали видеонаблюдението може да се счита за нарушаване на правата на здрави деца или деца с увреждания, при осъществяване на ежедневните дейности, провеждани в детските ясли и при какви условия. Отправеното предложение за поставяне на видеонаблюдение в детските ясли е в резултат на реакцията на конкретни родители, отразена широко в медиите. Съвсем естествено и основателно това предизвиква реакция и от страна на ръководствата и персонала в детските ясли не само в столицата, но и в цялата страна.

При разглеждането на административна преписка, и направения обстоен анализ на законовата уредба, първоначалният извод, който може да бъде направен е, че към момента няма яснота и конкретно нормативно регламентиране на поставените в искането въпроси.

Поради големия обществен интерес и с оглед обстоятелството, че Държавната агенция за закрила на детето, Министерството на здравеопазването и Министерството на труда и социалната политика имат пряко отношение към разглеждания казус, беше отправено искане за становище към ръководителите на изброените по-горе ведомства.

От Министерството на здравеопазването беше изразено следното становище:

Устройството и дейността на детските ясли се регламентира с разпоредбите на Наредба № 26 от 2008 г. за устройството и дейността на детските ясли и детските кухни и здравните изисквания към тях. Изискванията към детските градини се регламентират с разпоредбите на Правилника за прилагане на Закона за народната просвета и Наредба № 3 от 2007 г. за здравните изисквания към детските градини. Към настоящия момент разпоредбите на горепосочените подзаконовни нормативни актове не регламентират осъществяване на видеонаблюдение в детските ясли и градини.

Правен анализ:

Въпросът за законосъобразното извършване на видеонаблюдение е поставян многократно за произнасяне от КЗЛД, съобразно вменените нормативни правомощия като национален надзорен орган да осъществява защитата на лицата при обработването на личните им данни. Към настоящия момент работата на Комисията по този въпрос е отразена в решения по жалби на граждани, становища по приложението на Закона за защита на личните данни (ЗЗЛД), отговори на въпроси и издадени Наказателни постановления.

Практиката на КЗЛД по темата за видеонаблюдението в последните години показва, че с развитието на технологиите в национален и световен мащаб се развиват и технологиите, в областта на системите за видеонаблюдение. Посредством инсталиране на различен вид системи за видеонаблюдение, широко достъпни на пазара, се предоставя възможност на физически и юридически лица за наблюдение на различни субекти и обекти, както локално, така и чрез възможност за отдалечен достъп до изходящи образи от видеокамери и записи с

видеокадри.. Това развитие на технологиите и прякото им отражение в сферата на обществения и частния живот не може да не бъде отчитано от Комисията, когато решава въпросите за законосъобразността и допустимостта на видеонаблюдението.

Поради обстоятелството, че в България видеонаблюдението, като вид обработване на лични данни не е подробно уредено, при разглеждане на отделните казуси, КЗЛД анализира на международното законодателство и практика, свързани с обработването на лични данни, осъществявано чрез видеонаблюдение. При извършване на видеонаблюдение, като вид техническа форма на обработване на лични данни, която става все по-достъпна и лесно приложима в различни области на съвременния живот, се налага и нуждата от подробна нормативна регламентация. Във връзка с масовото навлизане на видеонаблюдението във всички сфери на живота, все по-актуален става въпросът за защита на неприкосновеността на личността и личния живот.

Най-общо, основните принципи за неприкосновеността на личния и семейния живот са заложили в редица европейски и международни актове – Конвенция за защита правата на човека и основните свободи, Харта за основните права на Европейския съюз, Конвенция 108 на Европейския парламент за защита на лицата при автоматизирана обработка на личните данни, както и най-новият европейски правен акт с пряко действие в държавите-членки – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните / General Data Protection Regulation (GDPR)). В Конвенция 108 на Европейския парламент за защита на лицата при автоматизирана обработка на личните данни се прокламира една обща цел за зачитане на правата и основните свободи на всяко физическо лице и по-конкретно правото му на личен живот по отношение на автоматизираната обработка на лични данни, отнасящи се до него. Видеонаблюдението като вид автоматизирана обработка на лични данни попада под регламентацията на тази конвенция. Детайлизиране на общия принцип за неприкосновеност на личния и семеен живот е постигнато в Общият регламент за защита на данните, като основен правен акт, който урежда защитата на личните данни в Европейския съюз. Приложението на Регламент (ЕС) 2016/679 е с отложено действие, а именно: от 25 май 2018 година. Едновременно с посочените правни актове, по отношение на разглежданата категория субекти (деца и подрастващи), разпоредбите на Конвенцията на ООН за правата на детето гарантират правото на децата на неприкосновеност на личния живот.

При извършване на нормативно проучване се установява, че отделните страни в Европейския съюз са регламентирали по различен начин въпроса с видеонаблюдението – посредством закони, указания, становища. Това е наложило в Евразоната да бъдат приети и

обща правила с оглед разнообразната практика. Основна роля по уеднаквяването на практиката в различните страни-членки е на Работната група по Член 29 от Директива 95/46/ЕО. На заседание на РГ 29 е изработен „Работен документ относно обработването на лични данни чрез видеонаблюдение“. По този въпрос РГ 29 има изразено и „Становище 4/2004 относно обработване на лични данни чрез средства за видеонаблюдение“.

Въпросите, свързани с видеонаблюдението, могат да бъдат анализирани в няколко насоки:

- Защита на живота и здравето на лицата, обект на видеонаблюдение;
- Обществен интерес;
- Разкриване, предотвратяване и контрол на нарушения/престъпления;
- Защита на собствеността;
- Други законни интереси.

Изводът, който може да се направи е, че при използването на технически средства за видеонаблюдение е изключително важно да се прилагат принципите за адекватност и пропорционалност при обработване на лични данни чрез видеонаблюдение:

- На първо място това е въпросът с качеството на обработваните данни. Изображенията от видеокамерите, както и записите с видеокадри, съхранени на различен тип носители, трябва да се обработват добросъвестно и законосъобразно, за конкретни и точно определени цели;

- Предвид посоченото по-горе относно липсата на конкретна нормативна регламентация във връзка с искането за становище, е необходимо да бъде спазено поне едно от следните условия: защита на значими жизнени интереси на субектите на данни, изпълнение на задача, извършвана в обществен интерес;

- На трето място това са правото на информация, правото на достъп и правото на искане за коригиране от страна на лицето, обект на видеонаблюдението;

- Не на последно място е и необходимостта от предприемане на достатъчно технически и организационни мерки за защита на обработваните чрез системите за видеонаблюдение лични данни.

Факт е, че към момента не е създаден регламент, който да указва правила за инсталиране и внедряване на системи за видеонаблюдение, както в детските заведения (ясли и градини), така и в училищата. Посочените действия съставляват действия по обработване на лични данни по смисъла на § 1, т. 1 от Допълнителните разпоредби на ЗЗЛД, както и легалната дефиниция, разписана в чл. 4, т. 2) от Регламент (ЕС) 2016/679.

По-нататък в изложението ще се посочват само разпоредбите на Регламент (ЕС) 2016/679 (приложим от 25 май 2018 год.).

Обработването на лични данни, в случая чрез видеонаблюдение, може да се извършва при наличие на една от хипотезите, разписани в чл. 6 от Регламент (ЕС) 2016/679 и при стриктно спазване на принципите, визирани в чл. 5 от регламента.

В конкретно разглеждания казус приложение може да намерят две от алтернативно изброените предпоставки за законосъобразност на обработването, разписани в чл. 6 от Регламент (ЕС) 2016/679, а именно: чл. 6, пар. 1, буква г) – обработването е необходимо, за да бъдат защитени жизнено важни интереси на субекта на данните или на друго физическо, както и чл. 6, пар. 1, буква д), предл. първо - обработването е необходимо, за изпълнение на задача от обществен интерес.

Посоченият в искането за становище аргумент за необходимостта от въвеждане на видеонаблюдение за подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детските заведения, а също и в училищата, е основателен мотив с цел защита живота и здравето на най-уязвимата категория от обществото като цяло – децата и непълнолетните български граждани. В този смисъл относимостта на посочената по-горе разпоредба на чл. 6, пар. 1, буква г) от Регламент (ЕС) 2016/679 е в пряка връзка с анализирания казус.

Едновременно с дотук изложеното, разглежданият въпрос е и в резултат на реакциите на много родители, отразени широко в медиите. В случая следва да се вземе предвид и обществения интерес от въвеждане на прозрачност в грижите за децата и подрастващите. При позоваването на понятието „обществен интерес“ е необходимо да се държи сметка за обстоятелството, че става дума за абстрактна правна, политическа, философска и социално-икономическа категория, чието съдържание зависи както от състоянието на обществото в конкретен исторически момент, така и от индивидуалните интереси на отделните членове на обществото. На практика въпросът за сигурността, живота и здравето на българските деца и ученици е от първостепенна важност за обществото като цяло. Следователно разпоредбата на чл. 6, пар. 1, буква д), предл. първо от Регламент (ЕС) 2016/679 също е законосъобразна предпоставка за обработване на лични данни чрез извършване на видеонаблюдение.

Отделно от посоченото е важно да се отбележи, че предвид спецификата на детските ясли и градини (малката възраст на децата, определяща ги като едни от най-уязвимите групи), общите помещения за сън и игра, и общите санитарни помещения, въвеждането на видеонаблюдение в помещенията за почивка и лична хигиена на децата е в разрез с техните права. С оглед на защитата на личните права на децата е изключено поставянето на такова в спалните помещения, тъй като с наличните устройства в тези помещения не се дава право на децата на уединение и запазване на личното им достойнство, както и представлява нарушение на правото на неприкосновеност на личността. Това би създавало предпоставки за прекомерна

намеса в техния личен живот, в разрез с чл. 16 от Конвенцията на ООН за правата на детето. Според разпоредбата, в услугите за деца и в институциите трябва да бъде осигурено пространство, което да гарантира неприкосновеността на личния живот на децата, поради което денонощното наблюдение на личните им стаи е недопустимо.

Допустимо е постоянното видеонаблюдение в общите помещения и дворните пространства, което да гарантира безопасността на децата и учениците при игри, занимания и в свободното им време. Такова наблюдение е допустимо единствено да бъде приложено за местата на заниманията, ако са отделени от местата за сън и почивка, и в общите части на сградата.

Отделно от извършения по-горе нормативен анализ за законосъобразните предпоставки във връзка с разглеждания казус, е необходимо да се отчетат задълженията и отговорностите на администраторите на лични данни, които следва да съобразят действията по обработване на лични данни чрез системи за видеонаблюдение с новите стандарти защита на личните данни, въведени с разпоредбите на Регламент (ЕС) 2016/679.

Съгласно чл. 24 от Общия регламент за защита на личните данни, след като вземе предвид естеството, обхвата, контекста и целите на обработването, администраторът следва да въведе подходящи технически и организационни мерки, за да гарантира, както и във всеки един момент да е в състояние да докаже, че обработването се извършва в съответствие с правилата на Регламента. В конкретния казус, още на етапа на изграждането на системите за видеонаблюдение следва да се отчетат рисковете с различна вероятност и тежест за правата на физическите лица, обект на видеонаблюдението и съответно да се въведат подходящите мерки (технически и организационни), които ще осигурят законосъобразното протичане на дейностите по обработване. По този начин ще се отговори и на изискванията на чл. 25 от Регламента – защита на данните на етапа на проектирането и по подразбиране.

В случая е важно да се отбележи, че изискванията за законосъобразно и добросъвестно обработване на лични данни в съответствие с правилата на Общия регламент за защита на личните данни важат и за обработващите лични данни, които ще обработват данни от името на администраторите на лични данни (например трети лица, които ще поддържат системите за видеонаблюдение). Ако в хода на дейностите по обработване на данните за администраторите възникне необходимост да ползват услугите на обработващ лични данни, то взаимоотношенията и отговорностите следва да бъдат уредени съобразно разпоредбите на чл. 28 от Регламент (ЕС) 2016/679.

Важно задължение за администраторите е въведено с чл. 30 от Регламент (ЕС) 2016/679, съгласно който всеки администратор е длъжен да поддържа регистър на дейностите по обработване, за които отговаря. В случая за целите на извършваното видеонаблюдение на

определени категории лица, следва да поддържат отделен регистър „Видеонаблюдение“, с изчерпателно посочената в чл. 30 от регламента информация.

Съществен момент във връзка със законосъобразното поведение на администраторите на лични данни е изпълнението на разпоредбите на чл. 12 и 13 от Регламент (ЕС) 2016/679 относно предоставяне на необходимата информация на субектите на данни, както и уведомяване на физическите лица за правата им във връзка със същия регламент. Това е необходимо да се осъществи при регламентиран ред, в който да се посочат лицата, които ще осъществяват видеонаблюдението и ще имат достъп (локален и отдалечен такъв) до видеокадрите и записите от системите за видеонаблюдение, ясното обозначаване на обхвата на заснемане и зоните, в които ще се използват техническите средства за наблюдение, както и данни за връзка с администратора.

В контекста на разглеждания казус администраторите следва да уведомят родителите/настойниците на децата и малолетните ученици, както и непълнолетните ученици чрез информационни табели, поставени на видно място, за използването на технически средства за видеонаблюдение и контрол. По този начин действията на администраторите ще бъдат съобразени и с разпоредбите на чл. 32, ал. 2 от Конституцията на Република България, които постановяват, че никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без неговото знание.

Във връзка с горното и на основание чл. 10, ал. 1, т. 4 от Закона за защита на личните данни, Комисията за защита на лични данни изразява следното

СТАНОВИЩЕ:

От гледна точка защита на личните данни, въвеждането на видеонаблюдение в ясли, детски градини и училища е допустимо с оглед подобряване на сигурността и прозрачността на грижите, както и решаване на възникнали конфликти при отглеждането на децата в детските заведения, а също и в училищата, както и с цел защита живота и здравето на най-уязвимата категория от обществото като цяло – децата и непълнолетните български граждани.

Едновременно с посоченото, в случая следва да се вземе предвид и обществения интерес от въвеждане на прозрачност в грижите за децата и подрастващите, тъй като въпросът за сигурността, живота и здравето на българските деца и ученици е от първостепенна важност за обществото като цяло.

В конкретния казус като нормативна законосъобразна предпоставка следва да се приложат разпоредбите на Регламент (ЕС) 2016/679 (Общ регламент за защита на личните данни – приложим от 25 май 2018 год.), както и националната уредба, действаща до 25.05 2018 год., разписана в Закона за защита на личните данни. В случая приложение може да

намерят две от алтернативно изброените предпоставки за законосъобразност на обработването, разписани в чл. 6 от Регламент (ЕС) 2016/679, а именно: чл. 6, пар. 1, буква г) – обработването е необходимо, за да бъдат защитени жизнено важни интереси на субекта на данните или на друго физическо, както и чл. 6, пар. 1, буква д), предл. първо – обработването е необходимо, за изпълнение на задача от обществен интерес. В действащия Закон за защита на личните данни са валидни разпоредбите на чл. 4, ал. 1, т. 4 и т. 5.

С оглед на защита на правата на децата и учениците е недопустимо извършването на видеонаблюдение в помещения за сън, в санитарните помещения, в помещенията за почивка и лична хигиена на децата, тъй като с наличните устройства в тези помещения не се дава право на децата на уединение и запазване на личното им достойнство, както и представлява нарушение на правото на неприкосновеност на личността.

Допустимо е извършването видеонаблюдение в общите помещения и дворните пространства, което да гарантира безопасността на децата и учениците при игри, занимания и в свободното им време. Такова наблюдение е допустимо единствено да бъде приложено за местата на заниманията, ако са отделени от местата за сън и почивка, и в общите части на сградата.

Администраторите на лични данни е необходимо да отчетат задълженията и отговорностите си, произтичащи от разпоредбите на Регламент (ЕС) 2016/679, както и да съобразят действията по обработване на данните чрез видеонаблюдение с новите стандарти защита на личните данни, въведени с разпоредбите на регламента, подробно описани в мотивната част на настоящото становище.

Администраторите на лични данни задължително следва да уведомят родителите/настойниците на децата и малолетните ученици, както и непълнолетните ученици чрез информационни табели, поставени на видно място, за използването на технически средства за видеонаблюдение и контрол. По този начин действията на администраторите ще бъдат съобразени и с разпоредбите на чл. 32, ал. 2, предл. първо от Конституцията на Република България

Гласували четирима членове на КЗЛД - Цанко Цолов, Цветелин Софрониев, Мария Матева – за, Веселин Целков - против.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/

З А П О В Е Д

№ РД07 – 044/23.10.2018г.

На основание чл.258, ал.1 ; чл.259 от ЗПУО ; Закона за защита на личните данни;
ВЪТРЕШНИ ПРАВИЛА за защита на личните данни събирани, обработвани,
съхранявани и предоставяни от ДГ „Буратино“

УТВЪРЖДАВАМ

Вътрешни правила за защита на личните данни събирани, обработвани,
съхранявани и предоставяни от от Детска градина „Буратино“

ДИРЕКТОР


Галина Котленска

З А П О В Е Д

№ № РД07 – 045/23.10.2018г.

На основание чл.258, ал.1 ; чл.259 от ЗПУО ; **ВЪТРЕШНИ ПРАВИЛА** за защита на личните данни събирани, обработвани, съхранявани и предоставяни от ДГ „Буратино“

О П Р Е Д Е Л Я М:

Списъка на длъжностите на лицата, които обработват лични данни в Дружеството по Регистър „Видеонаблюдение“:

1. Директор

ДИРЕКТОР

Галина Котленска

ЗАПОВЕД

№ № РД07 – 046/23.10.2018г.

На основание чл.258, ал.1 ; чл.259 от ЗПУО ; **ВЪТРЕШНИ ПРАВИЛА** за защита на личните данни събирани, обработвани, съхранявани и предоставяни от ДГ „Буратино“

О П Р Е Д Е Л Я М:

Списъка на длъжностите на лицата, които обработват лични данни в Дружеството по Регистър „Пропусквателен режим“:

1. Учители
2. Помощен персонал
3. Медицински лица

ДИРЕКТОР

Галина Котленска

З А П О В Е Д
№ № РД07 – 047/23.10.2018г.

На основание чл.258, ал.1 ; чл.259 от ЗПУО ; **ВЪТРЕШНИ ПРАВИЛА** за защита на личните данни събирани, обработвани, съхранявани и предоставяни от ДГ „Буратино“

О П Р Е Д Е Л Я М:

Списъка на длъжностите на лицата, които обработват лични данни в Дружеството по Регистър „Персонал“:

1. Директор
2. ЗАС
3. Счетоводител

ДИРЕКТОР


Галина Котленска

З А П О В Е Д
№ № РД07 – 048/23.10.2018г.

На основание чл.258, ал.1 ; чл.259 от ЗПУО ; **ВЪТРЕШНИ ПРАВИЛА** за защита на личните данни събирани, обработвани, съхранявани и предоставяни от ДГ „Буратино“

О П Р Е Д Е Л Я М:

Списъка на длъжностите на лицата, които обработват лични данни в Дружеството по Регистър „Родители“:

1. Директор
2. Учители
3. ЗАС
4. Медицински персонал

ДИРЕКТОР

Галина Котленска

З А П О В Е Д

№ № РД07 – 049/23.10.2018г.

На основание чл.258, ал.1 ; чл.259 от ЗПУО ; **ВЪТРЕШНИ ПРАВИЛА** за защита на личните данни събирани, обработвани, съхранявани и предоставяни от ДГ „Буратино“

О П Р Е Д Е Л Я М:

Списъка на длъжностите на лицата, които обработват лични данни в Детската градина по Регистър „Обучаеми“:

1. Директор
2. Учители
3. ЗАС
4. Медицински персонал

ДИРЕКТОР

Галина Котленска