ОСНОВНО УЧИЛИЩЕ „ХРИСТО БОТЕВ“ С.ПАРТИЗАНИ С.ПАРТИЗАНИ УЛ.15 №11 ТЕЛ: 0997377641 ЕЛ.ПОЩА info-400143@edu.mon.bg

УТВЪРЖДАВАМ!

ДИРЕКТОР БОРИСЛАВ НИКОЛОВ

ВЪТРЕШНИ ПРАВИЛА

ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ НА ОУ“ХРИСТО БОТЕВ“ С.ПАРТИЗАНИ ОБЩ.ДЪЛГОПОЛ ОБЛ.ВАРНА

I. Общи положения

Чл. 1. (1) Основно училище „Христо Ботев" – с. Партизани, общ. Дългопол , обл.Варна,наричано по-долу УЧЕБНО ЗАВЕДЕНИЕ е юридическо лице със седалище: с. Партизани 9243, община Дългопол, област Варна, ул. „Петнадесета “ №11 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 неправомерен 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 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 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

прекъсването 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 ангажименти за поддържането 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, които 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 изискванията 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. 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 автоматизираните 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 автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с високо 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 реда 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, памети 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.

(2) С цел поддържане 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 съответните изисквания и позволява възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето й на сервизната фирма 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.

Законът 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 техното управление

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

1. Обучаеми

2. Родители

3. Персонал

4. Пропускателен режим

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 – роднствени 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:

Обработващите лични данни на регистър „Обучаеми" са: класните ръководители, ръководителят на групи. Операторите на лични данни на регистър „Обучаеми" са всички педагогически специалисти. Длъжностните лица – обработващи лични

данни и операторите 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 чрез поддържане на антивирусни програми, периодично архивиране на данните 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. земетресение, независещи от УЧЕБНОТО ЗАВЕДЕНИЕ – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари – евентуално 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 системата „Обучение" имат и държавните органи – МОН, РУО, дирекция „Инспекторат по образованието" 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 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 заличават физически, чрез изгаряне за което се изготвят актове-протоколи за унищожаване.

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

(2) Обхват относно 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 оперативните места за лични данни. Информацията се записва предвидените за това регистри със материалноправните изисквания 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 НЕЙОПУО за администрацията на УЧЕБНОТО ЗАВЕДЕНИЕ. Същите данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно нормативната уредба в УЧЕБНОТО ЗАВЕДЕНИЕ/Вътрешни срокове за съхранение;

(4) Определяне на длъжностите:

Обработващи личните данни на регистър „Родители" са: директора на училището, класните ръководители, ръководителите на ГЦОУД. Оператор на лични данни на регистър „Родители" е целият 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 охраняват само служителите с оглед изпълнение на служебните им задължения (не чистачки, външни 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 данните 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: обучение, план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. запознаване с опасностите, произтичащи от УЧЕБНОТО ЗАВЕДЕНИЕ – предприемат се конкретни действия в зависимост от конкретната ситуация;

2. защита от пожари – изгасяване чрез използване 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, РУО, дирекция.

„Сигнално подхождане" за изпълнение на техните задължения, предвидени в съответните специални и подзаконови нормативни актове.

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

(9) Личните данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със срокове 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 унищожаването.

Чл. 25. (1) В регистър „Персонал" се набират и съхраняват лични данни с цел индивидуализиране на физическите лица, назначени по трудово правоотношение и/или и по граждански договори.

(2) Обхват на обработваните данни в регистър „Персонал"

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение и

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. Дейности, свързани със: сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, досиетата на трудовите 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 помещения, намиращи 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 компютри.

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

(4) Определяне на длъжностите.

Обработващи лични данни по регистър „Персонал" са: директор на училището и касиер-счетоводител.

Определяне на лицата, които имат достъп до регистър „Персонал" с директора..

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

1. целостност – високо ниво;

2. изолираност – високо ниво;

3. надеждност – високо ниво;

4. общо за регистъра – високо 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 достъпът до тях е ограничен само за служители с оглед изпълнение на служебните им задължения от 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 срещу случайно унищожаване. Техническите мерки за физическа защита включват заключващи се шкафове, 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 постоянно поддържане на антивирусни програми, периодично архивиране на данните, 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 по твърд диск, на изолиран компютър.

При инсталиране на нов приложен продукт за обработване на лични данни се проверяват всички аспекти 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 определя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. Защита при аварии, възникнали 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 за изпомпва водата средства или загребва със собствени или наети средства.

(8) Достъп до регистър „Персонал" имат и държавните органи – НАП, НОИ, МОН и МВР по реда на възникване на трудовите задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съдилища, прокуратури, разследващи органи и др., когато са изискали данните във връзка с изпълнението на техните правомощия.

(9) Личните данни се съхраняват до осъществяване на целите, за които се обработват, но не по-дълго от периода, предвиден съгласно Номенклатурата на делата със срокове за тяхното съхранение в УЧЕБНОТО ЗАВЕДЕНИЕ

(10) След изтичане целите по предходната алинея личните данни се унищожават физически след изтичане за което се изготвят актови протоколи за унищожаване.

Чл. 29. (1) В регистър „Пропускателен режим" се набират и съхраняват лични данни с цел идентифициране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват данни, са посетителите в сградата на УЧЕБНОТО ЗАВЕДЕНИЕ.

(2) Обработването на регистър „Пропускателен режим"

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

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

(4) Определяне на длъжностите:

Обработващ личните данни в регистър „Пропускателен режим" е обслужващият персонал. Оператор на личните данни на регистър „Пропускателен режим е Директорът

(5) Вида на информационните масиви в регистъра по отношение на различните критерии е, както следва:

1. повсеместност – ниско ниво;

2. [illegible] – ниско ниво;

3. мащабност – ниско ниво;

4. обем на регистъра – ниско ниво

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

(7) Действия в случай на аварии, произшествия и бедствия: длъжностното лице уведомява прекият си ръководител.

(8) Достъп до регистъра „Пропускателен режим": Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните и на лица, само в предвидено в нормативен акт.

(9) Личните 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) [illegible] 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.

(13) Личните данни в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на УЧЕБНОТО ЗАВЕДЕНИЕ.

V. Права и задължения на лицата, обработващи лични данни

Чл. 28. (1) Лицата по защита на личните данни с 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 нивата на защита;

2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на поддържаните 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 регистрация на лични данни;

5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

6. спецификира техническите ресурси, прилагани за обработка на личните данни;

7. защитава организацията на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регламентиране на всички извършвани действия с регистрите в компютърната среда;

8. определя реда за съхраняване и унищожаване на информационни носители;

9. провежда периодичен контрол за спазване на изискванията по защита на данните и при откриване на нередности взема мерки за тяхното отстраняване.

Чл. 20. (1) Служителите на ОБЩИНСКО ЗАВЕДЕНИЕ са длъжни:

1. да обработват личните данни законосъобразно и добросъвестно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които те 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 разпространяват лични данни, до които са получили достъп при и по повод изпълнението 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 причинени вреди на трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако извършеното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

VI. Реда 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 на субекта 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 прилагат документите, ако същото се подава от упълномощено лице.

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

1. По електронен път на електронен адрес на длъжностното лице по защита на личните данни, което е определено от съответния администратор в структурата на УЧЕБНОТО ЗАВЕДЕНИЕ (email:400143@edu.mon.bg) по реда на Закона за електронния документ и електронните удостоверителни услуги;

2. На място, в УЧЕБНОТО ЗАВЕДЕНИЕ на адрес: с. Партизани, 9245, община Долна област Варна, ул. [illegible]

6. Лицето сред служители или външни служби до адреса на УЧЕБНОТО ЗАВЕДЕНИЕ. Преди УЧЕБНОТО ЗАВЕДЕНИЕ може да изиска да извърши допълнителни действия по идентификация на лицето.

(5) Исканията трябва да бъдат отправени лично или от пълномощник с нотариално заверено пълномощно.

(6). Искането се подава на УЧЕБНОТО ЗАВЕДЕНИЕ.

(7) Длъжностното лице, получило искането за упражняване на индивидуални права на субектите на данни, своевременно и срок от 48 часа информира всички звена, които обработват лични данни за лицето, както и съответните длъжностни лица по защита на личните данни.

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

(9) Администраторът не може да откаже действията за упражняването на правата на субекта на данните и не откаже 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, необходима за потвърждаване на самоличността му.

(11) За всички данни да бъдат взети се извършва служебна проверка за наличността им в регистри и масиви на електронен и хартиен носител, с които УЧЕБНОТО ЗАВЕДЕНИЕ работи.

Чл. 30. (1) При подадено искане за упражняване на права по защита на лични данни УЧЕБНОТО ЗАВЕДЕНИЕ предоставя информация относно предприетите действия по разглеждането му, в срок от един месеца от получаването му. Този срок може да бъде удължен с още два месеца, като се вземе предвид сложността и броя на направените искания от определено лице. УЧЕБНОТО ЗАВЕДЕНИЕ информира субекта на данните за всяко удължаване в срок от един месец от получаването на искането, като посочва и причините за удължаването.

(2) При подадено искане за достъп до личните данни, УЧЕБНОТО ЗАВЕДЕНИЕ потвърждава дали се обработват лични данни за субекта и съответно предоставя поисканата информация. УЧЕБНОТО ЗАВЕДЕНИЕ може да откаже да предостави искането за достъп в случаите, когато задължението за достъп е явно неоснователно или прекомерно, особено поради своята повторяемост.

Чл. 30. (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, което е направило искането. УЧЕБНОТО ЗАВЕДЕНИЕ не е задължено да отговаря на искания, в случай че не е в състояние да идентифицира субекта на данните или неговите пълномощия.

(2) УЧЕБНОТО ЗАВЕДЕНИЕ може да поиска предоставянe на допълнителна информация, когато е необходимо, за потвърждаване на самоличността и пълномощията на субекта на данните. 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

обработването на личните данни без заплащане на каквито и да е такси.

Чл. 37. (1) За всеки унищожаване на лични данни се издава нарочна заповед на административното ръководство, от която се комисия и се съставя надлежен протокол за унищожаването. Всяка служител, ръководител на звено, който е в пряк контакт с документи, съдържащи лични данни е отговорен за сигурното им унищожаване.

(2) Когато унищожаването на данните е в резултат на искане на субект на данни, то получава копие от протокола за унищожаване по електронен път или на посочения пощенски адрес.

(3) Физическите лица, субекти на данни, които са недоволни от действията на съответните длъжностни лица в УЧЕБНОТО ЗАВЕДЕНИЕ могат да отправят писмено 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 публичен орган, 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.

„Нарушение на сигурността на личните данни" е нарушение на обработката на личните данни в значителен обхват и/или от тях.

„Обработване на лични данни" е всяко действие или съвкупност от действия, които могат да бъдат извършени по отношение на личните данни с автоматични или неавтоматични средства, като събиране, записване, организиране, съхраняване, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

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

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

„Оценка на въздействието" е процес за определяне нивата на въздействие върху конкретно физическо лице или групи физически лица, в зависимост от

характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на сигурността, цялостността или наличността на личните данни.

„Поверителност" е изискване за криптиране на личните данни на неоторизирания достъп до тях по време на тяхното обработване.

„Предоставяне на лични данни" са действия по цялостно или частично прехвърляне 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, достъпът до които е осъществен 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 УЧЕБНИЯ ЗАВЕДЕНИЕ са длъжни срещу подпис да се запознаят с настоящата Заповед.

§3. За неуредените 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 ЕС.

ПРИЛОЖЕНИЕ№ 1

ОЦЕНКА НА РИСКОВО ВЪЗДЕЙСТВИЕ НА РЕГИСТРИТЕ

В ОУ"ХРИСТО БОТЕВ" С.ПАРТИЗАНИ

Име на регистъра ПЛАН НА БЪЗДЕЙСТВИЕ

поверителност цялостност наличност общо за регистъра

Обучаеми ниско ниско ниско ниско

Родители ниско ниско ниско ниско

Персонал ниско ниско ниско ниско

Пропускателен 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 имат 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 от Вас и Вашите обработващи 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 убеждения.

- 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 осъществявана по следните начини:

☐ на следния телефонен номер:

. . . . . .

☐ на посочен имейл адрес:

. . . . . .

☐ чрез кореспондентска 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 ОЗРД)

ОТ: .....

.....

(три имена и ЕГН)

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

Уважаеми господин/ Николай,

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 ОЗРД), както следва:

(В съответното квадратче поставете 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 удобен начин за комуникация.)

Искане за достъп до личните ми данни (чл. 15 ОЗРД)

Известно ми е, че съхранява

.....

.....

са свързани със следните операции по обработване в администратора. .....

.....

и са ми необходими за следната цел: .....

☐ Искане за достъп до личните 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 ОЗРД)

Известно ми е, че искам да се коригират 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 настоящото декларирам, че желая свързаните с мен лични данни да бъдат изтрити без ненужно забавяне, по следната причина*: . . . . . .

. . . . . .

Моля да ме уведомите при изтриване администратора и обработващи личните ми данни, че съм поискал изтриването 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 личните и няма друго правно основание за обработването; (iii) субектът на данните

възразява срещу обработването да 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 пред субекта на данните възразява срещу обработването за целите на директния маркетинг; (v) личните данни са били обработвани незаконосъобразно; (vi) 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, че оспорвам верността на следните ми лични данни . . . . . .

. . . . . .

се 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 моите 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 изтрити, а вместо това изисква ограничаване на използването им; в) администраторът вече не се нуждае 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)

Извършвам моето искане, като Ви информирам, че следните ми лични данни . . . . . .

. . . . . .

са свързани със следните операции по обработване в администратора. . . . . .

. . . .

. . . . . .

.

с мотивацията, че моето право на обработването на личните ми данни поради следните причини: . . . . . .

. . . .

☐ Искане за преносимост на данни за преносимост на личните данни (чл. 20 ОЗРД)

Извършвам моето искане, като Ви информирам, 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 предоставено по-горния администратор на лични данни . . . . . .
. . . . . на хартия, по следния адрес . . . . . .
. . . . . чрез по електронен път на следния защитен електронен адрес: . . . . . .
. . . . . чрез по куриер на следния адрес . . . . . .
. . . . . .

Допълнителна информация:
. . . . . .

. . . . . .
. . . . . .

Изразявам съгласието комуникацията с мен във връзка с изпълнението на

настоящото искане да бъде извършвана по следните начини:

на следния електронен адрес . . . . . .

☐ на следния пощенски адрес:

. . . . . .

☐ чрез комуникационни взаимоотношения 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 осъществяване на самоличността на личните му данни, осигуряване на правото му на информираност въз основа Общия ОРЗД. Данните ще се съхраняват за осигуряване на актуализиран интерес на администратора за проверки от КЗЛД до по-късната от двете дати – пет години след обработване на искането или датата на изтриване.