ВТОРО ОСНОВНО УЧИЛИЩЕ „ГОЦЕ ДЕЛЧЕВ”,
гр. Гоце Делчев, бул. ”Гоце Делчев” №13; тел.:0751/60299;
e-mail: info-103403@edu.mon.bg, web site: vtoro-ou-gd.com

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

I. ПРЕДМЕТ

Чл. 1. (1) Настоящите правила („Правилата“) определят реда, по който учебното заведение, с ЕИК 000012530 събира, записва, организира, структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подрежда или комбинира, ограничава, изтрива, унищожава или обработва по друг начин лични данни за целите на своята дейност.

(2) В зависимост от конкретната ситуация, учебното заведение може да обработва данни в качеството на администратор или обработващ.

(3) Правилата са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. 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.

Чл. 2. Настоящите Правила уреждат:

(1) Принципите, процедурите и механизмите за обработка на личните данни;

(2) Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;

(3) Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;

(4) Лицата, които обработват лични данни, и техните задължения;

(5) Правилата за предаване на лични данни на трети лица в България и чужбина;

(6) Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;

(7) Техническите ресурси, прилагани при обработката на лични данни.

ДЕФИНИЦИИ

Чл. 3. За целите на настоящите Правила, използваните понятия имат следното значение:

• **ЗЗЛД** – Закон за защита на личните данни.

• **КЗЛД** – Комисия за защита на личните данни.

• **ОРЗД** – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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);

• **„лични данни“** означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;• **„обработване“** означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

• **„ограничаване на обработването“** означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

• **„профилиране“** означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

• **„псевдонимизация“** означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

• **„съгласие на субекта на данните“** означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на

субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

• **„получател“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

• **„администратор“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

• **„обработващ лични данни“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

• **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;

• **„трета страна“** означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

• **„нарушение на сигурността на лични данни“** означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

• **„генетични данни“** означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

• **„биометрични данни“** означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо

лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

• **„регистър с лични данни“** означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

II.СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 4. (1) Учебното заведение събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на образователни услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от учебното заведение, са групирани в регистри на дейностите по обработване, съдържащи правила за обработване на лични данни, отнасящи се до:

• работници и служители;
• изпълнители по граждански договори;
• кандидати за работа;
• доставчици на услуги;
• ученици и родители;
• видеонаблюдение;
• пропусквателен режим.

(2) Относно ученици и родители се събират лични данни, подробно разписание в Инструкция за мерките и средствата за защита на личните данни събирани, обработвани,съхранявани и предоставяни от учебното заведение.

(3) Относно лицата, заети по трудови или граждански правоотношения в учебното заведение и на кандидатите за работа, се събират лични данни,подробно разписание в Инструкция за мерките и средствата за защита на личните данни събирани, обработвани,съхранявани и предоставяни от учебното заведение.Относно физически и юридически лица, контрагенти на учебното заведение, се събират лични данни, подробно разписание в Инструкция за мерките и средствата за защита на личните данни събирани, обработвани, съхранявани и предоставяни от учебното заведение.Относно физически лица, доставчици на услуги на учебното заведение, се събират лични данни, подробно разписание в Инструкция за мерките и средствата за защита на личните данни събирани, обработвани,съхранявани и предоставяни от учебното заведение. Относно физически лица кандидати за работа в учебното заведение, се събират лични данни, подробно разписание в Инструкция за мерките и средствата за защита на личните данни събирани, обработвани, съхранявани и предоставяни от учебното заведение.

(4) Учебното заведение заведение обработва специални категории лични данни, които попадат в обхвата на чл. 9 на Общия регламент относно защитата на данните, само доколкото това е необходимо за изпълнение на специфичните му права и задължения.

III. ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 5. Целите на обработването на лични данни са:

(1) Обучение и администрация: Провеждане на образователния процес, водене на задължителна училищна документация;

(2) Управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на учебното заведение в качеството му на работодател;

(3) Администриране на отношенията с контрагенти на учебното заведение и предоставяне на услуги;

(4) Сключване и изпълнение на договори с доставчици за предоставяне на услуги на учебното заведение.

(5) Безопасност и сигурност: Опазване здравето и живота на учениците, пропускателен режим в сградата и контрол на достъпа.

(6) Комуникация: Връзка с родителите или настойниците относно успеха, дисциплината и училищните мероприятия.

Чл. 6. Личните данни:

(а) да се обработват законосъобразно и добросъвестно;

(б) да се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели;

(в) допълнително обработване на личните данни за исторически, статистически или научни цели е допустимо, при условие че администраторът осигури подходяща защита, като гарантира, че данните не се обработват за други цели;

(г) да бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват;

(д) да бъдат точни и при необходимост да се актуализират;

(е) да се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

(ж) да се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

(з) личните данни, които ще се съхраняват за по-дълъг период за исторически, статистически или научни цели, се поддържат във вид, непозволяващ идентифицирането на физическите лица.

Чл. 7. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

(1) Субектът на данните е дал своето съгласие;

(2) Това е необходимо за изпълнение на нормативно установено задължение;

(3) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

(4) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

(5) Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;

(6) Обработването е необходимо за изпълнение на задача от обществен интерес;

(7) Обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание, трябва да са описани в приложимите известия по защита на данните;

(8) Всички служители в учебното заведение при встъпване в длъжност се задължават да спазват конфиденциалност по отношение на базата данни в т. ч. лични данни, както и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения, като за тази цел подписват декларация по образец;

(9) Учебното заведение поддържа вътрешен ред като администратор на лични данни, като осигурява технически и организационни мерки за защита.

IV.СЪГЛАСИЕ

Чл. 8. (1) Изразеното съгласие трябва да бъде свободно дадено, конкретно, информирано и недвусмислено заявено. Ако съгласието за обработка на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси. Съгласието трябва да бъде дадено свободно. Такова съгласие е налично в случаите, когато субектът на данни има истински и свободен избор и е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

(2) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

(3) Декларациите за съгласие се съхраняват от учебното заведение, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност.

(4) Учебното заведение трябва да може да докаже наличието на съгласие.Субектът на данните следва да бъде информиран за последиците при отказ да даде съгласие за обработване на отделни категории лични данни.

(5) Съгласието може да бъде дадено онлайн. Това може да бъде осъществено чрез отбелязване на отметка в поле, избиране на технически настройки за услуги на информационното общество или друго заявление или поведение, което ясно показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Мълчанието, предварително отметнатите полета или липсата на действие не представляват съгласие.

V. ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Процедура за обработване на личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в учебното заведение, както и на кандидатите за работа.

Чл. 9. (1) Администраторът възлага обработването на личните данни на определени негови служители, на които в длъжностната характеристика има вменени такива трудови функции. В зависимост от естеството на работа, обработването може да се възложи на повече от един обработващ данните. Обработващите личните данни лица, действат само по указания на администратора, освен ако в нормативен акт не е предвидено друго. Личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в учебното заведение, както и на кандидатите за работа, се събират при и по повод набирането на персонал. Данните на всеки работник и служител на учебното заведение се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси и интервюта или събеседване се съхраняват на технически и/или хартиен носител, в зависимост от нуждата.

(2) Личните досиета се подреждат в специални картотечни шкафове със заключване, находящи се в кабинета на Лицето, отговорно за личните данни. Достъпът до кабинета се предоставя само на лицата, оправомощени да обработват личните данни, като за целта се създава специален ред за влизане в помещението чрез ключ, магнитна карта или друго подходящо средство и/или устройство и това се регламентира в нарочна заповед/индивидуален административен акт/, която се свежда до знанието на персонала на учебното заведение.

(3) Администраторът на лични данни предприема всички организационно-технически мерки за съхраняването и опазването на личните досиета и класьорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

(4) Досиета на работниците и служителите, както и данните на кандидатите за работа, не се изнасят извън сградата на учебното заведение, освен в случаите когато това е предвидено в закон.

Чл. 10. (1) Личните данни, отнасящи се до доставчици на услуги, се събират при сключване на договор с доставчик на услуги, като обичайно личните данни се съдържат в текста на самите договори, което е презумпция за безусловно изразено съгласие на страните.

(2) Личните данни се съхраняват на електронен и хартиен носител (подписани копия на сключените договори), които се класират в отделни досиета. Досиетата се съхраняват в шкафове, които се заключват, в кабинета на Лицето, отговорно за личните данни. Електронните данни се съхраняват в бази данни.

VI. ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 11. (1) Учебното заведение, в качеството си на администратор на лични данни, има правно задължение да документира всяка дейност по обработване. Това изискване произтича директно от принципа за отчетност съгласно чл. 5 от GDPR.

Основната документация в едно училище включва следните задължителни елементи:

2. Регистър на дейностите по обработване

Това е най-важният документ, който доказва съответствието с правилата за защита на данните. Той съдържа писмена информация за:

(а) Името и координатите на училището и на Длъжностното лице по защита на данните (DPO);

(б) Целите на обработването (обучение, трудови досиета, сигурност);

(в) Категориите субекти (ученици, родители, учители, външни лица) и категориите лични данни (три имена, ЕГН, оценки, здравни данни);

(г) Категориите получатели, пред които се разкриват данните (МОН, РУО, НАП, НОИ, МВР, ДАЗД, Агенция социално подпомагане, съдебните органи и разследващите органи);

(д) Сроковете за съхранение на различните видове документи съгасно относимата нормативна уредба;

(е) Техническите и организационни мерки за сигурност (напр. криптиране, заключващи се шкафове, контрол на достъпа).

3. Вътрешна нормативна уредба (политики и правила):

(а) Политика за защита на личните данни: Стратегически документ, който описва как училището прилага принципите на GDPR;

(б) Вътрешни правила за обработване и защита: Конкретни инструкции към персонала как да борави с електронните платформи (напр. Школо/НЕИСПУО);

(в) Политика за видеонаблюдение: Ако в училището има камери, този документ урежда къде е разположено то, кой има достъп до записите и колко време се пазят те.

4. Информационни документи и форми за съгласие:

(а) Уведомление за поверителност**:** Задължителна информация, която се предоставя на родителите и служителите преди събирането на данните (съгласно чл. 13 от GDPR). Обикновено се публикува на сайта на училището или се предоставя при записване;

(б) Формуляри за съгласие: Декларации за информирано съгласие, когато обработването не е по закон (като публикуване на снимки в сайта на училището, фейсбук страницата или участие в извънкласни проекти).

5. Документи при инциденти и оценка на риска:

(а) Регистър на нарушенията на сигурността: Документират се всички случаи на изгубване, кражба или неправомерен достъп до лични данни, предприетите мерки и дали е уведомена КЗЛД;

(б) Оценка на въздействието върху защитата на данните: Извършва се задължително при въвеждане на нови технологии с висок риск.

VII. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 12 Приемане на план за действие за въвеждане на определените технически и организационни мерки:

(а) определяне на отговорник и екип.

(б) определяне на срокове и етапи за изпълнение.

(в) осигуряване на необходими финансови, технически и човешки ресурси.

(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.

Основните приложими организационни мерки за физическа защита в учебното заведение включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп. Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и

административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения.

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

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

Като зони с контролиран достъп се определят всички помещения на територията на учебното заведение, в които се събират, обработват и съхраняват лични данни.

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

Чл. 13. (1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа. Възможните технически средства за контрол на достъпа са:

(а) охрана на помещенията;

(б) устройства за разпознаване чрез магнитна карта и/или ключ;

(в) наблюдение с видеокамери в коридорите;

(г) политика на допускане на външни лица до помещенията на учебното заведение само с придружител от персонала на същото.

(2) Помещенията на учебното заведение са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

VIII. МЕРКИ ЗА ДОКУМЕНТАЛНА ЗАЩИТА

Чл. 14. (1) Учебното заведение установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение. За отделни категории данни може да се предвиди псевдонимизиране по предложение на Лицето, отговорно за личните данни.

(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.

IX. ПЕРСОНАЛНИ МЕРКИ ЗА ЗАЩИТА

Чл. 15. (1) Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни:

(а) поемат задължение за неразпространение на личните данни, до които имат достъп;

(б) запознават се с нормативната база, вътрешните правила и политики на учебното заведение относно защитата на личните данни;

(в) задължават се да не споделят критична информация помежду си и с външни лица, освен по установения с тези Правила ред.

(2) При постъпване на работа всички служители преминават обучение за реакция при събития, застрашаващи сигурността на данните, и обучение относно задълженията на учебното заведение, свързани с обработката на лични данни, и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

X. МЕРКИ ЗА ЗАЩИТА НА АВТОМАТИЗИРАНИ ИНФОРМАЦИОННИ СИСТЕМИ И КРИПТОГРАФСКА ЗАЩИТА.

Чл. 16 (1) Защитата на автоматизираните информационни системи и прилагането на криптографска защита в училище са критични за опазването на личните данни на ученици, родители и учители, както и за сигурността на учебния процес. Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

(2) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, се осигурява посредством:

(а) поддържане на антивирусни програми;

(б) въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни, и файловете, които съдържат лични данни;

(в) периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;

(г) периодично архивиране;

(д) периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител.

Когато данните се намират на сървър, архивирането им се извършва от определено за целта лице, с вменена трудова функция, относима към ЗЗЛД. Когато данните се намират на изолирани компютри, архивирането им се извършва от оператора на съответния компютър.

(3) Периодичното архивиране на лични данни на технически носител е фундаментална мярка за сигурност, която гарантира защитата на информацията от загуба, унищожаване или неправомерен достъп.

(4) Криптографска защита :

(а) защита на мрежовия трафик;

(б) шифриране на устройствата;

(в) сигурна комуникация.

XI. НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 17. (1) Нарушение на сигурността на данни възниква, когато данните, за които учебното заведение отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта. Ако това се случи и има вероятност нарушението да представлява риск за правата и свободите на дадено лице, учебното заведение трябва да ***уведоми надзорния орган, без ненужно забавяне най-късно до 72 часа, след като е узнало за нарушението.*** Нарушенията на сигурността в училище могат да бъдат разделени на три основни категории: физическа сигурност (заплахи за здравето и живота), дигитална/информационна сигурност (хакерски атаки и теч на данни) и психологическа сигурност (тормоз и насилие).

Ако нарушението на сигурността на данните представлява висок риск за засегнатите лица, всички те също трябва да бъдат информирани, освен ако не са въведени ефективни технически и организационни мерки за защита или други мерки, които гарантират, че вече няма вероятност рискът да се случи на практика.Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Лицето, отговорно за личните данни, като му предоставят цялата налична информация.

(2) Лицето, отговорно за личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) Лицето, отговорно за личните данни, докладва незабавно на Директора на учебното заведение наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

(4) След съгласуване с ръководството на учебното заведение, Лицето, отговорно за личните данни, предприема мерки за предотвратяване или

намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, Лицето, отговорно за личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай Лицето, отговорно за личните данни, уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

Чл. 18. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, Лицето, отговорно за личните данни, организира уведомяването на КЗЛД.

(2) Уведомлението до КЗЛД съдържа следната информация:

(а) описание на нарушението на сигурността; категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

(б) посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

(в) описание на евентуалните последици от нарушението на сигурността;

(г) описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(3) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Лицето, отговорно за личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

Чл. 19. (1) Учебното заведение води регистър на нарушенията на сигурността, който съдържа следната информация:

(а) дата на установяване на нарушението-точният момент или дата, на която е открито пробиването на сигурността;

(б) описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението;

(в) описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;

(г) предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за учебното заведение;

(д) предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

(2) Регистърът се води в електронен формат от Лицето, отговорно за личните данни.

XII. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 20. (1) Учебното заведение може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, когато това е предвидено в нормативен акт или въз основа на изричен договор.

(2) В случаите на предоставяне на лични данни , учебното заведение:

(а) изисква достатъчно гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;

(б) сключва писмено споразумение, като лицето подписва декларация или се изготвя друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679;

(в) информира физическите лица, чиито данни ще бъдат предоставени на обработващ.

(3) Обработване на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато:

(а) обработването на лични данни от обработващи извън ЕС/ЕИП е допустимо само при спазване на конкретни условия и гаранции,съгласно Общия регламент за защита на данните(ОРЗД/GDPR). То е допустимо при наличие на адекватно ниво на защита, признато с решение на Европейската комисия,подходящи гаранции като стандартни клаузи, изрично съгласие на субекта след оценка на рисковете, или при конкретни правни необходимости, регламентирани в ОРЗД.

(б) налице са подходящи мерки за защита – като например, стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;

(в) субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове;

(г) трансферът е необходим за една от целите, изброени в ОРЗД, включително изпълнението на договор със субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

XIII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 21. (1) Оценката на въздействието върху защитата на данните (ОВЗД/DPIA) в училище е задължителен процес по чл. 35 от GDPR, когато предвидените операции по обработване могат да породят висок риск за правата и свободите на ученици, родители и персонал.

Тъй като децата се считат за „уязвими субекти“, училищата попадат под по-строг контрол. Съгласно критериите на Комисията за защита на личните данни (КЗЛД) ОВЗД е задължителна в конкретни ситуации в образователната среда.

(2) Кога се изисква ОВЗД в училище:

(а) високорискови дейности: Комисия за защита на личните данни (КЗЛД) изисква оценка при мащабно обработване на специални категории данни или при систематично и мащабно наблюдение на публично достъпна зона (например видеонаблюдение в сградата на училището);

(б) нови технологии: Въвеждане на нови софтуерни решения за електронни дневници, биометричен достъп или онлайн платформи за обучение с поведенчески анализ;

(в) обработване на специални категории данни: Когато училището събира и обработва дигитално здравни данни (медицински бележки, ТЕЛК решения), данни за специални образователни потребности (СОП) или психологически профили на учениците.

(3) Основни екипи и отговорности:

(а) администратор (Училището): Носи отговорност за извършването на оценката преди стартиране на обработването;

(б)длъжностно лице по защита на данните (ДЛЗД): Администраторът задължително изисква становището на ДЛЗД по време на процеса;

(в) заинтересовани страни: При необходимост се иска мнението на самите субекти на данни (родители/ученици) или техните представители и персонал.

(4) Съгласно Член 35, параграф 7 от GDPR, Оценката на въздействието върху защитата на данните (ОВЗД) в училище е официален документ, който трябва да съдържа минимум следните елемента**:**

(а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес**;**

(б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

(в) оценка на рисковете за правата и свободите на субектите на данни-ученици ,педагогически и непедагогически персонал;

(г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

XIV. УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 22. (1) Унищожаването на лични данни в училище е задължителен етап от жизнения цикъл на информацията, регламентиран от Регламент (ЕС) 2016/679 (GDPR) и Закона за предучилищното и училищното образование (ЗПУО). Процесът изисква баланс между спазването на сроковете за задължително съхранение на училищната документация и правото на „да бъдеш забравен“ на учениците, родителите и персонала.

(2) Унищожаване на личните данни се извършва от учебното заведение или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването и при спазване на разпоредбите на относимите нормативни актове.

(3) Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

(4) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина или изгаряне. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

XV. ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТКАТА И СЪХРАНЕНИЕТО НА ЛИЧНИТЕ ДАННИ И ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл. 23. Лицето, отговорно за личните данни и лицата, обработващи личните данни от името на учебното заведение, са физически или юридически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт.

Чл. 24. Лицето, отговорно за личните данни:

(а) подпомага учебното заведение и лицата, обработващите личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;

(б) осигурява нормалното функциониране на гореспоменатите системи за защита;

(в) осъществява контрол през целия процес на събиране и обработване на данните;

(г) изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;

(д) периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;

(е) уведомява ръководството на учебното заведение своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;

(ж) унищожава данните от хартиените и техническите носители съгласно закона и съгласно указанията на оправомощените за това органи.

Чл. 25. (1) Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.Тези задължения следва да са предвидени в длъжностната характеристика на лицето или в сключеният между страните договор.

(2) При възлагане на дейности, налагащи обработката на лични данни от регистрите на учебното заведение, доставчиците на услуги следва да спазват приложимите нормативни изисквания относно обработката на личните данни.

(3) Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ДАЗД, Агенция социално подпомагане, РУО, МОН, ревизиращи органи и други такива определени със закон.

Гореспоменатите органи могат да изискат данните по надлежен ред във връзка с изпълнението на техните правомощия.

XVI. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 26. (1) Според Общия регламент относно защитата на данните (GDPR), субектите на данни в училището (ученици, родители, педагогически, непедагогически персонал,кандидати за работа, външни контрагенти и доставчици на услуги) разполагат с права, за които администраторът, е длъжен да осигури условия за тяхното упражняване.

(2) Основни права на физическите лица:

(а) право на информираност: Училището трябва да предоставя ясна, прозрачна и лесно достъпна информация, за това какви данни събира, защо ги обработва и колко време ги съхранява;

(б) право на достъп: Всяко лице (или родител, когато става въпрос за непълнолетен ученик) има право да поиска потвърждение дали се обработват негови лични данни и да получи копие от тях, заедно с информация за целите на обработването;

(в) право на коригиране: Субектите могат да изискат училището да коригира неточни или да допълни непълни техни лични данни (например сгрешено име и адрес);

(г) право на изтриване („право да бъдеш забравен“): Лицето може да поиска данните му да бъдат изтрити.

Важно: Това право е ограничено в училищна среда, тъй като училището обработва по-голямата част от данните въз основа на закон (Закона за предучилищното и училищното образование) и няма право да изтрива задължителна документация преди изтичане на законовия срок;

(д) право на ограничаване на обработването: Субектът може да поиска училището временно да спре обработването на данните му (например докато се проверява точността на коригирани данни);

(е) право на преносимост на данните: Лицето има право да получи личните данни, които е предоставило на училището, в структуриран и общоизползван формат, за да ги прехвърли на друг администратор (приложимо главно, когато обработването се основава на съгласие или договор);

(ж) право на възражение: Субектът може да възрази срещу обработването на данните му, ако то се основава на легитимен или обществен интерес. Училището трябва да докаже, че съществуват убедителни законови основания, които имат предимство пред интересите на лицето;

(3) право на защита срещу автоматизирано вземане на решения: Лицата имат право да не бъдат обект на решение, основаващо се единствено на автоматизирано обработване (например профилиране), което ги засяга в значителна степен;

(и) права на непълнолетните: За учениците до 14-годишна възраст правата се упражняват изцяло от техните родители или законни представители. За учениците между 14 и 18 години правата се упражняват от тях със съгласието на родителите им.

(3) Учебното заведение е длъжно да предостави информация на лицето (заявителя) относно предприетите действия по негово искане за упражняване на права (например право на достъп, коригиране или изтриване) в срок от 1 месец от получаване на заявлението.

XVII. ПРОМЕНИ НА ВЪТРЕШНИТЕ ПРАВИЛА

Чл. 27. Учебното заведение може да променя тези Правила по всяко време. Всички промени следва да бъдат незабавно сведени до знанието на лицата, които засягат.

Настоящите Правила са приети и влизат в сила на деня на подписването им.

Директор:……. Дата……..