ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ИКОНОМИЧЕСКА ИНФОРМАТИКА "ДЖОН АТАНАСОВ"
7700 Търговище, ул. " Братя Миладинови " № 42 , тел.0878150124,
счетоводство: 0878150122, email : info-2500601 @edu.mon.bg

УТВЪРЖДАВАМ: .....
Виолета Вичева-Иванова
Директор на ПГИИ „Джон

ИНСТРУКЦИЯ

за мерките и средствата за защита на личните данни събирани, обработвани, съхранявани и предоставяни от ПГИИ „Джон Атанасов"

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) ПГИИ „Джон Атанасов" е юридическо лице със седалище гр./с/....., Република България с основен предмет на дейност учебно – възпитателна дейност.

(2) ПГИИ „Джон Атанасов" обработва лични данни във връзка със своята дейност.

Чл. 2. (1) Настоящата инструкция урежда организацията на обработване и защитата на лични данни на педагогическия и непедагогическия персонал, обучаемите (ученици), родители, посетителите, както и на други физически лица, свързани с осъществяването на дейността на учебното заведение.

(2) Целта на настоящата инструкция е установяването на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от учебното заведение регистри, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събираните и обработвани такива данни.

(3) Инструкцията се приема с цел да регламентира:

(а) създаването на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;

(б) необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване

(случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни);

(в) правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

(4) Инструкцията се утвърждава, допълва, изменя и отменя от Директора на учебното заведение.

Чл. 3. (1) Учебното заведение е администратор на лични данни.

(2) Субект на лични данни е всяко живо физическо лице, което е идентифицирано или може да бъде идентифицирано (пряко или косвено) чрез определена информация.

II. ТЕРМИНОЛОГИЯ

Чл. 4. Основни понятия:

• **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

Чл. 5 (1) Личните данни се събират и обработват:

(а) за изпълнение на правомощията и присъщата дейност на учебното заведение, предоставени чрез ЗПУО, подзаконовите нормативни актове относими към системата на образованието, както и законодателството на Република България и ЕС;

(б) образователен процес: за изпълнение на задълженията на училището, предоставени от закона и държавните образователни стандарти;

(в) трудови отношения и гражданскоправни: събиране на данни от педагогическия и непедагогическия персонал във връзка с Кодекса на труда и Кодекса за социално осигуряване, както и при възникването на гражданскоправни отношения;

(г) сигурност и контрол: изграждане на системи за видеонаблюдение и поддържане на регистър „Пропускателен режим" с ограничен достъп.

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

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

(ж) 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;

(з) 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;

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

(2) Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(3) Обработването на лични данни в училище се извършва в строго съответствие с принципите, заложени в **член 5 от Общия регламент относно защитата на данните (GDPR)**. Тези принципи гарантират, че данните на учениците, родителите, персонала, кандидатите за работа и външните контрагенти се съхраняват и използват правилно и безопасно.

III. ОСНОВНИ ПРИНЦИПИ ЗА ОБРАБОТВАНЕ НА ДАННИ В УЧЕБНОТО ЗАВЕДЕНИЕ

Чл. 6 (1)Принципи;

(а) **законосъобразност, добросъвестност и прозрачност:** данните се обработват само на валидно правно основание (напр., нормативно

задължение по Закона за предучилищното и училищното образование) Училището е длъжно да информира ясно и разбираемо родителите, учениците, персонала и посетителите на институцията как и защо използва техните данни;

(б) **ограничение на целите:** данните се събират за конкретни, точно определени и законни цели (напр. за провеждане на обучение, издаване на дипломи, сигурност чрез видеонаблюдение). Те не могат да се използват по-нататък по начин, несъвместим с тези цели;

(в) **минимизиране на данните:** училището изисква и обработва само информация, която е строго необходима за постигане на целите;

(г) **точност:** личните данни трябва да бъдат точни и поддържани в актуален вид. Всички неточни данни (напр. сгрешено име във воденета в училище документация или грешен адрес) трябва да бъдат незабавно коригирани или заличени;

(д) **ограничение на съхранението:** данните се пазят във форма, която позволява идентифицирането на лицата за период, не по-дълъг от необходимото. Сроковете за пазене на училищната документация са нормативно определени в Наредба № 8/11.08.2016 г. за информацията и документите за системата на предучилищното и училищно образование.

(е) **цялостност и поверителност:** училището прилага технически и организационни мерки за защита на данните срещу неразрешено или незаконосъобразно обработване, случайни загуби, унищожаване или повреждане;

(ж) **отчетност:** училищното ръководство носи отговорност и трябва да е в състояние да докаже, че спазва всички горепосочени принципи.

Чл. 7. 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. 8. 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.

Чл. 9. За всяка дейност по събиране на лични данни се поддържа регистър на дейностите, където е определено кой, за какви цели и на какво основание обработва личните данни.

Чл. 10. (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, в съответствие с КТ.

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

Чл. 11. (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 и Закона за счетоводството, както и относимата нормативна уредба в системата на образованието.

(4) Документите на електронен носител се съхраняват на специализирани компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността и за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият лични данни и оторизираните длъжностни лица.

Чл. 12. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 13. (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 директора 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 бил докладван, последствията от него и мерките за отстраняването му.

(3) За настъпилия инцидент се уведомява Комисията за защита на личните данни до 72 часа от узнаването за неправомерния достъп.

Чл. 14. (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. 15. (1) 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 сигурно и необратимо, чрез **физическо унищожаване на самия носител**, така че данните да не могат да бъдат възстановени с никакви съвременни технически средства. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване или изгаряне.

(2) Унищожаване се осъществява от служителя, на когото е възложена тази функция.

Чл. 16. (1) Достъпът до данните от регистъра и разкриването им се осъществява като се предоставят на:

(а) физическите лица, за които се отнасят данните;

(б) трето лице ако е предвидено в нормативен акт;

(в) обработващият лични данни.

(2) Достъп до лични данни може да бъде предоставен под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(3) Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

(4) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(5) Заявлението съдържа:

(а) името, адреса и други необходими данни за идентифициране на съответното физическо лице;

(б) описание на искането;

(в) предпочитана форма за предоставяне на достъпа до личните данни;

(г) подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Директорът на институцията разглежда заявлението за достъп и се произнася по него в срок от един месец от получаването на заявлението.

(7) Директорът на институцията взема решение за предоставянето на пълен или частичен достъп на заявителя или мотивира отказ за предоставяне на достъп.

(8) Директорът на институцията писмено уведомява заявителя за решението си. Уведомяването е лично срещу подпис или по пощата с обратна разписка.

IV. МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 17. (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 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. 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.

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.

(3) 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. 18. (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:

(а) познаване на нормативната уредба в областта на защитата на личните данни;

(б) познаване на политиката и ръководствата за защита на личните данни;

(в) знания за опасностите за личните данни, обработвани от администратора;

(г) споделяне на критична информация между персонала;

(д) съгласие за поемане на задължение за неразпространение на личните данни, изразено в декларация по образец в трудов договор или длъжностна характеристика.

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае".

Чл. 19. (1) Основните приложими мерки за документална защита на личните данни са нормативно и организационно разписани правила, които уреждат как учебното заведение събира, обработва, съхранява и унищожава лична информация. Тяхната цел е да осигурят съответствие с правната рамка (като Общия регламент относно защитата на данните – GDPR и

Закона за защита на личните данни). Тези мерки за документална защита на личните данни са:

(а) определяне на регистрите, които ще се поддържат на хартиен носител;

На хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на училището.

(б) 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.

(в) регламентиране на достъпа до регистрите;

Достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае".

(г) 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.

(д) 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.

Чл. 20. (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 ниско ниво на въздействие, включват:

(а) идентификация и автентификация;

Използване на потребителско име и пароли за всяко лице, което има право на достъп до мрежата и компютърните ресурси.

(б) управление на достъпа;

Този процес съобразен с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка.

(в) поддръжка и софтуерна защита;

Осигуряване на базови технически мерки за сигурност, като използване на лицензиран софтуер, периодично обновяване на операционните системи и наличие на антивирусни програми за защита срещу зловреден софтуер.

(г) политиката по създаване и поддържане на резервни копия за възстановяване на информацията;

Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на учебното заведение.

(3) Основни електронни носители на информация са:

(а) 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.) ;

(б) персоналната защита на данните е част от цялостната охрана на учебното заведение;

(в) личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на учебното заведение;

(г) данните, които вече не са необходими и чийто срок за съхранение е изтекъл, се унищожават.

(д) по отношение на личните данни се прилагат и мерки, свързани с криптографска защита на данните чрез стандартните криптографски възможности на операционните системи, на програмите за управление на бази данни и на специализирания софтуер, с който се работи в учебното заведение, когато това е необходимо.

V.БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 21. (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 повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на отпадане на основанието за достъп до лични данни, правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 22. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказ устойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

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

Чл. 23. (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 осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 24. Служителите, на който е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

IV. Поддържани регистри и тяхното управление

Чл. 25. Поддържаните от учебното заведение регистри с лични данни са най-малко следните такива:

1. „Ученици" ;
2. „Родители";
3. „Персонал" ;
4 „Други специалисти";
5. „Пропускателен и регистрационен режим";
6. „Видеонаблюдение";
7. „Контрагенти и партньори";
8. „Кандидати за работа".

Чл. 26. (1) В регистър **„ученици"** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици ", обучавани в учебното заведение в областта/района.

(2) Общо описание на регистър „ученици"

Регистърът съдържа следните категории лични данни:

(а) име, ЕГН/ЛНЧ, гражданство, адрес, месторождение и телефони за връзка;

(б) родствени връзки;

(в) лични данни, които се отнасят до здравето.

Нормативното основание е ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър „ученици". Носители на данни:

(а) на хартиен носител: Данните се набират в писмена форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения, снабдени със заключващи механизми.

(б) регистър на учениците, които се обучават в специални училища за обучение и подкрепа на деца със сензорни увреждания и в центрове за специална образователна подкрепа на територията на съответната област/район;

(в) дневник за дейности за подкрепа за личностно развитие;

(г) личен картон за ресурсно подпомагане със задължителни реквизити съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите изолирани помещения;

(е) на технически носител: личните данни се въвеждат в специализирана Информационна система - НЕИСПУО. Базата данни се намира на твърдия диск на изолирани компютри;

(ж) срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение.

(4) Определяне на длъжностите:

(а) обработващи лични данни на регистър **„ученици"** са: директор, зам.-директор УД, ЗАС, РУ, учители, психолози, логопеди и сензорни терапевти.

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

(а) поверителност – средно ниво;
(б) цялостност – средно ниво;
(в) наличност – средно ниво;
(г) общо за регистъра – средно 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.

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

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

(а) защита при аварии – предприемат се конкретни действия в зависимост от конкретната ситуация;

(б) защита от пожари – незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

(в) защита от наводнения – предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(9) Достъп до регистър „ ученици" имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане", ДАЗД за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(10) 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.

(11) Лични данни на учениците се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно нормативната уредба и Номенклатурата на делата със сроковете за тяхното съхранение в институцията.

Чл. 27. (1) В регистър **„Родители"** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.

(2) Общо описание на регистър „**Родители**"

(3) Регистърът съдържа следните групи данни:

(а) име, ЕГН/ЛНЧ, адрес, телефони за връзка и месторабота;

(б) данни за родителски права и родствени връзки;

(в) телефонен номер, актуален имейл адрес и постоянен/настоящ адрес;

(г) образование и трудова заетост-по преценка на лицето.

(4) Нормативното основание – ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(5) Технологично описание на регистър „**Родители**". Носители на данни:

(а) когато са на хартиен носител, данните се набират в писмена форма и се съхраняват в папки;

Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на операторите на лични данни, снабдени със заключващ механизъм.

(б) на технически носител: наличие на електронен дневник на всяки клас;

(в) срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(б) Определяне на длъжностите: обработващи лични данни на регистър **„Родители"** са: Директор, учители, зам.-директор УД, РУ, психолози, логопеди и сензорни терапевти.

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

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

(8) 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.

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

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

(а) защита при аварии, независещи от институцията – предприемат се конкретни действия в зависимост от конкретната ситуация;

(б) защита от пожари – незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

(в) защита от наводнения – предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(11) Достъп до регистър „Родители" имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане", ДАЗД за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

(12) 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.

(13) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно нормативната уредба и Номенклатурата на делата със сроковете за тяхното съхранение в институцията.

(14) След постигане целите по предходната алинея личните данни се унищожават.

Чл. 28. (1) В регистър **„Персонал"** се набират и съхраняват лични данни, с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(2) Общо описание на регистър **„Персонал"**

Регистърът съдържа следните групи данни:

(а) физическата идентичност – име, ЕГН/ЛНЧ, месторождение, телефони за връзка и банкови сметки;

(б) документи относно психическото здраве;

(в) образование и придобита квалификация, длъжност по щатно разписание, трудов стаж и професионален опит;

(г) медицински данни;

(3) 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.

(4) Предназначението на събираните данни в регистъра е свързано с:

(а) индивидуализиране на трудовите правоотношения;

(б) изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

(в) дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.;

(г) установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(5) Технологично описание на регистър **„Персонал".** Носители на данни:

(а) на хартиен носител: Данните се набират в писмена форма и се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на администратора на лични данни, снабдени със заключващи механизми;

(б) на технически носител: Личните данни се въвеждат в специализирана счетоводна програма: счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри;

(в) срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(6) Определяне на длъжностите:

Обработващи лични данни на регистър **„Персонал"** са: директор, гл. счетоводител, ЗАС и касиер.

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

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

(8) 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.

(9) Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Трудовите досиета на персонала не се изнасят извън сградата на институцията. Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител. При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на институцията.

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

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

(а) защита при аварии, независещи от учебното заведение – предприемат се конкретни действия в зависимост от конкретната ситуация;

(б) защита от пожари – незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

(в) защита от наводнения – предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

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

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

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

(13) След постигане целите по предходната алинея личните данни се унищожават.

Чл. 29. (1) В регистър **„Други специалисти",** обхваща лицата, които не са част от постоянния педагогически или непедагогически персонал на трудов договор, но предоставят специализирани външни услуги на учениците. Такива специалисти са: специалисти осъществяващи допълнителни дейности като спорт, танци, изкуство и др.такива. Специалисти от съответния РЦПППО, медицински специалисти и др.

(2) Общо описание на регистър „**Други специалисти**"

(3) Регистърът съдържа следните групи данни:

(а) име, ЕГН/ЛНЧ, адрес, месторождение, телефони за връзка и банкови сметки;

(б) документи относно психическото здраве;

(в) образование и професионална квалификация, както и доказателства за трудов стаж и професионален опит;

(г) лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, ЗЗД, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

(4) Предназначението на събираните данни в регистъра е свързано с:

(а) изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;

(б) дейностите, свързани със сключване, съществуване, изменение и прекратяване на правоотношенията, изготвяне на договори, допълнителни споразумения или анекси, служебни бележки, справки, удостоверения и др.;

(г) установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по съществуващото с учебното заведение правоотношение..

(5) Технологично описание на регистър **„Други специалисти".** Носители на данни:

(а) на хартиен носител: Данните се набират в писмена форма и се съхраняват в папки и класьори. Папките и класьорите се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на администратора на лични данни, снабдени със заключващи механизми;

(б) на технически носител: Личните данни се въвеждат в специализирана счетоводна програма: счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри;

(в) срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение.

(6) Определяне на длъжностите: Обработващи лични данни на регистър **„Други специалисти"** са: директор, гл. счетоводител, ЗАС и касиер.

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

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

(8) 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.

(9) Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител. При изготвяне на счетоводната документация. данните се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на институцията.

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

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

(а) защита при аварии, независещи от институцията – предприемат се конкретни действия в зависимост от конкретната ситуация;

(б) защита от пожари – незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;

(в) защита от наводнения – предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(11) Достъп до регистър **„Други специалисти"** имат и държавните органи – НАП, НОИ, МОН, РУО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове. Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

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

(13) След постигане целите по предходната алинея личните данни се унищожават.

Чл. 30. (1) В регистър **„Пропусквателен и регистрационен режим"** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Категориите физически лица, за които се обработват лични данни, са родители,настойници, външни посетители и контрагенти, външни специалисти.В случите когато пропусквателният режим е автоматизиран, служителите на учебното заведение също попадат в тази категория лица.

(3) Обработващи лични данни на регистър **„Пропусквателен и регистрационен режим"** са: Охранител/портиер изпълняващ дейността по организация на охранителната дейност и пропускателния режим, служителите от фирмата, която обслужва учебното заведение извършващи монтаж и техническа поддръжка на системите.

(4) Регистърът съдържа следните групи данни:

(а) физическа идентичност на лицето: трите имена на посетителя;

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

(7) Източниците, от които се събират данните- физическите лица.

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

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

(9) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на институцията.

(10) На хартиен носител: дневникът на хартиен носител се съхранява в съответствие с **„Инструкция за съхранение на документи на хартиен носител".** В случай на извънредна ситуация служителят се евакуира заедно с дневника.

Чл. 31 (1) В регистър **„Видеонаблюдение"** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Физическа идентичност – видеообраз на служители, родители, ученици, контрагенти и и други посетители на учебното заведение.

(3) Обработващи лични данни на регистър **„Видеонаблюдение"** са: служителите от фирмата, която обслужва учебното заведение извършващи монтаж и техническа поддръжка на системите.

(5) Регистърът съдържа следните групи данни:

(а) физическа идентичност на лицето – видеообраз;

(б) поведение и действие на лицата в обхвата на камерите;

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

(6) Източниците, от които се събират данните – физическите лица.

(7) Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз).

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

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

(9) Видеонаблюдението се извършва чрез изградена система за видеонаблюдение.

(10) Записите се изтриват автоматично от системата след определено време – 30 дни. При установен инцидент в училището, случаи на агресия, тормоза, насилие, разрушение на материалната база и др., при проверка на спазване на Правилника за дейността на училището, други правила и изисквания, записите се преглеждат от директора на учебното заведение. Директирът преглежда записите и съставя протокол за това.

Чл. 32 (1) В регистър „***Контрагенти и партньори***" се набират и съхраняват лични данни на лица, участващи в процеса на осъществяваната дейност на учебното заведение.

(2) В регистъра се съдържат данни от следните групи:

(а) за физически лица-три имена, ЕГН/ЛНЧ, постоянен адрес, банкова сметка, телефонен номер, имейл адрес, данни за данъчно облагане и осигуряване;

(б) за юридически лица – три имена на законния представител на търговското дружество или упълномощено лице, три имена, телефон и имейл на лицето за контакт;

(3) Определяне на длъжностите: обработващи лични данни на регистър ***„Контрагенти и партньори***" са: зам.-директор АСД, гл. счетоводител и ЗАС.

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

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво.

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

(6) Срок за съхранение на данните.

Поради изискванията на данъчното заяконодателство, документите в този регистър се съхраняват за срок от 10 години, считано от първи януари на годината, следваща годината на приключване на договора или плащането.

Чл. 33 (1) В регистър ***„Кандидати за работа"*** се набират и съхраняват лични данни на лица, кандидатстващи за работно място в учебното заведение.

(2) Регистърът съдържа следните категории лични данни:

(а) име, адрес, телефон за връзка, електронен адрес за кореспонденция;

(б) информация за дипломи и други документи за образование и допълнителна квалификация;

(в) трудов стаж и професионален опит;

(г) друга информация предоставена от кандидата за работа по свое усмотрение.

(3) Цел и основание за събиране на лични данни в регистър „кандидати за работа"- законното основание и цел на събраните лични данни е да се даде възможност на потенциалния работодател да направи информиран подбор на персонал.

(4) Технологично описание на регистър „кандидати за работа".

(а) на хартиен носител – когато кандидата за работа подава документи на място в учебното заведение;

(б) на електронен носител – когато кандидата за работа изпраща необходимите документи по електронна поща;

(5) Срок на съхранение:

(а) на хартиен носител – 6 календарни месеца;

(б) на електронен носител – 6 календарни месеца.

(6) Длъжности, които имат достъп до личните данни от регистър „кандидати за работа" са Директор, Комисията по подбор и счетоводител.

(7) Правила за обработка- Документите съдържащи лични данни на кандидата за работа се комплектоват в досие на кандидата (в папка или джоб за документи). Всички досиета на кандидати, които не са одобрени за назначаване, се комплектоват в обща папка с етикет „Кандидати за работа/ Година" и се предават за съхранение в архив.

(8) Ниво на въздействие на регистър „кандидати за работа"

(а) поверителност – ниско ниво;

(б) цялостност – ниско ниво;

(в) наличност – ниско ниво;

(г) общо за регистъра – ниско ниво;

(9) Организационни, технически и мерки за зашита на електронни данни.

Длъжностните лица, които обработват лични данни на кандидати за работа, са подписали „Декларация за конфиденциалност" и длъжностната характеристика, преминали са обучение за правилата за обработка на лични данни. Има назначено Длъжностно лице за защита на личните данни, което контролира правилното прилагане на мерките за защита и управление на лични данни. Документите на хартиен носител се съхраняват в съответствие с „Инструкция за съхранение на документи на хартиен носител". Електронните данни се съхраняват в съответствие с „Инструкция за техническо съответствие на информационната среда".

(10) Защита при извънредни ситуации – при извънредни ситуации се действа в съответствие с Авариен план и Противопожарни правила. Взети са мерки за защита – осигурени са пожарогасителни средства. Служителите са преминали инструктаж.

(11) Личните данни на кандидати за работа не се предоставят на трети страни. След изтичане на срока за съхранение данните се унищожават в съответствие с вида на носителя. Попълва се „Бланка за унищожени лични данни".

Чл. 34 (1) Лице по защита на данните(ДЛЗД) е такова, което е в трудово-правни отношения с институцията или е в гражданско правоотношение със същата.

(2) Лицето наречено за краткост (длъжностно лице) по защита на данните има следните задължения:

(а) да информира и съветва организацията и нейните служители относно спазването на изискванията за защита на данните;

(б) да наблюдава спазването на изискванията за защита на данните;

(в) да предоставя съвети по искания във връзка с извършването на оценка на въздействието върху защитата на данните (ОВЗД);

(г) контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

(д) следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите в компютърната среда;

(е) извършва обучение на персонала;

(ж) провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

(3) да действа като точка за контакт за Комисията за защита на личните данни (КЗЛД) по въпроси, свързани с обработването;

(и) да бъде лице за контакт за гражданите по всички въпроси, свързани с упражняването на техните права.

Чл. 35. Служителите на институцията са длъжни:

(а) да обработват лични данни законосъобразно и добросъвестно;

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

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

(г) 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;

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

Чл. 36. (1) За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

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

Преходни и заключителни разпоредби

§1. Всички служители на институцията са длъжни да се запознаят с инструкцията и да я спазват.

§2 За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Общ регламент относно зашитата на личните данни(GDPR).

§3. Инструкцията е утвърдена със Заповед № РД-07-179/ 03.11.2026 г.