МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

РЕГИОНАЛЕН ЦЕНТЪР ЗА ПОДКРЕПА НА ПРОЦЕСА НА ПРИОБЩАВАЩОТО ОБРАЗОВАНИЕ

ОБЛАСТ ВЕЛИКО ТЪРНОВО

УТВЪРЖДАВАМ :
ДОНКА ДОНЧЕВА
Директор на Регионален център
за подкрепа на процеса на приобщаващото образование
област Велико Търново

Donka Ivanova Doncheva
Digitally signed by Donka Ivanova Doncheva
Date: 2024.02.21 14:34:31 +02'00'

/съгласно Заповед № 18-904/21.02.2023г./

ИНСТРУКЦИЯ

за мерките и средствата за защита на личните данни събирани, обработвани, съхранявани и предоставяни от Регионален център за подкрепа на процеса на приобщаващото образование-област Велико Търново

I.Общи положения

Чл.1.(1)Регионален център за подкрепа на процеса на приобщаващото образование (РЦПППО)-област Велико Търново е юридическо лице със седалище град Велико Търново, Република България с основен предмет на дейност учебно –възпитателна дейност.

(2)РЦПППО-област Велико Търново обработва лични данни във връзка със своята дейност и определя целите и средствата за обработването им.

Чл.2.(1)Настоящата инструкция урежда организацията на обработване и защитата на лични данни на преподавателите, служителите, обучаемите (деца/ученици), посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност 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 РЦПППО-област Велико Търново 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: - Създаване 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; - 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). - 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 РЦППО-област Велико Търново.

Чл.3.Настоящата инструкция се прилага за обработването и съхранението на лични данни по смисъла на Регламент 679/2016 г.

Чл.4.(1)Учебното заведение е администратор на лични данни.

(2)Според Регламент 679/2016 „субект на лични данни— е: идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

Чл.5.(1)Според Регламент 679/2016 „лични данни— са: 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.

(2)Според Регламент 679/2016 „обработване— е: 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

(3)Личните данни се събират и обработват: - за изпълнение на правомощията и присъщата дейност на центъра, предоставени чрез Закона и училищното и предучилищно образование и законодателството на Република България и ЕС; - въз основа на законови задължения, възложени чрез законодателството на Република България и ЕС /закони, наредби, инструкции, правилници, регламенти и др./; - при сключване на договори или подготовка за тяхното сключване; - за защита на жизненоважни интереси на субекта на данните или на друго физическо лице; - при

липса на някое от горепосочените основания – единствено след съгласие на субекта на лични данни, дадено чрез подписана декларация за съгласие ; - освен това когато обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни.

(4)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.

(5)Личните данни се обработват при спазване на следните принципи, въведени чрез Регламент 679/2016 г.: законосъобразност, добросъвестност, прозрачност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност, поверителност, отчетност.

(6)Събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин; личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели; личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват; личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

Чл.6.РЦППО-Велико Търново 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.7.(1)Центъра прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2)Тя включва:

1. Физическа защита;

2. Персонална защита;

3. Документална защита;

4. Защита на автоматизирани информационни системи и/или мрежи;

Чл.8.(1)Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

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

(3)Събирането, обработването и съхраняването на лични данни в регистрите на Центъра се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразено с посочените мерки за защита и нивото на въздействие на съответния регистър.

Чл.9.За всяка дейност по събиране на лични данни се поддържа регистър на дейностите в Приложение № 1 към настоящата инструкция, 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.

(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.

(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/операторът/ на лични данни и оторизираните длъжностни лица.

(5)Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани 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)Ръководство трябва да уведоми 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 й, учебното заведение може да определи друго ниво на защита за регистъра.

Чл.15.(1)След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от учебното заведение регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни . При промени в структурата на учебното заведение, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(2)В случаите, когато се налага унищожаване на носител на лични данни, учебното заведение прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3)Унищожаване се осъществява от служителя, отговорен за архива на Центъра.

Чл.16.(1)Достъпът до данните от регистъра и разкриването на личните данни се осъществява :

- физическите лица, за които се отнасят данните;

- трето лице, ако е предвидено в нормативен акт;

- обработващия личните 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 (Приложение № 3), респ. искане за достъп на информация, и след тяхното легитимиране.

(5)Заявлението съдържа:

1. името, адреса и други необходими данни за идентифициране на съответното физическо лице;

2. описание на искането;

3. предпочитана форма за предоставяне на достъпа до личните данни;

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

(6)Директорът разглежда заявлението за достъп и се произнася по него в 14-дневен срок.

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

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

II. Мерки по 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. 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 Центъра, 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:

1.познаване на нормативната уредба в областта на защитата на личните данни;

2.познаване на политиката и ръководствата за защита на личните данни;

3.знания за опасностите за личните данни, обработвани от администратора;

4.споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

5.съгласие за поемане на задължение за неразпространение на личните данни; изразено в декларация по образец .

(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“.

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

1.нормативната уредба в областта на защитата на личните данни;

2.политиката и ръководствата за защита на личните данни;

3.опасностите за личните данни, обработвани от администратора.

Чл.19. (1)Основните приложими мерки за документална защита на личните данни са: 1. Определяне на регистрите, които ще се поддържат на хартиен носител: на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на Центъра;

2.Определяне на условията за обработване на лични данни: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на учебното заведение, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;

3.Регламентиране на достъпа до регистрите: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае“;

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

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

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:

1.Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на учебното заведение. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае;

2.Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;

3.Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от ръководител компютърен кабинет или от лице с вменени трудови функции и технически познания.
4.Политиката по създаване и поддържане на резервни копия за възстановяване

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

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

6.Персоналната защита на данните е част от цялостната охрана на учебното заведение.
7.Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на учебното заведение.

8.Данните, които вече не са необходими и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

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

Чл.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.

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

IV. Поддържани регистри и тяхното управление

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

1. Персонал

2. Информационна система за приобщаващо образование

3. Видеонаблюдение

Чл.26.(1)В регистър „**Персонал** се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(2)Общо описание на регистър „**Персонал** Регистърът съдържа следните групи данни:
1. физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;

2. психологическа идентичност - документи относно психическото здраве;

3. социална идентичност - образование и трудова дейност;

4. семейна идентичност - семейно положение и родствени връзки;

5. лични данни, които се отнасят до здравето;

6. други - лични данни относно гражданско-правния статус на лицата.

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

Предназначението на събираните данни в регистъра е свързано с :

1.Индивидуализиране на трудовите правоотношения;

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

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

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

(2)Технологично описание на регистър „**Персонал**“: носители на данни:

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

- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма: счетоводство, ТРЗ и личен състав. Базата данни се намира на твърдия диск на изолирани компютри. - Срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(3) Определяне на длъжностите:

Обработващи лични данни на регистър **„Персонал**“ са: директор, зам. директор по УД, гл.счетоводител, технически секретар и касиер-домакин. Оператор на лични данни на регистър „Персонал“ е директора.

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

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

(5) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Трудовите досиета на персонала не се изнасят извън сградата на 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.

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

1. защита при аварии, независещи от учебното заведение - предприемат се конкретни действия в зависимост от конкретната ситуация;

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

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

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

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

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

Чл.27.(1) В регистър **„Информационна система за приобщаващо образование“** се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици/деца —, обучавани в училищата/ДГ в областта/района.

(2) Общо описание на регистър „Информационна система за приобщаващо образование“ — Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка;

2. социална идентичност - образование;

3. семейна идентичност - родствени връзки;

4. лични данни, които се отнасят до здравето. Нормативното основание е ЗПУО, НПО, ЗЗО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър „Информационна система за приобщаващо образование“ носители на данни: На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, снабдени със заключващи механизми. Информацията от хартиените носители за всеки ученик/деца , се записва в Регистър на децата и учениците, които се обучават в детските градини и в училищата на територията на областта; На технически носител: Личните данни се въвеждат в специализирана Информационна система - НЕИСПУО. Базата данни се намира на твърдия диск на изолирани компютри. - срок на съхранение: съгласно Номенклатурата на делата в институцията със срокове на съхранение;

(4)Определяне на длъжностите: Обработващи лични данни на регистър „Информационна система за приобщаващо образование“: директор, главен счетоводител , технически секретар, касиер-домакин , РУ, учители , психолози, логопеди и сензорен терапевт. Оператор на лични данни на регистъра е целия педагогически персонал. Длъжностните лица - обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

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

1. поверителност - средно ниво;

2. цялостност - средно ниво;

3. наличност - средно ниво;

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

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

1.защита при аварии, независещи от учебната институция - предприемат се конкретни действия в зависимост от конкретната ситуация;

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

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

(8)Лични данни на децата/учениците 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.

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

Чл.28(1)В регистър **„Видеонаблюдение“** 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 посетителите на РЦППО-Велико Търново.

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

(4)Оператор на лични данни на регистър **„Видеонаблюдение“** е директора.
(5)Регистърът съдържа следните групи данни:

-физическа идентичност на лицето;видеообраз;

(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, са: от физически лица.Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите.Видеонаблюдението се извършва чрез изградена система за видеонаблюдение.

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

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

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

V. Права и задължения на лицата, обработващи лични данни

Чл.29.(1)Лице по защита на личните данни 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 личните данни има следните правомощия:

1.осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;

2.следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно, спецификата на водените регистри;

3.осъществява контрол по спазване на изискванията за защита на регистрите;

4.поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;

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

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

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

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

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

Чл.30.Служителите на институцията са длъжни:

1.да обработват лични данни законосъобразно и добросъвестно;

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

3.да актуализират регистрите на личните данни (при необходимост);

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

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

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

Чл.31.(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. По смисъла на настоящата инструкция: • **„Лични данни—** са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.
2. •**„Администратор** е физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, който сам или съвместно с друг определя целите и средствата за обработване на личните данни.
3. • **„Администратор на лични данни** е институцията(учебно или детско заведение) с адрес:..... •
4. **„Ниво на защита** е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.

5. **„Обработване на лични данни“** е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.
6. • „**Обработващ лични данни** е лице, което обработва лични данни от името на администратора на лични данни. •
7. „**Оператор на лични данни** е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на институцията.
8. • **„Оценка на въздействие** е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.
   • **„Поверителност** е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
9. • **„Предоставяне на лични данни** са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.
10. • „**Регистър на лични данни** е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип. •
11. „**Съгласие на физическото лице** е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява, те да бъдат обработвани.
12. • „**Трето лице** е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.
13. 2. Всички служители на Центъра са длъжни срещу подпис да се запознаят с инструкцията и да я спазват.
14. 3 За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Регламент 679/ 2016.

-

МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

РЕГИОНАЛЕН ЦЕНТЪР ЗА ПОДКРЕПА НА ПРОЦЕСА НА ПРИОБЩАВАЩОТО ОБРАЗОВАНИЕ

ОБЛАСТ ВЕЛИКО ТЪРНОВО

З А П О В Е Д

№ РД 18 - 904/21.02.2024 г.

На основание чл.259, ал.1 от Закона за предучилищното и училищното образование, и във връзка с чл.2, ал.2 от Закона за защита на личните данни, чл.30,параграф1 от Регламент (ЕС)2016/679

У Т В Ъ Р Ж Д А В А М

Инструкция за мерките и средствата за защита събирани, обработвани, съхранявани и предоставени от Регионален център за подкрепа на процеса на приобщаващото образование – област Велико Търново.
С настоящата Инструкция е запознат колектива на РЦППО-област Велико Търново
Измененията и допълненията в настоящата Инструкция се извършват по реда на нейното утвърждаване.

Настоящата заповед да се сведе до знанието на лицата срещу подпис за сведение и изпълнение.

ДОНКА ДОНЧЕВА
Директор на РЦППО
област Велико Търново

РЕГИОНАЛЕН ЦЕНТЪР ЗА ПОДКРЕПА НА ПРОЦЕСА НА ПРИОБЩАВАЩОТО ОБРАЗОВАНИЕ ОБЛАСТ ВЕЛИКО ТЪРНОВО
Donka Ivanova Doncheva
Digitally signed by Donka Ivanova Doncheva
Date: 2024.02.21 15:06:41 +02'00'

Велико Търново 5000, ул. „Мармарлийска" 26, тел.: 062 / 60 33 12
e-mail:info-300139@edu.mon.bg www: regionalencentar-vt.com