„ЦСОП“ - гр. Велинград,
бул. ”Съединение” №256, тел. 0359/5-30-35
e-mail: draganmanchov@abv.bg

Утвърдил.....
Елена Канлиева
Директор на ЦСОП

ИНСТРУКЦИЯ

за начина на обработване на личните данни във ЦСОП - гр. Велинград

I. Общи положения

Чл. 1. Настоящата **Инструкция** (вътрешни правила) за технически и организационни мерки и допустимия вид на защита на личните данни, урежда организацията на обработване на лични данни и тяхната защита на клиентите, персонала, кандидатите за работа и контрагентите на „**Център за специална образователна подкрепа**“ **-гр. Велинград**, **с ЕИК 000342694**.

В зависимост от конкретната ситуация, Дружеството може да обработва данни в качеството на администратор. **ЦСОП-Велинград** обработва лични данни във връзка със своята дейност и сам определя целите и средствата за обработването им.

Инструкцията е изготвена в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива.

Чл. 2 Настоящата **Инструкция** урежда:

- Принципите, процедурите и механизмите за обработка на личните данни;
- Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;
- Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;
- Лицата, които обработват лични данни, и техните задължения;
- Правилата за предаване на лични данни на трети лица в България и чужбина;
- Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;
- Техническите ресурси, прилагани при обработката на лични данни.

Чл. 3. (1) „**Обработване на лични данни**“ 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.

(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл. 4. (1) **„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. Принципите за защита на личните данни са:
(2) **„Регистър с лични данни“** представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.
(3) **„Поверителност”** е изискване за не разкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
(4) **„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.
(5) **„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.
(6) **„Хартиен носител“** е физически обект, на който по механичен път могат да се запишат данни или могат да се възстановят от същия.
(7) **„Електронен носител“** е компютъризирано устройство, на което в електронен вид могат да се запишат данни или могат да се възстановят от същото.

Чл. 5. (1) Като администратор на лични данни, при обработването на лични данни **ЦСОП - Велинград** спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.
Чл. 6. (1) Принципите за защита на личните данни са:

1. **Законосъобразност, добросъвестност и прозрачност** - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни.
2. **Ограничение на целите** – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели.
3. **Свеждане на данните до минимум** – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването.
4. **Точност** – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването.
5. **Ограничение на съхранението** – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки.
6. **Цялостност и поверителност** – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки.

7. **Отчетност** – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 7. (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 училището и 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 предвидените мерки за защита и нивото на въздействие на съответния регистър.

Чл. 8. Когато не е налице хипотезата на, физическите лица, чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679 чиито лични данни се обработват, подписват декларация за съгласие по образец. (Приложение № 1).

II. Общо описание на регистрите. Предназначение.

Чл. 9. (1) **ЦСОП -Велинград** поддържа четири обособени регистъра съдържащи и съхраняващи лични данни, както следва:

1. Регистър **„Ученици“** ;
2. Регистър **„Персонал“** ;
3. Регистър **„Родители“** ;
4. Регистър **„Видеонаблюдение“.**

Чл.10.(1) В регистър **„Ученици“** се обработват и съхраняват лични данни с цел индивидуализиране на ученици, обучавани в центъра и запазване на тяхното здраве. Личните данни на 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 ЦСОП. След постигане на целите данните на учениците се унищожават физически, чрез шредер машина, за което се изготвят протоколи за унищожаване.

(2) В регистър **„Персонал“** се обработват лични данни на служителите, работниците и изпълнителите по трудови и граждански договори в **ЦСОП** по време на дейността им по изпълнение на тези договори , с оглед:

1. Индивидуализиране на трудовите и граждански правоотношения;

2.Изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социалното осигуряване, Закона за счетоводството, Закона за държавния архив и други;

3.Използване на събраните данни за служебни цели;

4.Всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения- за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи удостоверяващи трудов стаж, справки, удостоверения и други);

5.За водене на счетоводна отчетност, относно възнагражденията на посочените по-горе лица по трудови и граждански договори.

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

Данните се набират на хартиен носител /в писмена форма/ и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в помещения, съгласно Наредба № 8 от

11.08.2018г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите помещения.
Личните данни от регистър **"родители"** се въвеждат в специализирана Информационна система за училищна администрация Админ OS. Базата данни се намира на твърдия диск на изолиран компютър.

(4) Регистър **„Видеонаблюдение"** – създаден и поддържан с цел осигуряване на безопасността на ученици и служители и за обезпечаване на вътрешния ред на **ЦСОП.** Камерите са разположени отвън на сградата и са четири на брой. Регистъра се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на учениците и служителите и посетителите на центъра. Записите с видеообрази се съхраняват на дигитални устройства (DVR). Данните в регистъра се съхраняват за период не по-малък от 30-дни, като след изпълване на дисковото пространство те автоматично се презаписват. DVR-ите са електрически обезпечени чрез непрекъсваеми токозахранващи устройства (UPS).
На входовете на центъра са поставени предупредителни табели, че обектът се намира под видеонаблюдение.

Чл.11. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защита на данните.
(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на управителя на дружеството.
(3) Работниците и 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 по отношение на съответните служители.
(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

III. Лични данни, съхранявани в регистъра.

Чл. 12. (1) В регистър **„Ученици"** се обработват следните категории лични данни:
-Относно физическа идентичност на лицата- име, ЕГН, адрес, паспортни данни, месторождение, телефон, електронен адрес за връзка.
- Относно социална идентичност на лицата- образование, документ за придобито образование, професионална квалификация.
-Данни за здравословно състояние: медицинско свидетелство, имунизационен картон и решения на ТЕЛК/ НЕЛК и др.п. .
(2) В регистър **„Персонал"** се обработват следните категории лични данни:
- Относно физическа идентичност на лицата- име, ЕГН, адрес, паспортни данни, месторождение, телефон, електронен адрес за връзка, снимка;
- Относно икономическа идентичност- банкови сметки;
- Относно социална идентичност на лицата- образование, трудова дейност, документи, удостоверяващи професионална квалификация, документи удостоверяващи членство в профсъюзи и др.
-Други данни- медицинско свидетелство, свидетелство за съдимост и др.
(3) Регистър **„Родители"** се обработват лични данни касаещи:
- Физическата идентичност на лицата- име, ЕГН, адрес и телефон.
- Социална идентичност на лицата- информация за образование, трудова заетост и др.
-Данни за здравословно състояние: решения на ТЕЛК/ НЕЛК.

IV. Технологично описание.

Чл. 13. (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 пожарогасители 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 ѝ 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.
Техническото описание на използваните от **ЦСОП - Велинград** регистри е уредено в (Приложение № 2- Таблица №1).

V. Длъжности и отговорности.

Чл. 14. (1). С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.
(2) Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност два пъти годишно. За проведения инструктаж се съставя Протокол по образец.

Чл. 15. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на директора на училището, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.
(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.

Чл. 16. При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, администратора може да определи друго ниво на защита за регистъра.
Приложение № 3/ Таблица 2/

Чл. 17.(1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от **ЦСОП** регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящата **Инструкция**.

(2) В случаите, в които се налага унищожаване на носител на лични данни, **ЦСОП** прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите.

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3) Унищожаване се осъществява от служителя, отговорен за архива на центъра и след уведомяване на Длъжностното лице по защита на данните.

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал. 3, съгласно образец.

VI. Достъп до личните данни. Предоставяне .

Чл. 18. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление лично или чрез нотариално заверено пълномощно, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, Администратора съобщава в 14-дневен срок от подаване на заявлението, респ. искането.

(3) Срокът по ал. 2 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

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

1.Устна справка.

2.Писмена справка.

3.Преглед на данните от самото лице.

4.Предоставяне на исканата информация на технически и/или електронен носител.

(5) Администраторът на лични данни или изрично оправомощено от него длъжностно лице писмено уведомява заявителя за решението или отказа си по чл. 18, ал. 2 в съответния срок.

(6) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(7) Третите страни получават достъп до лични данни, обработвани в **ЦСОП**, при наличие на законово основание за обработването на лични данни (МОН, РУО, дирекция „ Социално подпомагане, НАП, НОИ и др.).

VII. Мерки по осигуряване на защита на личните данни

Чл. 19. Технически мерки: Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа. Възможните технически средства за контрол на достъпа са: устройства за разпознаване чрез магнитна карта и/или ключ; наблюдение с видеокамери на касите; политика на допускане на външни лица до помещенията на дружеството само с придружител от персонала на центъра. Обектите /сградите / на **ЦСОП** са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

Чл. 20. Мерки за документална защита: Центъра установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани в тази **Инструкция**. Размножаването и разпространението на

документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.

Чл. 21. Персонални мерки на защита: Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни: поемат задължение за неразпространение на личните данни, до които имат достъп; се запознават с нормативната база, вътрешните правила и политики на училището относно защитата на личните данни; преминават обучение за реакция при събития, застрашаващи сигурността на данните; са инструктирани за опасностите за личните данни, които се обработват от центъра; се задължават да не споделят критична информация помежду си и с външни лица, освен по установения с тази Инструкция ред.

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

Чл. 22. Правила и мерки за осигуряване на защита на личните данни при компютърна обработка
(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 центъра 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. 23. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране в разумна степен на 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. 24. (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 спазване изискванията на Регламент 2016/679, Закона за защита на лични данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.
Чл. 25. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица, респ. да споделят своя PIN с трети лица.

VIII. Нарушения на сигурността

Чл. 26. Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Лицето, отговорно за личните данни, като му предоставят цялата налична информация.

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

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

След съгласуване с ръководството на дружеството, Лицето, отговорно за личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

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

Чл.27. В случай, че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от ръководството на училището, Лицето, отговорно за личните данни, организира уведомяването на КЗЛД.

Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението.

Уведомлението до КЗЛД съдържа следната информация:

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

(б) името и координатите за връзка на Лицето, отговорно за личните данни;

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

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

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

Чл.28. ЦСОП води регистър на нарушенията на сигурността, който съдържа следната информация:

(а) дата на установяване на нарушението;

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

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

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

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

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

IX. Предоставяне на лични данни на трети лица

Чл. 29. ЦСОП може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор.

В случаите на предоставяне на данните на служители, родители и др. на услуги на обработващ, Центъра:

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

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

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

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

(а) Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;

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

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

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

X. Оценка на въздействието и ниво на защита

Чл. 30. Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от Центъра. Оценка на въздействието се извършва за високорискови дейности по обработване.

Оценка на въздействието е необходимо при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с обработване на лични данни, включително:

- първоначалното въвеждане на нови технологии или прехода към нови технологии;
- автоматизирано обработване, включително профилиране или автоматизиране вземане на решения;

За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

Чл. 31. (1) Нивото на въздействие върху личните данни в регистър " **Ученици**" и съответно ниво на защита, приложимо към него, се определят на **„високо“** ;

(2) Нивото на въздействие върху личните данни в регистър " **Персонал**" и съответно ниво на защита, приложимо към него, се определят на **„средно“** ;

(3) Нивото на въздействие върху личните данни в регистър " **Родители**" и съответно ниво на защита, приложимо към него, се определят на **„високо “** ;

(4) Нивото на въздействие върху личните данни в регистър " **Видеонаблюдение**" и съответно ниво на защита, приложимо към него, се определят на **„средно“** ;

Приложение № 4

XI. Унищожаване на данните

Чл.32. Унищожаване на личните данни се извършва от **ЦСОП** или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.

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

Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина. Електронните данни се изтриват от електронната база данни по начин, не позволяващ възстановяване на информацията.

XII. Права и задължения на лицата, обработващи лични данни

Чл.33.Лицата, обработващи личните данни от името на дружеството, са физически или юридически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящата Инструкция.

Чл.34. Лицето, отговорно за личните данни:

- подпомага Дружеството и лицата, обработващите личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;
- осигурява нормалното функциониране на гореспоменатите системи за защита;
- осъществява контрол през целия процес на събиране и обработване на данните;
- изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;
- периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;
- уведомява Дружеството своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;
- унищожава данните от хартиените и техническите носители съгласно закона и сроковете, установени в тази Инструкция;
- преупълномощава физически или юридически лица с писмен акт, които да осъществяват защитата на личните данни.

Чл. 37. Служителите на **ЦСОП** 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 при необходимост регистрите на личните данни.
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.

Чл.38. Събирането, обработката и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.

Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др. Гореспоменатите могат да изискат данните по надлежен ред във връзка с изпълнението на техните правомощия.

XII. Права на субектите на данни

Чл.39. Всяко лице има право да иска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

- Правото на достъп се осъществява чрез искане на засегнатото физическо лице, получено на адреса по седалището на Центъра или официалната електронна поща.
- Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона.
- Дружеството е длъжно в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако Дружеството установи, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.
- Субектите на данни имат също правото да:
- оттеглят съгласието си за обработване по всяко време;
- възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;
- бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;
- подават жалби до регулаторния орган;
- в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене (право на преносимост).

XIII. Допълнителни разпоредби

Чл. 40. Всички служители на ЦСОП са длъжни да се запознаят с настоящата Инструкция и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

Чл. 41. (1) За всички неуредени в настоящата Инструкция, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

Настоящата Инструкция е утвърдена със Заповед №.336/30.08.2018.....на директора на ЦСОП - **Велинград** и влиза в сила от датата на нейното утвърждаване.