



МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА
ЦЕНТЪР ЗА СПЕЦИАЛНА ОБРАЗОВАТЕЛНА ПОДДКРЕПА „ЛОЗЕНЕЦ“
гр. София, район Лозенец, ул. „Русалийски проход“ №12, тел: 02/862-11-83, e-mail: info-2211607@edu.mon.bg

В Ъ Т Р Е Ш Н И П Р А В И Л А

ЗА МЕРКИТЕ И СРЕДСТВАТА

ЗА ОБРАБОТВАНЕ

И ЗАЩИТА НА ЛИЧНИ ДАННИ

В ЦЕНТЪР ЗА СПЕЦИАЛНА ОБРАЗОВАТЕЛНА ПОДДКРЕПА

„ЛОЗЕНЕЦ“

ГР. СОФИЯ

2024 г.

ГЛАВА ПЪРВА
ОБЩА ИНФОРМАЦИЯ, ОБХВАТ, ПРАВНО ОСНОВАНИЕ И ЦЕЛИ

Раздел I
Обща информация

Чл. 1. (1) С тези вътрешни правила се уреждат редът и условията за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни, както и мерките и средствата за тяхната защита.

(2) Настоящите правила се издават с оглед изискванията на Регламент (ЕС) 2016/679 на ЕС, Закон за защита на лични данни и утвърдените от Министерството на образованието и науката (МОН) Общи методически указания за прилагане на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните/ОРЗД), в т.ч. и във връзка с обмена на данни между и прилежащите му централни и регионални структури и образователни институции.

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на Центъра за специална образователна подкрепа „Лозенец“ (Център/Центъра) – Администратор на лични данни.

Раздел II
Цели и обхват

Чл. 2. (1) Настоящите правила имат за цел да регламентират:

1. общите принципи, приложими в Центъра при обработване на лични данни;
2. обучението на лицата, обработващи лични данни в Центъра;
3. задълженията на лицата, обработващи лични данни в Центъра;
4. необходимите технически и организационни мерки за защита личните данни от неправомерно обработване;
5. воденето на съответните регистри;
6. защитата на правата и свободите на субектите на данни;
7. правилата при обмен на информация;
8. механизмите за докладване и реагиране при инциденти, свързани със сигурността на данните осъществяването на оценка на риска;
9. механизмите за оценка на въздействие и защита на данните.
10. отговорностите при неизпълнение на задълженията по настоящите правила;

(2) Настоящите правила и свързаните с тях процедури, образци на формуляри и всякакви други прилежащи документи са задължителни за всички лица, боравещи с лични данни за нуждите на Центъра.

(3) Настоящите правила и свързаните с тях процедури, образци на формуляри и всякакви други документи се прилагат по отношение на всички лични данни (структурирани и неструктурирани), събирани, съхранявани и/или обработвани, на всички субекти на данни и на всички дейности по обработване, извършвани от Центъра, в качеството му на администратор на лични данни.

(4) Настоящите правила и свързаните с тях процедури, където изрично е отбелязано, се прилагат по отношение на всички лични данни (структурирани и неструктурирани), събирани, съхранявани и/или обработвани, на всички субекти на данни и на всички дейности по обработване, извършвани от Центъра, в качеството му на обработващ лични данни. В тези случаи приложение намират и нормативните актове, регулиращи това правоотношение, както, когато е приложимо, и изричните указания, дадени от съответния администратор на лични данни.

Раздел III

Принципи на обработване на лични данни

Чл. 3. (1) При упражняването на своите правомощия и дейности по обработване Центърът съблюдава принципите за защита на личните данни, заложи в Закона за защита на лични данни, Регламента (ЕС) 2016/679 на ЕС. По-конкретно, личните данни:

1. се обработват от Центъра законосъобразно, добросъвестно и по прозрачен начин по отношение на субектите на данни;
2. се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели;
3. са подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват;
4. са точни и поддържани в актуален вид, като се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни данни, като се имат предвид целите, за които те се обработват;
5. се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите на обработването, с изключение на случаите, в които данните се обработват единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие, че са приложени съответните технически и организационни мерки за защита на правата и свободите на субекта на данни;
6. се обработват по начин, който гарантира подходящо ниво на тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като за тази цел се прилагат подходящи технически или организационни мерки;

(2) Всички извършвани от Центъра операции, които включват дейности по обработване на лични данни следва да бъдат начално планирани на етапа на проектиране и под подразбиране да бъдат осъществявани в съответствие с принципите, посочени в ал. 1.

(3) Съблюдаването на принципите, посочени в ал. 1, се осигурява чрез спазване изискванията на настоящите правила и на всички други относими актове и свързани инструкции, процедури и формуляри прилагане на подходящи технически и организационни мерки за физическа и информационна сигурност; извършване, при необходимост, на оценки за въздействието; следване на процедури за справяне с нарушенията на сигурността и др., като всички предприети мерки и действия следва надлежно да се документират.

ГЛАВА ВТОРА

ОБУЧЕНИЯ И ИНСТРУКТАЖ НА ПЕРСОНАЛА

Чл. 4. (1) Разпоредбите на тази глава се отнасят до обучението на работниците и служителите – педагогически и непедагогически персонал по трудово и служебно и до инструктажа на лицата в гражданско правоотношение с Центъра (общо наричани „служители“) относно приложимите изисквания, принципи и правила за обработване и защита на лични данни, предвидени в настоящите вътрешни правила и съответното приложимо законодателство.

(2) Обучението, съответно инструктажът по ал. 1 включва запознаване със съдържанието на настоящите правила и инструктаж относно съблюдаването на въведените задължения и използване на свързаните процедури и образци.

(3) Всички нови служители следва да получат въвеждащо обучение и инструктаж съгласно тази глава и да бъдат запознати и инструктирани с всички приложими политика и процедури в Центъра.

(4) Настоящите служители получат обучение, отговарящо на описаното в предходната точка, освен ако такова вече не им е било предоставено.

(5) Всички лица по ал.1 трябва да получат опреснително обучение най-малко веднъж на всеки тридесет и шест месеца, както и след всяка съществена промяна в приложимата правна регулация относно защитата на личните данни.

(6) За всяко проведено обучение се води и съхранява Регистър на обученията, посочващ имената и длъжността на съответния работник/служител, както и датата на провеждане на обучението (Приложение № 1).

ГЛАВА ТРЕТА

ПРАВИЛА ОТНОСНО ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Раздел I

Отговорни лица и основни задължения при обработването на лични данни

Чл. 5. (1) Директорът на Центъра:

1. организира и определя изпълнението на задачите във връзка с обработването на лични данни, които произтичат от настоящите правила и приложимото законодателство;

2. определя длъжностно лице по защита на личните данни, включително извън състава на Центъра;
3. определя служителите, имащи достъп до и упълномощени да обработват лични данни и правомерно да използват водените регистри, съдържащи лични данни, и поддържаните в Центъра бази данни и документация, съдържащи лични данни.
4. следи за стриктното прилагане на настоящите правила и на приложимото законодателство;
5. осъществява всички необходими действия, целящи да повишават сигурността на данните;
6. развива и стимулира добри практики за обработването на лични данни в Центъра;
7. планира и извършва дейностите по обработване на лични данни при спазване на правилата за защита и сигурност на данните;
8. при необходимост извършва оценка на въздействието върху защитата на данните, по-специално в случаите, в които има вероятност въвеждането на нови технологии, като се имат предвид естеството, обхватът, контекстът и целта на обработването, да доведе до висок риск за правата и свободите на субектите на данни;
9. упражнява контрол върху изпълнението на дейностите в случай на инциденти във връзка с нарушения на сигурността на данните и гарантират своевременното и последователно установяване на инцидентите, предприемането на последващите мерки за предотвратяване или намаляване и контрол на възникналите негативни последици, изпълнението на съответните стратегии за намаляване на рисковете и при необходимост - уведомяване за нарушения до КЗЛД и/или до субектите на данни в случай на високорисково нарушение на сигурността.
10. в съответствие с Глава втора осигурява въвеждащи и текущи обучения и инструктаж на всички работници и служители в Центъра в относно приложимите изисквания, принципи и правила за обработване и защита на лични данни, предвидени в приложимото законодателство и в настоящите правила и съответните процедури и инструкции.
11. съгласува действията си по предходните точки с определеното длъжностно лице по защита на лични данни

(2) Определеното длъжностно лице по защита на личните данни:

1. участва по подходящ начин и своевременно във въпросите, свързани със защитата на личните данни в Центъра;
2. участва в провеждането на обученията и информира и съветва служителите за техните задължения;
3. предоставя съвети при изготвянето на инструкции, вътрешни правила, оценки на въздействието и др. задължителни документи по провеждане и поддържане на дейността на Центъра в съответствие с изискванията на приложимото законодателство;
4. си сътрудничи с Комисията за защита на личните данни (КЗЛД) и действа като нейна точка за контакт по въпроси, свързани с обработването на лични данни в Центъра;
5. комуникира със субектите на данни при въпроси, свързани с обработването на личните им данни и упражняването на правата им по приложимото законодателство;

6. се отчита пряко пред Директора.

(3) Заместник директор по учебната дейност (ЗДУД) с помощта на Длъжностното лице за защита на личните данни:

1. развиват и стимулират добри практики за обработването на лични данни в Центъра, включително и следят за стриктното прилагане на настоящите правила и на приложимото законодателство, както и осъществяват всички необходими действия, целящи да повишават сигурността на данните.

2. планират и извършват дейностите по обработване на лични данни при спазване на правилата за защита и сигурност на данните и на изисквания от ОРЗД;

3. извършват при необходимост оценка на въздействието върху защитата на данните, по-специално в случаите, в които има вероятност въвеждането на нови технологии, като се имат предвид естеството, обхватът, контекстът и целта на обработването, да доведе до висок риск за правата и свободите на субектите на данни;

4. упражняват контрол върху изпълнението на дейностите в случай на инциденти във връзка с нарушения на сигурността на данните и гарантират своевременното и последователно установяване на инцидентите, предприемането на последващите мерки за предотвратяване или намаляване и контрол на възникналите негативни последици, изпълнението на съответните стратегии за намаляване на рисковете и при необходимост - уведомяване за нарушения до КЗЛД и/или до субектите на данни в случай на високорисково нарушение на сигурността.

(4) ЗДУД и/или длъжностното лице за защита на личните данни и осигуряват въвеждащи и текущи обучения на всички работници и служители в Центъра в съответствие с чл. 4 от настоящите правила.

(5) При изпълнението на всички нормативно установени дейности по обработване на лични данни, всички служители и работници в Центъра са длъжни да:

1. спазват всички разпоредби на настоящите правила и приложимото законодателство по отношение на личните данни и защита на правата и свободите на субектите на данни, чиито данни събират, съхраняват и/или обработват по-друг начин;

2. поддържат необходимата документация относно дейностите по обработване на лични данни, съхраняват копия от изготвените документи и при необходимост периодично да ги актуализират;

3. допринасят за изготвянето на необходимата документация, като предоставят съответната информация за конкретния процес на обработване;

4. осигуряват и подпомагат упражняването от страна на субектите на данни на техните права във връзка с обработването на личните им данни в съответствие с изискванията на настоящите правила.

5. проявяват предпазливост при постъпила молба за разкриване на лични данни/упражняване на права във връзка с личните им данни и съгласуват последващите си действия със ЗДУД и длъжностното лице по защита на личните данни като окончателното решение се взема от Директора на Центъра.

(6) Обработваните от Центъра лични данни не се разкриват на трети страни, включително на неупълномощени лица от състава на Центъра и на свързани с тях лица (членове на семействата,

приятели и др.), нито на държавни и охранителни органи и други получатели, освен при наличието на законово основание и основателна причина за това и при съблюдаване изискванията на чл. 27 по-долу.

(7) Извън случаите по ал.6, трети лица, достъпващи и/или обработващи лични данни от името на Центъра имат право на достъп регистрите и базите данни след изрично упълномощаване и/или възлагане и само след подписването на споразумение за поверителност на данни и/или друг договор по регламентиращ обработването на лични данни и съблюдаване настоящите правила.

(8) Всички извършвани от Центъра операции, които включват дейности по обработване на лични данни от името на администратори на лични данни, се разкриват на трети лица в съответствие с указанията и разпорежданията на съответния администратор на лични данни след съгласуване с Директора на Центъра.

Раздел II

Законосъобразност на обработването на лични данни

Чл. 6. (1) В Центъра се обработват лични данни само при наличието на поне едно от следните правни основания за законосъобразност на обработването:

1. субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;
2. обработването е необходимо за изпълнението на договор, по който субектът е страна, или за предприемане на стъпки по искане на субекта преди сключването на договор;
3. обработването е необходимо за спазването на законово задължение, приложимо спрямо Центъра и произтичащо от националното законодателство или от законодателството на Европейския съюз;
4. обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
5. обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, предоставени на Центъра;
6. обработването е необходимо за защитата на легитимните интереси на Центъра 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;

(2) Когато не е приложимо някое от основанията от ал.1, т.2 - т.6 вкл., следва да се получи съгласието на субектите на данни за всяко конкретно обработване съобразно Раздел IV от настоящата Глава.

(3) Специални категории лични данни не се събират и не се обработват, освен ако не се прилага поне едно от следните изключения:

1. субектът на данни е дал своето изрично писмено съгласие за обработването им за една или повече конкретни цели, освен когато това е изрично забранено от закон;

2. обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на Центъра или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила;
3. обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът е физически или юридически неспособен да даде своето съгласие;
4. обработването е свързано с лични данни, които явно са направени обществено достояние от субекта;
5. обработването е необходимо с цел установяване, упражняване или защита на правни претенции;
6. обработването е необходимо по причини от важен обществен интерес на законово основание;
7. обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи; или
8. обработването е необходимо от съображения от обществен интерес в областта на общественото здраве;
9. обработването е необходимо за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели.

(4) Преди обработката на лични данни съгласно ал. 1, т. 6, се осъществява задължителна оценка за наличието на легитимен интерес за обработване на лични данни съгласно Въпросник за оценяване на наличието на легитимен интерес за обработване на лични данни (Приложение № 2).

(5) Извършването на операции по обработка на лични данни от страна на Центъра като обработващ лични данни се извършват по силата на закон, въз основа на изрично разпореждане на съответния администратор на лични данни или по силата на рамково споразумение за обработване на лични данни, сключено с администратора.

Раздел III

Прозрачна информация

Чл. 7. (1) Личните данни в Центъра следва да бъдат обработвани по прозрачен начин спрямо субектите на данни като моментът, начинът и средствата за това се определят с оглед спецификата на конкретните дейности по обработване.

(2) Ако личните данни са получени от субекта на данни в момента на събирането им се предоставя следната информация:

1. данни за контакт на Центъра и на назначеното длъжностното лице по защита на личните данни;
2. целите и правното основание за планираното обработване;

3. ако е приложимо, конкретните легитимни (законни) интереси на Центъра, представляващи основание за обработването;
4. информация относно необходимостта от обработването, ако се изисква по закон или по договор, и евентуалните последици, ако тези данни не бъдат предоставени;
5. срокът, за който ще се съхраняват личните данни, а ако това е невъзможно - критериите, използвани за определянето му;
6. потенциалните получатели или категории получатели на личните данни;
7. ако е приложимо, намерението за разкриване на лични данни на трети страни и международни организации извън ЕС, както и приложимите гаранции за защита на сигурността на данните и как субектът може да получи копие от тях;
8. наличието на автоматизирано вземане на решение и/или профилиране;
9. другите цели на обработване, различни от първоначалния замисъл на събирането на данни;
10. информация относно правата на субектите на данни;
11. правото на жалба до КЗЛД и на защита по съдебен ред;
12. всяка друга информация, допринасяща за повишаване информираността и прозрачността на конкретното обработване.

(3) Ако личните данни са получени от източник, различен от субекта на данни, заедно с информацията по ал. 2, на субекта се посочва и източника на личните данни и, ако е приложимо, дали данните са от публично достъпен източник.

(4) Информацията по ал. 3 се предоставя:

1. в разумен срок, но не по-късно от един месец след получаването на личните данни, съгласно специфичните условия на обработването;
2. незабавно при съобщаването, ако личните данни са използвани за комуникация със субекта на данните;
3. при първоначално разкриване на личните данни в случаи на разкриване на данни пред друг получател.

(5) Информацията по ал. 3 не се предоставя, ако

1. същата е вече сведена до знанието на субекта и/или същият разполага с нея;
2. това се окаже невъзможно или включва несъразмерно големи усилия;
3. получаването или разкриването на лични данни е изрично установено по закон;
4. личните данни трябва да останат поверителни поради задължение за професионална тайна или поради друг вид нормативно задължение за опазване на тайна.

(6) Оценката за наличието на обстоятелствата по ал.5 задължително се документира.

(7) Информацията по ал. 2 и 3 се предоставя в лесно достъпен формат, на ясен и разбираем език под формата на уведомление за поверителност, което:

1. следва да бъдат диференцирано според вида на обработваните данни, категориите субекти на данни или конкретните дейности по обработване;
 2. надлежно се свежда до знанието на засегнатите субекти на данни в съответствие със спецификата на съответното обработване, в това число чрез лично връчване, обявяване на информационните табла и/или на обществено достъпни места в Центъра и/или чрез публикуването им на интернет страницата на Центъра.
- (8) Директорът на Центъра утвърждава списък с поддържаните в Центъра уведомления за поверителност (Приложение № 4) като ЗДУД или друг определен от Директора служител следи за тяхната наличност и достъпност.
- (9) Когато се прецени за необходимо, се води списък на лицата, на които лично са били връчени уведомления за поверителност (Приложение № 5).
- (10) Списъкът по ал.9 може да съставлява електронен документ, програмен продукт, автоматизиран процес или друга система за проследяване информацията по този раздел.
- (11) При еднократни и/или спорадични обработвания, Директорът на Центъра утвърждава политика за поверителност с необходимата информация за целите на конкретния процес и параметри на обработката.

Раздел IV

Правила за предоставяне и оттегляне на съгласие за обработване от субекта на данни

- Чл. 8.** (1) Когато по отношение на конкретен процес по обработване на лични данни не е приложимо никое от предвидените в чл. 6 ал.1, т.2 - т.6 вкл. основания за законосъобразно обработване, следва да бъде потърсено съгласието на субекта на данни в съответствие с настоящия Раздел.
- (2) За целите на настоящите правила „съгласие“ означава:
1. всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласие личните му данни да бъдат обработвани от Центъра, което субектът на данните може да оттегли по всяко време;
 2. че субектът е напълно информиран за предвиденото обработване и е дал съгласието си в дееспособно състояние и без за целта да му е бил оказан какъвто и да било опит за въздействие/натиск; съгласие, получено под натиск или въз основа на подвеждаща информация, не се счита за валидно основание за обработване на лични данни от Администратора.
- (3) Директорът, ЗДУД или определен със заповед друг служител съблюдава спазването на правилата за надлежното получаване на съгласието на субектите на данни.
- (4) Отговорните за процеса по ал.1 служители, преди започването му, следва да се сдобият със съгласието на субекта на данни, като

1. стриктно спазват предвидените задължения за предоставяне на ясно уведомление за поверителност по реда на Раздел III;
 2. информират субекта на данни по отношение на правото му да оттегли предоставеното съгласие по всяко време съгласно ал. 9;
 3. не оказват какъвто и да било опит за въздействие/натиск за предоставяне на съгласие по ал.1.
- (5) Когато по отношение на конкретен процес по обработване на лични данни не е приложимо никое от предвидените в чл. 6 ал.1, т.2 - т.6 вкл. основания за законосъобразно обработване, се забранява обработването на лични данни преди надлежното получаване на съгласие от съответните субекти на данни. Липсата на отговор или отсъствието на активно потвърдително действие от страна на субекта на данни не може да послужи като заключение за дадено съгласие.
- (6) Получаването на съгласие по ал.2 се документира чрез:
1. получаване и съхранение на декларация за съгласие от страна на субекта на данни в свободна форма, на хартиен и/или електронен носител или чрез попълване и съхранение на хартиен или електронен формуляр по образец за предоставяне на съгласие от субекта на данни (Приложение № 6). Когато формулярът за предоставяне на съгласие е попълнен от пълномощник, към него се прилага и копие на пълномощното, заверено „Вярно с оригинала“ от титуляря, а когато същото е отправено от законен представител – копие от надлежните документи, удостоверяващи представителната му власт, заверени „Вярно с оригинала“.
 2. попълване и съхранение на хартиен или електронен формуляр за предоставяне на съгласие от субекта на данни при еднократни и/или спорадични обработвания, изготвен за целите на конкретния процес и параметри на обработката.
 3. съхранение на доказателства за активни изявления и потвърждаващи действия на субекта на данни, които ясно демонстрират неговите свободно дадени, конкретни, информирани и недвусмислени указания, че е съгласен с обработването на личните му данни, например електронна кореспонденция, системни инструменти и/или лог (log) файлове.
- (7) Обработването на специални категории лични данни въз основа на съгласие от страна на субекта на данни се осъществява само след получено изрично писмено съгласие в съответствие с образца по ал.6, т.2. Писмената форма се счита за спазена и при електронни документи, надлежно подписани по реда на Закона за електронния документ и електронните удостоверителни услуги.
- (8) Обработването на лични данни по реда на този раздел се ограничава само до начина и до целите, за които субектът е предоставил своето съгласие и до момента на оттеглянето му съгласно чл. 18, ал.9, когато е приложимо.
- (9) При оттегляне на съгласие на субекта на данни служителите преустановяват всички дейности по обработване на лични данни, които са се основавали на съгласието на субекта.
- (10) Надлежно оттегляне на съгласие от субекта по ал.9 се документира чрез:

1. получаване и съхранение на декларация за оттегляне на съгласие от страна на субекта на данни в свободна форма, на хартиен и/или електронен носител или чрез попълване и съхранение на формуляр за оттегляне на съгласието на субекта на данни (Приложение № 7). Когато формулярът за предоставяне на съгласие е попълнен е попълнен от пълномощник, към него се прилага и копие на пълномощното, заверено „Вярно с оригинала“ от титуляря, а когато същото е отправено от законен представител – копие от надлежните документи, удостоверяващи представителната му власт, заверени „Вярно с оригинала“.
 2. съхранение на доказателства за негови изявления/действия, които ясно демонстрират неговото решение да оттегли съгласието си, например електронна кореспонденция, системни инструменти и/или лог (log) файлове.
- (11) Всеки класен ръководител води регистър (списък) на предоставените съгласия за обработване на лични данни на децата/учениците.
- (12) Извън случаите по ал.11, ЗДУД или определен от него служител, когато е целесъобразно, води регистър (списък) на предоставените съгласия за обработване на лични данни, в който, когато е приложимо, се отразява и всяко оттегляне на дадено съгласие (Приложение № 8). Регистърът може да съставлява електронен документ, програмен продукт, автоматизиран процес или друга система за проследяване информацията по този раздел

ГЛАВА ЧЕТВЪРТА

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ, ФОРМИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

- Чл. 9.** (1) Настоящата глава определя техническите и организационни мерки за недопускане на неправомерен достъп, неразрешено разкриване или случайно или неправомерно унищожаване, загуба, промяна или други незаконни форми на обработка на съхраняваните или обработени по друг начин лични данни в Центъра.
- (2) Внедрените технически и организационни мерки за сигурност на обработването в Центъра целят гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на методите и системите за обработване и своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент.
- (3) Всички служители са длъжни да гарантират, че по отношение на личните данни, събирани, обработвани и съхранявани от Центъра, за които те отговарят, е осигурено подходящо ниво на защита съобразно настоящите правила и всички свързани актове.
- (4) Данни в Центъра следва да се обработват само от лицата, обработващи тези данни по указание, чиито служебни задължения или конкретно възложена задача налагат това обработване, при спазване на правилата на чл.12 по-долу.

(5) В случай, че Центърът е обработващ данни, съответните технически и организационни мерки се определят в договора със съответния администратор или нормативен акт, който регулира това отношение. Центърът си запазва правото самостоятелно да въведе мерки за сигурност, които смята за необходими.

Чл. 10. (1) Техническите и организационни мерки по чл. 9 се категоризират както следва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизираните информационни системи и/или мрежи и криптографска защита.

(2) Конкретните мерки по ал.1 се определят отчитайки:

1. Достиженията на техническия прогрес.
2. Разходите за прилагане на мерките.
3. Естеството на обработването.
4. Обхвата на обработването.
5. Контекста и целите на обработването.
6. Възможните рискове за правата и свободите на физическите лица.
7. Рискове от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

(3) Не всички мерки е възможно да се отнасят към обичайната дейност на Центъра, но е възможно необходимостта от тях да възникне при дейността на обработващите за Центъра данни от трети страни или такива, които създават специфични решения за него.

(4) Техническите и организационни мерки се прилагат, доколкото се поддържа от функционалността на съответното устройство или операционна система, и се използват от Центъра във връзка с осъществяването на съответния процес.

Чл. 11. (1) Физическа защита Центъра се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградата и помещенията, в които се обработват и съхраняват лични данни.

(2) Достъп до сградата на Центъра се осъществява в условията на установения пропускателен режим и контрол на достъп.

(3) Достъпът до определените помещения и работни кабинети, в които се събират и съхраняват лични данни и/или се съхраняват електронни носители и/или документация, съдържащи лични данни, както и помещения, в които се обработват лични данни, е физически ограничен само за оправомощени служители с оглед изпълнение на служебните им задължения, само когато е необходимо на принципа

„Необходимост да се знае“ и при съблюдаване на установения режим на достъп. Помещенията са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

(4) Когато в помещения по ал.3 имат достъп и външни лица, се обособява част, която е физически ограничена и достъпна само за или единствено в присъствието на служители, на които е необходимо да имат достъп до съответната информация с оглед изпълнението на служебните им задължения.

(5) Всички служители и работници на Центъра предприемат необходимите мерки, за да гарантират, че хартиени документи, електронни носители и/или регистри, съдържащи лични данни, не се поставят на места, където неупълномощени лица могат да имат физически или визуален достъп до тях.

(6) Комуникационно-информационните системи (компютри, мрежови устройства и др.) и технически носителите (твърди дискове, сървъри и др.), 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 с поддръжката на нормалното функциониране на тези системи.

(7) Всички документи, съдържащи лични данни трябва да се съхраняват:

1. в заключващо се помещение (кабинет) с контрол на достъпа; и/ или
2. в заключващо се чекмедже, шкаф или метална каса в съответния кабинет ; и/ или
3. ако се съхраняват на преносимо устройство (твърд диск, USB и друг технически носител), това решение задължително следва да бъде съгласувано предварително с Директора или ЗДУД и при задължително съблюдаване на правилата по чл. 14 като, когато преносимото устройство не се използва от съответния служител, да се съхранява в заключващо се чекмедже, шкаф или метална каса в съответния кабинет или работно място;
4. ако се съхраняват на компютърно устройство – в съответствие с правилата на чл. 14.

(8) Помещението, определено за архив, е оборудвано с рафтове, пожарогасител и задължително се заключва. Документация се съхранява задължително на отстояние от пода.

(9) Изнасянето и обработването на лични данни извън сградата на Центъра е строго забранено, освен когато се извършва от изрично упълномощени за това лица и след предварително разрешение на ЗДУД и/или Директора на Центъра и ако се налага с оглед осъществяване на функциите на служителя, доставчика на услуги и/или е предвидено в нормативен акт.

Чл. 12. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни в Центъра.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на вътрешните правила, инструкции и ръководствата за защита на личните данни в Центъра.;
3. знания за рисковете за личните данни, обработвани в Центъра.;

4. инструктаж за реакция при събития, застрашаващи сигурността на данните;
 5. забрана за споделяне на критична информация между персонала и с външни лица (например идентификатори, пароли за достъп и т.н.);
- (3) Достъпът до лични данни се осъществява само от 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 само след получен инструктаж съгласно Глава втора. Последващи обучения на персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.
- (5) От всички работници/служители, както и физически лица, които по гражданско правоотношение обработват лични данни от името на Центъра, се изисква да подпишат декларация, преди да им бъде предоставен достъп до каквато и да било информация на Центъра (Приложение № 10).

Чл. 13. (1). Документална защита представлява система организационни мерки спрямо съхраняваната в Центъра документация, независимо дали същата е на хартиен носител или в електронна форма.

(2) Основните приложими мерки за документална защита на личните данни са:

1. Документи, съдържащи личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или дейността на Центъра, а сроковете и начинът на тяхното съхранение се осъществява в съответствие с утвърдените Номенклатура на делата със срокове за съхранение (НДСС) на Центъра;
2. 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 и съблюдаване на свързаните вътрешни правила;
3. Достъпът до електронни документи и документи, съдържащи лични данни в компютризиран формат, следва да бъдат защитени с парола/чрез криптиране или друг аналогичен начин;
4. Достъпът до документацията и поддържаните в Центъра регистри е ограничен и се предоставя на определените от Директора служители, в съответствие с принципа на „Необходимост да знае“;
5. Документация се размножава и разпространява само в случаите, когато това е пряко свързано с изпълнение на законовите задължения и/или дейността на Центъра и се извършва само и единствено от упълномощени служители при възникнала необходимост;
6. На унищожаване по подходящ и сигурен начин в съответствие с НДСС на Центъра и с чл.16. ал. 7 от настоящите правила подлежат документите, съдържащи лични данни:
 - по отношение на които са изтекли установените срокове за съхранение;
 - които не са необходими за нормалното функциониране на Центъра;
 - които не подлежат на издаване към Централен държавен архив.

7. При необходимост от обявяване на определени документи (на информационно табло, интернет сайт, публикации, обяви и др.), съдържащи лични данни, същите се заличават от копието, преди да бъдат обявени, служителите, които подготвят данните за публикуване, отговарят за тяхната достоверност, актуализация и заличаване.

Чл. 14. (1) Защитата на автоматизираните електронни системи и/или мрежи в Центъра 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, приложени в съответствие с обема, целите и особеностите на конкретния процес по обработване.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни:

1. отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;
2. предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;
3. предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;
4. предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни – контрол на потребителите;
5. гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;
6. осигуряват възможността за проверка и установяване до кои лица са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;
7. осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;
8. предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;
9. осигуряване на възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;
10. осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

(3) Контролът на достъпа до данни по ал.2 се осъществява чрез употребата на лични потребителски профили и пароли за достъп, които:

1. следва да се подновяват/сменят/ периодично;
2. не се запаметяват в автоматизирани процеси на влизане и не се съхраняват на видими и леснодостъпни за трети лица места;
3. не съвпадат с паролите на служителите за лична употреба;
4. не се споделят с други лица, включително от състава на Центъра.

(4) Лични данни трябва:

1. ако са в компютъризиран формат, следва да бъдат защитени с парола/чрез криптиране или друг аналогичен начин; и/ или
2. ако се съхраняват на компютърно/мобилно и/или преносимо устройство (твърд диск, USB и друг технически носител) то следва да е защитено с парола/чрез криптиране;
3. ако се съхраняват на компютърно устройство посредством специализирани софтуерни продукти и операционна система, същите следва да бъдат лицензирани, редовно актуализирани до най-актуална продуктова версия и задължително защитени с антивирусен софтуер и достъпвани посредством персонална парола или друг аналогичен начин.

(5) Всички служители и работници на Центъра предприемат необходимите мерки, за да гарантират, че:

1. компютърните екрани не са видими за други лица, освен за упълномощените за това служители;
2. използват само лицензиран софтуер;
3. регулярно обновяват антивирусните софтуери;
4. няма активни потребителски сесии и/или не оставят компютъра си активен, когато не са на работното си място;
5. взимат съгласие от страна на ЗДУД или Директора за въвеждането на каквито и да е промени (хардуерни и/или софтуерни) на служебното оборудване/работна станция.

(6) За работа с електронни данни се използват само лицензирани софтуерни продукти. Достъп до операционната система, съдържаща файлове за обработване на лични данни имат само служителите, упълномощени да работят с нея;

(7) Защитата на електронните данни се осигурява посредством поддържане на антивирусни програми, периодично архивиране, както и чрез поддържане им и на хартиен носител.

(8) Техническите носители могат да се разпространяват само ако данните са защитени с парола, криптирани, псевдонимизирани или ако е използван друг подходящ механизъм, гарантиращ, че те не могат да се четат или променят при пренасянето им;

(9) Личните данни в електронен вид се съхраняват съобразно спецификата и нуждите на Центъра, но при всяко положение в съответствие с Номенклатура на делата със срокове за съхранение на Центъра.

(10) Защитата на автоматизираните електронни системи и/или мрежи в Центъра следва да се осъществява и в съответствие със Закона за киберсигурност и Наредбата за минимални изисквания за мрежова и информационна сигурност.

ГЛАВА ЧЕТВЪРТА

РЕГИСТРИ И ЛИЧНИ ДАННИ

Раздел I

Регистър на дейностите по обработване на лични данни.

Чл. 15. (1) ЗДУД или определен от него служител поддържа и съхранява регистър на дейностите по обработване на лични данни (Приложение № 11), който да съдържа най-малкото следната информация:

1. координати за връзка с Центъра и на длъжностното лице по защита на данните;
2. наименование на дейността;
3. целите на обработването на лични данни;
4. описание на категориите субекти на данни и на категориите обработвани лични данни;
5. категориите получатели, пред които са или ще бъдат разкрити данните, включително получателите в трети държави или международни организации;
6. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация;
7. когато е възможно, предвидените срокове за съхраняване и дати на изтриване на различните категории съхранявани лични данни;
8. общо описание на техническите и организационни мерки за сигурност в Центъра.

(2) В регистъра по ал.1 се включват дейностите на Центъра, във връзка с които се поддържат регистри с лични данни и вътрешноведомствени регистри и неструктурирани и структурирани документи и книжа, които съдържат информация и/или се поддържат с цел обслужване, включително, но не само на учебната дейност, човешки ресурси, деловодното обслужване и други операции, в хода които се набира, съхранява и обработва информация, необходима за целите на изпълнение на дейността и правомощията и законовите задължения на Центъра.

(3) Регистърът по ал. 1 се актуализира при въвеждането на нови процеси и/или се преглежда най-малко веднъж годишно и при необходимост се актуализира.

(4) Регистърът по ал.1 се предоставя на КЗЛД при поискване след съгласуване с Директора на Центъра.

(5) В случай, че Центърът е обработващ данни, ЗДУД или определен от него служител поддържа и съхранява в писмена форма, включително в електронен формат, регистър на всички категории

дейности по обработване, извършени от Центъра от името на администратори на лични данни, в който се съдържат:

1. координати за връзка с Центъра и с длъжностното лице за защита на данните;
2. името и координатите за връзка с всеки администратор, от чието име Центъра действа;
3. категориите обработване, извършвано от Центъра от името на всеки администратор;
4. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация;
5. общо описание на техническите и организационни мерки за сигурност в Центъра.

(6) Регистърът по ал. 5 се актуализира при въвеждането на нови процеси и/или администратори и се преглежда най-малко веднъж годишно, и при необходимост се актуализира.

(7) След съгласуване с Директора на Центъра, регистърът по ал.5 се предоставя на всеки администратор, от чието име Центърът действа, но само в частта, засягаща дейностите по обработване от името на съответния администратор.

(8) Регистърът по ал.5 се предоставя и на КЗЛД при поискване след съгласуване с Директора на Центъра.

Раздел II

Актуализация и архивиране на информация.

Чл. 16. (1) Личните данни включени в информацията по чл.15, ал.2 се преглеждат за тяхната актуалност и необходимост от съхранение веднъж годишно и при необходимост се актуализират или архивират и/или унищожават в съответствие с настоящия член.

(2) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в Центъра. Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;
2. по инициатива на Центъра – при наличие на документ, даващ основание за актуализация;
3. при установена грешка при обработката на личните данни ;

(3) При актуализация на лични данни в съответния информационен масив се отразяват на документът - източник на данните за актуализацията и дата на актуализацията. Актуализацията се извършва от упълномощения за това служител.

(4) Архивирането на документацията, съдържаща лични данни трябва да се извършва периодично след изтичане на установените в Номенклатура на делата срокове за съхранение на Центъра.

(5) Архивиране на личните данни на технически носител се извършва периодично с оглед запазване на информацията 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 конкретните данни. Достъп до архивите имат само оторизираните лица.

(6) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Номенклатурата на делата срокове за съхранение на Центъра и Закона за националния архивен фонд.

(7) Извън случаите по ал.6, след като се вземе решение за изтриване на определени хартиени документи и/или регистри, същите се унищожават физически чрез машинно нарязване или се предават за изгаряне, за което надлежно се изготвя протокол за унищожение (Приложение № 12), а техническите носители (компакт дискове, преносими устройства за съхранение, твърди дискове и др.) следва да бъдат изчистени от всякакво съдържание и данни, а когато това е невъзможно – да бъдат физически унищожени.

(8) В случай, че Центърът е обработващ данни, действията по настоящия раздел предварително се съгласуват със съответния администратор на лични данни.

Чл. 17. Контролът върху прилагането на правилата на настоящата глава се осъществява от ЗДУД.

ГЛАВА ПЕТА

ПРАВА НА СУБЕКТИТЕ НА ДАННИ И УСЛОВИЯ ЗА УПРАЖНЯВАНЕТО ИМ

Раздел I

Права на субектите на данни

Чл. 18. (1) Субектите на данни разполагат със следните права във връзка с обработването на личните им данни:

1. Право на информация относно и на достъп до обработваните лични данни;
2. Право на коригиране на неточни данни;
3. Право на изтриване на личните данни;
4. Право на ограничаване на обработването;
5. Право на преносимост на личните данни;
6. Право на възражение, включително срещу обработване за целите на директния маркетинг;
7. Право да не бъдат обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за субекта на данните или по подобен начин го засяга в значителна степен;
8. Право на оттегляне на съгласие.

(2) Субектите на данни могат да упражняват правата по ал.1 с искане до Директора на Центъра в свободна писмена форма или чрез използването на съответните Формуляри за упражняване на правата на субектите на данни (Приложения № 13 до № 17 и, както и Приложение № 19).

(3) Искането може да бъде отправено и по електронен път на указаните в уведомлението по чл. 7 адреси на електронни пощи по реда на Закона за електронния документ и електронните удостоверителни услуги.

(4) Искането се отправя лично от физическото лице, от негов законен представител или от писмено упълномощено от него лице.

(5) Искането съдържа:

1. три имена,

2. ЕГН/ЛНЧ/

3. адрес на искателя;

4. описание на искането;

5. предпочитана форма за комуникация;

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

(6) При подаване на искането от упълномощено лице към същото се прилага и копие на пълномощното, заверено „Вярно с оригинала“ от титуляря, а когато същото е отправено от законен представител – копие от надлежните документи, удостоверяващи представителната му власт.

(7) Когато молбата се подава лично, от субектите на данни се изисква да предоставят доказателства, удостоверяващи самоличността им като представят документ за самоличност, който се връща веднага, а при подаване на искане по електронен път по ал. 3, проверката на самоличността се осъществява по реда на Закона за електронната идентификация, както и по други начини, установени със закон.

(8) При приемане на искането, съответният служител извършва регистрация в деловодната система на Центъра в съответствие с установените правила.

(9) Служителите извършват първоначална проверка дали при уважаването на искането няма да бъдат предоставени и лични данни на трети лица и при необходимост заличават данните, идентифициращи тези лица.

(10) ЗДУД и длъжностното лице по защита на лични данни следят за постъпили искания на електронните пощи съгласно ал.3.

(11) ЗДУД или определен от него служител поддържа Регистър на постъпилите искания на субектите на данни, в който се посочва и датата, на която на субекта на данни е предоставена информация относно предприетите действия по отправеното искане (Приложение № 18).

(12) Регистърът по ал.11 може да съставлява електронен документ, програмен продукт, автоматизиран процес или друга система за проследяване на информацията и обстоятелствата по този раздел.

Чл. 19. (1) Всички служители в Центъра следва незабавно да докладват на и уведомяват ЗДУД за всички постъпили искания и възражения по тази глава.

(2) На всички искания и възражения следва да бъде отговорено без ненужно забавяне и най-късно в рамките на един месец от получаването им.

(3) При необходимост срокът по ал.2 може да бъде удължен с още два месеца, като се вземат предвид сложността и броят на исканията. В случай на удължаване на срока, съответният субект на данните следва да бъде информиран за това в срока по ал. 2, заедно с изрично посочване на причините за забавянето.

(4) Ако искането/възражението на субекта на данни не бъде уважено, същият следва да бъде уведомен в срока по ал. 2 за причините за отказ както и за възможността за подаване на жалба до КЗЛД и търсене на защита по съдебен ред.

(5) Информацията, както и всяка комуникация и действия по реда на тази глава се предоставят безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, е позволено:

1. да се наложи разумна такса за обработване на искането, като се вземат предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или

2. да се откаже да предприемат действия по искането. В този случай се прилага ал.4.

(6) Всички действия по този раздел се съгласуват със ЗДУД и длъжностното лице за защита на лични данни, като окончателното решение се взема от Директора на Центъра.

(7) В случай, че Центърът е обработващ данни, всички постъпили искания и възражения по тази глава се препращат без забавяне на съответния администратор, засегнат от искането / възражението. Последващите действия във връзка с постъпилите искания се съгласуват със съответния администратор и на същия се указва необходимото съдействие.

Раздел II

Право на достъп на субекта на данните

Чл. 20. (1) Всеки субект на данни (физическо лице) има право на достъп до отнасящите се до него лични данни, обработвани от Центъра.

(2) В случаите, когато при осъществяване правото на достъп могат да се разкрият лични данни и за трето лице, съответният достъп се предоставя само за частта от данните, отнасяща се до отправилния искането.

(3) При упражняване на правото си на достъп субектът на данни има право по всяко време да поиска от Центъра:

1. потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

2. справка, съдържаща личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) В своето искане субектът на данни следва да посочи конкретните съхранявани данни, до които желае да му бъде предоставен достъп. Това не ограничава правото му на достъп до всички съхранявани негови лични данни.

(5) Когато искането на субекта на данни е явно неоснователно или прекомерно, същото може да бъде оставено без уважение, като субектът на данни се уведомява за взетото решение в съответствие с чл. 19, ал.2.

(6) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници или от други лица с доказан правен интерес.

Чл. 21. (1) Субект на данни може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(2) Служителите са длъжни да се съобразят с предпочитаната от молителя форма на предоставяне на информацията .

(3) Изключения от ал.2 са възможни, когато:

1. за исканата форма няма техническа възможност;
2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

(4) Субсидиарно приложение намират правилата на чл.19.

Раздел III

Право на коригиране и изтриване

Чл. 22. (1) Всеки субект на данни има право да поиска:

1. коригиране на своите данни, когато същите са неточни; и/или
2. изтриване на своите лични данни без ненужно забавяне.

(2) Служителите следва да предприемат подходящи действия по заличаване на съответните лични данни, ако:

1. субектът на данни оттегли съгласието си, когато то е правното основание за конкретното обработване;
2. правното основание за обработването отпадне и/или се установи, че данните са били обработвани незаконосъобразно;
3. личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
4. субектът на данни възрази изцяло или отчасти на обработването и няма законни основания за обработването, които да имат преимущество;
5. данните следва да бъдат заличени по силата на задължение, произтичащо от приложимото законодателство.

(3) В случай, че субектът на данни поиска данните му да бъдат коригирани или изтрети, следва да се съберат достатъчно доказателства и данни за основателността на искането, като задължително се изисква становището на длъжностното лице по защита на личните данни.

(4) Искането по ал. 1, т. 2 не се уважава, ако обработването е необходимо за:

1. упражняване на правото на свобода на изразяването и правото на информация;
2. спазване на нормативно задължение, вменено на Центъра;
3. упражняването на официални правомощия на Центъра;
4. по причини от обществен интерес в областта на общественото здраве;
5. целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;
6. за установяването, упражняването или защитата на правни претенции.

(5) В случай, че искане по ал. 1 бъде уважено, служителите:

1. следва да премахнат, съответно коригират личните данни в системите и операциите по обработване без излишно забавяне;
2. когато Центърът е направило личните данни обществено достояние, и доколкото това е възможно, да се свържат с другите организации - администратори и/или обработващи лични данни на съответния субект, и да ги уведомят, че е необходимо да коригират, съответно преустановят обработването и заличат тези лични данни.

(6) Субектът на данни се уведомява за предприетите действия в съответствие с чл. 19.

Раздел IV

Право на ограничаване на обработването

Чл. 23. (1) В случай, че субектът на данни поиска ограничаване на обработването, съответните лични данни следва да бъдат маркирани и тяхното обработване да се преустанови, когато:

1. точността им се оспорва - за срока, необходим да бъде проверена точността им;
2. обработването е неправомерно, но субектът не желае данните да бъдат изтрети, а изисква вместо това ограничаване на използването им;
3. Центърът не се нуждае повече от данните за целите на обработването, но субектът ги изисква за установяването, упражняването или защитата на правни претенции;
4. субектът е възразил срещу обработването - за срока до произнасяне по възражението;

(2) Когато обработването е ограничено, маркираните лични данни се обработват само:

1. със съгласието на субекта на данните;
2. за установяването, упражняването или защитата на правни претенции или за защита на правата на друго физическо лице
3. поради важни основания от обществен интерес.

- (3) По отношение на съхранението на маркираните лични данни ал. 2 не намира приложение.
- (4) Когато личните данни са направени обществено достояние, и доколкото това е възможно, при уважаване на искането по ал. 1 служителите следва да се свържат с другите организации - администратори и/или обработващи лични данни на съответния субект, и да ги уведомят, че е необходимо да ограничат обработването на неговите данни.
- (5) Субектът на данни се уведомява за предприетите действия в съответствие с чл. 19.
- (6) Преди отмяната на наложеното ограничение на обработването субектът на данните, изискал ограничаването на обработването им съгласно ал. 1, следва да бъде надлежно информиран в съответствие с чл. 19.

Раздел V

Право на преносимост на данните

Чл. 24. (1) Всеки субект на данни има право да поиска:

1. да получи личните данни, които го засягат, в структуриран, широко използван и пригоден за машинно четене формат и/или
2. неговите лични данни да бъдат прехвърлени на друга организация (администратор).

(2) Ал. 1 се прилага само ако едновременно са налице следните условия:

1. обработването на данните се осъществява на основание дадено от субекта съгласие или във връзка с изпълнение на договорно задължение спрямо субекта;
2. обработването се извършва по автоматизиран начин;
3. обработването не се извършва в изпълнение на обществени или законови задължения, нито за изпълнението на задача от обществен интерес или при упражняване на официални правомощия на Центъра.

(3) Субектът на данни следва в искането си да посочи конкретно личните данни, които желае да му бъдат предадени за негово лично използване или да бъдат прехвърлени.

(4) Исканата информация следва да бъде предоставена в подходящ машинно четим формат, който позволява ефективното повторно използване на данните.

(5) При прехвърлянето на данни към друга организация, служителите изпращат данните във машинно четимия формат по ал.4, ако това е технически възможно. В случай че технически затруднения възпрепятстват прякото прехвърляне, на субекта на данни следва да бъдат дадени разяснения относно тези затруднения в съответствие с чл.19.

Раздел VI

Право на възражение

Чл. 25. (1) Субектите на данни могат по всяко време и на основания, свързани с конкретната им ситуация, да подадат възражение срещу обработване на лични данни, когато обработването:

1. се осъществява в изпълнение на задача от обществен интерес или при упражняването на официални правомощия на Центъра;

2. е необходимо за целите на легитимните интереси на Центъра или на трета страна;

3. се осъществява за целите на директния маркетинг;

4. се осъществява за целите на научни или исторически изследвания или за статистически цели;

(2) Оспореното обработване на лични данни следва да бъде преустановено, освен ако не съществуват преимуществени законови основания за обработването или същото се осъществява за установяването, упражняването или защитата на правни претенции на Центъра, а когато възражението е във връзка с ал.1 т.4 - освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от публичен интерес.

(3) Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели задължително се прекратява.

(4) На всички получени възражения следва да бъде отговорено в срока по чл.19, ал.2.

(5) ЗДУД или определен от него служител водят Регистър на възраженията, съдържащ информация относно датата, на която е бил предоставен отговор на възражението на субекта на данни (Приложение № 20).

(6) Регистърът по ал.5 може да съставлява електронен документ, програмен продукт, автоматизиран процес или друга система за проследяване на информацията и обстоятелствата по този раздел.

Раздел VII

Автоматизирано вземане на решения

Чл. 26. (1) В Центъра се забранява вземането на решения, включително профилиране, основаващо се единствено на автоматизирано обработване на лични данни без човешка намеса (софтуер, компютризиран процес и др.), имаща за цел осъществяването на автоматична оценка на аспекти, свързани с него, като представянето му на работа, надеждност, поведение и т.н., което поражда правни последиствия за субекта на данни или по подобен начин го засяга в значителна степен.

(2) Забраната по ал. 1 не се прилага, когато такова обработване:

1. е необходимо за сключването или изпълнението на договор между субекта на данни и Центъра;

2. е разрешено от приложимото законодателство; или

3. се основава на изричното съгласие на субекта на данни.

(3) Независимо от изключенията по ал. 2, забраната по ал. 1 се прилага по отношение на всякакво автоматизирано обработване на специални категории лични данни.

(4) Автоматизирането на вече съществуващи процеси, съответно въвеждането на нови такива, се осъществява при съблюдаване на чл. 6, ал. 5 и при предварително съгласуване със ЗДУД и длъжностното лице по защита на лични данни, като крайното решение се взема от Директора на Центъра. В рамките на това автоматизиране винаги се предвижда етап на човешка намеса в процеса.

ГЛАВА ШЕСТА

ОБМЕН НА ИНФОРМАЦИЯ. МЕЖДУНАРОДНО ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ

Раздел I

Обмен на информация и достъп на трети лица

Чл. 27. (1) Обменът на информация в рамките на дейността на Центъра се осъществява в съответствие с настоящите правила и всички други свързани правила и инструкции.

(2) Достъп до обработваните от Центъра лични данни имат субектите на данни съгласно чл. 20, както и тези получатели, за които същият произтича от законово или договорно основание като държавни, централни и местни органи и органи на надзор, на съдебната власт, на образователната система и други легитимни получатели на документи, информация и лични данни.

(3) Достъп на представители на органите и получателите по ал.2 се предоставя след надлежно легитимиране със съответни документи, в това число единствено въз основа на изрични разпореждания/искания на съответния орган/получател (Комисия за защита на лични данни, Министерство на образованието и науката, РУО, Столична община, МВР, съд, прокуратура, следствени органи и др.), в които се посочва основанието и целите, за които е необходимо да им се осигури достъп до определена информация.

(4) Решението за предоставяне или отказване на достъп до лични данни от Центъра се взема отделно за всеки конкретен случай и следва да бъде мотивирано с оглед необходимостта от разкриването, съответно обработването на данните, категориите лични данни и техния обем, както и целите, за които данните биха се предоставили в конкретен случай, в рамките на указания в искането срок, но не по-късно от 30 дни от подаване на молбата, респ. искането, освен ако специален закон не предвижда друг срок.

(5) Лични данни се предоставят на трети лица само с решение на Директора на Центъра.

Чл. 28. (1) Когато обработване на лични данни се извършва от името на Центъра от обработващ лични данни, Центърът използва услугите само на такива обработващи, за които може да бъде счетено, че предоставят достатъчни гаранции и прилагат подходящи технически и организационни мерки, за да гарантират, че:

1. ще спазват стриктно всички изисквания на приложимото законодателство;

2. ще осигурят необходимото ниво на защита на правата на субектите на данни;
- (2) В случаите, в които Центърът ангажира обработващи лични данни от свое име, както и когато действа като обработващ лични данни от името на администратори на лични данни, задължително се сключва договор за обработване на лични данни, включващ информацията по ал.5 и ал.6.
- (5) Договорът за обработване на лични данни задължително следва да регламентира:
1. предмета и срока на действие на обработването;
 2. естеството и целта му;
 3. видовете лични данни, които ще се обработват от обработващия;
 4. категориите субекти на данни.
- (6) Договорът за обработване на лични данни задължително предвижда, че обработващият лични данни:
1. ще обработва личните данни само по документирано нареждане на Центъра и съгласно писмените инструкции на Центъра, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато обработващият е длъжен да направи това по силата на законово задължение (като в този случай обработващият следва предварително да информира Центъра за това правно изискване, освен ако това е забранено от закон на важни основания от публичен интерес);
 2. ще гарантира, че лицата, оправомощени да обработват лични данни, са договорно или законово задължени да осигурят тяхната поверителност;
 3. ще вземе всички необходими технически и организационни мерки за осигуряване подходящо ниво на сигурност на личните данни;
 4. като взема предвид естеството на обработването, подпомага, доколкото е възможно, чрез подходящи технически и организационни мерки Центърът при изпълнението на задължението ѝ да отговори на исканията на субектите на данни за упражняване на техните правата ;
 5. подпомага Центъра да гарантира изпълнението на задълженията си във връзка с осигуряването на сигурността на данните, нарушенията на сигурността и извършването на ОВЗД, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия;
 6. по избор на Центъра заличава или връща всички обработвани лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако не е законово задължен да ги съхранява;
 7. незабавно уведомява Центъра, ако според него дадено нареждане нарушава приложимото законодателство относно защитата на данните;
 8. незабавно уведомява Центъра след като узнае за нарушаване на сигурността на личните данни.
- (7) Контролът върху прилагането на правилата на настоящия раздел се осъществява от ЗДУД.

Раздел II

Международно предаване на лични данни

Чл. 29. (1) Настоящият раздел съдържа описание на процесите за предаване на лични данни от Центъра на организации, установени в други държави извън Европейската икономическа зона (ЕИЗ), за да се гарантира изпълнение на съответните правни изисквания.

(2) Предаването на лични данни извън ЕИЗ се забранява, освен ако не са в сила една или повече от посочените предпазни мерки или изключения:

1. Налично решение Европейската комисия (ЕК) относно осигуряването на адекватно ниво на защита по отношение на територия и/или конкретен сектор по местонахождение на третата страна – получател.

2. Третата страна – получател е страна по двустранно споразумение с Центъра, основано на одобрени стандартни договори с клаузи за предаване на данни извън ЕИЗ;

(3) При липса на някоя от гореописаните предпоставки, предаването на лични данни към трета държава или международна организация се осъществява при наличие на едно от следните условия:

1. Субектът на данните изрично е дал съгласието си за извършването на предлаганото предаване на данни, след като е бил информиран за свързаните с предаването рискове за себе си, произтичащи от липсата на решение относно адекватното ниво на защита и на подходящи гаранции;

2. Предаването е необходимо за изпълнението на договор между субекта на данните и Центъра или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;

3. Предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между Центъра и друго физическо или юридическо лице;

4. Предаването е необходимо поради важни причини от обществен интерес;

5. Предаването е необходимо за установяването, упражняването или защитата на правни претенции;

6. Предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

7. Предаването се извършва от регистър, който съгласно приложимото законодателство е предназначен да предоставя информация на обществеността и е публично достъпен за справки по принцип или за справки от лица, които могат да докажат, че имат законен интерес от извършването на справките, но само доколкото условията за справка, установени в приложимото законодателство, са изпълнени в конкретния случай.

(4) Проверка за наличието на необходимите предпоставки или изключения за предаване на данни извън ЕИЗ се осъществява винаги преди такова предаване да бъде иницирано от ЗДУД със задължителното участие на длъжностното лице по защита на лични данни, като окончателното решение се взема от Директора на Центъра.

ГЛАВА СЕДМА
ЗАДЪЛЖЕНИЯ ВЪВ ВРЪЗКА С НАРУШЕНИЯТА
НА СИГУРНОСТТА НА ДАННИТЕ

Раздел I
Отговорности

Чл. 30. (1) Всички служителите на Центъра следва да спазват правилата, предвидени в тази глава, при всички случаи на инциденти на сигурността на личните данни.

(2) Всички работници и служители на Центъра са длъжни да докладват на ЗДУД всеки евентуален инцидент на сигурността на личните данни незабавно след забелязването/установяването му посредством попълването на Част I от Отчет за инцидентите в сигурността на данните (Приложение № 22).

(3) В случай на нарушение и/или установен инцидент и след като незабавно уведоми за това Директора на Центъра, ЗДУД координира последващите действия и мерки за документиране и справяне с нарушението на сигурността, като изисква становище от длъжностното лице по защита на личните данни.

(4) По време на идентифицирането на евентуален инцидент на сигурността не се позволява на служителите да продължат работата си по процеса, техниката и/или активите, засегнати от нарушението до предприемането на подходящи мерки за неговото отстраняване.

Раздел II
Нарушения на сигурността на данните

Чл. 31. (1) Нарушение на сигурността на лични данни означава инцидент, който води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

(2) Всички нарушения и инциденти се разследват веднага след установяването им и подлежат на непосредствена оценка от ЗДУД и длъжностното лице за защита на личните данни посредством попълването на Част II и Част III от получения отчет по чл.30, ал.2.

(3) Всички нарушения на сигурността на лични данни, обработвани от Центъра от името на администратори на лични данни, се докладват на същите не по-късно от 24 часа от тяхното установяване ведно с информация относно нарушението и предприетите от Центъра мерки за неговото справяне, като се оказва необходимото съдействие на администраторите да осъществят оценка на нарушението на сигурността на данните.

(4) При извършването на оценката на нарушението на сигурността на данните се вземат предвид най-малкото следните критерии:

1. вид на нарушението (компютърно проникване, загуба на устройство, физическа кражба или друго);
2. обем и чувствителност на засегнатите лични данни;
3. брой засегнати субекти на данни;
4. степен на идентифициране на лицата;
5. особени характеристики на засегнатите лица (напр. служители, деца);
6. потенциални вреди и тежест на последиците за засегнатите субекти (риск от кражба или измама, физическо или психологическо увреждане, уронване на репутацията и др.).

(5) Оценката на потенциални вреди и последиците съгласно ал.4, т.6 за засегнатите субекти се документира в случаите, в които са засегнати процеси по обработка, които Центъра осъществява в качеството си на администратор на лични данни и се осъществява в съответствие с Методология за оценка на въздействието от нарушението на сигурността (Приложение № 23) и се отбелязва в Част III от получения по ал.1 отчет.

(6) При необходимост следва да бъде потърсено допълнително съдействие от квалифицирани технически или правни консултанти при анализа и установяването на инцидента и определянето на уместните действия за овладяването му и прилагането на кризисни планове. Преди да бъдат ангажирани външни консултанти и/или трети страни, те подписват споразумение за конфиденциалност.

(7) Ако има данни, че нарушението на сигурността може да съставлява престъпление, следва да бъде потърсено съдействието на компетентните органи още на най-ранен етап, но само след изрично разрешение от Директора на Центъра.

(8) След приключване на действията по предходните алинеи, пълният отчет по чл. 30 и чл. 31 се предоставя за съгласуване на Директора на Центъра.

(9) ЗДУД или определен от него служител поддържа Регистър на нарушенията на сигурността на данните, в който документира всяко нарушение (Приложение № 24).

(10) Регистърът по ал.9 може да съставлява електронен документ, програмен продукт, автоматизиран процес или друга система за проследяване на информацията и обстоятелствата по този раздел.

(11) При поискване Регистърът на нарушенията на сигурността на данните се предоставя на КЗЛД след съгласуване с Директора на Центъра.

Раздел III

Уведомяване компетентния надзорен орган

Чл. 32. (1) Нарушения на сигурността, за които в хода на оценката по чл.30 и чл.31 се установи, че има вероятност да породят риск за правата и свободите на субектите на данни, след изрично решение на Директора на Центъра, се докладват в срок от 72 часа на КЗЛД.

(2) Уведомлението до КЗЛД се изготвя съгласно образец на писмо (Приложение № 25), към който задължително се прилага пълният отчет по чл. 31 и съдържа следата информация:

1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, на категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителното количество засегнати записи на лични данни;

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

3. описание на евентуалните последици от нарушението на сигурността на личните данни;

4. описание на предприетите или предложени мерки за справяне с нарушението на сигурността, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(3) Уведомлението се изпраща в писмен вид по пощата с обратна разписка и, когато се сметне за подходящо, по електронен път посредством електронна поща с потвърждение за получаване и при спазване изискванията на Закона за електронния документ и електронните удостоверителни услуги.

(4) Ако уведомлението не може да бъде подадено в срока по ал. 1, то следва да се изпрати при първа възможност заедно с информация относно причините за забавянето.

(5) Ако няма възможност в Уведомлението да бъде предоставена цялата необходима информация, тя може да се предостави и на етапи.

(6) Действията по този раздел задължително се съгласуват с длъжностното лице по защита на лични данни.

Раздел IV

Уведомяване субекта на данни

Чл. 33 (1) Нарушения на сигурността, за които в хода на оценката по чл.30 се установи се установи, че има вероятност да породят висок риск за правата и свободите на физическите лица, след изрично решение на Директора на Центъра се съобщават на засегнатите субектите на данни без ненужно забавяне .

(2) Съобщаването по ал. 1 се осъществява:

1. в писмен вид чрез връчване на уведомление лично, по пощата с обратна разписка или по електронен път чрез имейл с потвърждение за получаването;

2. чрез публично оповестяване или друг подходящ начин за информирание на засегнатите субекти, ако нарушението засяга голям брой субекти на данни и регистри с лични данни и съобщаването по предходната точка би довело до непропорционални усилия.

(3) Уведомлението до субекта на данни се изготвя по образец на писмо (Приложение № 26) и описва нарушението на ясен и разбираем език и задължително съдържа информацията по предходния член.

(4) Уведомление до субектите на данни не се изпраща ако:

1. са предприети подходящи технически и организационни мерки за защита по отношение на засегнатите лични данни, които не позволяват разчитането и идентифицирането на информацията (напр. псевдонимизация, криптиране и др.);

2. са предприети последващи мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни.

(5) Действията по този раздел задължително се съгласуват с длъжностното лице по защита на лични данни.

ГЛАВА ОСМА

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

Чл. 34. (1). Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, когато съществува вероятност определен вид обработване да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването.

(2) При планирането и организирането на всяка нова извършвана от Центъра дейност, включваща обработване на лични данни, ЗДУД след съгласуване с длъжностното лице по защита на данните установява дали е необходимо да се извърши Оценка на въздействието върху защитата на данните (ОВЗД), като за целта се оценява съответната дейност, вида на обработваните лични данни и планираното обработване на лични данни.

(3) ОВЗД задължително се осъществява при извършване на която и да е от следните видове дейности:

1. систематична и подробна оценка на личните аспекти, отнасящи се до субектите на данни, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за субекта на данни или по подобен начин сериозно го засягат;

2. мащабно обработване на специални категории лични данни или на данни, свързани с присъди и нарушения; или

3. систематично и мащабно наблюдение на публично достъпна зона.

4. КЗЛД е постановила, че за съответно обработването се изисква извършването на ОВЗД.

(4) ОВЗД не се извършва, ако:

1. дейността по обработването се извършва с цел спазване на законово задължение или за защита на обществен интерес;

2. дейността по обработването се извършва при упражняването на официални правомощия на Центъра;

3. няма вероятност обработването на данни да доведе до голям риск;

4. характерът, обхватът, контекстът и целите на обработването са много сходни с обработването, за което вече има изготвена ОВЗД;
 5. разглежданите дейности по обработване вече са били проверени от КЗЛД при специфични условия, които не са се променили;
 6. КЗЛД е постановила, че за съответно обработването не се изисква извършването на ОВЗД.
- (5) Когато в резултат на ОВЗД се установи, че обработването може да породи риск за правата и свободите субектите на данни, въпросът се отнася за решаване до Директора на Центъра.
- (6) Ако в резултат на извършената ОВЗД се установи, че планираното обработване ще породи висок риск за правата и свободите на субектите на данни, въпросът се отнася за решаване до КЗЛД.
- (7) Всяко решение относно извършването на ОВЗД се документира.

Чл. 35. (1) При извършване на ОВЗД по предходния член, оценката се изготвя по задължително по критериите поверителност, цялостност и наличност.

(2) Изготвяне на ОВЗД се осъществява съгласно Методология за оценка на въздействието върху защитата на личните данни (Приложение № 27).

ГЛАВА ДЕВЕТА

ОТГОВОРНОСТ

Чл. 36. (1) За неизпълнение на задълженията, вменени на съответните компетентни лица по тези правила, по ЗЗЛД и по ОРЗД, се налагат дисциплинарни наказания по Кодекса на труда, съответно Закона за държавния служител.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на Центъра на виновните лица се търси имуществена отговорност по Кодекса на труда, съответно Закона за държавния служител или Закона за задълженията и договорите, съответно Търговския закон.

(3) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение от страна на външни лица, са причинени щети на Центъра на виновните лица се търси имуществена отговорност в съответствие с българското законодателство.

ГЛАВА ДЕСЕТА

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. По смисъла на настоящите вътрешни правила:

1. „Лични данни“ е всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, пряко или непряко, независимо от използваното средство.

Примери за лични данни са както следва: имена, ЕГН, контакт (адрес, електронна поща, телефон), информация за трудова дейност, семейно положение, родствени връзки, финансови данни, пароли, IP адреси, снимки, бисквитки, информация за геолокацията, данни, свързани със здравето, информация за съдебно минало и др.

2. „Специални категории лични данни“ са лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, профсъюзни членства, както и обработване на генетични и биометрични данни за целите на конкретно идентифициране на дадено физическо лице, данни, засягащи здравословно състояние или свързани със сексуалния живот или сексуалната ориентация на физическото лице;

3. „Субект на данни“ е всяко физическо лице, за когото се отнасят личните данни, като например: учители, ученици, родители, служители, контрагенти, консултанти, заявители на административни услуги, посетители, ползватели на интернет страницата.

4. „Структурирани данни“ са електронни данни, които се обработват автоматично или се съхраняват в бази данни, офис приложения (например във формат „Excel“) или споделени папки.

5. „Неструктурирани данни“ са електронни данни, които не могат да се обработват автоматично и за обработването на които се изисква преди всичко човешка намеса (например, сканирани документи, фотокопия на изображения в дигитален формат).

6. „Обработване“ е всяко използване на лични данни от Центъра (или трето лице обработващ лични данни от името на Центъра), включително 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 (самото съхранение на данни се счита за обработване).

7. „Администратор на лични данни“ е всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други такива определя целите и средствата за обработването на лични данни; когато целите и средствата за подобно обработване се определят от законодателството на Европейския съюз или на негова държава членка, администраторът или специалните критерии за неговото назначение могат да бъдат предвидени в правото на Съюза или на държавата членка;

8. „Съгласие на субекта на данни“ е всяко свободно дадено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, чрез изявление или ясно утвърждаващо действие, което изразява съгласието му за обработването на личните му данни;

9. „Трета страна“ е всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, Центъра, обработващия лични данни и лицата, които имат право да

обработват личните данни под прякото ръководство на администратора или на обработващия лични данни;

10. „Приложимо законодателство“ е Регламент 2016/679, Законът за защита на личните данни и свързаната подзаконова нормативна уредба;

11. „Нарушение на сигурността на личните данни“ е всяко събитие, при което е нарушена или може да бъде нарушена сигурността, поверителността, целостта или наличността на лични данни, което води до случайно, незаконосъобразно или неразрешено унищожаване, загуба, промяна или разкриване на лични данни или достъп до лични данни, или друг вид неправомерно използване на лични данни. Пример за нарушения на сигурността на данните са: съобщение по електронна поща, съдържащо лични данни, което неволно е изпратено до погрешен получател; изгубен или откраднат документ на хартиен носител, съдържащ лични данни; кибератака, извършена от хакери; изгубен или откраднат служебен лаптоп.

12. „Инцидент“ е непредвидимо обстоятелство, което би могло да засегне сигурността на данните;

13. „Профилиране“ представляват всякакви форми на автоматизирано обработване на лични данни за оценка на личните аспекти във връзка с даден субект на данни, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към резултатите в работата на субекта, икономическото му състояние, здравето, личните предпочитания или интересите му, благонадеждността или поведението му, местоположението или движенията му, когато такова автоматизирано обработване поражда правни последици по отношение на лицето или го засяга също толкова значително.

14. „КЗЛД“ означава Комисията за защита на лични данни

ГЛАВА ЕДИНАДЕСЕТА

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. С настоящите вътрешни правила се отменя действието на преходни правила и инструкции. Разпоредбите настоящите вътрешни правила влизат в сила от момента на утвърждаването им от Директора на Центъра.

§ 2. Настоящите вътрешни правила се преглеждат най-малко веднъж на тридесет и шест месеца и (при необходимост) се правят съответни изменения.

§ 3. За всички неуредени случаи се прилагат разпоредбите на Регламент 2016/679, ЗЗЛД и разпоредженията на Директора на Центъра.