Наръчник за защита на лични данни на ЦПО към МАРИЦАТЕКС АД

I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) Център за професионално обучение (ЦПО) към Марицатекс АД е юридическо лице със седалище гр. Пловдив с основен предмет на дейност „Организиране и осъществяване на професионално обучение за придобиване на степен на професионална квалификация по професия или по част от професия, както и нейното усъвършенстване, също така и на непрекъснато професионално обучение в страната и чужбина , разработване на учебни планове, програми, модули и друга учебна документация“.

(2) ЦПО обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им.

(3) ЦПО е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679 и като такъв спазва принципите за защита на личните данни, предвидени в регламента и законодателството на Европейския съюз и Република България.

Чл.2. Настоящият Наръчник урежда организацията на обработване и защитата на лични данни на обучаеми и служители, включително и на кандидатите за работа в ЦПО, на контрагентите и партньорите на ЦПО, както и на всички други групи физически лица, с които ЦПО влиза в отношения при осъществяването на дейността си. Ръководството на ЦПО е убедено, че с политиката за обработване на лични данни , заявена чрез Декларация за политиката по качество (***Приложение 1***), формулира своите основни намерения и стремеж към укрепване и успешно развитие на ЦПО.

Чл.3. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко

или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) „Данни за здравословното състояние“ са такива лични данни, които са свързани със здравословното състояние, физическото и психическото развитие на лицата, както и всяка друга информация, съдържаща се в медицинските рецепти, предписания, протоколи, удостоверения и в друга медицинска документация. Те се ползват със специална защита, тъй като представляват т.нар. „чувствителни данни“.

(3) „Генетични данни“ са лични данни, които дават информация за наследени или придобити генетични белези на дадено лице, съдържащи уникална информация за отличителните черти или здравословното състояние, получени от анализ на биологична проба на това физическо лице.

(4) „Субект на лични данни“ е физическо лице, чийто лични данни подлежат на обработка от друго лице по силата на нормативен акт или конкретно, изрично, информирано изразено от него съгласие за това. Като учебно заведение събираме лични данни от следните субекти:

- Служители на дружеството, независимо от вида на договора /трудов или граждански/, неговата продължителност, както и дали вече е приключил или още не е влезнал в сила, включително и кандидати за работа и/или техни законни представители;
- Обучаеми и/или техни законни представители, както и техни близки, когато изрична норма ни задължава за това;
- Трети лица - контрагенти, посетители и други, които имат или ще имат каквито и да било правоотношения с Дружеството и когато нормативен акт ни задължава за това;

(5) Обработването на лични данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхранение, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните. 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.

(6) „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.

(7) „Администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни.

(8) „Обработващ лични данни” означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

(9) „Получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Граждани, институции и др., които правят проверка на издаваните от ЦПО документи в регистъра на НАПОО по идентификатор (регистрационен номер на документа или ЕГН се явяват «получатели».

(10) „Трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, 13 които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни. Агенция по заетостта се явява «трета страна».

(11) „Надзорен орган“ Комисията за защита на личните данни е българският надзорен орган, отговорен за защита основните права и свободи на физическите лица във връзка с обработването и улесняване свободното движение на личните данни в рамките на Европейския съюз.

Чл.4. (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.

8. Принцип на сигурността и опазването – личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

(2) 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. При обработване на личните данни от ЦПО, служителите, преподавателите и обучаемите лица подписват декларация за съгласие – ***Приложение № 2.***

Чл.5. (1) ЦПО организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

(2) ЦПО прилага адекватна защита на личните данни, която включва:

1. Физическа защита;
2. Персонална защита;

3. Документална защита;
4. Защита на автоматизирани информационни системи и мрежи;
5. Криптографска защита.

Чл.6. (1) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на ЦПО и/или нормалното му функциониране.

(2) Събирането, обработването и съхраняването на лични данни в регистрите на ЦПО се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл.7.(1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица. Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на ЦПО към Марицатекс АД

(2) 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.

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

Чл. 8. (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 задължително се заключва.

(3) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност. Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец, съгласно ***Приложение № 3.***

(4) Съхранението на документите и преписките на хартиен носител, архивирането/ унищожаването на тези с изтекъл срок, се извършва съгласно нормативната база.

(5) 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.

(6) 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 ЦПО, 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. 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.
(7) Данните от регистъра „Видеонаблюдение" се съхраняват 14 дни.

Чл.9. (1) При промяна на нормативната база и необходимост от събиране на допълнителни лични данни ЦПО може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.
(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни. Докладите се изготвят от назначеното длъжностно лице за обработка на лични данни в ЦПО и могат да бъдат изготвени на хартиен и/или електронен носител и се предават на Директора на ЦПО.

Чл.10. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от ЦПО регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящия наръчник.

(2) В случаите, в които се налага унищожаване на носител на лични данни, ЦПО 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 Длъжностното лице по защита на данните, след уведомяване на Директора на ЦПО.

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от Длъжностното лице по защита на данните, съгласно образец, представляващ ***Приложение № 4.***

II. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ СТРАНИ

Чл.11. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице взема Директора на ЦПО.

(3) 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.

(4) 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 по образец съгласно ***Приложение № 5***, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

(5) Третите страни получават достъп до лични данни, обработвани в ЦПО, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ, НАПОО, Агенция по заетостта и др.)

Чл.12. (1) По силата на действащите нормативни актове в Република България ЦПО е задължен да предоставя информация на трети лица (НАПОО, Агенция по заетостта), във връзка с основната си дейност – провеждане на обучения, когато:

- обучението на лицето е приключило;
- е необходима за нуждите на застраховател.

(2) ЦПО не носи отговорност за начина, по който се обработват данните от третото лице. Въпреки това ЦПО взима всички обективно възможни мерки с оглед максимално гарантиране на предоставените лични данни на трети лица.

(3) ЦПО може да предоставя лични данни на трети страни и когато е задължено по силата на друг нормативен акт и/или договорно задължение, в който случай субектът на данните ще бъде конкретно уведомен.

III. СЪБИРАНЕ И ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл.13. Поддържаните от ЦПО регистри с лични данни са:

- Регистър „Служители и лица по граждански договори“

- Регистър „Обучаеми лица“
- Регистър „Контрагенти и партньори“

Чл.14. (1) В Регистър „Служители и лица по граждански договори“ се събират и съхраняват личните данни на служителите и преподавателите, заети по трудови или граждански правоотношения 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 социално осигуряване, Закона за счетоводството, Закона за държавния архив и др.
3. Използване на събраните данни за съответните лица за служебни цели.
4. За 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, служебни бележки, справки, удостоверения и др. подобни).
5. За установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори.
6. За водене на счетоводна отчетност, относно възнагражденията на посочените по-горе лица по трудови и граждански договори.

ЦПО е длъжен да оформя и поддържа в актуалност лични досиета на своите служители на трудов и/или граждански договор.

(2) Регистърът се води на хартиен и на електронен носител.

(3) Хартиените носители на лични данни се съхраняват в папки за всеки преподавател, служител, работник или наето по граждански договор лице.

(4) Достъп до досиетата имат само обработващите лица на лични данни. Възможността за предоставяне на друго лице на достъп до личните данни при обработката им е ограничена и изрично регламентирана в този наръчник.

(5) Личното досие съдържа задължително следните документи:

1. Граждански/ трудов договор
2. Длъжностна характеристика
3. Професионална автобиография
4. Документи доказващи образователно-квалификационната степен и професионална квалификация
5. Декларация за съгласие
6. Служебна бележка за проведен първоначален инструктаж

За служители на трудови договори допълнително към досието се прилагат и:

1. Свидетелство за съдимост
2. Медицинско свидетелство за постъпване на работа, заверено от личния лекар
3. Заявление за ползване на отпуск
4. Заявление за постъпване на работа

Чл.15. (1) В Регистър „Обучаеми лица“ се събират и съхраняват личните данни с оглед:

1. Индивидуализиране на съответните обучаеми лица.
2. Предоставяне на услуги от ЦПО, за които са необходими лични данни на обучаемите лица.
3. Изпълнение на нормативните изисквания на Закона за счетоводството и други относими нормативни актове.

4. Използване на събраните данни за съответните лица за служебни цели само и единствено след получаването на надлежно съгласие от лицата за обработване на техните лични данни за следните цели:

a. за всички дейности, свързани с провеждане на обучението

b. за установяване на връзка с лицата по телефон, адрес и/или електронна поща, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията им по време на обучението;

c. за водене на счетоводна отчетност;

(2) В регистъра се вписват следните видове лични данни:

1. Физическа идентичност – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
2. Социална идентичност – данни относно образование и допълнителна квалификация, трудова дейност и професионална биография;
3. Семейна идентичност – данни относно семейното положение на лицето;
4. Данни за здравословно състояние – медицинска бележка/ медицинско свидетелство
5. Информация за расов или етнически произход

Чл.16. В Регистър „Контрагенти и партньори“ се вписват следните видове лични данни:

1. Физическа идентичност – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
2. Икономическа идентичност – обща банкова информация, информация за номер на банкова сметка;

IV. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл.17. Физическата защита в ЦПО се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл.18. (1) Основните организационни мерки за физическа защита в ЦПО включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни,
3. определяне на организацията на физическия достъп;

(2) Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична“ част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп

външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

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

(4) Организацията на физическия достъп до помещения, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(5) Зони с контролиран достъп са всички помещения на територията на ЦПО, в които се събират, обработват и съхраняват лични данни.

(6) Използваните технически средства за физическа защита на личните данни в ЦПО са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения.

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

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

Чл.19. (1) Основните технически мерки за физическа защита в ЦПО включват:

1. използване на сигнално-охранителна техника;
2. използване на ключалки и заключващи механизми;
3. шкафове, метални каси;
4. оборудване на помещенията с пожароизвестителни и пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в шкафове или картотеки, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично назначените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

(3) Оборудването на помещенията, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, ключалки (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица; заключваеми шкафове и пожарогасителни средства.

(4) Пожароизвестителните средства и пожарогасителните средства се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл.20. (1) Основните мерки за персонална защита на личните данни, приложими в ЦПО, са:

1. Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящия Наръчник, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец (***Приложение № 6***);
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от ЦПО;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между персонала и всякакви други лица, които са неоторизирани;
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки:

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

Чл.21. (1) Основните мерки за документална защита на личните данни, са:

1. Определяне на регистрите, които ще се поддържат на хартиен носител - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на ЦПО, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. Определяне на условията за обработване на лични данни - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на ЦПО, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. Регламентиране на достъпа до регистрите с лични данни – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;
4. Определяне на срокове за съхранение - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.
5. Процедури за унищожаване: Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на ЦПО или за установяването, упражняването или защитата на правни претенции, се унищожават по

подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(2) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. Контрол на достъпа до регистрите, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае", за да изпълняват техните задължения;

2. Правила за размножаване и разпространение, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Чл.22. (1) Защитата на автоматизираните информационни системи и/или мрежи в ЦПО включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

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

1. Идентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на ЦПО. Прилагането на тази мярка е с цел да се регламентират нива на

достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае";

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

3. Управление на външни връзки и/или свързване, включващо от своя страна:

• Дефиниране на обхвата на вътрешните мрежи: Като вътрешни мрежи се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка", които се намират под контрола и администрацията на ЦПО. Като външни мрежи се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на ЦПО.

• Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от Директора на ЦПО лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае". Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

• Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки,

връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

- Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на ЦПО, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. Защитата от зловреден софтуер включва:

- Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста на ЦПО.
- Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.
- Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.
- Забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от Директора на ЦПО лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по създаване и поддържане на резервни копия за възстановяване, която регламентира:

- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на ЦПО.
- Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.
- Отговорност за архивиране има лицето, обработващо личните данни.
- Срокът на архивиране следва да е съобразен с действащото законодателство.
- Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

6. Основни електронни носители на информация са: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)
7. Персоналната защита на данните е част от цялостната охрана на ЦПО.
8. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на ЦПО.
9. Данните, които вече не са необходими за целите на ЦПО и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на ЦПО:

• Отдалечен достъп до вътрешни мрежи на ЦПО не е предвиден. По изключение, и след изричната оторизация от Директора на ЦПО, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

• На персонала на ЦПО може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до елекронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на Директора на ЦПО. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на ЦПО, както и в случаите на заплаха за сигурността на данните.

• Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Директора на ЦПО.

2. Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на ЦПО, включват:

• Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на ЦПО от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените

аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на ЦПО, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.

3. Мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Чл.23. (1) По отношение на личните данни се прилагат и мерки, свързани с криптографска защита на данните чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

(2) Криптирането се използва и за защита на личните данни, които се предават от ЦПО по електронен път или на преносими носители.

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

Чл.24. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) ЦПО прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секунди), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от ЦПО период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(6) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, неизключане на работна станция след изтичане на работното време и др.п.), системният администратор незабавно уведомява Директора и Длъжностното лице по защита на данните за извършване на проверка по случая.

Чл.25. Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

Чл.26. (1) В ЦПО се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от Директора на ЦПО лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(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 личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл.27. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

VI. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл.28. (1) Длъжностно лице по защита на данните може да бъде служител на фирмата или външно лице и се назначава със заповед на Директора на ЦПО. В случай на назначаване на външно лице предварително е него се сключва граждански/трудов договор. Задълженията на лицето, обработващо лични данни, се изписват в длъжностна характеристика.

(2) Длъжностно лице по защита на данните има следните правомощия и длъжностни задължения:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри с лични данни;

3. осъществява контрол по спазване на изискванията за защита на регистрите съобразно действащото законодателство и настоящият наръчник;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;
10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;
11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

Чл.29. Служителите на ЦПО 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.30. (1) За неспазването на разпоредбите на настоящия наръчник служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ЦПО или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

Чл.31. (1) С оглед извършване на основната дейност - провеждане на начално и непрекъснато професионално обучение на лица навършили 16 години и най-вече събиране на статистическа информация след завършване на обучението, ЦПО може да инициира свързване със субекта на личните данни на посочените от него телефон/и, адрес и e-mail.

(2) ЦПО гарантира, че няма да се свързва със субекта на лични данни за маркетингови цели, реклами и др. по e-mail, телефон, чрез текстови

съобщения, или по пощата, освен ако той не е дал предварително изрично желание и съгласие за това и няма законова забрана за това, при стриктно спазване на изискванията на Общия регламент.

VII. ПРАВА НА СУБЕКТА НА ЛИЧНИ ДАННИ

Чл.32. (1) Всеки субект на лични данни, обработвани от ЦПО има следните права:

- право да получи достъп до всички негови лични данни, включително да получи копие от тях, като посочи начина, по който иска да получи копието - на електронен или хартиен носител. Това право се упражнява след заплащане на съответната такса за копието, ако такава е предвидена в ценоразписа на ЦПО.
- право да ограничи обработването - по време, по обем, по място, освен ако в нормативен акт и/или договор, ЦПО не е задължено да обработва данните за по-дълъг срок, в по-голям от поискания обем и в различни от поисканите от субекта места.
- право да поиска данните да бъдат коригирани, редактирани и/или допълнени, когато те са неточни, неверни, неактуални или непълни.
- право на преносимост на негови лични данни, които той е предоставил на ЦПО към трети лица, посочени от субекта. Субектът има право да избере начина и формата, по които да стане пренасянето, но те трябва да са широко използвани и годни за машинно четене. В случай, че ЦПО обективно не може да предостави данните в избрания от субекта начин/форма, то тогава ги изпраща в друг широкоизползван и годен за машинно четене формат.

- право на възражение, касаещо обработката на данните му, в това число начин, срок, предоставяне на трети страни, без да е обвързан от време и място. Това право се упражнява само в случай, че не съществуват законови и/или договорни основания за отхвърляне на възражението, които имат предимство пред интересите, правата и свободите на субекта на данни, или поради висящо съдебно производство.
- право да поиска данните му да бъдат изтрити, тоест право да бъде „забравен“. Това право може да се упражни, само ако ЦПО не е задължено по силата на нормативен акт и /или договор да съхранява данните на лицето, въпреки неговата воля. В тези случаи ЦПО уведомява писмено субекта, че по силата на конкретна разпоредба то е задължено да съхранява и/или обработва и/или предоставя на трети лица неговите данни, като посочи и срокът, за който е задължен.

(2) В съответствие със Закона за защита на личните данни, посочените по-горе права могат да се упражнят чрез подаване на писмено заявление на адрес: гр.Пловдив , ул. „ Васил Левски’’ № 144 , съгласно Искане за лични данни ***Приложение № 7*** Заявлението може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронните удостоверителни услуги на следната електронна поща: enkin@maritzatex.com

Искането съдържа:

1. име, адрес и други данни за идентифициране на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за предоставяне на информацията;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

5. нотариално заверено пълномощно, когато се подава от упълномощено лице.

(3) ЦПО изготвя писмен отговор на заявлението в 14 работни дни, считано от деня на получаването му. Заявителят получава екземпляр от отговора, по начин заявен от него предварително, а един екземпляр от него заедно с искането остава при ЦПО.

VIII. ЗА ПОДАВАНЕ НА ЖАЛБИ:

Чл. 33. Жалба, свързана с нарушение на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни може да се подава в Комисията за защита на личните данни по един от следните начини:

• Лично, на хартиен носител – в деловодството на КЗЛД на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2.

• С писмо на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2, Комисия за защита на личните данни.

• По електронен път на имейла на КЗЛД (kzld@cpdp.bg). В този случай жалбата трябва да бъде оформена като електронен документ, подписан с електронен подпис (не сканирана!).

• Чрез сайта на КЗЛД https://www.cpdp.bg/?p=pages&aid=6 – с помощта на приложена електронна бланка. В този случай жалбата трябва да бъде оформена като електронен документ, подписан с електронен подпис. Този документ се прикачва по стандартния за това начин в полето „Прикачи документ” чрез натискане на бутона „Browse” и избор на документа. Файлът трябва да е не по-голям от 5 MB.

Задължително е да се попълнят полетата за връзка – име, адрес, електронен адрес.