ВЪТРЕШНИ ПРАВИЛА

за мерките за защита на личните данни

в УД "Капман Асет Мениджмънт" АД, гр. София

I. Общи положения

Чл. 1. (1) УД "Капман Асет Мениджмънт" АД, (УД) е юридическо лице със седалище гр. София, Р България с предмет на дейност управляващо дружество.

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

Чл. 2. Настоящите правила уреждат организацията на обработване и защитата на лични данни на служителите, контрагентите и партньорите, посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на УД.

Чл. 3. (1) Като „обработване на лични данни“ се възприема всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

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

Чл. 4. УД е администратор на лични данни по смисъла на чл. 4, пар.7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Регламент за защита на личните данни).

Чл. 5. (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) Принципите за защита на личните данни са:

1. *Принцип на ограничено и целесъобразно събиране* – събирането на лични данни трябва да бъде в рамките на необходимото за конкретни, изрично указани и легитимни цели. Информацията се събира по законен и обективен начин;
2. *Принцип на ограниченото използване, разкриване и съхраняване* – личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели;
3. *Принцип на точност* – личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват;
4. . *Принцип на сигурността и опазването* – личните данни трябва да се съхраняват и обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки

(3) В съответствие с чл. 11 ал. 3 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 6. УД организира и предприема мерки, за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) УД прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и/или мрежи;
5. Криптографска защита.

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

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

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

Чл. 9. Когато не е налице хипотезата на чл. 6, пар. 1, б. б) и в) от Регламент (ЕС) 2016/679, физическите лица, чиито лични данни се обработват, подписват декларация за съгласие по образец.

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изричен акт на Ръководството на УД.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.

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

Чл. 11. (1) Документите и преписките, по които работата е приключила, се архивират.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив задължително се заключват.

(3) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд, Закона за счетоводството и на Наредба № 44 на КФН .

(4) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на вторичен сървър (бекъп сървър) 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. Вторичният сървър се помещава на различно местоположение от мястото

на основния сървър и компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица.

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

Чл. 13. (1) Длъжностното лице за личните данни извършва периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от УД регистри, и изготвя съответни доклади не по-малко от веднъж годишно.

(2) Тези доклади трябва да включват преценка на необходимостта за обработка на личните данни и за унищожаване или архивиране на личните данни.

Чл. 14. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на прекия си ръководител, който от своя страна е длъжен, своевременно да информира Длъжностното лице за личните данни.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

(3) При наличие на инцидент от естество да доведе до изтичане на голям брой лични данни Длъжностното лице по защита на данните уведомява КЗЛД, а ако е необходимо и субектите на данни в срок не по-късно от 72 часа.

Чл. 15. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, УД може да определи друго ниво на защита за регистъра.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години.

Чл. 16. (1) След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването личните данни, съдържащи се в поддържаните от УД регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Регламент (ЕС) 2016/679 и при спазване на долупосочените процедури.

(2) В случаите, когато се налага унищожаване на носител на лични данни, УД прилага необходимите действия за тяхното заличаване по начин който позволява възстановяване на данните и злоупотреба с тях. Личните данни, съхранявани на електронен вариант на вътрешни програми за отчетност, се заличават чрез прикриването им по начин, изключващ възможността същите да бъдат видими за служителите имащи достъп до системите.

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

(3) Унищожаване се осъществява от служители, упълномощени с изричен писмен акт на Ръководството на УД, под контрола на Длъжностното лице за личните данни.

(4) За унищожаването на данните се съставя съответния протокол.

Чл. 17. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, УД съобщава в 30-дневен срок от подаване на заявлението, респ. искането. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията.

(3) Информацията по алинея 1 и всяка комуникация и действия във в ръзка с нея се предоставят безплатно. Когато исканията на субекта на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът предоставя исканата информация срещу предварително заплащане на такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия

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

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(5) Всички трети лица, обработващи данните, които имат достъп до лични данни, задължително следва да подпишат споразумение за обработка на данни, включващо клауза за спазване на строги задължения за поверителност.

(6) Изключение се допуска единствено за тези органи и/или институции, които извършват това въз основа на изискване на закона (напр. съд, прокуратура, НАП, НОИ и др.).

II. Мерки по осигуряване на защита на личните данни

Чл. 18. *Физическа защита* в УД се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се създават, обработват и съхраняват лични данни.

Чл. 19. (1). Основните приложими *организационни мерки за физическа защита* в УД включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

(2) В случай че УД оцени, че събирането, обработването и съхраняването на дадени лични данни има „средно“ ниво на въздействие, към посочените мерки се включват и определяне на зоните с контролиран достъп и на използваните технически средства за физическа защита.

(3) 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 само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения.

(4) *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.

(5) *Организацията на физическия достъп до помещения*, обработващи лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми, система за достъп до сградата и помещенията - магнитни карти и кодове за достъп) 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.

(6) Като *зони с контролиран достъп* се определят всички помещения на УД, в които се събират, обработват и съхраняват лични данни с определено ниво на въздействие повисоко от „ниско“.

(7) *Използваните технически средства за физическа защита* на личните данни в УД 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.

(8) Всички записи и документи на хартиен носител, съдържащи лични данни, са в помещения с ограничен достъп, достъпен само от упълномощен персонал.

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

Чл. 20. (1). Основните приложими *технически мерки за физическа защита* в УД включват използване на чип-кари, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

(2) *Чип-картите* и свързаните с тях електронни устройства за заключване, като способ за физическа защита, се използват, за да осигурят защита на зоните, в които се съхраняват лични данни. Тези зони са достъпни само чрез чип-карти, предоставен единствено на оторизираните (с изрична заповед или в изпълнение на служебни задължения) за това лица.

(3) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки*, като последните са разположени в зони с ограничен (контролиран) достъп. Трудовите досиета се съхраняват в помещения с ограничен достъп.

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

(5) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 21. (1). Основните приложими *мерки за персонална защита* на личните данни, оценени с ниска степен на въздействие, са:

1. Задължение на служителите да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящата инструкция срещу подпис (Приложение № 3);
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от УД;
3. Забрана за споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на въздействие, се прилагат и:

1. Познаване на политиката и ръководствата за защита на личните данни;
2. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения и/или изисква подобно;
3. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения и/или изисква подобно.

Чл. 22. (1). Основните приложими *мерки за документална защита* на личните данни, оценени с ниска степен на въздействие, 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 бизнес дейност на УД;
2. *Определяне на условията за обработване на лични данни*: личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на УД, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;
3. *Регламентиране на достъпа до регистрите*: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае";
4. *Определяне на срокове за съхранение*: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.
5. *Процедури за унищожаване*: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на УД, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи).

(2) За лични данни, оценени с по-висока степен на въздействие, се прилагат и мерки, свързани с:

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 по-висш 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 представлява нарушение на вътрешния ред в дружеството и подлежи на дисциплинарни санкции, включ. прекратяване на трудовите взаимоотношения.

Чл. 23. (1) *Защитата на автоматизираните информационни системи и/или мрежи* в УД включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

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

1. *Идентификация и автентификация* чрез използване на уникални потребителски акаунти и пароли (буквено-цифрови с минимум 8 символа) за всяко лице, осъществяващо достъп до мрежата и ресурсите на УД. 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 въвеждане, 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 УД. 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 УД.
    - Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служители и/или специално упълномощени от Ръководството 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 буквено-цифрова парола.

- Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на външно дружество осъществяващо софтуерната и хардуерна подръжка и системите в УД. 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 служители осъществяващи софтуерната и хардуерна подръжка на системите в УД (IT), както и на фирми-подизпълнители, на които е възложена колокация на сървърите на УД. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на УД, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. *Защитата от вируси*, включва:
   - използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизиран персонал на IT-консултант. Забранено е инсталирането на софтуерни продукти без изричното одобрение на IT-консултантите.
   - използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от IT-консултант. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.
   - активиране на автоматична защита и сканиране за компютърни вируси и обновяване на антивирусни дефиниции. Забранено е, потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните подписи.
   - забрана за пренос на данни от заразени компютри. При съмнение и/или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми IT-консултант 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 вирусите заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политиката по *създаване и поддържане на резервни копия за възстановяване* регламентира:
   - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на УД.
   - 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, но не по-кратък от 6 години.
   - Съхраняването на архива следва да бъде в друго физическо помещение, като в случаите, когато носителят на електронна информация е преносим и в заключен шкаф. 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 УД.
8. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на УД.
9. Данните, които вече не са необходими за целите на УД 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 въздействие, се прилагат и мерки, свързани с:

1. Организация на *телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на УД:
   - Отдалечен достъп до вътрешни мрежи на УД не е предвиден. По изключение, и след изричната оторизация от страна на ръководството, IT-консултанта съдейства за осъществяване на подобен достъп от оторизира-

ните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

- На персонала на УД може да бъде предоставен Интернет достъп за изпълнение на служебните им задължения. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се извършва по преценка и предложение на преките ръководители, съгласувано с IT-консултанта за степента на осъществимост, пряка връзка с използваните задължения и свързаните с този достъп рискове. Достъпът до Интернет, определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на УД, 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 оторизация от Ръководството на УД.

2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на УД, включват:
   - Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на УД от външни и вътрешни атаки, вкл. 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 УД и обучаваните лица, 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 и/или софтуер, който отдалечено наблюдава трафика в мрежа и/или опериращ компютър. Неоторизирано използване на подобни инструменти се наказва дисциплинарно.
3. Мерките, свързани със създаване на *физическа среда (обкръжение),* включват физически контрол на достъпа (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. 24. По отношение на лични данни, оценени със степен на въздействие по-висока от „ниско“, 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. Криптирането и/или защитата на информацията с пароли се използва за защита на личните данни, които се предават от УД по електронен път или на преносими носители. Паролата за достъп до информацията се съхранява отделно от носителя на информация с лични данни.

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

Чл. 25. (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 буквено-цифрова парола.

(2) IT-консултантът и външните подизпълнители прилагат адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола), като по този начин гарантират, че само упълномощени служители получават достъп до решаване на възложените задачи.

(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 IT-консултанта период. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта). При наличие на информация съхраняваща се само на единични устройства, достъп до които има само едно лице, това лице е задължено да предостави паролата за достъп до устройството в запечатан плик на Длъжностното лице по личните данни. Пликът може да бъде отворен само при извънредни обстоятелства след решение на ръководството на КАПМАН.

(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 работа, смяна на пароли.

Чл. 26. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

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

Чл. 27. (1) В УД се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е строго забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от IT-консултанта. 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 Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 28. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

IV. Поддържани регистри и тяхното управление

Чл. 29. Поддържаните от УД регистри с лични данни са:

1. Персонал
2. Кандидати за работа
3. Клиенти
4. Контрагенти и партньори
5. Видеонаблюдение

Чл. 30. (1) В регистър „**Персонал**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или по граждански договори. Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

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

1. Индивидуализиране на трудовите правоотношения;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.
4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(3) Регистърът съдържа следните групи данни:

1. физическата идентичност на лицето: имена, ЕГН, номер на лична карта, дата и място на издаване, месторождение/телефони за връзка и др.
2. семейна идентичност на лицата: семейно положение – наличие на брак, развод, членове на семейството, в това число деца до 18 години – данните са необходими при установяване правата на лицата за получаване на семейни добавки за деца до 18 години и ползване на данъчни облекчения за деца.
3. образование: вид на образованието, място, номер и дата на издаване на дипломата – данните са необходими с оглед спазване изискванията, посочени в класификатора на длъжностите, нормативни или установени в договор /споразумение/ с Агенцията по заетостта изисквания за заемане, респективно за освобождаване от

длъжности на лицата. Предоставят се лично от лицата на основание нормативно задължение във всички случаи, когато е необходимо.

4. трудова дейност: професионална биография – данните са от значение при избора на подходящо за съответната длъжност лице и за определяне на допълнителното трудово възнаграждение за придобит трудов стаж и професионален опит и за пенсиониране. Предоставят се на основание нормативно задължение във всички случаи, когато е необходимо.
5. медицински данни: здравен статус – данните са от значение при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рисковите групи. Имат отношение при определяне на трудовото възнаграждение, при определяне на пенсията по болест, при определяне размера на данъчната основа по ЗДДФЛ, обработване и изплащане на обезщетения за временна нетрудоспособност поради болест, защита от уволнение и др.
6. други: лични данни относно гражданско-правния статус на лицата - данните са необходими за длъжностите, свързани с материална отговорност (отчетнически длъжности), като свидетелство за съдимост. Предоставят се лично от лицето на основание нормативно задължение.

(4) Източниците, от които се събират данните, са: от физическите лица, за които се отнасят, от публични регистри, както и от външни източници (от съдебни, финансови, осигурителни, данъчни и други институции в изпълнение на нормативни изисквания).

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

1. поверителност – средно ниво;
2. цялостност – средно ниво;
3. наличност – средно ниво;
4. общо за регистъра – средно ниво.

(6) Трудовите досиета на персонала не се изнасят извън сградата на УД.

(7) Данните за здравен статус на лицата (болнични листове) се съхраняват отделно от трудовите досиета при засилен режим на сигурност на съхранението и достъпа – в отделни класьори в заключен метален шкаф (каса).

Чл. 31. Категориите лица, на които личните данни могат да бъдат разкривани, са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

Чл. 32. (1) При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на УД.

(2) При внедряване на нов програмен продукт за обработване на лични данни се съставя нарочна комисия по тестване и проверка възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 33. (1) Данните от реигъра се съхраняват в норамитвно установените срокове съгласно Закона за счетоводството:

1. ведмости за заплати и други данни относно възнагражденията на лицата – 50 години;
2. счетоводни регистри – 10 години
3. други – 6 години;

(2) След изтичане на горните срокове данните се унищожават с протокол

Чл. 34. (1) В регистър „**Кандидати за работа**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица кандидатстващи за работа в УД. Нормативното основание е Законът за задълженията и договорите, Кодекса на труда и други приложими закони.

(2) Регистърът съдържа следните групи данни:

1. физическата идентичност на лицето: имена, номер на лична карта, дата и място на издаване, ЕГН, месторождение, адрес, и-мейл и телефони за връзка и др.
2. образование: квалификация и вид на образованието, място и дата на издаване на дипломата.
3. трудова дейност: професионална биография – данните са от значение при избора на подходящо за съответната длъжност лице.

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

(4) Източниците, от които се събират данните, са: от физическите, за които се отнасят, от публични регистри, от интернет.

(5) Данните се събират с изричното съгласие на лицата, за които се отнасят данните;

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

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;

4. общо за регистъра – ниско ниво.

(7) Данните от регистъра се съхраняват на физически и/или електронни носители и се съхраняват не повече от 6 месеца, след което се унищожават с протокол.

Чл. 35. (1) В регистър „**Клиенти**“ се събират и съхраняват лични данни с цел индивидуализиране на физически лица клиенти на УД. Нормативното основание е ЗПФИ, ЗППЦК, ЗМИП и други приложими закони.

(2) Регистърът съдържа следните групи данни:

1. Физическата идентичност на лицето: имена, номер на лична карта, дата и място на издаване, ЕГН, месторождение, адрес, и-мейл и телефони за връзка, банкови сметки и др.
2. Юрисдикция за данъчни цели , данъчен номер
3. Заемане на висша държавна длъжност и свързаните с клиента лица
4. Семейно положение, семеен годишен доход,семейни връзки, финансово състояние и възможности на клиента, опит в инвестирането и др.

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

(4) Източниците, от които се събират данните, са: от физическите и/или юридическите лица, за които се отнасят, от публични регистри, от интернет.

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

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

(6) Данните от регистъра се съхраняват на физически и/или електронни носители и се съхраняват не повече от 6 година (за счетоводните регистри 10 години) на основание Закона за счетоводството и данъчните закони, след което се унищожават с протокол.

Чл. 36. (1) В регистър „**Контрагенти и партньори**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица и персонализиране на юридическите лица, имащи търговски и/или партньорски взаимоотношения с КАПМАН. Нормативното основание е Законът за задълженията и договорите, ЗПФИ и други приложими закони.

(2) Регистърът съдържа следните групи данни:

1. физическата идентичност на лицето: имена, номер на лична карта, дата и място на издаване, ЕГН, месторождение, адрес, и-мейл и телефони за връзка и др.
2. образование: квалификация и вид на образованието, място, номер и дата на издаване на дипломата – данните се събират само когато са необходими съгласно действащото законодателство за доказване на наличие на квалификация по търгове и други специфични взаимоотношения. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо.

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

(4) Източниците, от които се събират данните, са: от физическите и/или юридическите лица, за които се отнасят, от публични регистри, от интернет.

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

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

(6) Данните от регистъра се съхраняват на физически и/или електронни носители и се съхраняват минимум 6 години (за счетоводните регистри 10 години) на основание Закона за счетоводството и данъчните закони, след което се унищожават с протокол.

Чл. 37. (1) В регистър „**Видеонаблюдение**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Категориите физически лица, за които се обработват лични данни, са посетителите и служители в сградите на УД и подходите към тях.

(3) Регистърът съдържа следните групи данни:

1. физическата идентичност на лицето: видеообраз

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

(5) Източниците, от които се събират данните, са: от физическите лица. Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движе-

нието на служителите и посетителите към подходите към и в сградите на УД. Видеонаблюдението се извършва чрез изградена система за видеонаблюдение.

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

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

(7) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградите на УД.

(8) На входовете на сградата се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал. 1, т. 1, буква „а" и „б" от ЗЧОД и за използването на технически средства за наблюдение и контрол съгласно чл. 30, ал. 2 и ал. 4 от ЗЧОД.

(9) Данните от регистъра се съхраняват на сървър на дружеството за срок от 32 дни, след което автоматично се изтриват.

V. Права и задължения на лицата, обработващи лични данни. Длъжноистно лице за защита на данните.

Чл. 38. (1) Длъжностно лице по защита на личните данни в УД се назначава с решение на СД, като служителя би могъл да съвместява и други функции, както и да се използва и лице от икономическата група на Капман.

(2) Длъжностно лице по защита на личните данни има следните правомощия:

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно, спецификата на водените регистри;
3. осъществява контрол по спазване на изискванията за защита на регистрите;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. 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.

(3) Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано за изпълнението на своите задачи по смисъла на предходната алинея. Длъжностното лице по защита на данните се отчита пряко пред Изпълнителният директор на УД.

Чл. 39. Служителите на УД са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.
6. по всеки въпрос и възникнала ситуация във връзка със събиране, обработка и съхранение на лични данни да се обръщат към Длъжностното лице по защита на данните

Чл. 40. (1) За неспазването на разпоредбите на настоящата инструкция служителите носят административна и дисциплинарна отговорност.

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

Преходни и заключителни разпоредби

§ 1. По смисъла на настоящата инструкция:

- **„Лични данни“**означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентифика- ционен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице
- „**Администратор“** е физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, който сам или съвместно с друг определя целите и средствата за обработване на личните данни.
- „**Администратор на лични данни**” е УД "КАПМАН АСЕТ МЕНИДЖМЪНТ" АД, ЕИК 131126507.
- . "**Псевдонимизация (Анонимни данни)**“ означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано
- „**Високо ниво на въздействие**” е неправомерното обработване на лични данни, което би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице.
- **„Външни мрежи“** са 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 УД.
- **„Вътрешни мрежи“** са всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на УД.

- „**Голяма група физически лица**” е съвкупност от физически лица, чиито брой надхвърля 10000.
- „**Група физически лица**” е съвкупност от физически лица, чийто брой надхвърля 2.
- „**Длъжностно лице**“ е служител, на когото е възложено да упражнява ръководство на процес в УД, в нейните структурни и/или функционални единици, както и служител, който изпълнява работа на специалист във функционалните и обслужващите звена на УД.
- **„Документална защита на лични данни“** е система от организационни мерки при обработването на лични данни на хартиен носител.
- **„Защита на автоматизирани информационни системи и/или мрежи**“ е система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.
- „**Изключително високо ниво на въздействие**” е неправомерното обработване на лични данни, което би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица.
- „**Инцидент**” е непредвидимо обстоятелство, което би могло да засегне сигурността на личните данни.
- **„Криптографска защита на лични данни“** е система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.
- „**Длъжностно лице по защита на личните данни**” е физическо лице, притежаващо необходимата компетентност, което е упълномощено или назначено от администратора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.
- „**Наличност**” е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.
- „**Ниво на защита**” е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.
- „**Ниско ниво на въздействие**” е неправомерното обработване на лични данни, което би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

- „**Носител на лични данни**” е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.
- „**Обработване на лични данни**“означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване
- „**Обработващ лични данни**“ е физическо или юридическо лице, държавен орган или орган на местно самоуправление, който обработва лични данни от името на администратора на лични данни.
- „**Оператор на лични данни**” е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на КАПМАН.
- „**Особено голяма група физически лица**” е съвкупност от физически лица, чийто брой надхвърля 1000000.
- „**Оторизирано лице**“ е лице, което по силата на естеството на преките си служебни задължения и/или изричното оторизиране от Ръководството на КАПМАН, има право за достъп до определена категория лични данни.
- **„Оценка на въздействие“** е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.
- **„Персонална защита на лични данни“** е система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.
- „**Поверителност**” е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
- „**Получател**“ е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, на когото се разкриват лични данни, независимо дали е трето лице или не. Органите, които могат да получават данни в рамките на конкретно проучване, не се смятат за получатели.

- „**Предоставяне на лични данни**“ са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.
- **„Регистър на лични данни**“ е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.
- „**Резервни копия за възстановяване**” са копия на данните, съхранявани на носител, чрез които може да се осъществи възстановяването.
- „**Специфични признаци**“ са признаци, свързани с физическа, физиологична, генетична, психическа, психологическа, икономическа, културна, социална или друга идентичност на лицето.
- „**Средно ниво на въздействие**” е неправомерното обработване на лични данни, което би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица.
- „**Съгласие на физическото лице**“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени
- „**Трето лице**“ е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.
- „**Физическа защита на лични данни“** е система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
- „**Цялостност**” е изискване, данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

§2. Всички служители на УД са длъжни срещу подпис да се запознаят с инструкцията и да я спазват.

§3. Настоящите вътрешни правила се приемат на основание решение на Съвета на Директорите на УД от 25.05.2018г. и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Регламент за защита на личните данни), чл. 23, ал. 4 от Закона за защита на личните данни и Наредба № 1/30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни, издадена от Комисията за защита на личните данни.

§4. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и действащото приложимо законодателство на Р. България.