I. Въведение

1. Общ регламент за защита на личните данни

Регламент (ЕС) 2016/679 (Общ регламент за защита на данните) замества Директивата 95/46 / ЕО за защита на данните. Има пряко действие и предполага изменение в законодателството на страните -членки в областта на защитата на личните данни. Неговата цел е да защитава "правата и свободите" на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработва с тяхно съгласие.

2. Обхват очертан от Общия регламент за защита на данните

Материален обхват (член 2) – Общият регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (например ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват (член 3) – правилата на Общия Регламент ще важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Ще се прилага и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

Принципът, е че правилата на ОРЗД „следват“ личните данни на субектите на данни, които се намират в Европейския съюз.

3. Понятия

„Лични данни" - 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, както и всяка друга информация, която се определя от приложимото право като лични данни;

„Специални (чувствителни) категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация , както и всички други лични данни, които се определят от приложимото право като специални.

„Обработване" - 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;

„Администратор" - всяко 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; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

„Субект на данните“ – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора.

„Съгласие на субекта на данните" - 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;

„Дете“ – Общият Регламент определя дете като всеки на възраст под 16 години въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

„Профилиране" - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

„Нарушение на сигурността на лични данни" - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

„Основно място на установяване “ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването.

Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи. (Член 4 т.16) от ОРЗД)

„Получател" - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи

отговаря на приложимите правила за защита на данните съобразно целите на обработването;

„Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

Виж чл. 4 от ОРЗД, където са дадени определенията за всяко от горните.

II. Декларация относно политиката по защита на личните данни

1. Ръководството на МБАЛ „Света София“ се ангажират да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на "правата и свободите" на лицата, чиито лични данни МБАЛ „Света София“ събира и обработва съгласно Общия регламент за защита на данните (Регламент (ЕС) 2016/679).

Администраторът се задължава да осигури съответствието на всички дейности, които извършва, по събиране и обработване на лични данни, съгласно изискванията на ОРЗД.

2. В съответствие с Общия регламент към тази политика са описани и други релевантни документи, както и свързани процеси и процедури.

3. Настоящата политика се отнася до всички дейности по обработването на лични данни, включително тези, които се извършват относно лични данни на клиенти, служители, доставчици и партньори и всякакви други лични данни, които организацията на МБАЛ „Света София“ обработва от различни източници.

4. Администраторът води Регистър на дейностите по обработване. В случаите, когато воденето на регистъра е възложено на Длъжностното лице по защита на данните/отговорника по защита на личните данни, то отговаря за въвеждането в този регистър на всякакви промени в дейностите на МБАЛ „Света София“, както и на всички други допълнителни изисквания, в т.ч. оценки на въздействието върху защитата на данните. Този регистър трябва да бъде на разположение по искане на надзорния орган.

5. Тази политика се прилага за всички служители/работници (и заинтересовани страни) на МБАЛ „Света София“, както и за обработващите и членовете на техния персонал. Всяко нарушение на Общия регламент ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай, че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане в най-къс възможен срок на съответните държавни органи за ангажиране на наказателна отговорност.

6. Трети страни, които работят с или за МБАЛ „Света София“, в т.ч. партньори, външни доставчици, клиенти и др., както и които имат или могат да имат достъп до личните данни на администратора, са длъжни да се запознаят и съобразят с тази политика. Администраторът е длъжен да сключи споразумение за поверителност на данните с всяка трета страна, на която предоставя достъп до личните данни, обработвани от него, което дава право на МБАЛ „Света София“ да извършва проверки на спазването на наложените със споразумението задължения, освен ако обработването не се изисква от правото на ЕС или от правото на държава-членка..

III. Задължения и отговорности по Регламент (ЕС) 2016/679

1. МБАЛ „Света София“ е администратор на данни съгласно Регламент (ЕС) 2016/679 и носи цялата отговорност и рисковете от евентуално несъответствие с изискванията на ОРЗД, включително е отговорен за разработване и насърчаване на добри практики в областта на обработване на личните данни в МБАЛ „Света София“.

2. Обработващ лични данни е всяко лице извън организацията на администратора, което обработва пряко личните данни от името на администратора - съхранява, дигитализира, каталогизира и т.н. цялата информация.;

3. Длъжностното лице по защита на данните, респ. лицето, което по длъжностна характеристика или по възлагане, изпълнява задачи, свързани със защита на личните данни (отговорно лице/отговорник по защита на данните), взема участие на заседанията на ръководството на администратора, на които се обсъждат въпроси от областта на защита на личните данни, и съветва администратора за доказване на съответствието със законодателството в областта на защита на данните и добрите практики.

(Примерна длъжностна характеристика на ДЛЗД (GDPR_FORM_03) и (Примерна длъжностна характеристика на Отговорник по защита на данните (GDPR_FORM_03A).

Длъжностно лице по защита на данните (ДЛЗД) - ролята на длъжностното лице по защита на данните, кога неговото назначаване е задължително и какви са изискванията към него са подробно описани в чл. 37-39 от ОРЗД.

Отговорник по защита на данните - в случаите, когато не е задължително да се назначи ДЛЗД, работната група по чл. 29 казва следното: „Нищо не пречи на организация, която не е задължена по закон да определя ДЛЗД и не желае да определя ДЛЗД на доброволна база, все пак да наеме персонал или външни консултанти, които да изпълняват задачи, свързани със защитата на личните данни. В този случай е важно да се гарантира, че няма да има объркване по отношение на званието, статута, длъжността и задачите. Поради това във всички съобщения в рамките на дружеството, както и с органите за защита на данните, субектите на данни и обществеността като цяло, трябва да се пояснява, че длъжността на въпросното физическо лице или консултант не е длъжностно лице по защита на данните (ДЛЗД).“ (Виж: Насоки за длъжностните лица по защита на данните, Раздел 2.1.) Наименованието на тази длъжност сме нарекли за удобство „Отговорник“, но може да бъде заменено с друго, което Администратора смята за подходящо.

Тази отчетност на ДЛЗД включва:

- разработване и внедряване на изискванията на РЕГЛАМЕНТ (ЕС) 2016/679 както се изисква от настоящата политика;
- управление на сигурността и риска по отношение на съответствието с политиката.

4. Длъжностното лице по защита на данните, което следва да бъде подходящо, квалифицирано и опитно, се избира от ръководния орган на администратора (в зависимост от неговата структура и правно-организационна форма). ДЛЗД е длъжно да съветва и информира администратора за прилагането на ОРЗД и други актове от вътрешното и европейското законодателство в областта на защита на личните данни, съобразно задълженията си по договор и съгласно изискванията на ОРЗД, включително да следи за прилагането на тази политика.

5. ДЛЗД има и специфични задължения по ОРЗД – до него се отправят всички искания на субектите на данни (виж „Процедура за управление на исканията от субектите“ (GDPR_PROC_02) и е контактна точка за служителите на администратора, които искат

разяснения по всеки аспект на спазването на защитата на данните. ДЛЗД е лицето за контакт и пред надзорния орган.

6. Спазването на законодателството за защита на данните е отговорност на всички служители на МБАЛ „Света София“, които обработват лични данни, в зависимост от задълженията им длъжностните характеристики.

7. Политиката за обучение на МБАЛ „Света София“ (Политика за провеждане на обучение (GDPR_POL_02)) определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на служителите/работници на МБАЛ „Света София“.

IV. Принципи за защита на данните

Цялото обработване на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите на МБАЛ „Света София“ имат за цел да гарантират спазването на тези принципи.

1. Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно.

Законосъобразно – да идентифицира законна основа, преди да обработва лични данни. Това са т. нар "основания за обработване", например „съгласие“. Съгласието на субекта е едно от основанията за обработване на личните данни. Такова може да бъде също изпълнение на договор или законен интерес на администратора, в които случаи съгласие не е нужно да бъда давано.

Добросъвестно - за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субектите на данни, необходима във всеки конкретен случай и за всяка конкретна цел, по разбираем, кратък и достъпен за субекта на данни начин. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

Прозрачно – Регламент (ЕС) 2016/679 поставя изисквания относно това, каква информация трябва да бъде предоставена на разположение на субектите на данни, която е обхваната от принципа за "прозрачност", регламентиран в членове 12, 13 и 14 от ОРЗД. Съгласно цитираните разпоредби на ОРЗД, информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език, т.е. декларациите за поверителност, които се подписват от субектите на данни, трябва да бъдат подробни и конкретни, разбираеми и достъпни.

Правилата за уведомяване на субекта на данни от МБАЛ „Света София“ са определени в Процедура за прозрачност при обработката на лични данни (GDPR_PROC_02) и уведомлението се записва в Образец на Декларация за поверителност (уведомление за поверително третиране на личните данни) (GDPR_FORM_01).

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;
- контактите на ДЛЗД (когато има определено);

- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни могат да се събират само за конкретни, изрично указани и законни цели.

Данните, получени за конкретни цели, следва да се събират и обработват само за тези цели, които съответстват на дейностите по обработване, включени в Регистъра на дейностите по обработване на данни (чл. 30 ОРЗД) на МБАЛ „Света София“.

Процедура за прозрачност при обработката на лични данни (GDPR_PROC_02) определя съответните правила.

3. Личните данни, които администраторът събира, трябва да бъдат ограничени до това, което е необходимо за съответната цел на обработване *(принцип на минимизиране на данните, които могат да бъдат обработвани за конкретния субект)*

- ДЛЗД/Отговорникът по защита на данните следи за събиране само на тази информация, която е строго необходимо за целта на обработване.
- Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват декларация за добросъвестно обработване или връзка Уведомление за поверително третиране на личните данни (Декларация за поверителност) (GDPR_FORM_01) и да бъдат одобрени от ДЛЗД.
- Длъжностното лице по защита на данните / отговорникът по защита на данните има задължения за извършването на периодични проверки (посочете периодичност, но поне веднъж годишно), които да гарантират, че събраните данни продължават да бъдат адекватни, релевантни и не са прекомерни (Процедура за оценка на въздействието върху защитата на данните (GDPR_PROC_09) и използваната от вас методология за оценка на въздействието).

4. Личните данни трябва да бъдат точни и актуални във всеки един момент, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

- Данните, които се съхраняват от администратора на данни, трябва да бъдат

преглеждани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.

- Длъжностното лице за защита на данните / отговорникът по защита на данните трябва да гарантира, че целият персонал е обучен в значението на събирането на точни данни и поддържането им.

- Също така, задължение на субекта на данните е да декларира, че данните, които предават за съхраняване от МБАЛ „Света София“ са точни и актуални. Попълването на формуляр от субекта на данни, предназначени за администратора, ще включва изявление, че съдържащите се в него данни са точни към датата на подаване.

- От служителите / работниците (клиентите / други) трябва да се изисква, да уведомяват МБАЛ „Света София“ за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Инструкции и правила за актуализиране на записите се съдържат (тук)[1]. Отговорността на МБАЛ „Света София“ е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.

- Длъжностното лице по защита на данните / отговорникът по защита на данните гарантира, че са налице подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени, други относими фактори.

- Най-малко веднъж годишно Длъжностното лице по защита на данните / отговорникът по защита на данните ще прегледа сроковете на съхранение на всички лични данни, обработвани от МБАЛ „Света София“, като се позовава на инвентаризацията на данните и ще идентифицира всички данни, които вече не се изискват в контекста на посочената цел. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.

- Длъжностното лице по защита на данните / отговорникът по защита на данните следи за отговаряне на искания за корекция на данни в рамките на един месец (Процедура за управление на исканията от субектите (GDPR_PROC_03). Този срок може да бъде удължен с още два месеца за сложни заявки. Ако МБАЛ „Света София“ реши да не се съобрази с искането, Длъжностното лице по защита на данните / Отговорникът по защита на данните трябва да отговори на субекта на данните, за да обясни мотивите за отказа и да го информира за правото му да подаде жалба пред надзорния орган, и да потърси правна защита.

- Длъжностното лице за защита на данните/Отговорникът по защита на данните следва да информира всички трети страни, на които са предоставени неточни или остарели лични данни, че информацията е неточна или остаряла и да не се използва за вземане на решения относно субектите на данни, както и да препраща всяка корекция на лични данни към третите страни, където това е необходимо.

5. Личните данни трябва да се съхраняват в такава форма, която позволява субектът на данните да бъде идентифициран за периода, необходим за обработването.

- Когато личните данни се запазват след срока на обработването, те ще бъдат съхранявани по подходящ начин (минимизирани, криптирани, псевдонимизирани), за

[1] В случай, че са изработени такива правила, могат да бъдат посочени тук.

да се защити самоличността на субекта на данните в случай на нарушение на данните.

- Лични данни ще бъдат пазени в съответствие с Процедура за съхраняване и унищожаване на данните (GDPR_PROC_07) и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени по указания в тази процедура ред.

- Длъжностното лице за защита на данните / Отговорникът по защита на данните специално трябва да одобри всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в Процедура за съхраняване и унищожаване на данните (GDPR_PROC_07) и трябва да гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде писмено.

6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност (чл. 24, чл. 32 от ОРЗД)

Длъжностното лице за защита на данните / Отговорникът по защита на данните ще извърши първоначална оценка на въздействието[2], когато такава се налага, като вземе предвид всички обстоятелства, свързани с операциите по обработване на данни от МБАЛ „Света София“.

Във всеки конкретен случай, когато има нарушение на защитата на лични данни, ДЛЗД/отговорникът/съответното отговорно лице в предприятието на администратора следва да извърши оценка на риска и при отчитане на висок риск да уведоми надзорния орган и/или субекта на данни. При съобразяване на риска в конкретния случай, Длъжностното лице по защита на данните трябва да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физическите лица (напр. персонал или клиенти), ако възникне нарушение на сигурността, всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите и др.

Гарантирането на сигурността на личните данни е свързана и с предприемането на подходящи технически мерки, за които длъжностното лице по защита на данните следи и които могат да включват най-малкото:

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Премахване на права на достъп за USB и други преносими носители с памет (може да има изключение при осигурени задължителна проверка за вируси и регистриране на трансфера на данни);
- Антивирусен софтуер и защитни стени;
- Правата за достъп основани на роли, включително тези, на назначен временно персонал
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;

[2] Препоръчително е в документите относно използваната от Вас методология за оценка на въздействието да посочите този пункт от политиката Ви.

- Сигурност на локални и широкообхватни мрежи;
- Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;
- Идентифициране на подходящи международни стандарти за сигурност подходящи за МБАЛ „Света София“.

При оценяването на подходящите организационни мерки Длъжностното лице за защита на данните ще вземе предвид следното:

- Нивата на подходящо обучение в МБАЛ „Света София“;
- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;
- Приемането на политика на „чисто работно място“[3];
- Съхраняване на хартия на базата данни в заключващи се стенни шкафове;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Ограничаване на използването от служителите на лични устройства на работното място;
- Приемане на ясни правила за създаване и ползване на пароли;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса;
- Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

При преценката за подходящи мерки се вземат предвид идентифицираните рискове за лични данни, както и възможността за нанасяне на вреди на лицата, чиито данни се обработват.

7. Спазване на принципа на отчетност.

Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в чл. 5, пар. 2 изисква от администратора да докаже, че спазва останалите принципите в ОРЗД и изрично заявява, че това е негова отговорност.

[3] При напускане на работното място, цялата работна документация е премахната или прибрана в подходящи за това и с ограничен достъп места - специални шкафове, заключени помещения, унищожаване на вече ненужни документи и т.н.

МБАЛ „Света София“ ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като се присъединява към кодекси за поведение, внедрява подходящи технически и организационни мерки, както и чрез приемане на техники по защита на данните на етапа на проектирането и защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

V. Права на субектите на данни

1. Съгласно ОРЗД субектът на данни има следните права по отношение на обработването на личните му данни:

- Да получи информация за личните данни, свързани с него, които се обработват от администратора, и за целта, за която се обработват, включително да получи достъп до данните, както и информация кои са получателите на тези данни и третите страни, на които данните се предават;
- Да поиска копие от своите лични данни от администратора;
- Да иска от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;
- Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");
- Да иска от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани.;
- Да направи възражение срещу обработване на негови лични данни;
- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг.
- Да се обърне с жалба до надзорен орган, ако смята, че някоя от разпоредбите на ОРЗД е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;
- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

2. МБАЛ „Света София“ осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

- Субектите на данни могат да направят искания за достъп до данни, както е описано в процедурата за Процедура за управление на исканията от субектите (GDPR_PROC_03); тази процедура също така описва как МБАЛ „Света София“ ще гарантира, че отговора на искането на субекта на данни отговаря на изискванията на Общия регламент.

- Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, МБАЛ „Света София“ може или да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията, комуникацията или предприемането на исканите действия, или да откаже да предприеме действия по искането.

- Субектите на данни имат право да подават възражения до МБАЛ „Света София“, свързани с обработването на личните им данни. Обработването на искане от субекта на данни и подаването на възражения от страна на субекта на данни, се извършва в съответствие с Процедура за начините на комуникация при жалби и искания от субекта на данни (GDPR_PROC_04). Жалбите могат да се подават направо до надзорния орган, като компетентният за това орган в България е Комисия за защита на личните данни, адрес: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2 (www.cpdp.bg).

VI. Съгласие

1. Под „съгласие“ МБАЛ „Света София“ ще разбира 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. Субектът на данните може да оттегли своето съгласие по всяко време. Съгласие на субекта на лични данни се изисква винаги, когато не съществува алтернативно правно основание за обработването.

2. МБАЛ „Света София“ разбира под "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

3. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие[4] за дейностите по обработване.

4. За специални категории данни трябва да се получи изрично писмено съгласие Процедура по получаване на съгласие за обработване на лични данни (GDPR_PROC_06) на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

5. Съгласието на субекта за обработване на лични или специални категории данни се дава - въз основа на съответния документ за съгласие, предоставен от субекта на данни на администратора за всяка конкретна цел на обработване. Когато субектът подписва договор, съгласие не е необходимо, защото данните му се събират на друго законово основание.

6. Когато МБАЛ „Света София“ обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това

[4] Администраторът трябва да реши как иска да направи това. Възможно е чрез формуляр, който трябва да бъде подписан. Възможно е също така с известие за поверителност, което трябва да бъде изрично прието от някого, преди да се обработва информацията или пък по някакъв друг способ. Каквото и да е решението, трябва да бъде посочено тук.

изискване се прилага за деца на възраст под 16 години (освен ако държавата-членка не е предвидила по-ниска възрастова граница, която не може да бъде по-ниска от 13 години).

VII. Сигурност на данните

1. Служителите на администратора, които съгласно длъжностните си характеристики имат задължение да обработват определени лични данни от името на администратора са длъжни да осигурят сигурността при обработването и съхраняването на данните от тяхна страна, включително да гарантират, че няма да разкриват данните на трети страни, освен ако МБАЛ „Света София“ не е дал такива права на тази трета страна за достъп до данните (например, въз основа на договор/клауза за поверителност (посочете тук ако имате разработени такива).

2. Личните данни или част от тях трябва да бъдат достъпни само за тези, които имат задължение да ги обработват/ съхраняват, като достъпът[5] може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа. Всички лични данни трябва да се съхраняват например:

- в самостоятелна стая с контролиран достъп; и/или в заключен шкаф или в картотека; и/или
- ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация (например правила за контрол на достъпа) ; и / или
- съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

3. Да се създаде организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители / работници на МБАЛ „Света София“. От всички служители / работници се изисква да бъдат обучени и да приемат съответните договорни клаузи / декларация за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

4. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа по поддръжката на клиенти, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол[6].

5. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедура за съхраняване и унищожаване на данните (GDPR_PROC_07). Записите на хартиен носител, за които е изтекъл срокът за съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила/процедури[7].

6. Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

VIII. Разкриване на данни

1. МБАЛ „Света София“ трябва да осигури условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители/работници трябва да бъдат предпазливи, когато се поиска от тях да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от организацията.

Необходимо е на служителите да се извърши специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат координирани с Длъжностното лице за защита на данните / Отговорникът за защита на данните, което да даде становище.

3. Личните данни ще се предоставят на компетентните публични власти при и по повод упражняване на техните властнически правомощия.

IX. Съхраняване и унищожаване на данните

1. МБАЛ „Света София“ не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период, отколкото е необходимо, по отношение на целите, за които са били събрани данните.

2. МБАЛ „Света София“ може да съхранява данни за по-дълги периоди единствено, ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

3. Периодът на съхранение за всяка категория лични данни е посочен в процедурата за Процедура за съхраняване и унищожаване на данните (GDPR_PROC_07) както и на критериите, използвани за определяне на този период, включително всякакви законови задължения, изискващи от МБАЛ „Света София“ да запази данните.

4. Процедура за съхраняване и унищожаване на данните (GDPR_PROC_07), както и (ако сте изработили) правилата за унищожаване на информацията върху неизползвани записващи носители МБАЛ „Света София“ ще се прилагат във всички случаи.

5. Личните данни трябва да бъдат унищожени, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар. 1 б. е) от Общия регламент) – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

X. Трансфер на данни

1. Всеки трансфер на данни от ЕС към страни извън ЕС (посочени в Общия регламент като "трети страни") са незаконни, освен ако няма подходящо "ниво на защита на основните права на субектите на данни.

Прехвърлянето на лични данни извън ЕС е забранено, освен ако не се прилагат една или повече от указаните гаранции или изключения:

Тук трябва да се вземе предвид и съществуването на Европейско икономическо пространство. (ЕИП), което е с по-широк обхват от ЕС, и включва още страни, които не са членки на ЕС (Лихтенщайн, Норвегия и Исландия). Тези страни обаче прилагат регламенти на ЕС чрез решение на Съвместния комитет, както и в случая с Общия регламент.

2. Решение за адекватност

Европейската комисия може да оцени трети страни, територия и/или специфични сектори в трети страни, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица. В тези случаи не се изисква разрешение.

Държавите, които са членки на Европейското икономическо пространство (ЕИП), но не и на ЕС, се приемат като отговарящи на условията за решение за адекватност.

Чл. 45 пар. 8 от ОРЗД - Комисията публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита. Повече за политиката на адекватност при трансфера на лични данни:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

3. Прехвърляне на личните данни между ЕС и САЩ (EU-U.S. Privacy Shield)

Ако Организацията желае да прехвърли лични данни от ЕС на трета страна в САЩ, тя трябва да провери дали организацията е подписала Рамковото споразумение „Privacy Shield“ с Министерство на търговията на САЩ.

Американското министерство на търговията отговаря за управлението и администрирането на Privacy Shield и гарантира, че компаниите изпълняват своите ангажименти. За да могат да се сертифицират пред министерството, фирмите трябва да имат политика за защита на личните данни в съответствие с принципите на ОРЗД, напр. използват, съхраняват и прехвърлят личните данни в съответствие набор от строги правила и предпазни мерки за защита на данните.

4. Задължителни фирмени правила

МБАЛ „Света София“ може да приеме одобрени задължителни корпоративни правила за прехвърляне на данни извън ЕС. Това изисква одобрението им от съответния надзорен орган.

5. Стандартни договорни клаузи

МБАЛ „Света София“ може да приеме утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство. Ако МБАЛ „Света София“ приема стандартни договорни клаузи, одобрени от съответния

надзорен орган, това има автоматично признаване на адекватността за защита[8].

6. Изключения

При липса на решение за адекватност, членство в US Privacy Shield, задължителни фирмени правила и / или договорни клаузи, прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:

- субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;
- предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
- предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
- предаването е необходимо поради важни причини от обществен интерес;
- предаването е необходимо за установяването, упражняването или защитата на правни претенции;
- предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
- предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

XI. Регистър на обработванията на данни (инвентаризация на данните)

1. МБАЛ „Света София“ е създал процес на инвентаризация на данните като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламент (ЕС) 2016/679. При инвентаризацията на данните в МБАЛ „Света София“ и в работния поток от данни се установяват:

- бизнес процесите, които използват лични данни;
- източниците на лични данни;
- броя на субектите на данни;
- описание на категориите лични данни и елементите на във всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;

[8] При положение, че използвате такива клаузи, посочете ги тук като връзка към документ.

- правното основание за обработването;
- получателите или категориите получатели на личните данни;
- основните системи и места за съхранение;
- всички лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

Виж Процедура по приемане на план за технически и организационни мерки (GDPR_PROC_10).

2. МБАЛ „Света София“ е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. МБАЛ „Света София“ оценява нивото на риска за лицата, свързани с обработването на личните им данни. Когато е задължително се извършват оценки на въздействието върху защитата на данните във връзка с обработването на лични данни от МБАЛ „Света София“ и във връзка с обработването, предприето от други организации от името на МБАЛ „Света София“. (Процедура за оценка на въздействието върху защитата на данните (GDPR_PROC_09) и използваната от вас Методология за оценка на въздействието).

4. МБАЛ „Света София“ управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с правилата, заложени при изготвяне на оценката.

Когато вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване МБАЛ „Света София“ следва да извърши оценка на въздействието на предвидените операции по обработване върху защитата на личните данни. Една обща оценка на въздействието може да разглежда набор от подобни операции по обработване, които представляват подобни високи рискове.

5. Когато в резултат на Оценката на въздействието е ясно, че МБАЛ „Света София“ ще започне да обработва лични данни, които поради висок риск биха могли да причинят вреди на субектите на данни, решението дали обработването да продължи или не, трябва да бъде предадено за преглед от страна на Длъжностното лице за защита на данните / отговорника по защита на личните данни.

6. Ако ДЛЗД / отговорника по защита на личните данни има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да отнесе въпроса пред надзорния орган.

7 .Длъжностното лице по защита на данните, прави периодичен (ежегоден)[9] преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в „Регистъра на дейностите по обработване“ в светлината на всякакви промени в дейностите на МБАЛ „Света София“.

[9] Възможен е и по-кратък срок ако се прецени, че е необходимо.