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 обработват 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, и 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 социалната 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, членство в синдикални организации, обработка на генетични данни, биометрични данни за уникално идентифициране на физическо лице, данни, отнасящи се до здравето, или данни относно сексуалния живот 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, извършвани 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 всяко лице под 16 години, въпреки че това може да бъде намалено на 13 от правото на държавата-членка. Обработката на лични данни на дете е законна само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия да провери, че лицето, притежаващо родителска отговорност за детето, е дало или е упълномощено да даде съгласие.
- **„Профилиране"** - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценка на определени лични аспекти, свързани с физическо лице, включително за анализ или прогнозиране на аспекти като професионалните задължения, 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 целите и средствата на своите дейности по обработване на данни. Ако обработващият лични данни няма централно управление в ЕС, мястото на установяване ще бъде там, където се осъществяват основните дейности по обработването.
- **„Получател"** - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Публичните органи, които получават лични данни в рамките на разследване, не се считат за „получатели", а обработването на тези данни трябва да отговаря на приложимите правила за защита на данните.
- **„Трета страна“** – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора или обработващия лични данни, които имат право да обработват личните данни под прякото ръководство на администратора или обработващия лични данни.

II. Декларация относно политиката по защита на личните данни

1. Ръководството на **Кабинет „Д-р Светослав Димитров“** се ангажира 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 **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“**, както и на всички други допълнителни изисквания, включително 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 **Кабинет „Д-р Светослав Димитров“**, 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 **Кабинет „Д-р Светослав Димитров“**, включително 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 **Кабинет „Д-р Светослав Димитров“** 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. **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“**.
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, респективно 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 **Кабинет „Д-р Светослав Димитров“**, които обработват лични данни, в зависимост от техните длъжностни характеристики.
7. Политиката за обучение на **Кабинет „Д-р Светослав Димитров“** (Политика за провеждане на обучение (GDPR_POL_02)) определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на служителите/работниците на **Кабинет „Д-р Светослав Димитров“**.

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 **Кабинет „Д-р Светослав Димитров“** имат за цел да гарантират спазването на тези принципи.

1. **Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно.**
    - **Законосъобразно** – да се идентифицира законна основа, преди да се обработват лични данни. Това са т.нар. "основания за обработване", например „съгласие“. Съгласието на субекта е едно от основанията за обработване на лични данни. Такова може да бъде също изпълнение на договор или законен интерес на администратора, в които случаи съгласие не е нужно.

- **Добросъвестно** – администраторът на данни трябва да предостави определена информация на субектите на данни, необходима за всяка конкретна цел, по разбираем, кратък и достъпен начин.
- **Прозрачно** – информацията трябва да бъде съобщена на субекта на данните в разбираема форма, с ясен и разбираем език. Декларациите за поверителност, подписвани от субектите на данни, трябва да бъдат подробни, конкретни и достъпни.

Правилата за уведомяване на субекта на данни от **Кабинет „Д-р Светослав Димитров“** 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).

2. **Лични данни могат да се събират само за конкретни, изрично указани и законни цели.**
   Данните, събрани за конкретни цели, следва да се обработват само за тези цели, които съответстват на дейностите по обработване, включени в Регистъра на дейностите по обработване на данни (чл. 30 ОРЗД) на **Кабинет „Д-р Светослав Димитров“**. 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):
   - ДЛЗД/Отговорникът по защита на данните следи да се събира само тази информация, която е строго необходима за целта на обработване.
   - Всички формуляри за събиране на данни трябва да включват декларация за добросъвестно обработване и да бъдат одобрени от ДЛЗД.
   - Длъжностното лице по защита на данните трябва да извършва периодични проверки, за да гарантира, че събраните данни продължават да бъдат адекватни, релевантни и не са прекомерни.
4. **Личните данни трябва да бъдат точни и актуални във всеки един момент**, и да са положени необходими усилия, за да е възможно незабавно изтриване или коригиране.
   - Данните, които се съхраняват от администратора, трябва да бъдат преглеждани и актуализирани при необходимост.
   - Субектите на данни трябва да декларират, че предаваните данни са точни и актуални.
   - Служителите на **Кабинет „Д-р Светослав Димитров“** трябва да уведомяват кабинета за всякакви промени в обстоятелствата, за да могат да се актуализират записите.
5. **Личните данни трябва да се съхраняват в такава форма, която позволява идентификация на субекта за периода, необходим за обработването.**
   - Когато личните данни се запазват след срока на обработването, те ще бъдат съхранявани по подходящ начин, за да се защити самоличността на субекта на данните.
   - Данните ще се съхраняват в съответствие с Процедурата за съхраняване и унищожаване на данни и след изтичане на срока им на съхранение, те ще бъдат надеждно унищожени.
6. **Личните данни трябва да бъдат обработвани по начин, който гарантира подходяща сигурност** (чл. 24, чл. 32 от ОРЗД).
   - Длъжностното лице по защита на данните ще извърши първоначална оценка на въздействието и ще следи за предприемането на подходящи технически мерки

за защита, включително защита с парола, автоматично заключване на работни станции, антивирусен софтуер, псевдонимизиране и др.

7. **Спазване на принципа на отчетност.**
   Кабинет „Д-р Светослав Димитров“ ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, внедряване на подходящи технически и организационни мерки, както и чрез оценка на въздействието върху защитата на личните данни.

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 или вече не са 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** 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. **Кабинет „Д-р Светослав Димитров“** 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 управление на исканията от субектите (GDPR_PROC_03); тази процедура също така описва как **Кабинет „Д-р Светослав Димитров“** ще гарантира, че отговорът 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, **Кабинет „Д-р Светослав Димитров“** 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 Кабинет „Д-р Светослав Димитров“**, свързани с обработването на личните им данни. Обработването на искане от субекта на данни и подаването на възражения се извършва в съответствие с Процедурата 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“ No 2.

VI. Съгласие

1. Под „съгласие“ **Кабинет „Д-р Светослав Димитров“** 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. **Кабинет „Д-р Светослав Димитров“** 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 него 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 за дейностите по обработване.
4. За специални категории данни трябва да се получи изрично писмено съгласие, съгласно 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 **Кабинет „Д-р Светослав Димитров“** обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т.н.). Това 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 **Кабинет „Д-р Светослав Димитров“** не е дал такива права на тази трета страна за достъп до данните (например, въз основа на договор/клауза за

поверителност).

2. Личните данни или част от тях трябва да бъдат достъпни само за тези, които имат задължение да ги обработват/съхраняват, като достъпът 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 са компютъризирани, защитени с парола в съответствие с вътрешните изисквания, посочени в организационните и технически мерки за контролиране на достъпа до информация; 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 **Кабинет „Д-р Светослав Димитров“**. 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.
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.
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.

Ако има нужда от още корекции или допълнителна информация, не се колебайте да ме информирате!

VIII. Разкриване на данни

1. **Кабинет „Д-р Светослав Димитров“** 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. **Кабинет „Д-р Светослав Димитров“** 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. **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“** ще се прилагат във всички случаи.
5. Личните данни трябва да бъдат унищожени, съгласно принципа за гарантиране на 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") е незаконен, 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 можете да намерите тук.

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

Ако **Кабинет „Д-р Светослав Димитров“** желае да прехвърли лични данни от ЕС на трета страна в САЩ, трябва да провери дали организацията е подписала Рамковото споразумение „Privacy Shield“ с Министерството на търговията на САЩ. Американското министерство на търговията отговаря за управлението и администрирането на Privacy Shield и гарантира, че компаниите изпълняват своите ангажименти.

4. **Задължителни фирмени правила**

Кабинет „Д-р Светослав Димитров“ 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**

Кабинет „Д-р Светослав Димитров“ може да приеме утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство. Ако **Кабинет „Д-р Светослав Димитров“** приема стандартни договорни клаузи, одобрени от съответния надзорен орган, това има автоматично признаване на адекватността за защита.

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. **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“** 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 във всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;
- 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. **Кабинет „Д-р Светослав Димитров“** е наясно с рисковете, свързани с обработването на определени видове лични данни.
3. **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“** и във връзка с обработването, предприето от други организации от името на **Кабинет „Д-р Светослав Димитров“**. (Процедура за оценка на въздействието върху защитата на данните (GDPR_PROC_09) и използваната от вас Методология за оценка на въздействието).
4. **Кабинет „Д-р Светослав Димитров“** 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, **Кабинет „Д-р Светослав Димитров“** 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 **Кабинет „Д-р Светослав Димитров“** 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 / отговорникът по защита на личните данни има сериозни опасения относно потенциалната вреда или опасност, или относно количеството на съответните данни, той следва да отнесе въпроса пред надзорния орган.
7. Длъжностното лице по защита на данните прави периодичен (ежегоден) преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в „Регистъра на дейностите по обработване“ в светлината на всякакви промени в дейностите на **Кабинет „Д-р Светослав Димитров“**.