GDPR	ПОЛИТИКА ЗА ПРАВОТО НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ И ЛИЧНИТЕ ДАННИ
Администратор: „УНИБИОМЕД” ООД	ДЛЗД/Отговорник: Управител

(1) ПОЛИТИКА ЗА ПОВЕРИТЕЛНОСТ

В ежедневните си бизнес операции „УниБиомед” ООД използва различни данни за идентифицирани лица, включително данни за:

- Настоящи, минали и бъдещи служители
- Клиенти

При събиране и използване на тези данни организацията е обект на различни законодателни актове, които контролират начина, по който тези дейности могат да се извършват и предпазните мерки, които трябва да бъдат въведени за тяхната защита.

Целта на тази политика е да определи съответното законодателство и да опише стъпките, които „УниБиомед” ООД предприема, за да гарантира, че организацията е в съответствие с него.

Този контрол се прилага за всички системи, хора и процеси, които съставляват информационните системи на организацията, включително служители, доставчици, клиенти и други трети страни, които имат достъп до системите на „УниБиомед” ООД.

Следните правила и процедури са свързани с този документ:

- Процес на оценка на въздействието върху защитата на данни
- Процедура за картотекиране и описване на потока на личните данни
- Процедура за оценка на законен интерес
- Процедура за реагиране при инциденти със сигурността на информацията
- GDPR Роли и отговорности
- Политика за запазване и защита на записите

Политика за правото на неприкосновеност на личния живот и личните данни

Общият регламент относно защитата на данни от 2016 (GDPR) е един от най-значимите законодателни актове, засягащи начина, по който „УниБиомед” ООД изпълнява дейностите по обработка на информацията. Значителни глоби се прилагат, ако се приеме, че е налице нарушение съгласно регулацията, предназначена да защитава личните данни на гражданите на Европейския съюз. Политиката на „УниБиомед” ООД е да гарантира своето съответствие с Регламент и с другите приложими законодателни актове и което да е ясно и доказуемо по всяко време чрез подходяща отчетност.

В рамките на GDPR са изброени голям обем определения и не е уместно те да бъдат възпроизведени тук. Въпреки това, най-фундаменталните определения по отношение на тази политика са следните:

„Лични данни“ са дефинирани като:

всяка информация, свързана с физическо лице, чрез която то може да бъде идентифицирано („субект на данни“) 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;

„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“ означава:

физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други, определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза 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;

Принципи, свързани с обработването на лични данни

Съществуват редица фундаментални принципи, на които се основава GDPR.

Те са както следва:

1. Личните данни са:

(а) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

(б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите“);

(в) подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

(г) точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);

(д) съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

(е) обработвани 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 („цялостност и поверителност“);

2. Администраторът носи отговорност и е в състояние да докаже спазването на параграф 1 („отчетност“).

„УниБиомед” ООД ще гарантира, че отговаря на всички тези принципи както при обработката, която извършва в момента, така и като част от въвеждането на нови методи за обработка, като например новите информационни системи.

Права на лицето

Субектът на данните също има права съгласно GDPR. Те се състоят от:

1. Правото да бъде информиран
2. Правото на достъп
3. Правото на коригиране
4. Правото за изтриване
5. Правото да се ограничи обработката
6. Правото на преносимост на данни
7. Право на възражение
8. Права във връзка с автоматизираното вземане на решения и профилиране

Всяко от тези права се подкрепя от подходящи процедури в рамките на „УниБиомед” ООД, които позволяват предприемането на необходимите действия в сроковете, посочени в GDPR.

Тези срокове са посочени в Таблица 1 - Срокове за искане на субекта на данни

Искане на субекта на данни	Срок
Правото да бъде информиран	В момента а събиране на данните (ако са предоставени от субекта на данни) или в рамките на един месец (ако не са предоставени от субекта на данни)
Правото на достъп	Един месец
Правото на коригиране	Един месец
Правото за изтриване	Без неоправдано забавяне
Правото да се ограничи обработката	Без неоправдано забавяне
Правото на преносимост на данни	Един месец
Право на възражение	При получаване на възражение
Права във връзка с автоматизираното вземане на решения и профилиране.	Неопределено

Съществуват шест алтернативни начина, по които законосъобразността на конкретен случай на обработка на лични данни може да бъде установена в рамките на GDPR. Политиката на „УниБиомед" ООД е да идентифицира подходящата база за обработка и да я документира в съответствие с регламента. Опциите са описани накратко в следващите раздели.

Съгласие

Освен ако не е необходимо поради причина, допустима в GDPR, „УниБиомед" ООД винаги ще получи изрично съгласие от субекта на данни да събира и обработва данните му. В случай на деца под 16-годишна възраст (по-ниска възраст може да бъде допустима в конкретни държави-членки на ЕС), ще бъде получено съгласието на родителите. Прозрачна информация за използването на личните данни ще бъде предоставена на субектите на данни в момента, в който се получи съгласието им и обяснени техните права по отношение на техните данни, като например правото да се оттегли съгласието. Тази информация ще бъде предоставена в достъпна форма, написана на ясен език и без такса.

Ако личните данни не се получават директно от субекта на данните, то тази информация ще бъде предоставена на субекта на данни в разумен срок след получаването на данните и определено в рамките на един месец.

Изпълнение на договор

Когато личните данни, събрани и обработени са необходими за изпълнение на договор със субекта на данните, не се изисква изрично съгласие. Това често се случва, когато договорът не може да бъде завършен без въпросните лични данни, напр. доставката не може да бъде извършена без адрес, на който да бъде доставена.

Правно задължение

Ако се изисква да се събират и обработват личните данни, за да се спази законът, не се изисква изрично съгласие. Това може да е случаят с някои данни, свързани например с трудовата заетост и данъчното облагане, и за много области, засегнати от публичния сектор.

Жизненоважни интереси на субекта на данни

В случаите, когато личните данни са необходими за защита на жизненоважните интереси на субекта на данните или на друго физическо лице, това може да се използва като законова основа на обработката. „УниБиомед” ООД ще запази разумни и документирани доказателства, че случаят е такъв, когато тази причина се използва като законова основа за обработката на лични данни. Като пример, това може да се използва в аспектите на социалните грижи, особено в обществения сектор.

Изпълнение на задача от обществен интерес

Когато „УниБиомед” ООД трябва да изпълни задача, която смята, че е в обществен интерес или като част от служебно задължение, тогава съгласието на субекта на данните няма да бъде поискано. Оценката на обществения интерес или на служебното задължение ще бъде документирана и предоставена като доказателство при необходимост.

Законни интереси

Ако обработването на конкретни лични данни е в законните интереси на „УниБиомед” ООД и се счита, че това не засяга съществено правата и свободите на субекта на данните, това може да се определи като законната причина за обработката. Отново, аргументите зад този възглед ще бъдат документирани.

Защита на правото на неприкосновеност на личния живот

„УниБиомед” ООД е приела принципа на неприкосновеност на личния живот по Темплейт и ще гарантира, че определянето и планирането на всички нови или значително променени системи, които събират или обработват лични данни, ще бъдат обект на надлежно отчитане на въпросите, свързани с поверителността, включително завършването на една или повече оценки на въздействието върху защитата на данните.

Оценката на въздействието върху защита на данните ще включва:

- Да се вземе предвид как ще се обработват личните данни и за какви цели
- Оценка дали предложената обработка на лични данни е необходима и пропорционална на целта (целите)
- Оценка на рисковете за физическите лица при обработката на личните данни
- Какви контролни механизми са необходими за справяне с установените рискове и за доказване на спазването на законодателството

Използването на техники като минимизиране на данните и псевдонимизиране ще се обсъжда, когато е приложимо и подходящо.

Договори, засягащи обработка на лични данни

„УниБиомед” ООД ще гарантира, че всички свързани с нея взаимоотношения, които включват обработката на лични данни, подлежат на документиран договор, който включва конкретната информация и условия, изисквани от GDPR.

Международни предавания на лични данни

Предавания на лични данни извън Европейския съюз ще бъдат внимателно прегледани преди извършването на трансфера, за да се гарантира, че те попадат в границите, наложени от GDPR. Това зависи отчасти от преценката на Европейската комисия относно адекватността на предпазните мерки за личните данни, приложими в приемащата страна, и това може да се промени с течение на времето.

Предаванията на лични данни извън Европейския съюз ще бъдат внимателно прегледани преди извършване на предаването, за да се гарантира, че те спадат към ограниченията, наложени от GDPR. Това зависи отчасти от преценката на Европейската комисия относно адекватността на предпазните мерки за личните данни, приложими в приемащата страна, и това може да се промени с течение на времето.

Международните прехвърляния на данни в рамките на група, ще бъдат предмет на правно обвързващи споразумения, наричани "Задължителни фирмени правила", които предоставят изпълними права на субектите на данни.

Длъжностно лице по защита на данни

Съгласно GDPR, ако дадена организация е публичен орган, ако извършва мащабен мониторинг или обработва особено чувствителни типове данни в голям мащаб, се изисква определена роля на Длъжностно лице по защита на данните (ДЛЗД). За ДЛЗД се изисква да притежава подходящо ниво на знания и може да бъде или вътрешен ресурс, или да се възложи на външен подходящ доставчик на услуги.

„УниБиомед" ООД в ролята си на АДМИНИСТРАТОР лични данни ще назначи Служител по защита на данните, ако техния брой надвиши 10000 записа.

Уведомление за нарушение

Политиката на „УниБиомед" ООД е справедлива и пропорционална, когато разглежда действията, които трябва да се предприемат, за да се информират засегнатите страни относно нарушения на лични данни. В съответствие с GDPR, когато е известно, че е налице нарушение, което може да доведе до риск за правата и свободите на физическите лица, съответният надзорен орган ще бъде информиран в рамките на 72 часа. Това ще бъде управлявано в съответствие с нашата Процедура за реагиране при инциденти със сигурността на информацията, която определя общия процес на работа с инциденти, свързани със сигурността на информацията.

Съгласно GDPR съответният орган по защита на данните има правомощието да налага глоби от до четири процента от годишния световен оборот или от двадесет милиона евро, което от двете е по-високо, за нарушения на регламентите.

Адресиране на съответствието с GDPR

Следните действия са предприети, за да се гарантира, че „УниБиомед" ООД отговаря по всяко време на принципа за отчетност на GDPR:

- Правната основа за обработването на лични данни е ясна и недвусмислена

- Служител по защита на данните е назначен със специална отговорност за защитата на данните в организацията (ако се изисква)
- Целият персонал, ангажиран с обработването на лични данни, разбира своите отговорности за спазването на добрите практики за защита на данните
- Обучението по защита на данните е предоставено на целия персонал
- Правилата за съгласие и уведомление се спазват
- Пътеките са на разположение на субектите на данни, които желаят да упражнят своите права по отношение на личните данни и тези запитвания се обработват ефективно
- Провеждат се редовни прегледи на процедурите, включващи лични данни
- Защита на правото на неприкосновеност на личния живот се приема за всички нови или променени системи и процеси
- Следната документация за обработващите дейности се записва:
    - Име на организацията и съответните детайли
    - Цел на обработката на лични данни
    - Категории лица и обработени лични данни
    - Категории получатели на лични данни
    - Споразумения и механизми за прехвърляне на лични данни към държави извън ЕС, включително подробности за въведените мерки за контрол
    - Графици за запазване на личните данни
    - Съществуващ технически и организационен контрол

Тези действия се преглеждат редовно като част от процеса на управление, свързан със защитата на данните.