МЕДИЦИНСКИ УНИВЕРСИТЕТ - СОФИЯ

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Версия 01 / 2018-05-08 г.

Утвърдил: .....

/ Проф. д-р Виктор Златков /

Съдържание

1. Предназначение, обхват и ползватели

МЕДИЦИНСКИ УНИВЕРСИТЕТ - СОФИЯ, наричана по-долу "Организацията" или “Дружеството”, се стреми да спазва приложимите закони и разпоредби, свързани със защитата на личните данни в държавите, в които Дружеството оперира. Тази политика определя основните принципи, чрез които организацията обработва личните данни на потребители, кандидат-студенти, студенти, докторанти, специализанти, доставчици, партньори, служители и други лица, и посочва отговорностите на отделите и служителите по време на обработката на лични данни.

Тази политика важи за МЕДИЦИНСКИ УНИВЕРСИТЕТ - СОФИЯ и неговите пряко или непряко контролирани изцяло притежавани дружества, които извършват дейност в рамките на Европейското Икономическо Пространство (ЕИП) или обработват личните данни на субекти на данни в ЕИП.

Потребителите на този документ са всички служители, постоянни или временни, и всички изпълнители, които работят от името на МЕДИЦИНСКИ УНИВЕРСИТЕТ - СОФИЯ.

2. Референтни Документи

- EU GDPR 2016/679 (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО)
- Закон за защита на личните данни
- НАРЕДБА № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни
- Политика за защита на личните данни на служителите
- Политика за съхранение на данни
- Описание на длъжността на служителя по защита на данните
- Насоки за опис на данните и обработка на данни
- Процедура за заявка за достъп до физически лица
- Насоки за оценка на въздействието на защитата на данните
- Процедура за Трансграничен трансфер на лични данни
- Политики за Информационна Сигурност
- Процедура за уведомяване за нарушение

3. Дефиниции

Следните определения на термините, използвани в този документ, са дефинирани в Общия регламент относно защита на данните на Европейския съюз:

„Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за

местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице

Чувствителни лични данни: Личните данни, които по своята същност са особено чувствителни по отношение на основните права и свободи, заслужават специфична защита, тъй като контекстът на тяхната обработка може да създаде значителни рискове за основните права и свободи. Тези лични данни включват лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикати, генетични данни, биометрични данни, с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни, отнасящи се до пола на физическо лице, живот или сексуална ориентация

Администратор на данни: 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

Обработващият данни: физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора

Обработване: 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

Псевдонимация: обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано

Трансгранично обработване: а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка

Надзорен орган: независим публичен орган, създаден от държава членка съгласно член 51 на Регламента

Водещ надзорен орган: надзорният орган, който носи основната отговорност за извършването на трансгранична дейност по обработка на данни. Например когато субект на данни подаде жалба относно обработката на личните му данни, органът е отговорен, наред с другото, за получаването на уведомления за нарушаване на данните, за уведомяване за рискова обработка и има пълна власт по отношение на задълженията си, за да гарантира спазването на разпоредбите на Регламента

Всеки "**местен надзорен орган**" ще продължи да поддържа на своя собствена територия и ще наблюдава всички местни обработки на данни, които засягат субектите на данни или които се извършват от администратор, или обработващ от ЕС, или извън ЕС, когато обработването им е насочено към субекти на данни, пребиваващи на нейна територия. Техните задачи и правомощия включват провеждане на разследвания и прилагане на административни мерки и глоби, насърчаване на обществената информираност за рисковете, правилата, сигурността и правата във връзка с обработката на лични данни, както и достъпа до помещенията на администратора и обработващия , включително оборудване и средства за обработка на данни

"Основно място на установяване" означава: а) по отношение на администратор, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, освен в случаите, когато решенията по отношение на целите и средствата за обработването на лични данни се вземат на друго място на установяване на администратора в Съюза и на това място на установяване има правомощия за прилагане на тези решения, в който случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване; б) по отношение на обработващ лични данни, установен в повече от една държава членка — 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 в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно Регламента

Групово предприятие: контролиращо предприятие и контролираните от него предприятия

4. Основни принципи, отнасящи се до обработката на лични данни

Принципите за защита на данните очертават основните отговорности за организациите, обработващи лични данни. В член 5, параграф 2 от EU GDPR се посочва, че *"администраторът е отговорен и е в състояние да докаже спазването на принципите."*

4.1. Законосъобразност, Честност и Прозрачност

Личните данни трябва да бъдат обработвани законосъобразно, справедливо и по прозрачен начин по отношение на субекта на данните.

4.2. Ограничение на Предназначението

Личните данни трябва да се събират за конкретни, изрични и законосъобразни цели и да не се обработват по начин, който е несъвместим с тези цели.

4.3. Минимизиране на Данните

Личните данни трябва да бъдат адекватни, уместни и ограничени до това, което е необходимо по отношение на целите, за които се обработват. Дружеството трябва да прилага анонимност или псевдонимация на личните данни, ако е възможно, за да намали рисковете за засегнатите субекти на данни.

4.4. Точност

Личните данни трябва да бъдат точни и, при необходимост, актуализирани; трябва да се предприемат разумни стъпки, за да се гарантира, че неточните лични данни, като се имат предвид целите, за които се обработват, се изтриват или коригират своевременно.

4.5. Ограничение на Сроковете за Съхранение

Личните данни трябва да се съхраняват не повече от времето, необходимо за целите, за които се обработват личните данни.

4.6. Почтеност и Поверителност

Вземайки предвид състоянието на технологиите и другите налични мерки за сигурност, разходите по внедряването, вероятността, и тежестта на рисковете, свързани с личните данни, Дружеството трябва да използва подходящи технически или организационни мерки за обработка на лични данни по начин, който гарантира подходяща сигурност на личните данни, включително защита срещу случайно или незаконно унищожаване, загуба, редуване, неразрешен достъп или разкриване.

4.7. Отговорност

Администраторите на данни трябва да отговарят и да могат да докажат съответствие с принципите, изложени по-горе.

5. Изграждане на Предпазване на Данните в Процесите

За да се докаже съответствие с принципите за защита на данните, Организацията трябва да изгради защита на данните в своите дейности/процеси.

5.1. Известяване на Субекта на Данни

Виж по-долу Секцията Насоки за Добросъвестна Обработка

5.2. Избор и Съгласие на Субекта на Данни

Виж по-долу Секцията Насоки за Добросъвестна Обработка

5.3. Събиране

Организацията трябва да се стреми да събере възможно най-малко количество лични данни. Ако личните данни се събират от трета страна, Отговорният служител по защита на личните данни трябва да гарантира, че личните данни се събират законно.

5.4. Използване, Съхранение и Премахване

Целите, методите, ограничаването на съхранението и периодът на запазване на личните данни трябва да съответстват на информацията, съдържаща се в известието за поверителност. Дружеството трябва да поддържа точността, целостта, поверителността и уместността на личните данни въз основа на целта на обработката. Трябва да се използват адекватни механизми за защита, предназначени за защита на личните данни, за да се предотврати откраднването или злоупотребата с личните данни, и да се предотврати нарушаването на личните данни. Отговорният служител по защита на личните данни отговаря за спазването на изискванията, изброени в този раздел.

5.5. Оповестяване на Трети Страни

Когато Дружеството използва услугите на доставчик или партньор (трета страна), за да обработва лични данни от негово име, Дружеството трябва да гарантира, че този доставчик ще предостави мерки за сигурност, за да защити личните данни, които са адекватни на свързаните с тях рискове. За тази цел трябва да се използва въпросника за съответствие с GDPR за обработващия лични данни.

Дружеството трябва да изисква по договор от доставчика или партньора да осигури същото ниво на защита на данните. Доставчикът или партньорът трябва да обработва само лични данни, необходими му, за да изпълнява своите договорни задължения към Дружеството или по нареждане на Дружеството, а не за други цели. Когато Дружеството обработва лични данни съвместно с независима трета страна, Дружеството трябва изрично да уточни своите съответни отговорности и третата страна в съответния договор или друг правно обвързващ документ, като например Споразумението за обработка на данни от доставчиците.

5.6. Трансграничен трансфер на лични данни

Преди да се предадат лични данни извън Европейското икономическо пространство (ЕИП), трябва да се използват адекватни предпазни мерки, включително подписването на споразумение за прехвърляне на данни, както се изисква от Европейския съюз, и при необходимост трябва да бъде получено разрешение от съответния орган за защита на данните. Дружеството, което получава личните данни, трябва да спазва принципите за обработка на лични данни, посочени в процедурата за трансгранично предаване на данни.

5.7. Право на Достъп от Субекти на Данни

Когато действа като администратор на данни, Дружеството е отговорно да предоставя на субектите на данни механизъм, който им позволява да имат разумен достъп до личните си данни, и трябва да им позволява да актуализират, коригират, изтриват или предават своите лични данни, ако е приложимо или се изисква по закон. Механизмът за достъп е допълнително описан в процедурата за заявка за достъп до субекта на данни.

5.8. Преносимост на Данни

Субектите на данни имат право да получат при поискване копие от данните, които са ни предоставили в структуриран формат, и да предадат тези данни на друг администратор безплатно. Отговорният служител по защита на личните данни е отговорен да гарантира, че тези искания се обработват в рамките на един месец, не са прекомерни и не засягат правата на лични данни на други лица.

5.9. Правото да бъдеш Забравен

При поискване, субектите на данни имат правото да получат от Дружеството изтриването на личните им данни. Когато Дружеството действа като Администратор на данни, Отговорният служител по защита на личните данни трябва да предприеме необходимите действия (включително технически мерки), за да информира третите лица, които използват или обработват тези данни (Обработващият данни), да се съобразят с искането.

6. Насоки за Добросъвестна Обработка

Личните данни трябва да се обработват само при изрично разрешение от Ръководството на Дружеството.

Организацията трябва да реши дали да извърши оценката на въздействието върху защитата на данните за всяка дейност по обработка на данни, съгласно насоките за Оценка на Въздействието върху Защитата на Данните.

6.1. Известия към Субектите на Данни

По време на събирането или преди събирането на лични данни за всякакъв вид обработка, включително, но не само, предоставяне на услуги или други дейности, организацията е отговорна да информира надлежно субектите на данни за следното: видовете събирани лични данни, целите на обработката, методите за обработка, правата на субектите на данни по отношение на техните лични данни, периода на запазване, потенциалните международни трансфери на данни, ако данните се споделят с трети страни и мерките за сигурност на дружеството за защита на личните данни. Тази информация се предоставя чрез Известие за поверителност.

Когато се споделят лични данни с трета страна, организацията трябва да гарантира, че субектите на данни са били уведомени за това чрез Известие за поверителност.

Когато се прехвърлят лични данни на трета държава, в съответствие с Трансграничната политика за прехвърляне на данни, съобщението за поверителност трябва да отразява това и ясно да посочва къде и кои лични данни се прехвърлят.

Когато се събират чувствителни лични данни, Отговорният служител по защита на личните данни трябва да се увери, че известието за поверителност изрично посочва целта, за която се събират тези чувствителни лични данни.

6.2. Получаване на Съгласие

Когато обработването на лични данни се основава на съгласието на субекта на данните или на други законови основания, Дружеството е отговорно за запазването на такова съгласие. То отговаря за предоставянето на съгласието на субектите на данни, които трябва да дадат съгласието си, и трябва да информира, и да гарантира, че тяхното съгласие (когато съгласието се използва като законно основание за обработка) може да бъде оттеглено по всяко време.

Когато събирането на лични данни е свързано с дете на възраст под 16 години, организацията трябва да гарантира, че родителското съгласие е дадено преди събирането, като се използва формулярът за съгласие от родител.

Когато се изисква да се коригират, изменят или унищожат записите с лични данни, организацията трябва да гарантира, че тези изисквания се обработват в разумен срок. Отговорният служител по защита на личните данни също трябва да записва заявките и да води дневник за тях.

Личните данни трябва да се обработват само за целите, за които първоначално са били събрани. В случай, че Дружеството иска да обработва събраните лични данни за друга цел, Дружеството трябва да потърси съгласието на своите субекти на данни в ясен и кратък срок. Всяко такова искане трябва да включва първоначалната цел, за която са събрани данните, както и новата или допълнителната (ите) цел (и). Искането трябва да включва и причината за промяната на целта / целите. Служителят по защита на данните отговаря за спазването на правилата в този параграф.

Сега и в бъдеще, организацията трябва да гарантира, че методите за събиране са в съответствие със съответните закони, добри практики и индустриални стандарти.

Отговорният служител по защита на личните данни е отговорен за създаването и поддържането на регистър на известията за поверителност.

7. Организация и Отговорности

Отговорността за осигуряване на подходяща обработка на лични данни се носи от всеки, който работи за или с Дружеството и има достъп до обработваните от него лични данни.

Основните отговорни при обработването на лични данни са следните организационни роли и длъжности:

Висшето ръководство взема решения и одобрява общите стратегии на Дружеството по повод защитата на личните данни.

Служителят по **Защита на Данните (ДЗД) или друг служител е отговорен** за управлението на програмата за защита на личните данни и отговаря за разработването и популяризирането на политики за защита на личните данни, както е определено в описанието на длъжностната характеристика на служителя за Защита на Данните;

Юридическият отдел заедно със Служителя по Защита на Данните наблюдава и анализира законите за личните данни и промените в нормативната уредба, разработва изисквания за съответствие и подпомага организацията в постигането на целите си за лични данни.

ИТ служителите са отговорни за:

- Осигуряване на всички системи, услуги и оборудване, използвани за съхраняване на данни, да отговарят на приемливи стандарти за сигурност.
- Извършване на редовни проверки и сканиране, за да се гарантира, че хардуерът и софтуерът за сигурност функционират правилно.

Администрацията е отговорна за:

- Одобряване на всички декларации за защита на данните, прикрепени към съобщения, имейли и писма.
- Отговори на всякакви запитвания за защита на данните от журналисти или медии.
- Когато е необходимо, работи със служителя по защита на данните, за да се гарантира, че инициативите на организацията спазват принципите на защита на данните.

Ръководителите Човешки Ресурси са отговорни за:

- Подобряване на информираността на служителите относно защитата на личните данни на потребителите.
- Организиране на експертни познания за защита на личните данни и обучение за повишаване на информираността на служителите, работещи с лични данни
- Защита на личните данни на служителите от „край до край“. Това трябва да гарантира, че личните данни на служителите се обработват въз основа на законните цели и необходимост на работодателя

Отдел ЗОП и Счетоводните отдели отговарят за предаването на отговорностите за защита на личните данни на доставчиците и за повишаването на нивата на информираност на доставчиците за защита на личните данни, както и за понижаване на изискванията за лични данни към трети страни, които използват. Отделът за поръчки/доставки трябва да гарантира, че Дружеството си запазва правото да извършва одит на доставчици.

8. Действия в отговор на Инциденти за Нарушаване на Личните Данни

Когато Организацията узнае за предполагаемо или действително нарушение на личните данни, Отговорният служител по защита на личните данни трябва да извърши вътрешно разследване и своевременно да предприеме подходящи мерки за отстраняване, в съответствие с политиката за нарушаване на данните. Когато съществува риск за правата и свободите на субектите на данни, Дружеството трябва да уведоми съответните органи за защита на данните без неоснователно забавяне и, когато е възможно - в рамките на 72 часа.

9. Одит и Отговорност

Може да бъде сформирано звено за извършване на одит, което да отговаря за проверката/одита на това, колко добре отделите прилагат тази политика.

Всеки служител, който нарушава тази Политика, ще бъде обект на дисциплинарно действие и служителят може също да бъде обвързан с граждански или наказателни задължения, ако неговото поведение нарушава закони или подзаконови актове.

10. Конфликт със Закона

Тази политика е предназначена да спазва законите и подзаконовите актове на мястото на установяване и на страните, в които Организацията работи. В случай на конфликт между тази Политика и приложимите закони и разпоредби, последните имат предимство.

11. Управление и съхранение на записи на базата на този документ

Име на записа	Място на съхранение	Отговорник за съхранението	Контроли за защита на записите	Време за съхранение
Формуляри за съгласие на субекта на данни	Защитен файлов сървър	Служителят по Защита на Данните	Само упълномощени служители имат достъп по формулярите	10 години
Формуляр за отказ от съгласие на Субекта на Данните	Защитен файлов сървър	Служителят по Защита на Данните	Само упълномощени служители имат достъп по формулярите	10 години
Формуляр за съгласие на родителите	Защитен файлов сървър	Служителят по Защита на Данните	Само упълномощени служители имат	10 години

			достъп по формулярите	
Формуляр за отказ на съгласие на родителите	Защитен файлов сървър	Служителят по Защита на Данните	Само упълномощени служители имат достъп по формулярите	10 години
Договори за обработка на данни на доставчици	Защитен файлов сървър	Служителят по Защита на Данните	Само упълномощени служители имат достъп по формулярите	5 години след изтичане на договора
Регистър на съобщенията за поверителност	Защитен файлов сървър	Служителят по Защита на Данните	Само упълномощени служители имат достъп по формулярите	Постоянно

12. Валидност и управление на документи

Този документ е валиден от 2018-05-08.

Собственикът на този документ е Ректорът, той трябва да провери и ако е необходимо да - актуализира документа най-малко веднъж годишно.