УНИВЕРСИТЕТ по БИБЛИОТЕКОЗНАНИЕ
и ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

ПОЛИТИКИ И СИСТЕМА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ

РЕГЛАМЕНТ (ЕС) 2016/679

НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 27 април 2016 година

влиза в сила на 25 май 2018 година

относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО

(Общ регламент относно защитата на данните)

(General Data Protection Regulation)

(GDPR)

СЪДЪРЖАНИЕ

ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ

Въведение

Принципите за защита на данните следва да се прилагат по отношение на всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано.

За да се определи дали дадено физическо лице може да бъде идентифицирано, следва да се вземат предвид всички средства, като например подбирането на лица за извършване на проверка, с които е най - вероятно да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице. За да се установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития.

1. Общ регламент за защита на данните (GDPR)

1.1 Предистория на Общия регламент за защита на данните (GDPR) Общият регламент за защита на данните 2016 заменя Директивата на ЕС за защита на данните от 1995 г. и заменя законите на отделните държави-членки, които са разработени в съответствие с Директива 95/46 / ЕО за защита на данните. Неговата цел е да защитава "правата и свободите" на физическите лица (т.е. живите индивиди) и да гарантира, че личните данни не се обработват без тяхното знание и, където е възможно, че се обработват с тяхното съгласие.

1.2 Обхват на Общия регламент (извлечени от GDPR)

1) Материален обхват (член 2) - GDPR се прилага за обработката на лични данни изцяло или частично с автоматизирани средства (например чрез компютър) и с обработката, различна от автоматизираните средства за лични данни (т.е. документи от хартиен носител), които са част от система или са предназначени да бъдат част от система за подаване.

2) Териториален обхват (член 3) - GDPR ще се прилага за всички администратори, които са установени в ЕС (Европейския съюз), които обработват личните данни на субектите на данни в контекста на това установяване. Той ще се прилага и за администратори извън ЕС, които обработват лични данни, за да предлагат стоки и услуги, или да наблюдават поведението на субектите на данни, които пребивават в ЕС.

1.3 Определения

За целите на настоящия регламент (член 4):

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

2) 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;

3) ограничаване на обработването означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

4) профилиране означава 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;

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

6) регистър с лични данни означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

7) 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;

8) обработващ лични данни означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

9) получател означава 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 4.5.2016 г. L 119/33 Официален вестник на Европейския съюз BG 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;

10) трета страна означава 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;

11) съгласие на субекта на данните означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

*12) **нарушение на сигурността на лични данни** означава 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;*

*13) **генетични данни** означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;*

*14) **биометрични данни** означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;*

*15) **данни за здравословното състояние** означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;*

*16) **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 настоящия регламент;

17) представител означава физическо или юридическо лице, установено в Съюза, което, назначено от администратора или обработващия лични данни в писмена форма съгласно член 27, представлява администратора или обработващия лични данни във връзка със съответните им задължения по настоящия регламент;

18) дружество означава физическо или юридическо лице, което осъществява икономическа дейност, независимо от правната му форма, включително партньорствата или сдруженията, които редовно осъществяват икономическа дейност;

*19) **група предприятия** означава контролиращо предприятие и контролираните от него предприятия;*

*20) **задължителни фирмени правила** означава политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност;*

*21) **надзорен орган** означава независим публичен орган, създаден от държава членка съгласно член 51/4.5.2016 г. L 119/34 Официален вестник на Европейския съюз BG. За България надзорен орган е **Комисия за защита на личните данни.***

*22) **засегнат надзорен орган** означава надзорен орган, който е засегнат от обработването на лични данни, тъй като:*

а) администраторът или обработващият лични данни е установен на територията на държавата членка на този надзорен орган;

б) субектите на данни с местопребиваване в държавата членка на този надзорен орган са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването;

в) до този надзорен орган е подадена жалба;

*23) **трансгранично обработване** означава или:*

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;

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;

24) относимо и обосновано възражение *означава възражение срещу проект на решение относно това дали е налице нарушение на настоящия регламент или не, или дали предвиждането действие по отношение на администратора или обработващия лични данни отговаря на изискванията на настоящия регламент, което ясно доказва, че проектът за решение води до значителни рискове за основните права и свободи на субектите на данни и, където е приложимо, за свободното движение на лични данни в рамките на Съюза;*

25) услуга на информационното общество *означава услуга по смисъла на член 1, параграф 1, точка б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета (1);*

26) международна организация *означава организация и нейните подчинени органи, регламентирани от международното публично право, или друг*

орган, създаден чрез или въз основа на споразумение между две или повече държави.

2. Декларация за политиката

2.1 Ръководството на УНИБИТ се ангажира да спазва всички съответни закони на ЕС и на държавите-членки по отношение на личните данни и защитата на "правата и свободите" на лицата, чиято информация УНИБИТ събира и обработва в съответствие с Общия регламент за защита на данните (GDPR).

2.2 Съответствието с GDPR е описано от тази политика и други съответни политики, като например политиката за информационна сигурност, заедно със свързани процеси и процедури.

2.3 GDPR и тази политика се отнасят до всички функции на УНИБИТ за обработка на лични данни, включително тези, които се извършват по лични данни на клиенти, клиенти, служители, доставчици и партньори и всякакви други лични данни, които организацията обработва от всеки източник.

2.4 УНИБИТ е установила цели за защита на данните и неприкосновеност на личния живот, които са включени в Система за управление на лични данни (Personal Information Management System или PIMS).

2.5 Служителят по защита на данните отговаря за преразглеждането на регистъра за дейностите по член 30, годишно в светлината на всички промени в дейностите на УНИБИТ, както и във всички допълнителни изисквания, определени чрез данни от оценка на въздействието върху

защитата. Този регистър трябва да бъде на разположение по искане на надзорния орган.

2.6 Тази политика се прилага за всички служители и заинтересовани страни от УНИБИТ, като доставчици или външни подизпълнители. Всяко нарушение на GDPR или на PIMS ще бъде разгледано в съответствие с дисциплинарната политика на УНИБИТ, като може да представлява и престъпление, за което да бъдат информирани съответните органи.

2.7 Партньори и трети страни, които работят с или за УНИБИТ и които имат или могат да имат достъп до лични данни, се очаква да са прочели, разбрали и спазват тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от УНИБИТ, без предварително да е сключила споразумение за поверителност на данните, което налага на трета страна задължения, не по-малки от тези прилагани в УНИБИТ. УНИБИТ има право на периодичен одит на спазване на споразумението.

Настоящата версия на този документ е достъпна за целия персонал.

Тази политика е одобрена от Ректора.

Издание	Описание на промените	Одобрен от	Дата на издаване
в.001	Първоначално издание	Ректор:..... Проф. д.ик.н. Стоян Денчев	*07.05.2018 г.*

СИСТЕМА ЗА УПРАВЛЕНИЕ НА ЛИЧНИ ДАННИ

Personal Information Management System

(PIMS)

Декларация за ангажимент към политиката

За да подкрепи спазването на GDPR, Ректорът одобри и подкрепи разработването, внедряването, поддръжката и непрекъснатото усъвършенстване на документирана Система за управление на личната информация ("PIMS") за УНИБИТ .

Всички служители на УНИБИТ и определени външни лица, идентифицирани в PIMS се очаква да спазват тази политика. Всички служители, както и определени външни лица, ще получат подходящо обучение. Последствията от нарушаването на тази политика са изложени в дисциплинарната политика на УНИБИТ и в договорите и споразуменията с трети страни.

При определянето на обхвата си за съответствие с GDPR, УНИБИТ е съобразила и отчела потенциалното влияние на:

- всякакви външни и вътрешни проблеми, които са свързани с целите на УНИБИТ и които влияят върху неговата способност да постига желаните резултати от своя PIMS;
- специфични нужди и очаквания на заинтересованите страни, които са от значение за изпълнението на PIMS;
- организационните цели и задължения;
- приемливите нива на риск и
- всички приложими законови, регулаторни или договорни задължения.

Целите на УНИБИТ за спазване на GDPR и PIMS :

- са в съответствие с тази политика;
- са измерими;
- вземат под внимание GDPR и резултатите от оценката на риска и третирането на риска;
- са наблюдавани;
- са съобщени;
- се актуализират според необходимостта;

За да постигне тези цели, УНИБИТ определи:

- какво ще бъде направено;
- какви ресурси ще бъдат необходими;
- кой ще отговаря;
- кога ще бъде завършено;
- как ще бъдат оценени резултатите;

3. Отговорности и роли съгласно Общия регламент за защита на данните (GDPR)

3.1 УНИБИТ е Администратор на данни или в някои случаи Обработващ лични данни, съгласно GDPR.

3.2 Ръководството на университета е отговорно за разработването и насърчаването на добри практики за обработка на информация в УНИБИТ; отговорностите са посочени в отделните длъжностни характеристики.

3.3 Служител по защита на данните носи отговорност, определена в GDPR, за управлението на лични данни в рамките на УНИБИТ и за гарантиране спазването на законодателството за защита на данните и добрите практики.

Тази отчетност включва:

3.3.1 разработване и прилагане на GDPR, както се изисква от тази политика; и

3.3.2 управление на сигурността и риска във връзка със спазването на политиката.

3.4 Служител по защита на данните, който Ректора счита за подходящо квалифициран и опитен, е назначен да поема отговорност за съответствието на УНИБИТ с тази политика на всекидневна база и по-специално е пряко отговорен за спазването на изискванията на GDPR в УНИБИТ.

3.5 Служителят по защита на данните има конкретни отговорности по отношение искания за предоставяне на информация по реда предвиден в GDPR е контактна точка за служители, които искат разяснения по всеки аспект от спазването на защитата на данните.

3.6 Съответствието със законодателството за защита на данните е отговорност на всички служители на УНИБИТ, които обработват лични данни.

3.7 Програмата за обучение на УНИБИТ ("*Програма за обучение с приложение*") определя обучения за познаване на GDPR и специфични

конкретни изисквания и осведоменост по отношение на изпълняваните функции на служители на УНИБИТ.

3.8 Служителите на УНИБИТ са отговорни да гарантират, че всички лични данни за тях и предоставените на тях на УНИБИТ са точни и актуални.

4. Принципи за защита на данните (член 5)

Цялата обработка на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от GDPR. Политиките и процедурите на УНИБИТ са предназначени да осигурят съответствие с принципите.

4.1 Личните данни трябва да се обработват **законно, справедливо и прозрачно**

1) Законно – Законната основа трябва да бъде идентифицирана, преди да се обработват лични данни. Те често се наричат "условия за обработка", например съгласие.

2) Справедливо - за да може обработването да бъде справедливо, администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи, независимо дали личните данни са получени директно от субектите на данни или от други източници.

GDPR увеличава обхвата на изискванията на това, каква информация следва да бъде на разположение на субектите на данни по отношение на изискването за "прозрачност".

3) Прозрачно - GDPR включва правила за предоставяне на информация за личните данни на субектите на данни в членове 12, 13 и 14. Те са подробни и конкретни, като се набляга на това, че известията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен език.

Политика за поверителност на УНИБИТ (Privacy notice) е изложена в [" *Политика за поверителност на УНИБИТ*"].

Специфичната информация, която трябва да бъде предоставена на субекта на данните е:

4.1.1 идентичността и данните за контакт на администратора и, ако има такъв, на представителя на администратора;

4.1.2 данните за контакт на Служителят по защита на данните;

4.1.3 целите на обработката, за която са предназначени личните данни, както и правното основание за обработката;

4.1.4 периодът, за който ще се съхраняват личните данни;

4.1.5 наличието на права за искане за достъп, коригиране, заличаване или възражение срещу обработката и за условията (или липсата) на упражняването на тези права, като например дали ще бъде засегната законността на предишната обработка;

4.1.6 категориите на съответните лични данни;

4.1.7 получателите или категориите получатели на лични данни, където е приложимо;

4.1.8 когато е приложимо, администраторът възнамерява да прехвърли лични данни на получател в трета държава и степента на защита, предоставена на данните;

4.1.9 всякаква допълнителна информация, необходима за гарантиране на честна обработка.

4.2 Личните данни могат да бъдат събирани само за конкретни, изрични и легитимни цели.

4.3 Личните данни трябва да бъдат адекватни, подходящи и ограничени до това, което е необходимо за обработка (минимизиране на данните).

4.3.1 Служителят по защита на данните носи отговорност да гарантира, че УНИБИТ не събира информация, която не е строго необходима за целта.

4.3.2 Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изисквания за събиране на данни в новите информационни системи, трябва да включват декларация за справедливо обработване или препратка към декларацията за поверителност и одобрени от Служителят по защита на данните.

4.3.3 Служителят по защита на данните ще гарантира, че на годишна база всички методи за събиране на данни се одитират, за да се гарантира, че събраните данни продължават да бъдат адекватни, уместни и не прекомерни Процедура за оценка на въздействието на защитата

[" *Процедура за оценка на въздействието DPIA / PIA*"].

4.4 Личните данни трябва да бъдат точни и актуални. Когато се получи информация за промяна е необходимо своевременно да бъдат коригирани.

4.4.1. Данните, които се съхраняват от администратора на лични данни, трябва да бъдат преглеждани и актуализирани при необходимост.

4.4.2 Служителят по защита на данните е отговорен да гарантира, че целият персонал е обучен за събиране на точни данни и поддържането им.

4.4.3 Задължение на субекта на данните да гарантира, че данните, съхранявани от УНИБИТ, са точни и актуални.

4.4.4 Всички субекти на данни (служители, клиенти и други) са длъжни да уведомяват УНИБИТ за промени в обстоятелствата, за да могат да се актуализират регистрите на лични данни. Инструкции за актуализиране на записите се част от работни инструкции, свързани с това как се съхраняват лични данни.

Отговорност на УНИБИТ е да гарантира, че е при постъпване на уведомление за промяна на обстоятелствата ще бъде предприето действие.

4.4.5 Служителят по защита на данните е отговорен да 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 променят, други релевантни фактори.

4.4.6 Най-малко на годишна база ще се извърши инвентаризация на данните и ще се идентифицират всички данни, които вече не се изискват в контекста на регистрираната цел.

Тези данни ще бъдат надеждно унищожени в съответствие с процедурата за сигурно унищожаване на носители за съхранение (Процедура за защитено унищожаване на носители на информация).

4.4.7 Служителят по защита на данните отговаря в рамките на един месец на искания за коригиране от заинтересованите лица („Процедура за отстраняване на несъответствия и корективни дейности"). Ако УНИБИТ реши да не изпълни искането, отговорникът по защита на данните трябва да отговори на субекта на данните, като обясни мотивите си и да ги информира за правото им да подадат жалба пред надзорния орган или да потърсят съдебна защита.

4.4.8 Служителят по защита на данните е отговорен за прилагането на подходящи мерки при взаимодействието с трети страни (обработващи), които да позволят да се синхронизира информацията, например: когато данните са неточни или неактуални, да ги информира, както и за предаването на всяка корекция на личните данни на третата страна, когато това се изисква.

4.5 Личните данни трябва да се съхраняват в такава форма, че лицето, за което се отнасят данните, да може да бъде идентифицирано, когато това е необходимо за обработка.

4.5.1 Когато личните данни се съхраняват след крайната дата на обработка, те ще бъдат анонимизирани, за да се защити самоличността на субекта на данните в случай на нарушение на сигурността на данните.

4.5.2 Личните данни ще се съхраняват в съответствие с Процедурата за съхранение на архивите на УниБИТ и след като бъде достигната датата

на задържане, те трябва да бъдат безопасно унищожени, както е посочено в тази процедура.

4.5.3 Служителят по защита на данните трябва специално да одобрява всяко съхранение на данни, което надвишава сроковете за съхранение, определени в Процедурата за съхранение на архив и трябва да гарантира, че обосновката е ясно идентифицирана и съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде писмено.

4.6 Личните данни трябва да се обработват по начин, който гарантира подходяща сигурност.

Служителят по защита на данните ще извърши оценка на риска, като вземе предвид всички обстоятелства, свързани с дейностите по обработка на УНИБИТ.

При определянето на целесъобразността Служителят по защита на данните трябва също така да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица, ако се допусне нарушение на сигурността.

При оценяването на подходящи технически мерки, Служителят по защита на данните, след предоставено писмено становище на IT специалист от УНИБИТ, ще вземе предвид:

- Защита с парола;
- Автоматично заключване на неизползван компютър;
- Премахване на права за достъп за преносими носители на информация, като USB, дискове и други;
- Софтуер за проверка на вируси и защитни стени;

- Правата за достъп въз основа на ролите, включително тези, назначени за определен срок;
- Шифроване на преносими устройства, които се изнасят от помещенията на организацията, като лаптопи, таблети, смартфони и други;
- Сигурност на локалните и външните мрежи;
- Технологии за подобряване на поверителността като псевдонимизация и анонимизация;
- Определяне на подходящите международни стандарти за сигурност, отнасящи се до УНИБИТ.

При оценяването на подходящи организационни мерки, Служителят по защита на данните, след предоставено писмено становище на IT специалист от УНИБИТ по определени точки, ще вземе предвид:

- Подходящите нива на обучение в УНИБИТ;
- Мерки, които отчитат надеждността на служителите;
- Включването на защитата на данните в трудовите договори;
    - Идентифициране на дисциплинарни мерки за нарушаване на неприкосновеността на данните;
    - Мониторинг на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиени записи;
- Приемане на ясна политика за обслужване на гражданите;

- Съхраняване на данни на хартиен носител в заключващи се огнеупорни шкафове;
- Ограничаване използването на преносими електронни устройства извън работното място;
- Ограничаване на използването на собствени преносими устройства, а когато това е необходимо, прилагане на подходяща (Bring your own device BYOD) политика;
- Приемане и прилагане на ясни правила относно паролите;
- Осъществяване на редовни архиви на лични данни и съхранение на медиите извън основният сайт;
- Прилагане на подходящи договорни задължения и мерки за сигурност при прехвърляне на данни извън Европейския съюз.

Прилаганите контроли са избрани въз основа на идентифицираните рискове за личните данни и вероятността за щети на лица, чиито данни се обработват. *Спазването на този принцип от страна на УНИБИТ се съдържа в политиката за информационна сигурност.*

4.7 Администраторът на лични данни трябва да може да докаже съответствие с другите принципи на GDPR, т.е. изискването за отчетност.

GDPR включва разпоредби, които насърчават отчетността и управлението. Те допълват изискванията за прозрачност на GDPR.

Принципът на отчетност в член 5, параграф 2 изисква организацията да може да докаже, че спазва принципите и декларира че това е нейна отговорност.

УНИБИТ ще демонстрира съответствие с принципите за защита на данните чрез прилагане на политики за защита на данните, спазване на кодекси за

поведение, прилагане на технически и организационни мерки, както и приемане на техники, като защита на данните за всеки проект, оценка на риска и на въздействието, процедури за уведомяване за нарушения и планове за реакция при инциденти.

5. Права на субектите на данни

5.1 Субектите на данни имат следните права по отношение на обработката на данни и данните, които се съхраняват за тях. Те могат:

5.1.1 Да отправят искане за получаване на информация относно характера на данните, които се съхраняват за тях и на кого са били предоставяни.

5.1.2 Да се прекрати обработка, която може да причини щети на субекта.

5.1.3 Да се прекрати обработка за целите на директния маркетинг.

5.1.4 Да бъдат информирани за механизма на автоматизиран процес на вземане на решения, който ги засяга в значителна степен.

5.1.5 Да не се вземат значими решения, които да ги засягат само чрез автоматизиран процес.

5.1.6 Да поискат обезщетение, ако са пострадали от нарушение на GDPR.

5.1.7 Да предприемат действия за отстраняване, блокиране, изтриване, включително правото да бъдат забравени или коригиране на неточни данни.

5.1.8 Да поиска от надзорния орган да прецени дали някоя от разпоредбите на GDPR е била нарушена.

5.1.9 Да им се предоставят лични данни в структуриран, често използван и машинно четим формат или да поискат данните да бъдат предадени на друг администратор.

5.1.10 Да възрази на автоматизирано профилиране, което е направено без съгласие.

5.2 УНИБИТ гарантира, че субектите на данни могат да упражняват тези права:

5.2.1 Субектите могат да правят заявки за достъп до личните им данни УНИБИТ гарантира, че нейният отговор на искането за достъп до данни отговаря на изискванията на GDPR.

5.2.2 Субектите на данни имат право да подават жалби до УНИБИТ, свързани с обработката на личните им данни.

6. Съгласие

6.1. УНИБИТ разбира, че "съгласие" означава, че то е изрично и свободно дадено, конкретно, информирано и изразява недвусмислено указание за желанията на субекта на данните. То е изявление на субекта, което означава одобрение за обработка на лични данни, отнасящи се до него или нея. Субектът на данните може да оттегли своето съгласие по всяко време.

6.2 УНИБИТ разбира, че "съгласието" означава, че субектът на данните е бил напълно информиран за планираната обработка и е изразил своето съгласие.

Съгласието, получено въз основа на подвеждаща информация, няма да бъде валидна основа за обработка.

6.3 Когато е приложимо, ще се прилага активна комуникация между страните, за да се демонстрира активно съгласие.

6.4 За чувствителни данни трябва да бъде получено изрично писмено съгласие от субектите на данни, освен ако не съществува алтернативна легитимна база за обработка.

6.5 В повечето случаи съгласието за обработка на лични и чувствителни данни се получава рутинно от УНИБИТ, използвайки стандартни документи за съгласие, напр. когато нов клиент подписва договор.

6.6 Когато УНИБИТ предоставя онлайн услуги на деца, трябва да се получи разрешение от родителите или настойниците. Това изискване се прилага за деца на възраст под 18 години.

7. Сигурност на данните

7.1 Служителите са отговорни да гарантират, че всички лични данни, които УНИБИТ притежава и за които отговарят, се съхраняват сигурно и не се разкриват при каквито и да е други условия, освен ако трета страна е получила специално разрешение от УНИБИТ да получи информация и е сключила споразумение за поверителност.

7.2 Всички лични данни трябва да бъдат достъпни само за онези, на които е необходимо, а достъпът може да бъде предоставен само в съответствие с политиката за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

- в заключващи се помещения с контролиран достъп;

- в заключени чекмеджета или шкафове; и/или
- ако е компютъризирана, защитени с парола в съответствие с корпоративните изисквания в Политиката за контрол на достъпа; и / или
- съхранявани на преносими компютърни носители, които са кодирани.

7.3 Компютърните дисплеи трябва да са видими единствено от оторизираните служители на УНИБИТ.

7.4 Информацията на хартиен носител не трябва да се оставят там, където тя може да бъде достъпна за неоторизиран персонал и не може да бъде изнасяна от търговските помещения без изрично разрешение. Веднага щом информацията на хартиен носител вече не изисква ежедневна обработка, тя трябва да бъде премахната чрез надеждно архивиране.

7.5. Ръчните записи, които са достигнали датата на задържане, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Твърдите дискове на излишните персонални компютри трябва да бъдат премахнати и незабавно унищожени.

7.6 Обработката на лични данни "от вкъщи" представлява потенциално по-голям риск от загуба, кражба или повреда на лични данни. Персоналът трябва да има специално упълномощаване да обработва данни извън университета.

8. Оповестяване на данни

8.1 УНИБИТ трябва да гарантира, че личните данни не се разкриват на неупълномощени трети страни, които включват членове на семейството,

приятели, държавни органи и при определени обстоятелства полицията. Всички служители персонал трябва да бъдат предпазливи, когато е поискано да разкрият лични данни, съхранявани от друго лице или трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с необходимото за извършване на дейността на УНИБИТ.

8.2 Всички искания за предоставяне на данни трябва да бъдат подкрепени с подходяща документация. Самото оповестяване да бъде специално разрешено от Служителят по защита на данните.

9. Запазване и унищожаване на данни

9.1 УНИБИТ не съхранява лични данни във форма, която позволява идентифициране на субектите на данни за по-дълъг период, отколкото е необходимо, във връзка с целите, за която първоначално са събрани данните.

9.2 УНИБИТ може да съхранява данни за по-дълги периоди, ако личните данни ще бъдат обработвани единствено с цел архивиране за обществени интереси, научни или исторически научноизследователски цели или за статистически цели, при условие че се прилагат подходящи технически и организационни мерки за защита на правата и свободите на субекта на данните.

9.3 Периодът на задържане за всяка категория лични данни ще бъде определен в Процедурата за съхранение на архиви на УниБИТ, заедно с критериите използвани за определяне на този период, включително всички законови задължения, въз основа на които УНИБИТ трябва да запази данните.

9.4 Личните данни трябва да се унищожават по сигурен начин в съответствие с шестия принцип на GDPR - обработени по подходящ начин, за да се поддържа сигурността, като по този начин се защитават "правата и свободите" на субектите на данни.

10. Трансфер на данни

10.1 Всеки трансфер на данни от Европейското икономическо пространство (ЕИП) към страни извън Европейското икономическо пространство, посочени в GDPR като "*трети страни*" е незаконосъобразен, освен ако не съществува подходящо "ниво на защита на основните права на субекти на данни".

Прехвърлянето на лични данни извън ЕИП е забранено, освен ако не се прилагат една или повече от посочените предпазни мерки или изключения:

10.1.1 Решение за адекватност. Европейската комисия може и оценява 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.

Списък на държавите, които понастоящем отговарят на изискванията за адекватност на Комисията, се публикува в Официален вестник на Европейския съюз. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.1.2 “Privacy shield”. Ако УНИБИТ желае да прехвърли лични данни от ЕС на организация в САЩ, тя трябва да провери дали организацията е подписала рамката на Privacy Shield в Търговското министерство на САЩ. Задължението, което се прилага към дружествата по Privacy Shield, се съдържа в "Принципите за поверителност". Предоставената защита на личните данни се прилага независимо дали личните данни са свързани с гражданин на ЕС или не.

Оценка на адекватността от администратора на данни

При извършване на оценка на адекватността трябва да се вземат предвид следните фактори:

- естеството на прехвърляната информация;
- страната или територията на произхода и крайното местоназначение на информацията;
- как ще бъде използвана информацията и колко дълго;
- законите и практиките на страната на получателя, включително съответните практически кодекси и международни задължения.

10.1.3 Задължителни корпоративни правила, които УНИБИТ може да приеме за предаване на данни извън ЕС, като ги съгласува със съответния надзорен орган за одобрение.

10.1.4 Модел на договорни клаузи. УНИБИТ може да приеме одобрени договорни клаузи за прехвърляне на данни извън ЕИП.

10.1.5 Изключения. При липса на решение за адекватност, членство в Privacy Shield, обвързващи корпоративни правила 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 за субекта на данните, поради липса на решение за адекватност и подходящи гаранции;
- Прехвърлянето е необходимо за изпълнението на договор между субекта на данните и администратора или изпълнението на пред договорни мерки, взети по искане на субекта на данните;
- Прехвърлянето е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данни между администратора и друго физическо или юридическо лице;
- Прехвърлянето е необходимо поради важни причини от обществен интерес;

- Прехвърлянето е необходимо за създаването, упражняването или защитата на правни искове; и / или
- Прехвърлянето е необходимо за защита на жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните физически или юридически не е в състояние да даде съгласието си.

11. Регистър на информационните активи инвентаризация на данните

11.1 УНИБИТ е въвела процес на инвентаризация на данните и на потоците от данни, като част от своя подход за справяне с рисковете и възможностите в целия си проект за спазване на GDPR.

Отчитат се:

- процеси, които използват лични данни;
- източник на лични данни;
    - обем на субектите на данни;
    - описание на всеки елемент от лични данни;
    - дейност по обработка;
    - поддържа опис на категориите данни за обработени лични данни;
    - документира целта/целите, за която се използва всяка категория лични данни;
    - получателите и потенциалните получатели на личните данни;
    - ролята на УНИБИТ в целия поток от данни;
    - ключови системи и хранилища;
    - всички прехвърляния на данни; и
    - всички изисквания за задържане и изхвърляне.

11.2 УНИБИТ е наясно с всички рискове, свързани с обработката на определени видове лични данни.

11.2.1 УНИБИТ оценява нивото на риска за лицата, свързани с обработката на техните лични данни. Извършват се оценки на въздействието върху защитата на данните (DPIA) (Процедура DPIA) във

връзка с обработката на лични данни от УНИБИТ и във връзка с извършената обработка от други организации от името на УНИБИТ .

11.2.2 УНИБИТ управлява всички рискове, идентифицирани от оценката на риска, с цел да се намали вероятността от несъответствие с тази политика.

11.2.3 Когато при вид обработка, чрез използване на нови технологии, отчитайки естеството, обхвата, контекста и целите на обработката, може да доведе до висок риск за правата и свободите на физическите лица, УНИБИТ, преди започване на обработката ще извърши оценка на въздействието на предвидените операции по обработка върху защитата на личните данни. Оценката на въздействието може да разглежда набор от подобни операции по обработка, които представляват подобни високи рискове.

11.2.4 Когато в резултат на оценката на въздействието стане ясно, че ако УНИБИТ направи обработката на лични данни, които биха могли да причинят щети на субектите на данни, решението за това дали УНИБИТ може да продължи или не трябва да бъде ескалирано за преглед на Служителят по защита на данните.

11.2.5 Служителят по защита на данните трябва да ескалира въпроса до надзорния орган, ако съществуват сериозни опасения относно потенциалната вреда или опасност или количеството на съответните данни.

11.2.6 Подходящи контроли ще бъдат избрани от приложение А към ISO 27001, ISO 27017, ISO 27018 и т.н., когато е подходящо и ще се прилагат, за да се намали нивото на риск, свързано с обработването на индивидуални данни до приемливо.

Собственик на документ и одобрение

Служителят по защита на данните е собственик на този документ и отговаря за това, че този документ за политиката се преглежда в съответствие с изискванията за преглед, посочени по-горе.

Настоящата версия на този документ е достъпна за целия персонал.

Тази политика е одобрена от Ректора.

Издание	Описание на промените	Одобрен от	Дата на издаване
в.001	Първоначално издание	Ректор:..... Проф. д.ик.н. Стоян Денчев	*07.05.2018 г.*

ПОЛИТИКА ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА

Ръководството на УНИБИТ се ангажира да пази поверителността, целостта и наличността на всички физически и електронни информационни активи в цялата си организация, за да запази конкурентно предимство, регулаторно и договорно съответствие и търговски имидж. Изискванията за защита на информацията ще продължат да бъдат съгласувани с целите на УНИБИТ. Предназначена да осигури механизъм за обмен на информация, за електронни операции и за намаляване на свързаните с информацията рискове до приемливи нива.

Настоящата политика и рамка за управление на риска на УНИБИТ осигуряват контекста за идентифициране, оценка и контрол на свързаните с информацията рискове. Оценката на риска, декларацията за приложимост и планът за третиране на риска определят начина, по който се контролират рисковете, свързани с информацията. Допълнителни оценки на риска могат, когато е необходимо, да се извършат, за да се определят подходящи проверки за специфични рискове.

Плановете за непрекъснатост на работата и плановете за действие при непредвидени обстоятелства, процедурите за архивиране на данни, избягването на вируси и хакери, контрола на достъпа до системите и докладването на инциденти по сигурността на информацията са от основно значение за тази политика.

УНИБИТ има за цел да постигне конкретни, определени цели за информационна сигурност, които са разработени в съответствие с целите на университета, контекста на организацията, резултатите от оценката на риска и плана за третиране на риска.

Всички служители на УНИБИТ и определени външни лица се очаква да спазват тази политика. Всички служители и определени външни лица ще получат подходящо обучение. Последствията от нарушаването на политиката за информационна сигурност са изложени в дисциплинарната политика и в договорите и споразуменията с трети страни.

Политиката подлежи на непрекъснат, систематичен преглед и усъвършенстване.

Тази политика ще бъде преразгледана, за да отговори на всякакви промени в оценката на риска или в плана за третиране на риска, и поне веднъж годишно.

В тази политика "информационна сигурност" се определя като:

1) Поверителност

Поверителност, означава да се гарантира, че информацията е достъпна само за онези, които имат разрешение за достъп до нея и следователно за предотвратяване както на преднамерен, така и случайно неоторизиран достъп до информацията на УНИБИТ и нейните системи (включително мрежи, интернет страница, и други).

2) Цялостност. Това включва запазването на точността и пълнотата на информацията и методите за обработка и следователно изисква предотвратяване на преднамерено или случайно частично или пълно унищожаване или неразрешено изменение на материални активи или електронни данни.

3) Наличност. Това означава, че информацията и свързаните с нея активи трябва да бъдат достъпни за оправомощените потребители, когато са

необходими и следователно физически сигурни. Компютърната мрежа трябва да е устойчива и УНИБИТ трябва да може да открива и да реагира бързо на инциденти (като вируси и други злонамерени програми), които застрашават постоянната наличност на активи, системи и информация. Трябва да има подходящи планове за непрекъснатост на работата.

4) Убеждение. Това означава, че ръководството, всички служители на пълен работен ден или на непълно работно време, подизпълнители, консултанти по проекти и външни лица ще бъдат запознати с техните отговорности (които са определени в техните длъжностни характеристики или договори) за запазване на сигурността на информацията, да съобщават за нарушения на сигурността. Всички служители ще получат обучение за повишаване на информираността относно сигурността на информацията, а извършващите по-специфични дейности служители ще получат подходящо специализирано обучение.

Активи на УНИБИТ

Активите на УНИБИТ биват:

- Физически активи
- Информационни активи

Физически активи

Физическите активи на УНИБИТ, включително, но не само компютърен хардуер, мрежово окабеляване за пренос на данни, телефонни системи, системи за архивиране и физически файлове с данни.

Информационни активи

Информационните активи включват информация, отпечатана или написана на хартия, предавана по пощата или показана във филми или вербална в разговор, както и информация, съхранена по електронен път на сървъри, уебсайтове, екстранет, интранет, персонални компютри, лаптопи, мобилни телефони и PDA устройства, както и на CD ROM дискове, флопи дискове, USB памети, резервни касети и всякакви други цифрови или магнитни носители и информация, предавана по електронен път по всякакъв начин. В този контекст "данни" включват и набор от инструкции, които указват на системата как да манипулират информацията (т.е. софтуера: операционни системи, приложения, помощни програми и т.н.) на УНИБИТ и такива партньори, които са част от интегрираната мрежа на УНИБИТ и са се присъединили към политиката за сигурност.

Нарушение на сигурността е всеки инцидент или дейност, която причинява или може да причини нарушение на наличността, поверителността или целостта на физическите или електронните информационни активи на УНИБИТ.

Настоящата версия на този документ е достъпна за целия персонал.

Тази политика е одобрена от Ректора.

Издание	Описание на промените	Одобрен от	Дата на издаване
в.001	Първоначално издание	Ректор:..... Проф. д.ик.н. Стоян Денчев	*07.05.2018 г.*