	ПРОЦЕДУРА ПО ПРИЕМАНЕ НА ПЛАН ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ		
	GDPR	Идент. № PROC_10	Версия 0.1
Администратор: УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ		ОЛЗД: Володя Николов Каменов	

Версия	Дата	Описание	Изготвил	Одобрил
0.1	25.05.2018г	Описание на отделните практически стъпки по предприемане на технически и организационни мерки за защита сигурността на личните данни	ОЛЗД Володя Николов Каменов	Ректор: проф. дтн. инж. Кольо Т. Динков

I. Предназначение на процедурата

Настоящата процедура има за цел да определи отделни практически стъпки по предприемане на технически и организационни мерки за защита сигурността на личните данни. Видът организационни и технически мерки, които са подходящи за УНИВЕРСИТЕТА ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ, се преценяват от администратора на база спецификите, на дейността на Университета, личните данни, които се събират и обработват от този администратор, рискът от нарушаване защитата на лични данни където той се явява администратор на личните данни и т.н.

Организационните мерки включват, определяне на служител – Отговорно лице по защита на данните, политики и обучение на персонала за обработване на лични и чувствителни лични данни и извършване на оценка на въздействието върху защитата на данните.

Техническите мерки за защита на лични или чувствителни лични данни включват, , класифициране на данни, предотвратяване на загуба на данни, криптиране, получаване на изрично съгласие за всяка конкретна цел, ограничения при пренос на данни и въвеждане на технологии, които позволяват на субектите на данни да упражняват своите права за достъп, коригиране и заличаване на лични данни и др.

При прилагането на конкретните мерки се вземат предвид: състоянието на техниката; разходите за внедряване на нови технологии; естеството, обхвата, контекста и целите на обработването на личните данни; рисковете за правата и свободите на субектите.


II. Нормативна уредба

[Чл. 25](#) и [32](#) от ОРЗД

III. Задължения и отговорници

Общият регламент разделя отговорностите и задълженията на администратора и обработващите лични данни. Съгласно изискванията на регламента отговорност за предприемане на подходящи мерки за защита на личните данни, респ. доказване, че

Контакт с Администратора на лични данни:		
Уебсайт: www.uft-plovdiv.bg	E-mail: pom_rektor_uht@abv.bg	Телефон: 0894337987

	ПРОЦЕДУРА ПО ПРИЕМАНЕ НА ПЛАН ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ		
	GDPR	Идент. № PROC_10	Версия 0.1
Администратор: УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ		ОЛЗД: Володя Николов Каменов	

такива са предприети, носи администраторът ([чл. 24, пар. 1 от ОРЗД](#)). От своя страна, администраторът е длъжен да работи само с онези обработващи лични данни, които предоставят "достатъчни гаранции за прилагане на подходящи технически и организационни мерки за защита на личните данни", за да изпълнят изискванията на Общия регламент и да защитят правата на субектите на данни. Обработващите лични данни трябва също така да предприемат всички мерки, изисквани съгласно [член 32](#), които очертават стандартите за "сигурност на обработването".

Координацията и контрола по създаването, внедряването и поддържането на правила и процедури по налагането на подходящи мерки за защита на личните данни, както организационни така и технически, е в рамките на задълженията на Отговорното лице по защита на данните/Отговорника по защита на данните.

УНИВЕРСИТЕТЪТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ отделя необходимите организационни, технически и финансови ресурси за подпомагане на тяхната дейност.

IV. Ход на процедурата

1. Анализ на рисковете и оценка на въздействието

При оценяването на подходящи технически и организационни мерки, Отговорното лице по защита на данните, респ. администраторът определя конкретните организационни и технически мерки, след като извърши оценка на въздействието върху защитата на данните (ОВЗД).

Освен при идентифициране на висок риск, ОВЗД се извършва задължително и в изброените в [член 35](#), параграф 3 от ОРЗД случаи:


- когато се извършва систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;
- при мащабно обработване на „чувствителни“ лични данни или на лични данни за присъди и нарушения;
- при систематично мащабно наблюдение на публично достъпна зона.

ОВЗД е задължителна също и за видовете операции по обработване, посочени в списък, приет и оповестен от националния надзорен орган ([чл. 35, пар. 4 от ОРЗД](#)).

Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни. Оценката на въздействието ще бъде извършена съгласно Процедура за оценка на въздействието върху защитата на данните (GDPR_PROC_09), както и методологията за ОВЗД.

2. Предприемане на стъпки по защита на данните на етап проектиране

Контакт с Администратора на лични данни:		
Уебсайт: www.uft-plovdiv.bg	E-mail: pom_rektor_uht@abv.bg	Телефон: 0894337987

	ПРОЦЕДУРА ПО ПРИЕМАНЕ НА ПЛАН ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ		
	GDPR	Идент. № PROC_10	Версия 0.1
Администратор: УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ		ОЛЗД: Володя Николов Каменов	

УНИВЕРСИТЕТЪТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ ще осигури съответствие с основните принципи за защита на данните в самата структура на техническите системи и организационните процеси – т.нар. защита на етап проектиране.

При етапа на проектиране УНИВЕРСИТЕТЪТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ ще следва критериите за защита, посочени в [член 25 от ОРЗД](#), като се отчита състоянието на техниката, разходите за изпълнението и естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, породени от обработването на личните данни.

На предварителен етап ще се взема решение как и кога да се извърши обработването на лични данни, като се извърши задълбочена оценка на четири отделни фактора - състоянието на техниката в организацията, цената на изпълнение по внедряване на нови технологии, ако се налагат такива, видовете обработване на лични данни и свързания риск за правата на субектите. Правата на субектите на данни по ОРЗД ще бъдат обезпечени практически съобразно техническите възможности и организационните процеси, които съществуват в организацията на УНИВЕРСИТЕТА ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ.

Извършва се анализ и се предприемат мерки по осигуряване на възможности за практическо упражняване на правата на субектите на данни съгласно Процедура за прозрачност при обработването на лични данни (GDPR_PROC_02), процедура за управление на исканията от субектите (GDPR_PROC_03), Процедура за начините на комуникация при жалби и искания от субекта на данни (GDPR_PROC_04).

3. Защита на данните по подразбиране

УНИВЕРСИТЕТЪТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ осигурява съответствие с принципа на защитата на данни по подразбиране. След като веднъж бъдат внедрени информационни системи за сигурност, за защита на данните в организацията на Университета настройките за поверителност трябва да могат да се прилагат по подразбиране, без ръчно въвеждане от крайния потребител. По подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването.

Това задължение се поема спрямо обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица ([чл. 25, ал.2 от ОРЗД](#)).


4. Въвеждането на подходящи организационни и технически мерки

Отговорното лице по защита на данните / Отговорникът по защита на данните, след като е извършил стъпките описани по-горе, координира и организира работата по определяне на конкретните технически и организационни мерки, които са подходящи за защита на данните, които УНИВЕРСИТЕТА ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ обработва.

4.1. По отношение на въвеждането на технически мерки се извършва анализ и се определят конкретни правила и решения най-малкото в следните направления:

- Начини на защита с парола;

Контакт с Администратора на лични данни:		
Уебсайт: www.uft-plovdiv.bg	E-mail: pom_rektor_uht@abv.bg	Телефон: 0894337987

	ПРОЦЕДУРА ПО ПРИЕМАНЕ НА ПЛАН ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ		
GDPR	Идент. № PROC_10	Версия 0.1	Стр. 4 от 6
Администратор: УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ		ОЛЗД: Володя Николов Каменов	

- Автоматично заключване на бездействащи работни станции в мрежата;
- Премахване/ограничаване на права на достъп за USB и други преносими носители с памет;
- Антивирусен софтуер и защитни стени;
- Защитата на преносими устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурността на локалните и широкообхватните мрежи;
- Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;
- Блокирането на зловреден софтуер чрез технологични средства;
- Правила за електронни таблици и други източници на данни, които се попълват чрез експортиране на данни за връзка с клиентите и профили за поща;
- Архивите за електронна поща, които съдържат лични данни и възможността за прилагане на криптиране към тази информация;
- Анализ на необходимостта от използване на решения за шифроване на имейли, които могат да се използват и за криптиране на всички данни, които текат в доставчик на облак-офис приложения, включително файлове;
- Преглед и анализ на необходимостта от прилагане на решения за шифроване на лични данни в съществуващ формат на базата данни, наречен Format Conservation Encryption (FPE);
- Преглед и анализ на необходимостта от решения за защита на компютърните устройства от загуба или кражба чрез възможностите за управление на мобилни устройства от разстояние.


Налагането на определени настройки, за да може едно устройство да се свърже изобщо с мрежата - като локално кодиране, сложност на паролата, наличието на софтуера за защита и премахването на акаунта на местния администратор - е съществена част от защитата на УНИВЕРСИТЕТА ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ..

- Идентифициране на подходящи международни стандарти за сигурност подходящи за Университета.

4.2. В случай на използване на облачни услуги за съхранение и споделяне:

- Анализ дали се гарантира, че са избрани и внедрени подходящи услуги за съхранение и споделяне на облак, които активно блокират или обезкуражават използването на неоторизирани услуги;
- Въвеждане на активно наблюдение на действията за споделяне, за да се сведе до минимум вероятността от нарушаване на данните;
- Като критерий за преимущество в УНИВЕРСИТЕТА ПО ХРАНИТЕЛНИ

Контакт с Администратора на лични данни:		
Уебсайт: www.uft-plovdiv.bg	E-mail: pom_rektor_uft@abv.bg	Телефон: 0894337987

	ПРОЦЕДУРА ПО ПРИЕМАНЕ НА ПЛАН ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ		
GDPR	Идент. № PROC_10	Версия 0.1	Стр. 5 от 6
Администратор: УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ		ОЛЗД: Володя Николов Каменов	

ТЕХНОЛОГИИ ще се отчита и използване на криптиране за защита на съхранените данни в услугата "облак" (криптиране на данни в режим на транзит, в употреба и в покой), предоставени пряко от самия доставчик или активирани от трето лице, за да се осигури правилното ниво на намаляване на риска;

- В организацията на Университета ще се използват само облачни услуги, които са разработени така, че да отговарят на правата за достъп, коригиране и заличаване на субектите на данни определени от Общият регламент.

4.3. При оценяването на подходящите организационни мерки Отговорното лице за защита на данните/Отговорникът по защита на данните взема предвид следното:


- Нивата на подходящо обучение на служителите в Университета;
- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- Включването на задълженията по защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;
- Приемането на политика на „чисто работно място“, включително и ограничаване на достъпа до определени сайтове и / или услуги;
- Съхраняване на хартия на базата данни в заключващи се стенни шкафове;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Ограничаване на използването от служителите на лични устройства на работното място;
- Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

4.4. Прилагането на горните технически и организационни мерки изисква изработването, налагането и поддържането на някои основни правила и процедури в Университета, като:

- Правила (процедура/работна инструкция) за начините на достъп и правата за достъп на мрежовите потребители /потребителските групи, чрез актуализиране на ПРАВИЛНИКА ЗА ОСИГУРЯВАНЕ НА ДОСТЪП И РАБОТА С ИНФОРМАЦИОННИ ПРОДУКТИ В УХТ;

Обхващат дефинирането на правилата за достъп в компютърната мрежа на Университета.

Контакт с Администратора на лични данни:		
Уебсайт: www.uft-plovdiv.bg	E-mail: pom_rektor_uht@abv.bg	Телефон: 0894337987

	ПРОЦЕДУРА ПО ПРИЕМАНЕ НА ПЛАН ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ		
GDPR	Идент. № PROC_10	Версия 0.1	Стр. 6 от 6
Администратор: УНИВЕРСИТЕТ ПО ХРАНИТЕЛНИ ТЕХНОЛОГИИ		ОЛЗД: Володя Николов Каменов	

- В съвместен с горните правила документ се определят и правилата за физически достъп до работните помещения и местата (шкафове, сейфове, други), където се съхраняват документи с лични данни;
- Правила за организационните и технически мерки, които се прилагат при унищожаване на различните категории лични данни, записани върху различни видове носители – идентифициране на данните, съгласуване, протоколи и т.н.;
- В правилата за унищожаване или в отделен документ се определя редът и начините за унищожаване на информацията върху вече неизползвани (бракувани) записващи носители, било чрез сигурно изтриване, било чрез унищожаване на самите носители;
- Инструкции и правила за актуализиране на записите с данни, така че при уведомяване от субектите на данни за промени в обстоятелствата да могат да се актуализират записите на лични данни. Правилата трябва да гарантират, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия по обновяване.

Контакт с Администратора на лични данни:		
Уебсайт: www.uft-plovdiv.bg	E-mail: pom_rektor_uht@abv.bg	Телефон: 0894337987