ПРОЦЕДУРА ЗА ОЦЕНКА НА РИСКА И НА ВЪЗДЕЙСТВИЕТО ЗА ЗАЩИТА НА ДАННИТЕ (DATA PROTECTION IMPACT ASSESSMENT DPIA / PIA)

1. Обхват

Всички проекти, които включват обработка на лични данни или всякакви дейности (вътрешни и външни), които засягат обработката на лични данни и засягат неприкосновеността на субектите на данни, попадат в обхвата на тази процедура и ще бъдат предмет на оценка на въздействието за защита на данните (Data Protection Impact Assessment, DPIA).

2. Отговорности

2.1 Служителят по защита на данните отговаря за извършването на необходимите проверки на личните данни, за да установи необходимостта от провеждане на DPIA.

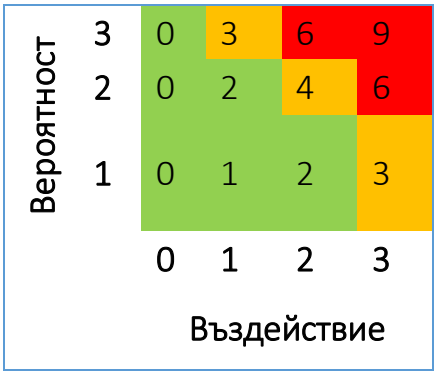
2.2 Служителят по защита на данните отговаря за проверката на подходящите мерки за контрол, за да се намалят рисковете, идентифицирани като част от процеса на DPIA и последващото решение за продължаване на обработката.

2.3 Ректорът е отговорен за прилагането на идентифицираните решения за риска за поверителността.

3. Процедура

3.1 Служителят за защита на данните идентифицира необходимостта от DPIA в началото на всеки проект, оценявайки проекта и вида на личните данни или обработващата дейност.

3.2 Използвайки критериите по-долу, в съответствие с матрицата за вероятност и въздействие, УНИБИТ определя рисковете за правата и свободите на субектите на данни като:



Рискове за правата и свободите на субектите на данни:

Ниво на риск	От	До	Установен по GDPR
Висок	6	9	Най-висок Неприемлив риск
Среден	3	5	Неприемлив риск
Нисък	1	2	Приемлив риск
Нулев	0	0	Няма риск

4. Работна книга за обработка на данни (поток от данни)

4.1 УНИБИТ записва ключова информация за обработваните лични данни в (*„GDPR регистър по Чл30 на дейностите по обработка на УНИБИТ“*). Това включва описание на обработката и целите; законни интереси, преследвани от администратора; оценка на необходимостта и пропорционалността на обработката; оценка на рисковете за правата и свободите на субектите на данни (съгласно матрицата и определенията на нивото на риска в точка 3.2 по-горе).

4.2 УНИБИТ обобщава вида на обработващата дейност, свързана с личните данни, които се обработват.

Те са категоризирани като:

- Събиране;
- Предаване;
- Съхранение;
- Достъп;
- Заличаване;

4.3 УНИБИТ установява на каква основателна база данните се обработват и подходящия период на съхранение.

4.4 УНИБИТ идентифицира категорията на обработените данни, независимо дали е лична, специална или тази на дете, както и формата на данните.

4.5 УНИБИТ идентифицира кой има достъп до данните (физически лица, екипи, трети страни или обработващ данни) или кой участват в обработката на лични данни или обработваща дейност, като регистрират географското местоположение на мястото, където се извършва обработката.

5. Определяне на рисковете за поверителността

5.1 УНИБИТ оценява рисковете за поверителност за всяка процесна дейност, както е описано в точка 3 по-горе, чрез:

5.1.1 Идентифициране и описание на риска за поверителността, свързан с тази дейност;

5.1.2 Като се използват критериите за вероятност (1 - нисък, 2 - среден и 3 - висок), се отчита вероятността от възникване на риск;

5.1.3 При използване на критериите за въздействие (0 - нулево въздействие, 1 - ниско, 2 - средно и 3 - високо) се установява въздействието на риска.

5.1.4 Изготвяне на пресметнат риск, идентифициращ риска за правата и свободите на субектите на данни.

5.2 При оценката на рисковете за неприкосновеността на личния живот УНИБИТ взема предвид:

- рисковете за правата и свободите на физическите лица, произтичащи от обработката на лични данни;
- рискове за дейността на организацията (включително вреди за репутацията); и
- неговите цели и задължения (регулаторни и договорни).

5.3 УНИБИТ идентифицира необходимите решения за редуциране на рисковете за поверителността, възлага на собственика на обработката да ги приложи, като определя крайната дата.

5.4 УНИБИТ дава приоритет на анализираните рискове за третиране на риска въз основа на критериите за ниво на риска, установени в точка 3.2 по-горе.

5.5 УНИБИТ, след консултация с служителя по защита на данните, одобрява и подписва всяка DPIA за всяка дейност по обработка на данни.

6. Предварително консултиране (член 36, GDPR)

6.1 Когато DPIA установи, че обработката на лични данни ще доведе до висок риск за субекта на данните, при липса на мерки за намаляване на риска и контрол, УНИБИТ се консултира с надзорния орган.

6.2 Когато УНИБИТ изисква консултация от надзорния орган, тя предоставя следната информация:

6.2.1 Подробности за ролите на УНИБИТ (като Администратор, Обработващ или Съвместен администратор) и за ролите (като Администратор, Обработващ или Съвместен администратор) на другите участващи в обработката;

6.2.2 Цел на предвидената обработка;

6.2.3. Подробно описание на всички мерки и контроли за защита на правата и свободите на субекта на данните;

6.2.4 Данни за контакт на служителя по защита на данните;

6.2.5 Копие от оценката на въздействието за защита на данните; и

6.2.6 Всякаква друга информация, поискана от надзорния орган.

Собственик и отговорник за актуализацията на документа е служителя по защита на данните.

Настоящата версия на този документ е достъпна за целия персонал.

Тази процедура е одобрена от Ректора.

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