ПРИЛОЖЕНИЕ №4:
СТАНДАРТ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Обхват

Всички проекти, които включват обработване на лични данни или всички действия (както вътрешни, така и външни), които засягат обработването на лични данни и оказват въздействие върху неприкосновеността на личния живот на субектите на данните, попадат в обхвата на настоящия стандарт и ще бъдат обект на оценка на въздействието върху защитата на данните.

Отговорности

1. Отговорното лице по защита на данните отговаря за извършване на необходимите проверки относно личните данни с цел установяване на необходимостта от извършване на оценка на въздействието върху защитата на данните.

2. Отговорното лице лице по защита на данните отговаря за проверките дали се прилагат подходящи контроли за ограничаване на всички рискове, идентифицирани при оценката на въздействието върху защитата на данните и последващото решение за пристъпване към обработване.

3. Собствениците на риска - ръководителни на отделите, обработващи личните данни, за които е идентифициран риск, в рамките на съответната организация - са отговорни за прилагането на всякакви идентифицирани решения за риска от нарушение на неприкосновеността на личния живот.

Процедура

1. Отговорното лице по защита на данните определя необходимостта от оценка на въздействието върху защитата на данните в началото на всеки проект, като оценява проекта и вида лични данни, свързани с него или дейността по обработване.

2. Като използва долупосочените критерии и следва матрицата на вероятностите и въздействието, длъжностното лице по защитата на данните в съответната организацията или в Групата, когато същото е определено за Групата като цяло, дефинира рисковете и правата и свободите на субектите на данните както следва:

Матрицата на вероятностите и въздействието:

Вероятност	0	3	6	9
	0	2	4	6
	0	1	2	3
	0	1	2	3
	Въздействие			

Рискове за правата и свободите на субектите на данните:

Ниво на риска	От	До	Оценка съгласно ОРЗД
Високо	6	9	Най-висок неприемлив риск
Средно	3	5	Неприемлив риск
Ниско	1	2	Приемлив риск
Нулево	0	0	Няма риск

Идентифициране на рискове за неприкосновеността на личния живот

1. Отговорното лице по защита на данните в съответната организация или на нивото на Групата като цяло оценява рисковете за неприкосновеността на личния живот на субектите на данни за всяка дейност по обработка от процеса, както е описано по-горе, като:
   • определя и описва риска за неприкосновеността на личния живот, свързан с тази дейност от процеса;
   • използва критериите за вероятност (1 - ниско, 2 - средно и 3 - високо) и оценява вероятността за възникване на риск
   • използва критериите за въздействие (0 - нулево въздействие, 1 - ниско, 2 - средно и 3 - високо) на риска, ако той възникне
   • пресметне риска чрез идентифициране на риска за правата и свободите на субектите на данните.
2. При оценяване на рисковете за неприкосновеността на личния живот отговорното лице по защитата на данните взема под внимание: рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни; рисковете за бизнеса (включително накърняване на репутацията) и целите и задълженията (както по закон, така и въз основа на договор).
3. Отговорното лице по защитата на данните идентифицира решения за рисковете за неприкосновеността на личния живот и заедно с висшия мениджмънт в съответната организация определя отговорник по третиране на риска и краен срок за изпълнение.
4. Отговорното лице по за защита на данните заедно с висшия мениджмънт на съответната организация определя като приоритетни за третиране анализирани рискове въз основа на критериите за ниво на риска, посочени в чл. 3.2 по-горе.

5. Собственикът на риска в организацията след консултация с отговорното лице по защита на данните одобрява и подписва оценката на въздействието върху защитата на данните за всяка дейност по обработване на данни.

Предварителна консултация (член 36 от ОРЗД)

1. Когато оценката на въздействието върху защитата на данните покаже, че обработването на лични данни ще породи висок риск за субекта на данните, ако не са взети мерки и контроли за ограничаване на риска, организацията се консултира с надзорния орган. Това консултиране се извършва в писмена, включително електронна форма.
2. Когато организацията поиска консултация от надзорния орган, тя предоставя следната информация:
   - информация за отговорностите на организацията и лицата, които се занимават с обработването;
   - целите на планираното обработване;
   - информация за всякакви/всички мерки и контроли, които се прилагат/ предоставят за защита на правата и свободите на субектите на данни;
   - данни за контакт на отговорното лице по защита на данните;
   - копие от оценката на въздействието върху защитата на данните и всякаква друга информация, поискана от надзорния орган.