ПРИЛОЖЕНИЕ №2:
СТАНДАРТ ЗА ИЗВЪРШВАНЕ НА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО НА РИСКА ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Проверки относно ефективността на мерките за защита на данните

1. Отговорникът относно защитата на данните провежда проверки относно:
    a. ефективността на мерките за защита на данните;
    b. спазването на Приложимото право относно защитата на данните; и
    c. съответствието с Приложимото право относно защитата на данните на Политиката и приложенията към нея, както и на останалите вътрешни актове на Сдружението.
2. Проверките по т.1 биват **периодични** и **текущи**:
    a. Периодичните проверки включват преглед на всички процеси, свързани с обработване на лични данни. Периодичните проверки се провеждат поне веднъж на всеки две години.
    b. Текущите проверки се провеждат при сезиране на Отговорника относно защитата на данните от страна на председателя на Управителния съвет, Надзорния орган или субектите на данните. Текущите проверки са ограничени до посоченото в сигнала.
3. Въз основа на проверките Отговорникът относно защитата на данните отправя препоръки. Председателят на Управителния съвет предприема необходимото за да гарантира спазването на препоръките, отправени в резултат на проведените периодични и/или текущи проверки.

Предварителни проверки за изготвяне на оценка на въздействието върху защитата на личните данни

1. За да установи дали е налице необходимост от извършване на оценка на въздействието на риска от нарушение на сигурността на обработваните в контекста на предвидените дейности по обработване данни (ОВЗД) Отговорникът относно защитата на данните провежда **предварителни проверки** и оценява риска съответно за всяка дейност по обработване.
2. Предварителните проверки се провеждат от Отговорника относно защитата на данните служебно или след получаването на уведомление за планиране на нова дейност (*project charter*), свързана с обработване на личните данни.
3. Изготвянето на ОВЗД за дадена дейност се посочва в съответния регистър на дейностите по обработване, поддържан от Сдружението.

Процедура по изготвяне на оценка на въздействието на риска

За да прецени дали е налице необходимост от извършване на ОВЗД Отговорникът относно защитата на данните използва посочените от Работната група по чл. 29 от Директива 95/46/ЕО критерии в съответствие с посочения по-долу механизъм за идентифициране на рисковете за субектите на данни.

Рискове за правата и свободине на субектите на данни

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

1. Отговорникът относно защита на данните оценява въздействието на риска върху защитата на данните за всяка дейност по обработване като:
   - определя и описва характерния за съответната дейността по обработване на лични данни риск от нарушение на сигурността на данните;
   - използва критериите за оценка на вероятността от реализиране на характерния за дейността по обработване риск;
   - използва критериите за оценка на въздействието върху защитата на личните данни (0 - нулево въздействие, 1 - ниско, 2 - средно и 3 - високо) на риска, ако той се реализира;
   - нивото на въздействие на риска (от 0 до 9) съответства на величина, производна на вероятността от реализиране на риска от нарушение на сигурността на данните, умножена по негово евентуално въздействие.
2. При оценката на вероятността и въздействието на риска Отговорникът относно защитата на данните взема предвид рисковете за правата и свободите на субектите на данни, произтичащи от обработването; рисковете за продължаването на дейността на Сдружението и целите и правните основанията за обработването на Данните.
3. След като установи вероятността и въздействието на риска Отговорникът относно защитата на данните идентифицира възможните мерки за третиране на риска, отговорното да предприеме мерките лице, крайния срок за прилагане на мерките и приоритетните за третиране рискове.

Провеждане на предварителна консултация

1. Когато установи, че мерките за третиране на даден процес/дейност по обработване, пораждаща висок риск за правата и свободите на субектите на данни (ниво на риск над 6), са недостатъчни, Отговорникът относно защитата на данните предлага на председателя на Управителния съвет на Сдружението да разпореди провеждане на предварителна консултация с Надзорния орган в съответствие с чл.36 от GDPR.
2. Председателя на Управителния съвет на Сдружението разпорежда провеждането напредварителна консултация с Надзорния орган в писмена, включително електронна, форма като задължава Отговорникът по защитата на данните да предостави на Надзорния орган информация за:
   - лицата, отговорни за обработването на данните;
   - целите на планираното обработване;
   - мерките за защита на правата и свободите на субектите на данни;
   - оценката на въздействието върху защитата на данните;
   - всякаква друга информация, поискана от Надзорния орган.