СЪВЕТ ЗА ЕЛЕКТРОННИ МЕДИИ

П О Л И Т И К А З А З А Щ И Т А Н А Л И Ч Н И Т Е Д А Н Н И

I. Въведение

1. Общ регламент за защита на личните данни

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 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, ОРЗД, Регламентът) поражда действие от 25 май 2018 г.

Регламентът има пряко действие и има за цел да защитава правата и свободите на физическите лица и да гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработва с тяхно съгласие.

Регламентът се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (*например ръчно и на хартия*), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Правилата важат за всички администратори на лични данни, които са установени в Европейския съюз (ЕС), които обработват лични данни на физически лица, в контекста на своята дейност. Принципът е, че правилата на ОРЗД „следват“ личните данни на субектите на данни, които се намират в Европейския съюз.

2. Понятия

Регламентът въвежда следните понятия във връзка с обработването и защитата на лични данни:

„Лични данни" – 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.

„Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.

„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.

„Администратор" – всяко 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 ЕС 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.

„Субект на данните“ – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора.

„Съгласие на субекта на данните" – 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.

„Дете“ – Общият Регламент определя дете като всеки на възраст под 16 години, въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

„Профилиране" – 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.

„Нарушение на сигурността на лични данни" – 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.

„Основно място на установяване“ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център.

„Получател" – 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 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.

„Трета страна“ – всяко 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.

II. Декларация относно политиката по защита на личните данни

1. **Съветът за електронни медии** (СЕМ, Съветът) се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на правата и свободите на лицата, чиито лични данни събира и обработва съгласно Общия регламент за защита на данните.

2. В съответствие с Общия регламент към тази политика са описани и други релевантни документи, както и свързани процеси и процедури.

3. Настоящият документ се отнася до всички функции по обработването на лични данни, включително тези, които се извършват относно лични данни на служители, доставчици, поднадзорни лица, партньори и всякакви други лични данни, които СЕМ обработва от различни източници.

4. СЕМ определя длъжностно лице по защита на данните, което да отговаря за ежегодния преглед на *Регистъра на дейностите по обработване* с оглед настъпили промени в дейностите на администратора, както и всички допълнителни изисквания, оценки на въздействието върху защитата на данните. Този регистър трябва да бъде на разположение по искане на надзорния орган – Комисия за защита на личните данни.

5. Настоящият документ се прилага за всички членове и служители на СЕМ, и за заинтересованите страни. Всяко нарушение на Общия регламент ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане в най-къс възможен срок на съответните държавни органи.

6. Партньори и трети лица, които работят със или за Съвета за електронни медии, както и които имат или могат да имат достъп до личните данни, ще се очаква да се запознаят, разбират и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от СЕМ, без предварително да е сключила споразумение за поверителност на данните, което налага на третата страна задължения, не по-малко обременяващи от тези, които Съветът е поел, и което дава право на Съвета да извършва проверки на спазването на наложените със споразумението задължения.

III. Задължения и роли по Общия регламент относно защитата на данните

1. Съветът за електронни медии е администратор на лични данни.

2. Съветът за електронни медии е отговорен за разработване и насърчаване на добри практики в областта на обработване на информация.

3. Длъжностното лице по защита на данните информира Съвета за електронни медии и неговия председател за управлението на личните данни и за гарантирането на възможността за доказване на съответствието със законодателството за защита на данните и добрите практики.

Длъжностното лице по защита на данните отговаря за, но не само: разработване и внедряване на изискванията на Регламента, както се изисква от настоящата политика; управление на сигурността и риска по отношение на съответствието с политиката.

4. Длъжностното лице по защита на данните е пряко отговорно, че цялостната дейност на Съвета за електронни медии и неговата администрация, която се извършва в рамките на неговата компетентност, съответстват на изискванията на Общия регламент относно защитата на данните.

5. Длъжностното лице по защита на данните има специфични отговорности по отношение на процедурите, включени в политиката и е контактна точка за служителите на СЕМ, които искат разяснения по всеки аспект на спазването на защитата на данните.

6. Спазването на законодателството за защита на данните е отговорност на всички служители на СЕМ, които обработват лични данни.

7. Съветът за електронни медии приема Политиката за обучение, която съдържа специфични изисквания за обучение и осведомяване във връзка с конкретните роли на членовете и служителите в администрацията на СЕМ.

IV. Принципи за защита на данните

Обработката на лични данни от СЕМ и неговата администрация се извършва в съответствие с принципите за защита на данните, определени в Регламента.

1. **Личните данни се обработват при спазване изискванията за законосъобразност, добросъвестност и прозрачност.**

Законосъобразност – идентифицират се законовите основания, преди да се обработват лични данни.

Добросъвестност – за да е обработването добросъвестно, администраторът на данни предоставя 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.

Прозрачност – Общият регламент включва подробни и конкретни правила относно предоставяне на поверителна информация на субектите на данни, поставяйки акцента върху това, че известията за поверителност са разбираеми и достъпни. СЕМ ще съобщава информацията на субекта на данните в разбираема форма, като ще използва ясен и разбираем език.

Правилата за уведомяване на субектите на данни СЕМ определя в *Процедура за прозрачност при обработката на лични данни,* като уведомлението се записва в Образец на Декларация за поверителност.

СЕМ предоставя на субектите на данни не по-малко от следната информация:

- ЕИК и адрес на СЕМ, тел. за контакт със СЕМ;
- контактите на Длъжностното лице по защита на данните;
- целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали СЕМ възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- друга допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни се събират само за конкретни, изрично указани и законни цели
СЕМ използва получени данни само за целите, официално обявени като част от Регистъра на дейностите по обработване на данни.
СЕМ определя съответните правила в *Процедура за прозрачност при обработката на лични данни*.

3. СЕМ събира лични данни на принципа на минимално необходимото – т.е личните данни, които се ползват са релевантни и ограничени до това, което е необходимо за дейността на администратора.
Определеното от СЕМ длъжностно лице по защита на личните данни осигурява и гарантира:
- да не се събира информация, която не е строго необходимо за целта, за която е получена;
- всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват декларация за добросъвестно обработване или връзка към Декларация за поверителност;
- ежегоден преглед на всички способи за събиране на данни от външни експерти, с цел оценка на данните като адекватни, релевантни, непрекомерни.

4. СЕМ осигурява мерки личните данни да бъдат точни и актуализирани във всеки един момент, както и полага необходимите усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.
В тази връзка:
- данните, които се съхраняват се преглеждат и актуализират при необходимост. Не се съхраняват данни, в случаите, когато има вероятност да не са точни.
- длъжностното лице за защита на данните организира обучение на целия персонал в значението на събирането на точни данни и поддържането им.
- във формулярите, попълвани от субекта на данни, предназначени за СЕМ, се включва изявление, че съдържащите се в тях данни са точни към датата на подаване.
- изисква от служителите, партньорите и други лица да уведомяват Съвета за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни.
- длъжностното лице по защита на данните отговаря и 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

промени, други относими фактори.

- ежегодно длъжностното лице по защита на данните преглежда сроковете на съхранение на всички лични данни, обработвани от Съвета за електронни медии. След идентифициране на всички данни, които вече не се изискват в контекста на регистрираната цел, същите ще бъдат унищожени в съответствие с процедурите и правилата на администратора.
- длъжностното лице по защита на данните осигурява корекция на данни в съответствие с постъпили такива искания в срок от един месец. Този срок може да бъде удължен с още два месеца за сложни заявки. Ако СЕМ реши да не се съобрази с искането, длъжностното лице по защита на данните отговаря на субекта на данните за мотивите на администратора и го информира за правото му да подаде жалба пред надзорния орган, и да потърси правна защита.
- длъжностното лице за защита на данните предприема подходящи мерки, в случаите когато организациите на трети страни имат неточни или остарели лични данни, като:

- ги информира, че информацията е неточна или остаряла и не се използва за вземане на решения относно лицата;
- информира съответните страни;
- препраща всяка корекция на лични данни към третите страни, където това е необходимо.

5. СЕМ съхранява личните данни в такава форма, че субектът на данните да бъде идентифициран само толкова дълго, колкото е необходимо за обработването.

- когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин (минимизирани, криптирани, псевдонимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на данните.
- лични данни ще бъдат пазени в съответствие с Процедура за съхраняване и унищожаване на данните и след като е преминал срокът им на съхранение, ще бъдат надеждно унищожени по указания в тази процедура ред.
- длъжностното лице за защита на данните одобрява специално всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в Процедура за съхраняване и унищожаване на данните и гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните. Това одобрение е писмено.

6. СЕМ гарантира подходяща сигурност при обработване на личните данни

Съветът извършва оценка на въздействието (оценка на риска), като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни. За да се минимизират рисковете за личните данни, както и рисковете за нанасяне на вреди на лицата, чиито данни се обработват, се предприемат всички или някои от следните технически мерки:

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Премахване на права на достъп за USB и други преносими носители с памет;
- Антивирусен софтуер и защитни стени;
- Правата за достъп основани на роли, включително тези на назначен временно персонал
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурност на локални и широкообхватни мрежи;

- Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;
- Идентифициране на подходящи международни стандарти за сигурност подходящи за СЕМ.

За да се минимизират рисковете за личните данни, както и рисковете за нанасяне на вреди на лицата, чиито данни се обработват, се предприемат всички или някои от следните организационни мерки:

- Осигуряване на подходящо обучение;
- Извършване на проверки за надеждността на служителите (атестационни оценки, препоръки и т.н.);
- Идентифициране на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Извършване на проверки 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“ ;
- Съхраняване на хартия на базата данни в заключващи се стенни шкафове или определени помещения;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Ограничаване на използването от служителите на лични устройства на работното място;
- Приемане на ясни правила за създаване и ползване на пароли;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса;
- Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

7. Спазване на принципа на отчетност

Съвет за електронни медии гарантира отговорното спазване на принципите за защита на данните чрез прилаганите от него политики по защита на данните, внедряване на подходящи технически и организационни мерки, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни.

V. Права на субектите на данни

1. Субектите на данни имат следните права по отношение на обработването на данни, както и на данните, които се записват за тях:

- Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни.
- Да поиска копие от своите лични данни от администратора;
- Да иска от администратора коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
- Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");
- Да иска от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани.;
- Да направи възражение срещу обработване на негови лични данни;

- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг.
- Да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на ОРЗД е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;
- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие.

2. СЕМ осигурява условия, които да гарантират упражняването на тези права от субекта на данни:
- Субектите на данни могат да направят искания за достъп до данни, както е описано в процедурата за Процедура за управление на исканията от субектите;
- Субектите на данни имат право да подават жалби до СЕМ, свързани с обработването на личните им данни, обработването на искане от субекта на данни и обжалване от страна на субекта на данни, относно начина на обработване на жалбите в съответствие с Процедура за начините на комуникация при жалби и искания от субекта на данни.

VI. Съгласие

1. Под „съгласие“ Съветът за електронни медии ще разбира 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. Субектът на данните може да оттегли своето съгласие по всяко време.

2. Съветът за електронни медии разбира под "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

3. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие за дейностите по обработване.

4. За специални категории данни трябва да се получи изрично писмено съгласие Процедура по получаване на съгласие за обработване на лични данни на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

5. В повечето случаи съгласието за обработка на лични и специални категории данни се получава рутинно от Съвета за електронни медии, като се използват стандартни документи за съгласие.

6. Когато Съветът за електронни медии обработва лични данни на деца, трябва да бъде

получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 16 години (освен ако държавата-членка не е предвидила по-ниска възрастова граница, която не може да бъде по-ниска от 13 години).

VII. Сигурност на данните

1. Всички служители са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които СЕМ държи, както и че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако Съветът за електронни медии не е дал такива права на тази трета страна, като са сключили договор/клауза за поверителност.

2. Всички лични данни са достъпни само за тези, които се нуждаят от тях, а достъпът се предоставя само в съответствие с изградените правила за контрол на достъпа. Всички лични данни се третират с най-голяма сигурност и се съхраняват посредством някои от следните способи:

- в самостоятелна стая с контролиран достъп и/или в заключен шкаф или в картотека, и/или
- ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания, посочени в организационните и технически мерки за контролиране на достъпа до информация, и / или
- съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

3. СЕМ създава организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители.
СЕМ изисква от всички служители да бъдат обучени и да приемат съответните договорни клаузи/декларация за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

4. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа по поддръжката на клиенти, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол.

5. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедура за съхраняване и унищожаване на данните. Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила/процедури.

6. Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

VIII. Разкриване на данни

1. СЕМ осигурява условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността извършвана от организацията.
СЕМ осигурява на служителите специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от длъжностното лице за защита на данните.

IX. Съхраняване и унищожаване на данните

1. Съвет за електронни медии не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

2. Съвет за електронни медии може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

3. Периодът на съхранение за всяка категория на лични данни е изложен в Процедура за съхраняване и унищожаване на данните.

4. Процедура за съхраняване и унищожаване на данните ще се прилага във всички случаи.

5. Личните данни се унищожават сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

X. Регистър на обработванията на данни (инвентаризация на данните)

1. СЕМ е създал процес на инвентаризация на данните като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламента. При инвентаризацията на данните в Съвета и в работния поток от данни се установяват:

- бизнес процесите, които използват лични данни;
- източниците на лични данни;
- броя на субектите на данни;
- описание на категориите лични данни и елементите на във всяка категория;
- дейностите по обработване;

- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването;
- получателите или категориите получатели на личните данни;
- основните системи и места за съхранение;
- всички лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

2. Съветът за електронни медии е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. Съветът за електронни медии оценява нивото на риска за лицата, свързани с обработването на личните им данни. Извършва оценки на въздействието върху защитата на данните във връзка с обработването на лични данни.

4. Съветът за електронни медии управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с тези правила.
Когато вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване СЕМ извършва оценка на въздействието на предвидените операции по обработване върху защитата на личните данни. Една обща оценка на въздействието може да разглежда набор от подобни операции по обработване, които представляват подобни високи рискове.

5. Когато в резултат на Оценката на въздействието е ясно, че Съветът за електронни медии ще започне да обработва лични данни, които поради висок риск биха могли да причинят вреди на субектите на данни, решението дали обработването да продължи или не, ще бъде предадено за преглед от страна на длъжностното лице за защита на данните.

6. Ако длъжностното лице по защита на данните има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да информира за въпроса КЗЛД.