Доставка на софтуер - особености и процеси

Тема №4

Разпространени стандарти и регулации, гарантиращи определени характеристики на даден продукт и услуга

Част 4: GDPR

Съдържание

1 Въведение

В тази лекция ще се фокусираме върху защитата на личните данни като разгледаме Общият регламент за защита на личните данни (GDPR / General Data Protection Regulation) - Регулация (ЕС) 2016/679. Въпреки че е съставен и приет от Европейския съюз (ЕС), той налага задължения на организации навсякъде, в случай че те са насочени към или събират данни, свързани с лица в ЕС. Регламентът влиза в сила на 25 май 2018 г. GDPR налага строги глоби на тези, които нарушават неговите стандарти за поверителност и сигурност, като глобите могат да достигнат до десетки милиони евро.

GDPR не е просто законодателство; това е катализатор за промяна в начина, по който обществото и бизнесът разглеждат личната неприкосновеност и защитата на личните данни. Регламентът има за цел да укрепи правата на гражданите в Европейския съюз в ерата на дигиталните технологии и глобалния обмен на данни.

С дигитализацията и глобализацията на световната икономика и ежедневието на индивидуалните хора възникват нови предизвикателства, свързани със защитата на личните данни. GDPR представлява

отговор на тези предизвикателства, като въвежда стриктни стандарти и изисквания за организациите, обработващи лични данни.

2 Ключови дефиниции

Глава 1, член 4 въвежда основните дефиниции на GDPR. Ще разгледаме ключовите.

- **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;

- **Обработване** - 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;

- **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;

- **Псевдонимизация** - обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

- **Администратор** - 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 Съюза 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;

- **Обработващ лични данни** - физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

- **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;

- **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;

- **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;

- **Задължителни фирмени правила** - политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност;

3 Принципи

GDPR дефинира 7 принципа отнасящи се до обработката на личните данни. Те са:

1. **Законосъобразност, добросъвестност и прозрачност** - личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните;

2. **Ограничение на целите** - личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели;

3. **Свеждане на данните до минимум** - личните данни са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;

4. **Точност** - личните данни трябва да са точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

5. **Ограничение на съхранението** - личните данни трябва да бъдат съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в GDPR с цел да бъдат гарантирани правата и свободите на субекта на данните;

6. **Цялостност и поверителност** - личните данни трябва да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;

7. **Отчетност** - администраторът носи отговорност и е в състояние да докаже спазването на изброените по-горе принципи.

4 Как да постигнем законосъобразна обработка на личните данни?

Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

- субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели (администратора ще трябва да може да докаже получаването на това съгласие);

- обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

- обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

- обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

- обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;
- обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

5 Относно съгласието

Съществуват строги правила относно какво представлява съгласие от страна на субекта на данни за обработката на тяхната информация.

- Съгласието трябва да бъде "дадено свободно, конкретно, информирано и ясно"
- Заявките за съгласие трябва да бъдат "ясно отличими от другите въпроси" и представени "на ясен и разбираем език"
- Субектите на данни могат да оттеглят предварително даденото съгласие по всяко време, и администраторите трябва да уважите техните решения
- Деца под 13 години могат да дават съгласие само с разрешение от родителите си
- Трябва да се съхраняват писмени доказателства за съгласието

6 Права на субекта на данни

Съществуват осем права, които GDPR предоставя на всички граждани на Европейския съюз:

1. **Право на информация** - Това право осигурява на субектите на данни ясна и разбираема информация относно начина, по който техните лични данни се събират, обработват и използват.
2. **Право на достъп** - Субектите на данни имат право да получат потвърждение дали личните им данни се обработват и да получат достъп до тези данни, както и към допълнителна информация за тяхната обработка.
3. **Право на корекция (право на промяна)** - Това право дава възможност на субектите на данни да коригират неточни или непълни данни, свързани с тях.
4. **Право на изтриване** - Известно още като "правото да бъдеш забравен", това право дава възможност на субектите на данни да поискат изтриване на своите лични данни, особено когато те вече не са необходими за първоначалната цел на обработката.
5. **Право на ограничаване на обработката** - Субектите на данни имат право да ограничат обработката на техните лични данни в определени обстоятелства, като например когато са изтъкнали неточността на данните.
6. **Право на пренос на данни** - Това право дава възможност на субектите на данни да получат своите лични данни в структуриран, общо използван и машинно четим формат и да ги предоставят на друг администратор на данни.
7. **Право на възражение** - Субектите на данни имат право да възразят срещу обработката на техните лични данни в определени обстоятелства, включително при профилиране и за научни или статистически цели.
8. **Права във връзка с автоматизирано вземане на решения и профилиране** - Субектите на данни имат права във връзка с автоматизирани решения, които ги засягат, включително право да не бъдат обект на решения, базирани само на автоматизирана обработка, ако тези решения имат значително въздействие върху тях.

7 Регистри на дейностите по обработване

Всеки администратор и — когато това е приложимо — представител на администратор поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа следната информация:

- името и координатите за връзка на администратора и — когато това е приложимо — на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива;
- целите на обработването;
- описание на категориите субекти на данни и на категориите лични данни;
- категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни - документация за подходящите гаранции;
- когато е възможно, предвидените срокове за изтриване на различните категории данни;
- когато е възможно, общо описание на техническите и организационни мерки за сигурност.

Всеки обработващ лични данни и — когато това е приложимо — представителят на обработващия лични данни поддържа регистър на всички категории дейности по обработването, извършени от името на администратор, в който се съдържат:

- името и координатите за връзка на обработващия или обработващите лични данни и на всеки администратор, от чието име действа обработващият лични данни и — когато това е приложимо —на представителя на администратора или обработващия лични данни и на длъжностното лице по защита на данните;
- категориите обработване, извършвано от името на всеки администратор;
- когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни - документация за подходящите гаранции;
- когато е възможно, общо описание на техническите и организационни мерки за сигурност.

Горепосочените регистри се поддържат в писмена форма, включително в електронен формат. При поискване, администраторът или обработващият лични данни и — когато това е приложимо — представителят на администратора или на обработващия личните данни, осигуряват достъп до регистъра на надзорния орган.

Задълженията за наличие на регистри не се прилагат по отношение на предприятие или дружество с по-малко от 250 служители, освен ако има вероятност извършваното от тях обработване да породи риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва специални категории данни или лични данни, свързани с присъди и нарушения.

8 Сигурност на личните данни

8.1 Сигурност на обработването

Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни трябва да прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, когато е целесъобразно, като:

- псевдонимизация и криптиране на личните данни;

- способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
- способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
- процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

Придържането към одобрен кодекс за поведение или одобрен механизъм за сертифициране може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно предходното изискване.

Администраторът и обработващият лични данни трябва да предприемат стъпки всяко физическо лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до лични данни, да обработва тези данни само по указание на администратора, освен ако от въпросното лице не се изисква да прави това по силата на правото на Съюза или правото на държава членка.

8.2 Уведомяване на надзорния орган за нарушение на сигурността на личните данни

В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, трябва да уведоми за нарушението на сигурността на личните данни надзорния орган, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

В уведомлението се съдържа най-малко следното:

- описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

Администраторът трябва да документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали са спазени съответните изисквания.

8.3 Съобщаване на субекта на данните за нарушение на сигурността на личните данни

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, трябва да съобщи на субекта на данните за нарушението на сигурността на личните данни. В съобщението до субекта на данните на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко следната информация и свързани мерки:

- посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Такова съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

- администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
- администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
- то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, надзорният орган може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията, изброени току що.

9 Оценка на въздействието върху защитата на данните (Data Protection Impact Assessment (DPIA))

Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове. При извършването на оценка на въздействието върху защитата на данните администраторът иска становището на длъжностното лице по защита на данните, когато такова е определено. Оценката на въздействието върху защитата на данните се изисква по-специално в случай на:

- 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;
- мащабно обработване на специални категории данни или на лични данни за присъди и нарушения; или
- систематично мащабно наблюдение на публично достъпна зона.

Надзорният орган съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните. Надзорният орган може също да състави и оповести списък на видовете операции по обработване, за които не се изисква оценка на въздействието върху защитата на данните.

Оценката съдържа най-малко:

- системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
- оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

- оценка на рисковете за правата и свободите на субектите на данни; и
- мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на GDPR, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

Когато е целесъобразно, администраторът се обръща към субектите на данните или техните представители за становище относно планираното обработване, без да се засяга защитата на търговските или обществените интереси или сигурността на операциите по обработване.

При необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване.

Администраторът се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска. Когато надзорният орган е на мнение, че планираното обработване нарушава GDPR, особено когато администраторът не е идентифицирал или ограничил риска в достатъчна степен, надзорният орган в срок до осем седмици след получаване на искането за консултация дава писмено становище на администратора или на обработващия лични данни, когато е приложимо, като може да използва всяко от правомощията си. Този срок може да бъде удължен с още шест седмици предвид сложността на планираното обработване. Надзорният орган информира администратора и, когато е приложимо, обработващия лични данни за такова удължаване в срок от един месец от получаване на искането за консултация, включително за причините за забавянето. Тези срокове може да спрат да текат, докато надзорният орган получи всяка евентуално поискана от него информация за целите на консултацията.

Когато се консултира с надзорния орган, администраторът предоставя на надзорния орган следната информация:

- където е приложимо — информация за съответните отговорности на администратора, съвместните администратори и обработващите лични данни, които се занимават с обработването, по-конкретно при обработване на данни в рамките на група предприятия;
- целите на планираното обработване и средствата за него;
- предвидените мерки и гаранции за защита на правата и свободите на субектите на данни съгласно GDPR;
- където е приложимо, координатите за връзка на длъжностното лице по защита на данните;
- оценката на въздействието върху защитата на данните;
- всякаква друга информация, поискана от надзорния орган.

Държавите членки се консултират с надзорния орган по време на изготвянето на предложения за законодателни мерки, които да бъдат приети от националните парламенти, или на регулаторни мерки, основани на такива законодателни мерки, които се отнасят до обработването.

Те също може да изисква от администраторите да се консултират с надзорния орган и да получават предварително разрешение от него във връзка с обработването от администратор за изпълнението на задача, осъществявана от администратора в полза на обществения интерес, включително обработване във връзка със социалната закрила и общественото здраве.

10 Сертификация

Насърчава се създаването на механизми за сертифициране за защита на данните с цел да се демонстрира спазването на GDPR при операциите по обработване от страна на администраторите и обработващите лични данни. Отчитат се конкретните нужди на микропредприятията, на малките и средните предприятия. Сертифицирането е доброволно и е достъпно чрез процедура, която е прозрачна. То не води до намаляване на отговорността на администратора или на обработващия лични данни за спазване на GDPR и не засяга задачите и правомощията на надзорните органи.

Сертифицирането се издава от сертифициращите органи или от компетентния надзорен орган, въз основа на критериите, одобрени от компетентния надзорен орган или от Комитета (European

Data Protection Board (EDPB). Когато критериите са одобрени от Комитета, това може да доведе до единно сертифициране — "Европейски печат за защита на данните" (European Data Protection Seal).

Администраторът или обработващият лични данни, който подлага своето обработване на механизма за сертифициране, осигурява на сертифициращия орган или ако е приложимо — на компетентния надзорен орган, цялата информация и достъп до своите дейности по обработване, които са необходими за извършване на процедурата по сертифициране.

Сертификатът се издава на администратора или обработващия лични данни за максимален срок от три години и може да бъде подновен при същите условия, ако съответните изисквания продължават да са спазени. Сертификатът се оттегля, ако е приложимо, от сертифициращите органи или от компетентния надзорен орган, ако изискванията за сертифицирането не са спазени или вече не се спазват.

11 Заключение

GDPR е може би най-разпознаваемата регулация, касаеща силно софтуерния сектор. Приложимостта ѝ към всяка една фирма обработваща лични данни на поне един гражданин на ЕС я правят изключително популярна и масова срещана във всякакви фирми с най-различно естество на продуктите и услугите им.