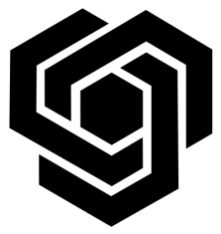
**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**



**Курсов проект**

Дисциплина*: Мрежова и информационна сигурност*

Тема: *Препоръки по внедряването на GDPR в организация.*

Изготвил:

Христо Ботушанов, 222гр., факултетен №: 121319046

Contents

[Какво е GDPR? 3](#_Toc42818096)

[Какви са целите на GDPR? 3](#_Toc42818097)

[КАК GDPR ще се отрази на малкия бизнес? 3](#_Toc42818098)

[Защо изискванията за спазване на GDPR са важни? 4](#_Toc42818099)

[Какви са последствията от неспазването на изискванията на GDPR? 5](#_Toc42818100)

[Как мога да подготвя моята организация за внедряване на GDPR? 5](#_Toc42818101)

[Одитирайте данните си и ги анализирайте 5](#_Toc42818102)

[Нека вашите клиенти знаят за GDPR 6](#_Toc42818103)

[Прегледайте Вашите известия за поверителност 7](#_Toc42818104)

[Разберете правата на Потребителя 7](#_Toc42818105)

[Подпомагане трансфери на данни 9](#_Toc42818106)

[Планиране за нарушения на данните 9](#_Toc42818107)

[Извод 10](#_Toc42818108)

[Източници 11](#_Toc42818109)

# Какво е GDPR?

GDPR e регламент за защита на данните е новаторски регламент, приет от Европейския съюз на 25 май 2018 г. Мярката има за цел да защити данните и поверителността на всички лица в Европейския съюз и около Европейското икономическо пространство. Регламентът също така работи за контрол на преминаването на данни извън тези области. В този документ ще опиша всичко, което трябва да бъде взето впредвид при имплементиране на GDPR.

## Какви са целите на GDPR?

GDPR замества предишната инициатива за данни, която ЕС имаше, Директивата за защита на данните 95/46 / ЕО. GDPR беше приет предимно с цел да се уеднаквят законите за поверителност на данните в Европа и да се осигури поверителност на данните за всички европейски граждани. Може би най-същественият е фактът, че законопроектът се стреми да преразгледа начина, по който финансовите институции и бизнесите в Европа подхождат към поверителност на данните.

Широкото законодателство засяга компании, които може да нямат физическо присъствие в Европейския съюз. Например, компания от Съединените щати, която събира данни по интернет чрез присъствие в мрежата в ЕС, се подчинява на регламентите.

В крайна сметка мярката контролира как можете финансовите институции да събират данни за своите клиенти. Той определя какви данни финансовите институции могат да получат и по-важното какви данни могат да съхраняват. Например, за да останат съобразени с GDPR, сега компаниите трябва да гарантират, че те отговарят на конкретни насоки при събиране на лични данни.

Те трябва също така да гарантират, че тези, които управляват данните, ще ги защитават от експлоатация. Ако не го направите, това ще доведе до строги санкции, до 4 процента от брутните приходи. Мерките трябва да помогнат за защита на потребителите в бързо развиващия се технологичен свят. Съществува значително повече юридическа отговорност върху организациите, отговорни за нарушение.

## КАК GDPR ще се отрази на малкия бизнес?

GDPR вероятно ще повлияе на всички бизнеси по някакъв начин. Ако сте собственик на малък бизнес в Европейския съюз, вероятно има няколко неща, които ще искате да разгледате. Първо и най-важното, ще трябва да бъдете в крак с нашите клиенти. Първото нещо, което трябва да направите, е да съберете съгласието си да получават имейли от вас. Също така ще искате да потърсите юридически съвет, който да преразгледа условията за услуги и политиките за поверителност, като гарантира, че те отговарят на новите разпоредби.

Също така ще искате да съставите план, който да определи кои данни ще събирате и как ще защитите данните, които се съхраняват. Малките фирми вероятно ще искат да спестят възможно най-малко данни. Жилището на големи хранилища за данни може бързо да стане скъпо. Освен това, компаниите биха били изложени на сериозна опасност, ако имаше нарушение на сигурността.

Може да има по-голям смисъл за малкия бизнес да инвестира в технология за разпознаване на лица в реално време, вместо да инвестира в сигурни решения за данни. По този начин гарантирайте, че компаниите все още са съобразени с разпоредбите на Know Your Customer. За щастие, KYC технологията се развива бързо. Например, камери за смартфони с две лещи позволяват на собствениците на малкия бизнес да проверяват идентичността на издадена от правителството холограма в реално време, без да се налага да събират или съхраняват никакви данни.

Едно от подобни неща, което трябва да се има предвид, е фактът, че съгласно GDPR потребителите могат да поискат изтриването на тяхната информация по всяко време. Има голям шанс все повече и повече потребители да се облегнат на това. По този начин малките предприятия не трябва да разчитат на жилища и съхраняване на тези данни, за да извършват ежедневни бизнес начинания. Каквато и информация да съхранява фирмата, трябва да бъде:

* Достъпна
* Преносима
* Завършена
* Точна

Какъвто и да е план на собствениците на малък бизнес, те ще искат да го съобщят на своите клиенти. Те трябва да изяснят мотивите си за съхраняване на данните и как ще ги запазят. Прозрачността ще извърви дълъг път към изграждане на доверие на клиентите.

И накрая, собствениците на малък бизнес ще искат да имат система в случай, че някога е имало нарушение на сигурността. Собствениците трябва да знаят кого трябва да уведомяват в случай на съмнение за нарушение и какво ще направят в часовете след откриването му. Прилагането на тези мерки ще извърви дълъг път към гарантиране, че малките предприятия са съобразени с GDPR.

# Защо изискванията за спазване на GDPR са важни?

Въвеждането на GDPR започна на 25 май 2018 г. с цел да се постави повече контрол и защита в ръцете на потребителите. Поверителността на данните в последно време се превърна в огромна загриженост и начинът, по който марките защитават своите клиенти, сега ще бъде в центъра на вниманието поради внедряването на GDPR. Идеята е да се подобри значително нивото на защита, предлагано на гражданите на ЕС, и техните данни. Той е изграден въз основа на изискванията на Директивата от 1995 г., но новите изисквания за спазване на GDPR ще бъдат по-строги и ще налагат по-строги наказания за всеки, който я наруши.

# Какви са последствията от неспазването на изискванията на GDPR?

От една страна щетите за компаниите ще бъдат парични. Компаниите, които не спазват изискванията за спазване на GDPR, могат да бъдат глобени до 20 милиона евро или до 4% от годишния световен оборот за предходната финансова година, в зависимост от това коя е по-голяма.

Глобите засягат както големите, така и малките и средни компании: в първия предварителен доклад Европейският съвет за защита на данните съобщава, че средната глоба на GDPR е била около 66 000 евро, с изключение на глобата от 50 милиона евро, получена от Google от френската агенция за защита на данните.

От друга страна, неспазването на изискванията на GDPR ще повлияе на имиджа на марката. Вашата организация може да има опетнена репутация и много потребители ще загубят вяра както във вашите продукти, така и в услугите.

Последните изследвания на Dentsu Aegis Network [3] показаха, че злоупотребата с лични данни е причина номер едно за недоверие в технологичната индустрия за 64% от хората. Друго проучване на IBM [4] установи, че около 85% от потребителите в САЩ смятат, че предприятията трябва да бъдат по-активни в защитата на своите данни, само 20% биха „напълно се доверили“ на организация, боравеща с личните им данни, а внушителните 75% от хората не биха искали Не купувам от компания, на която не се доверяват, за да защити своите данни, независимо колко добър е нейният продукт или услуга.

Накратко, неспазването на изискванията за спазване на GDPR ще принуди вашия бизнес в проблемна ситуация и в крайна сметка ще навреди на вашата организация. Наказанията са умишлено сурови, за да се гарантира, че всички организации следват стратегия за прилагане на GDPR.

# Как мога да подготвя моята организация за внедряване на GDPR?

За да улесните вашия бизнес да спазва изискванията за спазване на GDPR, важно е да започнете да планирате предварително, докато все още можете. За да ви помогнем да се подготвите за внедряване на GDPR, очертахме няколко от най-важните точки, които трябва да следвате.

## Одитирайте данните си и ги анализирайте

Регламентите за данни не трябва да се разглеждат като проклятие за бизнеса, а по-скоро като възможност за подобряване на качеството на събраните данни.

Въпреки че мнозина подозират, че GDPR ще има големи последствия срещу програмната реклама, в Обединеното кралство 67% [5] от специалистите в дигиталните медии са съгласни, че те действително увеличават програмните си разходи и същото важи за всички останали страни в Европа.

Маркетинг мениджърите във всички организации могат да използват този момент, за да преосмислят маркетинговата си стратегия около това, какви данни наистина имат значение за стимулиране на продажбите и какъв е най-добрият начин за събирането им. В същото време те могат да спрат да събират несъществени данни.

Много организации изглежда мислят в тази насока: според проучване, проведено от Института за бизнес стойност на IBM, 59% [6] от анкетираните ръководители казват, че GDPR е възможност „да предизвика нови бизнес модели, управлявани от данни“.

Интелигентното внедряване на GDPR означава да разгледате данните, които имате, и да се опитате да ги разберете, защо ги имате и за какво се използват. Попитайте вашия екип как се събира информацията и с кого се споделя. Определете различните видове данни, които имате, и връзките, които има с други сайтове, компании или дори услуги. Това е изключително отговорна задача, така че изисква да комбинирате всеки един елемент от вашата система, за да гарантирате, че той е в рамките на изискванията за спазване на GDPR.

Ето няколко въпроса, които трябва да си зададете:

* **От кого** събираме данни? **Кой** има достъп до тези данни? **Кой** е този, който го сортира и компилира в използваеми данни?
* **Какви** данни събираме? **Какви** предпазни мерки и механизми имаме за защита на личните данни, така че да не попаднат в грешни ръце?
* **Кога** събираме данни? За **колко време** планираме да ги запазим? Ще споделяме ли информацията, която имаме, с други системи?
* **Къде** съхраняваме данни? Съхранява ли се **локално** и се компилира автоматично или го прехвърляме към **трета страна**?
* **Защо** събираме данни? Смятаме ли, че информацията, която събираме е **полезна**? Използва ли се по **основателна причина**?
* **Как** събираме данни? **Как** смятаме да го обработим в бъдеще? **Колко дълго** съхраняваме данните си?

Тези въпроси трябва да формират основата на стратегията за прилагане на GDPR на всяка организация.

## Нека вашите клиенти знаят за GDPR

Друга важна стъпка към безопасното управление на личните данни е да бъдете прозрачни със собствените си клиенти. Същият доклад на IBM [6], споменат по-рано, подчертава, че 96% от лидерите на GDPR смятат, че спазването на GDPR може да се използва като източник на диференциация, тъй като това ще се разглежда като положителен атрибут от обществото. Според проучване на Otonomo и SBD Automotive [7], прозрачността и доверието са от решаващо значение за изграждането на доверие между компаниите и потребителите, като 60% от интервюираните казват, че за тях е много важно да се каже точно какви данни се събират, от кого и за какво какви цели.

Повечето хора не биха знаели нещо за прилагането на GDPR или как това ги засяга. В резултат на това може да искате да се свържете с тях по имейл или дори в социални медии и да повишите информираността за това какво представлява, как смятате да го прилагате и какви промени могат да очакват да видят.

Това не само ще се отрази на това колко лично знаете за внедряването на GDPR, но и може да повлияе значително на начина, по който клиентите ви виждат. Ако можете да привлечете аудиторията си на своя страна, следването на изискванията за спазване на GDPR може да има дълбоко въздействие върху доверието на потребителите и в крайна сметка да подобри репутацията ви.

## Прегледайте Вашите известия за поверителност

Изискванията за спазване на GDPR съдържат списък от изисквания, на които трябва да отговарят всички известия за поверителност, ако събирате данни. Това включва следното:

* Посочете дейностите по обработка, които се извършват по всяко време, когато събирате лични данни
* Ако личните данни не се получават директно, информирайте какви дейности по обработка се извършватИзвестията трябва да присъстват винаги, когато се събират лични данни и във всички точки
* Данните трябва да включват самоличността на администратора и на служителя по защита на данните, колко дълго ще се съхраняват, правата, които потребителят има, правото да подаде жалба, получателите и прехвърлянето на данни, изявление, което потребителят има правото да оттеглите съгласието си по всяко време, а също и обяснение защо вие или трета страна желаете да събирате данните.

## Разберете правата на Потребителя

За да следвате изискванията за спазване на GDPR [8], също така е важно да разберете правата, които потребителят има върху своите данни. Когато изпълнението на GDPR е активно, трябва да демонстрирате, че можете да направите следното:

* Потвърдете самоличността на всеки, който иска данните
* Дайте на потребителите възможност да изискват личните си данни
* Отговаряйте на искания за достъп до лични данни
* Проследете и потърсете личните данни на потребителите и ги предоставете в рамките на 30 дни
* Поискайте поправка и коригирайте всички събрани лични данни
* Поискайте изтриване на лични данни на потребителя
* Разберете към кои допълнителни данни на контролерите са били прехвърлени
* При нарушение на данните се свържете с тези субекти, за да ги изтриете
* Искане на ограничението за обработка на данни и покажете как и кога се прави това
* Искане на копия и предаване на лични данниНамерете личните данни и ги компилирайте в машинно четими формати
* Дайте на потребителите начин да възразят срещу събирането на техните данни
* Спрете цялата обработка на данни и демонстрирайте тяхното съответствие

Това са стандартните права, които трябва да бъдат разбрани от всички организации, които спазват изискванията за спазване на GDPR. Ако не го направите, това ще доведе до големи глоби, така че не забравяйте да разберете тези принципи.

Поддържайте актуализираните си аудитории въз основа на консенсус

Едно от изискванията за компаниите да отговарят на GDPR е да гарантират, че аудиториите, насочени за маркетингови цели, винаги се актуализират според потребителския консенсус, който трябва да бъде насочен.

Това трябва да бъде осигурено както за нови контакти, така и за контакти, които са изразили съгласието си преди 25 май 2018 г. Всъщност според GDPR, ако съгласието, предоставено от лице преди прилагането на Общия регламент за защита на данните (GDPR), е в съответствие с условията на GDPR, тогава не е необходимо отново да се иска съгласието на лицето. "

Потребителите също имат право да оттеглят съгласието си по всяко време и компаниите трябва да спазват тяхното решение, като ги изключват от всякакви маркетингови кампании. Това може да бъде предизвикателство особено за големи организации, които се занимават със сегменти от аудитории с голям обем в стотици активни кампании, които никога не могат да актуализират файловете на аудиторията ръчно всеки път, когато хората оттеглят съгласието си.

В тази връзка, най-добрият начин за компаниите да следят консенсуса на потребителите и съответно да актуализират целевите аудитории е автоматично да синхронизират своите аудитории и кампании чрез надежден софтуер на трети страни, като LeadsBridge [9].

LeadsBridge оперира с конвертиране на лични данни в HASHED ключове в реално време (в VCPU паметта), без да съхранява чувствителни данни на никое място, предлагайки на компаниите решение за защита на поверителността, за да поддържат непрекъснато актуализираната си аудитория при консенсус на потребителите.

Назначаване на служител по защита на данните

Като част от изискванията за спазване на GDPR се изисква служител по защита на данните във всяка компания, която обработва информация и данни в голям мащаб. Те ще трябва да направят следното:

* Поддържайте одитните следи и демонстрирайте отчетност и съответствие
* Поддържайте инвентаризация на данните, която категоризира потребителите
* Поддържайте подлежащи на проверка следи от обработващата дейност
* Извършвайте оценки на въздействието върху защитата на данните
* Наблюдавайте спазването на законите за защита на данните
* Свързват и подпомагат надзорните органи.

Ако не спазвате тези изисквания за спазване на GDPR, това може да доведе до тежко наказание, така че ще трябва да наемете нов служител или да назначите съществуващ такъв на тази роля. Поради необходимото обучение, би било разумно да се направи това възможно най-скоро като част от процеса на прилагане на GDPR.

## Подпомагане трансфери на данни

В изискванията за спазване на GDPR се посочва, че потребителите трябва да имат възможност да предават данни на себе си, когато пожелаят. Това означава, че ще трябва да върнете техните лични данни във всеки даден момент, така че трябва да сте напълно способни да компилирате информацията, която имате за всеки потребител, в машинно четим формат. По този начин можете лесно да прехвърляте техните данни към друг контролер на данни.

Ако вашите потребители искат техните данни, тогава трябва да ги задължите и да им ги изпратите в опростен и четим формат, който те могат да разберат. Ще трябва да говорите с всички софтуерни инженери или технологични консултанти, които наемате, за да създадете стратегия за внедряване на GDPR, която позволява този лесен трансфер на данни. Ако не се спазва това, това може да наруши изискванията за спазване на GDPR и да доведе до глоба.

## Планиране за нарушения на данните

Нарушаването на данни може да създаде огромни законови, финансови и репутационни неразположения, които могат да навредят на организацията и трябва да бъдат избягвани при разработването на стратегия за прилагане на GDPR. Поради това не трябва да е изненада, че сигурността на данните е важно съображение в GDPR и изисква да спазвате съответните процедури, за да отговаряте на изискванията за спазване на GDPR.

* Трябва да можете да осигурите механизми за псевдонимизиране, криптиране и защита на личните данни
* Трябва да приложите допълнителни мерки за сигурност
* Трябва да можете да потвърждавате текущата конфиденциалност, цялостност и наличност на лични данни
* Трябва да осигурите механизми за възстановяване на достъпа и наличността на личните данни
* Трябва да можете да улеснявате редовното тестване на вашите мерки за сигурност
* Трябва да сте в състояние да уведомите органа за защита на данните в рамките на 72 часа в случай на инцидент с нарушение на данните
* Трябва да можете да уведомите засегнатите потребители в случай на нарушение на високорискови данни

Това са невероятно важни точки, които трябва да се спазват, ако се съгласите с изискванията за спазване на GDPR. Отново, ако не го направите, това ще доведе до много сериозни последици, които в крайна сметка биха могли да навредят на вашия бизнес. Разумно е да следвате тези стъпки, за да планирате стратегията си за внедряване на GDPR и да разберете, че навлизаме в нова ера, в която потребителите контролират поверителността на техните данни. Въпреки това, както при всички бизнес възможности, подходът към това от правия ъгъл може да ви даде предимство във вашата индустрия.

# Извод

GDPR промени света на рекламата, като регулира начина, по който предприятията и потребителите придобиват и споделят лична информация. Въпреки че първоначално се възприема като ограничение за бизнеса, числата показват друго.

Данните от потребители увеличават своята стойност с времето. Това е причината да внимаваме за тяхното съхраняване. Пробив в системата би могъл да доведе до не само до вреда към самите потребител, той също така може да доведе и до загуба на доверието от компанията отговорна за самите данни. Загубата на доверие в повечето случаи води до намаление на клиентите и опетняване на името на компанията.

Импементиране на новите мерки, изискани в този закон, налага определени инвестиции във време и средства. Обаче ако всичко бъде имплементирано според регулации, можем да комуникираме ефективно с своите клиенти, по този начин клиентите могат уверено да използват услугите на бизнеса без да се тревожат за своите данни.

# Източници

1. https://www.au10tix.com/blog/what-is-gdpr/
2. https://leadsbridge.com/blog/guides/gdpr-compliance-implementation-for-dummies-all-the-requirements-and-things-to-do/
3. https://www.oxfordeconomics.com/recent-releases/digital-society-index-2019-human-needs-in-a-digital-world
4. https://newsroom.ibm.com/2018-04-15-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security
5. https://www.emarketer.com/content/why-gdpr-didnt-inhibit-programmatic-growth-in-the-uk-as-anticipated
6. https://www.ibm.com/downloads/cas/JEMXN6LV
7. https://www.forbes.com/sites/forbescommunicationscouncil/2020/03/10/gdpr-bridging-the-gap-between-consumer-and-marketer-perceptions/#65cfa73427d4
8. https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/
9. https://lp.leadsbridge.com/