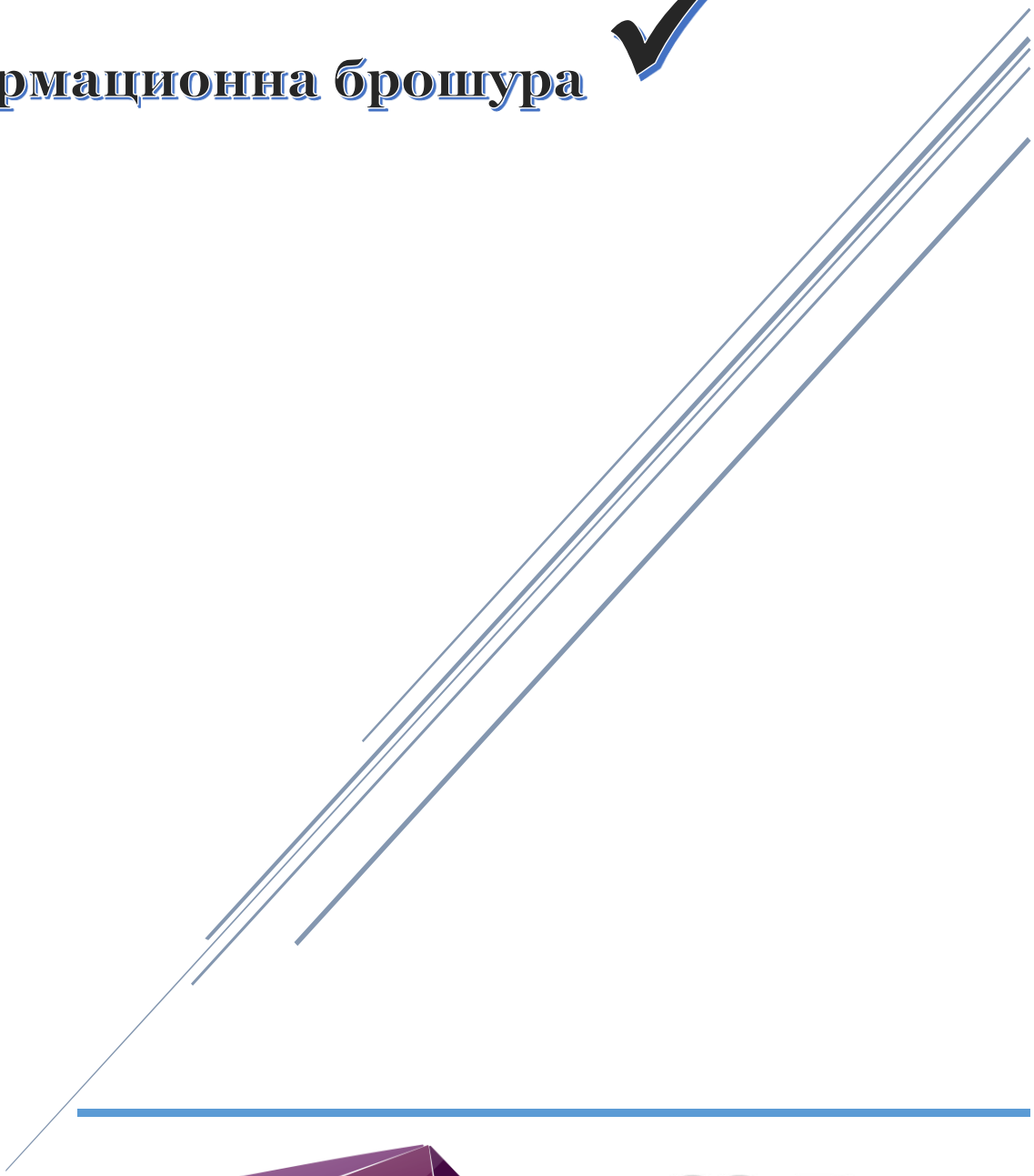
General Data Protection Regulation

GDPR

Информационна брошура



АСОЦИАЦИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

MyData

Светът ни е различен.

Глобализацията и дигитализацията, бързото технологично развитие и навлизането на нови бизнес модели превръщат личните данни във все по-важен ресурс и ги поставят във фокуса на световните икономика и пазари.

В същото време злонамерената употреба и недостатъчната защита на личните данни създават все повече заплахи за отделния човек.

Социалните и икономическите процеси в днешния свят и заплахите за гражданите мотивираха Европейския съюз да предприеме драстични мерки. Режимът за защита на личните данни днес е предмет на една от най-обсъжданите законодателни реформи, а санкциите за нарушения в тази област достигат безпрецедентни размери.

Така на 27 април 2016 г. беше приет Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на ЕС за защитата на физическите лица във връзка с обработването на лични данни и за отмяна на Директива 95/46/ЕО, придобил популярност като GDPR.

General Data Protection Regulation

GDPR

ЕДИН РЕГЛАМЕНТ, ЕДИН КОНТИНЕНТ!

✓ 25.05.2018 г.

Какво всъщност е GDPR?

GDPR е общ европейски закон, резултат от четири години усилена работа на европейските институции. Неговата роля е да защити правата на субектите на данни и да унифицира европейското законодателство във всички държави-членки.

> *"Висшето ръководство на всяка компания ще бъде държано отговорно и новият закон (GDPR) му дава 20 милиона причини да се вслушва."*
>
> *Кристофър Греъм, Британски надзорен орган за защита на личните данни*

Ще се прилага автоматично и в България от 25 май 2018 г. GDPR разширява правата на субектите на данни и въвежда редица нови задължения за администраторите и обработващите лични данни.

Освен драстичните санкции, GDPR урежда правото на гражданите на обезщетение за вреди, като това право може да бъде упражнено и по местоживеене на пострадалия. Например гражданин, живеещ в Австрия, може да потърси обезщетение пред австрийски съд, а не пред съда на държавата, в която е станало нарушението.
Не са малко и случаите, при които надзорен орган по Регламента може да бъде не националният орган, а институция от друга европейска държава.

За кого се прилага GDPR и какво трябва да се предприеме?

Почти няма компания, която да не обработва лични данни под една или друга форма. Основната цел на GDPR е да защити тези данни. Тоест, ако съхранявате или обработвате лични данни на ваши клиенти, потребители, служители, доставчици и други, Вие сте законово задължени да предприемете необходимите правни, организационни и технически мерки за защита на тези данни. Освен това всяко физическо лице има право да поиска от Вас достъп до своите лични данни, коригирането или изтриването им. Ако Вие не му отговорите до един месец, физическото лице има право на обезщетение.

GDPR се прилага за всяка организация, която събира, обработва и съхранява лични данни.

Прилага се както за администратори, така и за обработващи лични данни.

В практичен аспект това означава, че компаниите трябва да въведат промени в начините на събиране, обработване и съхраняване на личните данни.

Над 50 са мерките (организационни и технически), които, ако бъдат имплементирани, ще подпомогнат всяка организация да постигне съответствие с GDPR и съответно да го докаже.

За малките и средните предприятия GDPR предвижда някои облекчения, но това не ги освобождава от задължението им да приведат дейността си в съответствие с Регламента. Знаете ли, че според GDPR, независимо от големината на вашата компания, когато избирате доставчик на услуги (например някой, който да разработи интернет сайт или да извършва дейности по администриране на персонала), сте задължени да проверите дали той работи в съответствие с изискванията на GDPR. Така регламентът се превръща в много важен фактор за конкурентоспособността и на практика влияе върху пазарите.

Какви са рисковете?

Административните санкции по GDPR са в размер до 20 000 000 евро или 4% от годишния оборот на компанията, което от двете е по-голямо.

Тези санкции не включват загубата на доверие на клиентите и партньорите, загубата на пазарен дял, разходите за съдебни процеси, загубата на бизнес възможности.

Европейските експерти прогнозират, че надзорните органи ще съберат около 6 милиарда евро под формата на глоби през първата година от влизане в действие на GDPR.

Така защитата на личните данни в наши дни се превръща в част от необходимите условия за развиване на бизнес. Много компании ще поставят изисквания пред своите доставчици на продукти и услуги дейността им да е приведена в съответствие с GDPR като условие за търговски отношения.

Твърде висока цена за небрежност и закъснения!

GDPR – права и правомощия

Права на физическите лица:

- Право на информираност;
- Право на достъп до обработваните данни;
- Право на коригиране;
- Право на ограничаване на обработването;
- Право на преносимост на данните;
- Право на изтриване;
- Право на възражение срещу обработване на личните данни, включително при профилиране и при автоматизирано вземане на решения;
- Право на жалба

Основни правомощия на надзорните органи:

- да изискват доказателства за съответствие с GDPR;
- да налагат временни ограничения в обработването;
- да изискват уведомяване в случай на нарушение на сигурността на данните;
- да ограничават трансграничните потоци от данни;
- да налагат глоби в размер до 20 000 000 евро или 4% от годишния оборот в случай на нарушение на GDPR

След 25.05.2018 г. компаниите ще бъдат разделени на 3 типа:

1. Компании, които не спазват Регламента 

2. Компании, които спазват Регламента 

3. Компании, които спазват Регламента и могат да го докажат 

Организациите трябва да могат да докажат, че са **въвели правилните механизми в действие или** поне, че **полагат усилия в тази насока.**

Имплементиране	Съответствие	Доказване
• Въвеждане на подходящи технически и организационни мерки - чл. 24 от GDPR	• Надзорният орган може да поиска доказателства за съответствие по всяко време след влизането в сила на GDPR	• От 99 разпоредби 39 изискват доказване на съответствие

От къде да започна?

- Първо се информирайте за новите изисквания. Четейки тази информационна брошура, вече сте направили първата крачка.
- Следващата стъпка е да направите правен и технически анализ, или казано по друг начин - оценка на текущото състояние на организацията Ви. Този анализ ще Ви позволи да разберете кои са слабите места в организацията, кои области се нуждаят от промяна, подобрение или по-специално внимание.
- След анализа трябва да приемете План за действие. Планът следва да съдържа конкретните мерки, които ще предприемете и в какви срокове.
- Трябва да осигурите защита на данните още на етап проектиране и по подразбиране.
- Направете преценка дали спрямо Вашата компания е налице изискването за назначаване на длъжностно лице по защита на данните (DPO). Този служител може да е вътрешен, но може да бъде и нает от външна организация.
- Въведете всички необходими политики и процедури. Създайте други необходими документи, които да Ви помогнат да спазвате и да доказвате съответствие с Регламента.
- Запознайте служителите си с новите отговорности и стратегията на вашата организация относно защитата на личните данни.
- Извършвайте редовни проверки за реалното състояние на защитата на данни в компанията Ви и дали служителите ви изпълняват задълженията си по GDPR.

Комисията за защита на личните данни, която е националният контролен орган по Регламента, публикува на своята интернет страница 10 практически стъпки, които организациите трябва да извървят, за да имплементират GDPR.

А сега накъде?

Внимателно планирайте кой какво трябва да извърши за спазването на GDPR и в какъв времеви диапазон. Оставащото време до влизането на Регламента в действие е съвсем кратко, което означава, че срокът за организацията Ви може да се окаже недостатъчен. Процесът по имплементиране на изискванията и постигането на съответствие с Регламента може да отнеме месеци.
Този процес в общия случай преминава през следните **5 основни етапа**:

1. Вътрешен анализ. Целта на анализа е да се извърши оценка на текущото (техническо и организационно) ниво на съответствие на компанията с изискванията на GDPR;
2. Изготвяне на план за действие за отстраняване на несъответствията;
3. Имплементиране на плана. Изработване на всички необходими документи, правила и процедури за изпълнение на изискванията на Регламента и доказване на съответствие;
4. Обучение на служителите – въвеждащо и периодично;
5. Оценка и мониторинг на програмата за защита на лични данни – периодично.

Част от мерките, които трябва да бъдат предприети, са посочени изрично в GDPR, за други са дадени примери. Част от организационните мерки могат да бъдат извлечени чрез принципите и задълженията, посочени в Регламента. Някои от тях изискват коренна промяна в начините на обработване на личните данни и премоделиране на вътрешните процеси.

GDPR е комплексен регулаторен механизъм. Някой организации могат да се справят с наличния си вътрешен ресурс, докато за други е по-подходящо да използват външен експерт или екип от експерти, които да им помогнат с конкретни анализи, оценки, дейности по имплементацията, изработване на процедури и правила, поддържане на съответствието с GDPR, обучение на служители.
Независимо как ще предпочетете да подходите към GDPR, е необходимо като първа стъпка да отделите време, за да установите как вашата организация работи с лични данни и какво трябва да се предприеме.