Какво да очакваме от новата правна рамка на защитата на личните данни?

Новият Общ регламент относно защитата на данните или *General Data Protection Regulation* **(GDPR)** ще влезе в сила за всички страни-членки на ЕС на 25 май 2018 г. GDPR поднася една изключително променена правна регулация на защитата на личните данни. Това трябва да се вземе предвид от бизнеса в България максимално бързо, за да се създадат необходимите мерки и да се извърши подготовка за спазването на изискванията по новите правила.
С целия текст на GDPR можете да се запознаете **тук**.

Какви са основните промени?

Въпреки че на пръв поглед изглежда GDPR да следва подобен подход на регулиране с този на досега действащата уредба, регламентът предлага няколко значителни промени:

1. Много по-тежки санкции

GDPR значително увеличава размера на санкциите, които могат да бъдат наложени при неспазване на правилата за защита на личните данни. Санкциите за по-сериозни нарушения (напр. неспазване на правилата за трансфер на данни в държави извън ЕС, нарушаване на принципите за защита на личните данни и др.) могат да достигнат до EUR 20 млн. или **4% от общия годишен световен оборот** на администратора на лични данни (по-високата от двете суми). Съответно, санкция от EUR 10 млн. или 2% от общия годишен световен оборот на администратора (по-високата от двете суми) е предвидена за по-леки нарушения на GDPR. (Вж. чл. 83 от GDPR).

2. Разширен обхват

Целият бизнес на администратора на лични данни трябва да отговаря на изискванията на GDPR. Това важи и за **бизнеса, намиращ се извън ЕС** (когато, например, се предлагат стоки и/или услуги на физически лица в рамките на ЕС или когато организации следят поведение на жители на ЕС).

3. Изисквания за съответствие. Регистър за обработка на данни

GDPR въвежда задължение на администраторите и обработващите лични данни да демонстрират как обработката, съхранението и/или трансфера на данни се извършват в **съответствие** с принципите за защита на данните. Това включва създаването и поддържането на **регистри** за обработка на данни. Освен това, трябва задължително да се създадат **комплексни мерки и вътрешни политики** за управление на данните, за да се намали риска от незаконосъобразно обработване на лични данни (ако все още не са въведени такива). Мерките включват оценка на въздействието върху защитата на личните данни при обработка с висока степен на риск и гаранции, че защитата на данните се извършва по разработен план, а не представлява второстепенен приоритет за съответната организация (Вж. чл. 32 и следв. от GDPR).

www.ppglawyers.eu
office@ppglawyers.eu
+359 879 16 16 61

4. Допълнителни права

Правата на лицата, предоставящи своите данни, са разширени. Регламентира се правото **"да бъдеш забравен",** като едно лице може да поиска заличаване на данните си, при прилагане на определени основания. Изведено е и право да се ограничи обработка на данни при някои обстоятелства, заедно с ново право личните данни на лицата да бъдат предоставяни по начин, който позволява те да бъдат лесно прехвърляни - **преносимост на данните.**

5. Доказателства за съгласие

Когато обработката на данни се основава на съгласието на лицето, администраторът на лични данни ще трябва да **може да докаже,** че такова съгласие действително е дадено от лицето, като възможността **съгласието да се оттегли** трябва да бъде толкова лесна, колкото и даването на такова. По тази причина се изисква и дадените по старата уредба съгласия да се проверят за съвместимост с новите изисквания на GDPR. Друга възможност е директно да се премине към алтернативна правна основа за обработване на данни, като изпълнение на договор или наличие на законен интерес на администратора на лични данни.

6. Обработващ лични данни и длъжностно лице по защита на данните

Към момента, обработващите данни нямат никакви преки задължения (освен тези дадени от администратора на лични данни) и администраторът на лични данни е отговорен за всяко нарушение, извършено от неговия обработващ. GDPR **налага специфични задължения на обработващите данни,** включително за прилагане на подходящи стандарти за сигурност, осигуряване на адекватно архивиране на данни и информиране на администратора за нарушения. По тази причина обработващите данни ще бъдат и директен **обект на санкции** в случай на нарушение на GDPR. GDPR също така предвижда редица разпоредби, които трябва да бъдат включени във всички договори, свързани с обработването на лични данни. Това увеличава **регулаторната тежест и риска** за обработващите лични данни. При някои обстоятелства администратора или обработващия лични данни ще определят и **длъжностно лице по защита на данните.** Това ще се прилага преди всичко, когато обработването включва редовно и систематично наблюдение на данни в голям мащаб или е свързано с обществения сектор. Длъжностното лице по защита на данните трябва да има достатъчно познания, за да изпълняват своите функции. Длъжностно лице по защита на данните може да бъде определено и за група от предприятия.

7-те "П" или какво се очаква от бизнеса

Ако все още не сте се ориентирали в новите правила и не сте започнали подготовка за съответствието на Вашия бизнес с GDPR, сериозно Ви съветваме да направите собствена оценка на взаимодействието на бизнеса Ви с лични данни и как GDPR ще засегне неговото функциониране, както и функционирането на сектора на дейност, в който оперирате. Като се има предвид нивото на промяна в изискваните мерки и строгия санкционен режим, срокът до май 2018 може да се окаже крайно недостатъчен за някои организации. Не се колебайте да потърсите експертна консултация по право на защитата лични данни и винаги следвайте правилото на 7-те "П" - **Правилното Предварително Планиране Предотвратява Покъртителното Последващо Представяне!**

www.ppglawyers.eu
office@ppglawyers.eu
+359 879 16 16 61