Какво трябва да знаят администраторите на лични данни за задълженията си по Регламент 2016/679 на Европейския парламент и на Съвета от 27 април 2016

1. **От кога ще започне да се прилага новия 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) е обнародван в Официален вестник на Европейския съюз на 4 май 2016 г.

Общият регламент въвежда множество значителни промени спрямо действащата правна рамка и поставя завишени изисквания към субектите в системата за защита на личните данни, което е причина за неговото отложено прилагане, считано от **25 май 2018 г.**

2. Ще се прилага ли новият Регламент за администратори на лични данни, които обработват данни извън територията на Европейския съюз?

Да, с новия Регламент се разширява териториалният обхват на европейските правила за защита на личните данни и те ще важат и за администратори, които не са установени в ЕС, но обработват лични данни на граждани, които се намират в ЕС. Това ще важи в случаите, когато дейностите по обработване на данни от страна на такива администратори, са свързани с:

- Предлагането на стоки и услуги на физически лица, намиращи се в съюза, независимо дали от субекта на данни се изисква плащане;

или

- Наблюдението на тяхното поведение, доколкото това поведение са проявява в рамките на съюза.

3. Какво представлява фигурата „съвместни администратори“?

Понятието „съвместни администратори“ означава, че двама или повече администратори съвместно определят целите и средствата на обработването на лични

данни. Физическото лице, за което се отнасят данните (субект на данни), може да упражнява своите права в областта на защитата на личните данни по отношение всеки и срещу всеки от администраторите. Съвместните администратори са длъжни да определят по прозрачен начин съответните си отговорности за изпълнение на задълженията си по регламента.

4. Кои са задълженията за администраторите и обработващите лични данни спрямо новия Общ регламент за защита на данните?

Общият регламент за защита на личните данни въвежда редица задължения за администраторите и обработващи лични данни, някои от които са изцяло нови и непознати в досега действащата правна уредба. Те са :

- Обработване на данните в съответствие с принципите за защита на личните данни, заложени в регламента, като е в състояние да докаже това (отчетност);
- Осигуряване на защита на данните на етапа на проектирането и по подразбиране;
- Определяне на длъжностно лице по защита на личните данни в изрично посочените от регламента случаи, поддържане на регистър на дейностите по обработване, за които отговаря;
- Уведомяване на надзорния орган и субекта на данни в случай на нарушаване на сигурността на личните данни, както и да документиране на всяко нарушение на сигурността на личните данни, в т. ч. фактите, свързани с нарушението, последиците от него, предприетите действия за справяне с нарушението;
- Извършване на оценка на въздействието върху защитата на данните;
- Провеждане на предварителна консултация с надзорния орган преди обработването, когато оценката на въздействието покаже, че обработването ще породи висок риск, ако АЛД не предприеме мерки за ограничаване на риска
- Прилагане на подходящи технически и организационни мерки за осигуряване на сигурност на данните. В регламента са посочени и конкретни технически и организационни мерки за сигурност, като:
  - Псевдонимизация;
  - Криптиране;

– Гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

– Своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

– Редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки.

– Сътрудничество с надзорния орган за защита на личните данни при изпълнение на задълженията, произтичащи то регламента.

5. Кога администраторът и обработващият са длъжни да определят длъжностно лице по защита на данните?

Определянето на длъжностно лице по защита на данните е задължително в следните случаи:

- Когато обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- Когато основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни;
- Когато основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

6. Кои права на субекта на данни трябва да спазва администраторът съгласно Общия регламент за защита на личните данни?

Според Регламента субектът на данни (физическото лице, за което се отнасят данните) има право на:

- Информираност;
- Достъп до собствените си лични данни;
- Коригиране (ако данните са неточни);
- Изтриване на личните данни (правото „да бъдеш забравен“);

- Ограничаване на обработването от страна на администратора или обработващия лични данни;
- Преносимост на личните данни между отделните администратори;
- Възражение спрямо обработването на негови лични данни;
- Субектът на данни има право и да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен;
- Право на защита по съдебен или административен ред, в случай че правата на субекта на данни са били нарушени.

7. Въвежда ли новият Регламент по-строг контрол върху обработващите лични данни?

Да! Обработващият е задължен да спазва всички установени правила и норми за защита на личните данни и носи солидарна отговорност за причинени вреди заедно с администратора. Регламентът въвежда задължението обработващият лични данни да търси съгласието на администратора всеки път когато възлага обработването на подизпълнител. Съгласието на администратора в тези случаи следва да бъде дадено предварително, като може да бъде под формата на конкретно или общо разрешение, в писмена форма. В случай на общо писмено разрешение, обработващият е длъжен да информира администратора винаги за всякакви планирани промени за включване или замяна на други обработващи данни.

8. Трябва ли администраторите на лични данни в България да се регистрират пред Комисията за защита на личните данни както до сега?

Не, задължението за регистрация отпада, считано от 25 май 2018 г.

9. По какъв начин ще бъде осъществяван надзора за спазване на новата правна рамка по защита на личните данни?

Единственият надзорен орган по защита на личните данни в Република България е Комисията за защита на личните данни. Като такъв Комисията ще осъществява контрол за спазването на изискванията на регламента. В рамките на своите правомощия Комисията има право да разглежда жалби от физически лица, да извършва проверки на

администратори и обработващи лични данни, да издава становища, задължителни предписания и имуществени санкции. Новият Регламент значително увеличава максималния размер на налаганите глоби и имуществени санкции – до 10 млн. евро или до 2 % от годишния оборот на дружеството за предходната година (която от двете суми е по-висока).

10. Трябва ли администраторите на лични данни да спазват новия Регламент ако обработват единствено псевдонимизирани лични данни?

Най-общо – да! Псевдонимизираните лични данни[1] не са изключени извън приложното поле на новия Общ регламент. Псевдонимизация означава 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. Именно поради тези специфики на псевдонимизираните данни, Регламентът предвижда по-малко строги правила за обработване на псевдонимизирани данни, като по този начин насърчава администраторите да използват тази техника.

11. Задължени ли са администраторите на лични данни да осигуряват по-високо ниво на защита на личните данни на децата?

На децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, заплахи и евентуални неблагоприятни последици от неправомерното обработване на данни, както и своите права. Тази специална защита следва да се прилага по-специално за използването на лични данни на деца за целите на маркетинга или за създаване на личностни или потребителски профили и събирането на лични данни по отношение на деца при ползване на услуги, предоставяни пряко на деца. Когато обработването е насочено към дете, всяка информация и комуникация следва да се предоставя с ясни и недвусмислени формулировки, които да бъдат лесноразбираеми за детето.

[1] Псевдонимизация – техника за защита на неприкосновеността, при която личните данни се обработват по начин, които не позволява идентификацията на физическото лице без употребата на допълнителна информация, която следва да се съхранява отделно от тези данни, под защитата на технически и организационни мерки.

Във връзка с прякото предлагане на услуги на информационното общество на деца, обработването на данни на дете е законосъобразно, ако детето е поне на 16 години. Ако детето е под 16 години това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.