АСОЦИАЦИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Знаем ли достатъчно за Регистрите по чл.30 от Регламента – кой е задължен да ги поддържа, как се попълват и каква точно информация следва да включват?

Повече от месец след влизане в сила на Регламент (ЕС) 2016/679 едва ли има някой, който още да не е разбрал, че задължението на администраторите да се регистрират в Комисия за защита на личните данни (КЗЛД) преди да започнат да обработват лични данни отпадна. С това задължение отпадна съответно и задължението за подаването на информация в електронната система на КЗЛД за поддържаните от администраторите на лични данни регистри с дейностите по обработване. Въпреки това, като част от принципа за „отчетност“, с чл.30 от Регламента се въведе друго задължение, както за администраторите така и за обработващите лични данни, а именно да поддържат на Регистри на дейностите по обработване, които извършват.

Кой трябва да поддържа Регистър по чл.30, ал.1 и ал.2 от Регламента?

Чл. 30, ал.1 от Регламента гласи, че всеки администратор трябва да поддържа регистър на дейностите по обработване, за които отговоря.
Чл. 30, ал.2 от Регламента гласи, че всеки обработващ лични данни трябва поддържа регистър на всички категории дейности по обработването, извършени от името на администратора.

Как точно изглежда Регистъра по чл.30 ал.1 и ал.2 от Регламента?

Съгласно чл.30, ал.3 от Регламента, Регистрите следва да се поддържат в писмена форма, включително в електронен формат и при поискване от Надзорния орган да му бъде осигуряван достъп до тях.

Важното тук е, че към настоящия момент няма официално утвърден образец, нито на Регистър по чл.30, ал.1, нито на Регистър по чл.30 ал.2 от Регламента и следователно конкретният вид зависи от преценката на администратора или обработващия, които го води и поддържа. Въпреки това от съществено значение е той да включва минималните реквизити, посочени в цитираната разпоредба.

Каква информация следва да включва Регистъра по чл.30, ал.1 и ал2 от Регламента?

Съгласно чл.30, ал.1 б. „а – „ж“ от Регламента, администраторът следва да включи в Регистъра минимум следната информация:

1. Информация за организацията: име и координати за връзка на администратора, респективно когато е приложимо име и координати на съвместните администратори, или представителя на администратора, както и име и координати на длъжностното лице по защита на данните;
2. Цели на обработването. Тук следва да се изброят целите, за който данните се обработват – напр. „подбор на персонал“ или „наемане на служители“ и т.н.;
3. Описание на категориите субекти на данни (напр. „контрагенти“ и на категориите лични данни (напр. имена, електронна поща и т.н.);
4. С кого се споделят данните – категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

5. Предаване на лични данни на трета държава или международна организация -идентификация на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея, документация за подходящите гаранции;
6. Предвидените срокове за изтриване на различните категории данни – т.е. в какъв срок организацията съхранява личните данни, които обработва;
7. Общо описание на техническите и организационни мерки за сигурност по чл.32, ал.1 от Регламента .

Съгласно чл. 30, ал.2, б. „а“ – г“ от Регламента, обработващият, следва да включи в Регистъра минимум следната информация:

1. Информация за организацията: име и координати за връзка на обработващия или обработващите лични данни и на всеки администратор, от чието име действа обработващият лични данни, а когато е приложимо и на представителя на администратора, както и име и координати на длъжностното лице по защита на данните;
2. Категориите обработване, извършвано от името на всеки администратор;
3. При наличие на трансфер на лични данни към трета държава или международна организация – идентификация на третата държава или международната организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея, документация за подходящите гаранции;
4. Общо описание на техническите и организационни мерки за сигурност, посочени в член 32, ал.1 от Регламента.

Задължително ли е за моята организация, поддържането на Регистър по чл.30, ал.1 или ал.2 от Регламента?

Не винаги воденето на Регистрите по чл.30 от Регламента е задължително.

Още в Рецитал 13-и от Регламента е посочена дерогация от това задължение предвид „особеното положение на микро-предприятията и малките и средните предприятия“, които имат по-малко от 250 служители.

Това принципно положение е изрично упоменато и в чл.30, ал.5 от Регламента, която гласи, че по отношение на предприятие или дружество с по-малко от 250 служители, воденето на такива Регистри не е задължително, 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.

От своя страна, така заложеното в Регламента изключение от общото правило, породи голям брой запитвания към Надзорните органи в ЕС и стана причина през месец април 2018 г., Работната група по чл.29 да публикува своя „Позиция относно изключенията от задължението за поддържане на регистри на дейностите по обработване, съгласно чл.30, ал.5 от Регламента“. В „Позицията“, Работната група по чл.29 посочва, че хипотезите, при които компаниите са длъжни да водят регистри независимо от броя служители, са алтернативни и наличието, на която и да е от тях е основание за водене на регистър.

Следователно, въпреки че администраторът или обработващият данни имат по-малко от 250 служители, ако същите извършват обработване на данните, което:

1) има вероятност да породи риск (не само голям риск) за правата на субектите на данните;

2)обработването на данни не се извършва спорадично;

3) обработват се специални категории данни или данни, отнасящи се до присъди и нарушения,

те трябва да поддържат регистър на дейностите по обработване.

Работната група по чл.29 допълва, че тези организации трябва да поддържат регистри единствено за типовете обработване на данни, визирани в чл. 30, ал. 5 от Регламент.

Чрез дадения в „Позицията“ пример, Работната група по чл.29 посочва изрично, че когато малко предприятие, обработва данни за своите служители, то подобен вид обработване не може да се приеме за спорадично и за него също следва да се води регистър.
За сметка на това, други дейности, които се считат за спорадични (т.е. повтарят се рядко през неопределен интервал от време), не следва да се включват в такъв регистър, освен ако не пораждат риск за правата на субектите на данни или не включват обработване на специални категории лични данни или данни по чл.10 от Регламента.
Регистрите по чл.30 от Регламента са ново задължение за администратори и обработващи. Освен минимума информация изброена по-горе, дадена компания може да реши да включи и друга информация, която макар да не е задължителна по чл. 30 от Регламента, ще й бъде от помощ при доказването на други обстоятелства – напр. информация за правното основание на което данните се обработват съгласно чл.6, ал.1 от Регламента.

Като заключение, предвид обстоятелството, че Регистрите по чл.30 от Регламента не са толкова сложни за водене и поддържане, дори напротив събраната в тях информация може само да подпомогне администратора или обработващия при спазване и на други негови задължения съгласно Регламента, считаме, че е добре и ще бъде е полезно за Компаниите да поддържат Регистри по чл.30, ал.1 или ал.2 от Регламента, дори в случаите, в които те попадат в изключенията на Регламента.

Настоящата статия не представлява правен съвет. Тя съдържа мнение/коментар на нашите експерти и е само с цел подпомагане на компаниите при спазване изискванията на Регламент (ЕС)2016/679.