

Общият регламент за защита на личните данни - част от стратегията на ЕС за единния дигитален пазар

На 25 май 2018 г. влиза в сила Регламент 2016/679 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), който въвежда изцяло нов подход към защитата на личните данни.

Действащата към момента Директива 95/46/ЕО предвижда създаване на национални режими за защита на личните данни, като слага акцент върху регистрацията на администраторите на лични данни и на дейностите, които извършват. Тъй като обработката на данни често се извършва трансгранично, подходът на уредба чрез предоставяне свободна преценка на държавите-членки как да постигнат поставените от директивата цели, се оказва неефективен. Това налага приемането на регламент, който установява конкретни правила и е задължителен за цялата територия на ЕС от посочената дата на влизане в сила.

С въвеждането на новата уредба всяко лице, което обработва лични данни ще трябва да доказва спазване на принципите и правилата на Регламентта, включително прилагането на адекватни технологични и организационни мерки за гарантиране сигурността на информацията. На националните органи, които следят за защита на личните данни – в България това е Комисията за защита на личните данни, са предоставени значителни по обем нови правомощия, като нарушението на правилата на Регламентта може да бъде санкционирано с налагане на глоби в размер до 20 милиона евро или 4% от годишния оборот на санкционираното лице. Регламентът предвижда и задължение за всяко лице да предоставя обработваните от него лични данни на други лица, само ако установи, че те също спазват изискванията на новата уредба. Т.е. в случая е налице една косвена санкция – тъй като неспазването на Регламентта ще има за резултат загуба на контрагенти за съответното дружество.

С Регламентта изрично е предвидено и правото на лицето, чиито данни се събират, да получи обезщетение, когато правата му са нарушени – при незаконосъобразно събиране или достъп до данни.

Основните разлики спрямо действащата до 25.05.2018 г. Директива 95/46/ЕО са в няколко насоки – отпада задължението на администраторите на лични данни да се регистрират преди да започнат да събират данни. За сметка на това всяко лице може да бъде проверено от националния орган за защита на личните данни и, ако обработва такава информация е задължено да докаже спазването на всички изисквания на нормативната уредба.

Основните правила на новия регламент са насочени към гарантиране на законосъобразността на обработването на лични данни. Първото изискване в тази връзка е да има основание за събирането на лични данни – всъщност всяко действие с такива данни следва да е предвидено по договор или да следва от изпълнението на задължение по закон. Така например би било законосъобразно да се събират данни за банковата сметка на дадено лице, ако чрез същата следва да бъде извършено плащане

по договор. Специфичното условие, поставено от регламента е тази информация да не бъде ползвана в последствие за цел, различна от тази, за която е събрана. Законосъобразно е обработването на данните и когато физическото лице, за което те се отнасят, е дало изричното си съгласие. Това съгласие обаче трябва да е дадено свободно – в противен случай, дори и физическото лице да е дало такава, органите по защита на данните пак могат и ще наложат санкции.

Следващо изискване е да се обработва минималното количество лични данни – само тези, които са необходими за конкретната цел. Събирането и съхраняването на лични данни извън тези рамки – например събирането на данни за здравословното състояние при сключване на договор за телекомуникационни услуги – ще представлява нарушение на регламента. Наложени са и ограничения на последващото съхраняване и обработка на лични данни – такива действия са възможни само за целите, за които информацията е събрана първоначално.

Наложени са и ограничения на предаването на такава информация на трети лица, като се обръща внимание, че такива лица следва също да спазват правилата на регламента, независимо къде се намират. Съответно регламентът се прилага не само към администратори на лични данни, установени на територията на ЕС, но и към всички лица, които обработват лични данни на граждани на ЕС.

Наред с посочените задължения, всеки администратор на лични данни трябва да предприеме адекватни организационни и технологични мерки, за да гарантира опазването на предоставените му лични данни. Тези мерки включват както предвиждане на специфични задължения на служителите на администратора, така и въвеждане на софтуерни приложения, които да позволяват непрекъснат контрол върху достъпа до съхраняваните лични данни. Съответно трябва да бъдат предвидени процедури за вътрешна проверка, като при установяване на нерегламентиран достъп до информация администраторът е задължен незабавно да уведоми съответния национален орган /КЗЛД в България/, за да бъдат ограничени потенциалните вреди за физическите лица, за които данните се отнасят. Като специфична организационна мярка за администратори, които извършват масово обработване на лични данни, е предвидено по трудов или граждански договор да бъде ангажирано лице, което да следи за спазването на правилата на Регламента.

С Регламента са предвидени и няколко специфични правила на физическите лица, чиито данни се обработват, като администраторът на лични данни трябва да предвиди съответни процедури за упражняването им. Така е предвидено например, че всяко физическо лице има право на достъп до своите лични данни и може да поиска тяхната корекция, ако не са точни. Физическото лице може да поиска съхраняваните за него данни да бъдат изтрети или обработването да бъде ограничено (да бъде извършвано за по-малко цели или да се обработва по-малко информация).

Общият регламент относно защитата на данните променя съществено правилата за работа с лични данни – като на практика засяга почти всяко дружество, дали във връзка със съхраняваните данни за служители или за клиенти. Тези правила обаче са само част от предвидените от ЕС законодателни мерки във връзка с развитието на Дигиталния единен пазар. Като част от стратегията на ЕС в тази област в момента е започнало обсъждане на предложени за Регламент за защита неприкосновеността на

личния живот и електронните съобщения (E-privacy), който е предвиден да се прилага заедно с и да допълва режима за защита на личните данни. Тази нова уредба ще засяга сигурността на данните, съдържащи се в електронни съобщения, както и тези в крайните устройства на потребителите – от телефони до промишлено оборудване. В обхвата на промените за момента се включват въпроси като автоматично обновяване на софтуер, изпращане на информация за работа на конкретното устройство и обработването ѝ.