С изменения в българския Закон за киберсигурност са въведени изискванията на втората европейска директива за мрежова сигурност (NIS 2)

Въпреки забавянето при транспониране, през февруари 2026 г. с изменения в българския Закон за киберсигурност бяха въведени изискванията на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (NIS 2).

Измененията са в няколко насоки, като на първо място се разширява кръгът на лицата, които са задължени да спазват изискванията на изменения Закон за киберсигурност – а именно:

– административни органи (тук няма промяна);

– изброени в Приложение I и II видове средни или по-големи предприятия, които предоставят услуги или извършват дейност на територията на ЕС в секторите енергетика; транспорт; банково дело; финансови пазари; здравеопазване; снабдяване с питейна вода; обработване на отпадъчни води; цифрова инфраструктура; управление на ИКТ услуги; космически дейности; пощенски и куриерски услуги; управление на отпадъците; производство и дистрибуция на химикали; производство, преработка и дистрибуция на храни; изброени производствени сектори; доставчици на цифрови услуги; научноизследователски организции;

– субектите по Приложение I и II представляват задължени лица независимо от своя размер, ако предоставят обществени електронно-съобщителни мрежи или обществено достъпни електронно-съобщителни услуги; удостоверителни услуги; услуги като регистратор на домейни от първо ниво или системни услуги за имена на домейни; са единствени доставчици на услуги от съществено значение за поддържане на критични обществени и икономически дейности; ако смущение в услугата би представлявало системен риск, по-специално ако този риск би имал трансграничен характер; или ако субектът е критичен поради специфични фактори на национално или регионално равнище;

– субекти, определени като критични по съответния ред;

– субекти, предоставящи услуги за регистрация на домейни;

– образователни институции, които извършват научноизследователска дейност в секторите по Приложение I и II;

– лица, които осъществяват публични функции и предоставят административни услуги

CR legal DL 2018. Всички права запазени.

по електронен път;
– организациите, които предоставят обществени услуги по електронен път;
– органите на съдебната власт.
Т.е. налице е значително разширяване на обхвата на задълженията за спазване на изискванията за киберсигурност.
Тези задължения освен това вече имат различен характер – по-ясно изразено насочване към оценката на риска и предприемането на превантивни мерки. С влизане в сила на измененията управителните органи на основните категории задължени лица следва да одобряват мерки за управление на риска и да следят за тяхното спазване. Конкретизирани са задълженията за осигуряване на мерки в съответствие с изменения Закон за киберсигурност – като вече са посочени ясни критерии, на които тези мерки трябва да отговарят. Новото е установяването на съдържателни изисквания – например въвеждане за наличие на мерки за непрекъснатост на дейността или сигурност на веригите за доставки. По подобен начин са въведени подробни изисквания и за уведомяване при инцидент, който засяга киберсигурността – като за сметка на това задължението за уведомяване е ограничено само за сериозни инциденти.
По отношение на мерките е засилена ролята на контролните органи, като са предвидени възможности за Съвета по киберсигурността да въведе изисквания за използване на конкретни доказано подходящи продукти, услуги и процедури в сферата на информационните и комуникационни технологии, които са сертифицирани на ниво ЕС. Министерският съвет по предложение на Съвета по киберсигурността може да въвежда ограничения за използването на рискови технологии от лицата, задължени по българския Закон за киберсигурност, при условие, че тези ограничения не нарушават правото на ЕС.
Разширени са мерките за контрол и са предвидени допълнителни правомощия за административните органи. Съответно, предвидени са значителни по размер санкции – достигащи за най-тежките нарушения до 10 000 000 евро или 2% от световния оборот, по модела въведен в Общия регламент за защита на данните. Заедно с тези санкции срещу задължените лица са предвидени и глоби за техните управителни органи – което отразява значителната промяна в мерките за киберсигурност, като на практика се въвежда лична отговорност за спазването им.

CR legal DL 2018. Всички права запазени.

Всичко изложено ясно сочи, че всяко лице с дейност в някой от секторите по Приложение I и II от Закона за киберсигурност следва да прецени дали има задължение да спазва изброените в същия мерки и да предприеме съответни мерки.

CR legal DL 2018. Всички права запазени.