DJINGOV
GOUGINSKI
KYUTCHUKOV
VELICHKOV
ATTORNEYS AND COUNSELLORS AT LAW

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

Измененията на Закона за киберсигурност за въвеждане на Директива NIS2 са в сила от 17 февруари 2026 г.

Със Закона за изменение и допълнение на Закона за киберсигурност (**„ЗКС“**), обнародван на 13 февруари 2026 г., ДВ. бр. 17, беше транспонирана Директива (ЕС) 2022/2555 относно мерки за високо общо ниво на киберсигурност в Съюза (“**NIS2**”). NIS2 установява минимални изисквания за управление на риска и докладване на инциденти в ЕС в областта на киберсигурността и модернизира и разширява съществуващата правна рамка, установена с Директива NIS от 2016 г.

Измененията в ЗКС, в сила от 17 февруари 2026 г., *обхващат значително по-широк кръг от сектори и субекти в сравнение с действащия досега закон, конкретизират минималните мерки за управление на риска за киберсигурността им и предвиждат значителни по размер санкции при неизпълнение, вкл. персонални глоби на членовете на органите им на управление. Задължените субекти трябва да са в пълно съответствие с новите разпоредби към момента на влизането в сила на ЗИД на ЗКС.*

I. Какво регулира измененият ЗКС?

ЗКС задължава т.нар. съществени и важни субекти да въведат мерки за управление на риска в областта на киберсигурността и да докладват всеки значителен инцидент. Управителните органи на субектите носят отговорност и следят за прилагането на тези мерки. ЗКС има широк ефект върху вътрешната организация на субектите и отношенията им с трети страни. Киберзаконодателството може да засегне дейността ви косвено, ако предоставяте услуги на съществени или важни субекти или държавни органи, поради необходимостта да отговорите на техните мерки за контрол на риска от трети страни.

II. Кои са съществените и важните субекти, които попадат в обхвата на ЗКС?

ЗКС се прилага към предприятия в 17 критични сектора, които отговарят най-малко на критериите за средни предприятия, административните органи и органите на съдебната власт. Съществени субекти по силата на закона са всички оператори на съществени услуги към датата на влизане в сила на измененията в ЗКС. По изключение съществени или важни субекти ще могат да бъдат идентифицирани въз основа на критерии за критичност на дейността. Подробен списък на секторите е изложен в нашия предишен материал (вижте тук).

III. Как и кога ще бъдат идентифицирани съществените и важните субекти?

С решение на Министерския съвет в срок до 6 месеца от влизане на ЗИД на ЗКС, в сила ще бъдат определени компетентни органи по киберсигурност за секторите, попадащи в обхвата на закона. За следните сектори компетентните органи са определени *ex lege*: а) Комисията за регулиране на съобщенията - за предприятията в секторите на електронните съобщения, удостоверителните услуги, пощенските (вкл. куриерски) услуги; б) Министърът на енергетиката – за публичните предприятия в сектор енергетика. Висшият съдебен съвет ще бъде компетентен орган за съдебната власт, докато Министерството на електронното управление („**МЕУ**“) ще продължи да бъде национален компетентен орган по отношение на административните органи. Към МЕУ се създава Национален екип за реагиране при инциденти с компютърната сигурност, а останалите компетентни органи създават Секторни екипи за реагиране при инциденти с компютърната сигурност („**СЕРИКС**“).

Компетентните органи са задължени да идентифицират съществените и важните субекти като прилагат методика, която следва да бъде приета от Министерския съвет в срок от 6 месеца от влизане

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

в сила на закона. Срокът за идентифициране на съществените и важните субекти е до 5 месеца от решението на Министерския съвет за определяне на компетентни органи.

IV. Кои са основните задължения за съществените и важните субекти?

Съществените и важните субекти приемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи в основната си дейност или при предоставяне на своите услуги. При спазване на принципа за технологична неутралност и като се вземат предвид **последните постижения в тази област** и, когато е приложимо, съответните европейски и международни стандарти, както и разходите за прилагането им, чрез мерките за управление на риска се гарантира ниво на сигурност на мрежовите и информационните системи, съответстващо на риска. **При оценката на пропорционалността на тези мерки** надлежно се вземат предвид степента на излагане на рискове на субекта, размерът на субекта и вероятността от възникване на инциденти, както и тяхната значимост, включително тяхното обществено и икономическо въздействие.

Мерките се основават на подход, обхващащ всички опасности, които имат за цел да защитят мрежовите и информационните системи и физическата среда на тези системи от инциденти, и включват мерки в следните области:

- политики за анализ на риска и сигурността;
- действия при инцидент;
- непрекъснатост на стопанската дейност;
- сигурност на веригата за доставка;
- придобиване на системи;
- оценяване на ефективността на мерките за управление на риска;
- киберхигиенни практики и обучение;
- криптография и криптиране;
- човешки ресурси, достъпи, активи;
- удостоверяване на автентичността;
- управление на измененията;
- управление на риска за субекти по Директива CER

Минималният обхват на мерките за постигане на високо общо ниво на киберсигурност за субектите по ЗКС ще се определят с наредби, приети от Министерския съвет.

Управителните органи одобряват мерките за управление на риска и следят за прилагането им, както и са задължени да преминават на всеки две години обучения в областта на киберсигурността и да организират такива обучения за своите служители.

V. Какви са задълженията за подаване на уведомления?

Съществените и важните субекти уведомяват съответния СЕРИКС за всеки значителен инцидент чрез образци, определени с наредби на Министерския съвет:

- до 24 часа след установяването на значителен инцидент - ранно предупреждение;
- до 72 часа след установяването на значителния инцидент - уведомление за инцидент;
- окончателен доклад не по-късно от един месец след подаването на уведомлението или след приключване на инцидента, ако субектът не се е справил с него;
- по искане на СЕРИКС - междинен доклад.

Засегнатите субекти уведомяват, когато е подходящо и без ненужно забавяне, получателите на техните услуги за значителни инциденти, които има вероятност неблагоприятно да засегнат предоставянето на тези услуги.

МЕУ създава, води и поддържа регистър на съществените и важни субекти. Субектите, вписани в регистъра, уведомяват компетентният орган за всяка промяна в данните в срок до две седмици.

10 TSAR OSVOBODITEL BLVD
1000 SOFIA, BULGARIA
T: + 359 (2) 932 1100
F: + 359 (2) 980 3586
E: DGKV@DKGV.COM
W: WWW.DGKV.COM

VI. Какви са санкциите при неизпълнение?

Неизпълнението на задълженията за прилагане на мерки за управление на риска или уведомяване за значителен инцидент от страна на съществен субект може да бъде санкционирано с минимум 25 000 евро и максимум до 2% от световния оборот за предишната финансова година (но не по-малко от 10 млн. евро). За важните субекти санкциите са в размер на минимум 12 500 евро и максимум до 1,4% от световния оборот за предишната финансова година (но не по-малко от 7 млн. евро). Световният оборот се изчислява за предприятието, към което принадлежи съществения субект.

На управителите или членове на управителните органи на съществените и важните субекти ще може да се налага глоба в размер от 500 до 5 000 евро при нарушение на задълженията им по ЗКС.

VII. Как киберзаконодателството ще повлияе на цялостния контекст на Вашата организация?

ЗКС се превръща в част от рамката за корпоративно управление на съществените и важните субекти. Членовете на управителния орган носят лична отговорност за нарушения на закона и могат да отговарят за вредите, които са причинили виновно на дружеството поради неизпълнението на ЗКС. Обучението в областта на киберсигурността се превръща в лично задължение за участие и организация на обучения за служителите. Политиката за човешки ресурси следва да се преосмисли като се съобразят изискванията за проверка на миналото и продължаваща квалификация. Структурата на управление на субекта не трябва да допуска конфликти на интереси при изпълнение на задължения по ЗКС.

Кибер due diligence се превръща в неизменен елемент от всяка сделка за придобиване. Отношенията на субектите в обхвата на ЗКС с доставчиците на техните критични ИКТ услуги следва да бъдат приоритизирани. В договорите с трети страни се включват задължителни изисквания за управление на рисковете за сигурността на веригите за доставка.

Доставката на ИКТ услуги на държавни органи следва да бъде съобразена с мерките за сигурност на веригите за доставка, които са специфични за рисковете, идентифицирани от съответния орган. Субектите следва да са готови за надзор от компетентните органи и предстоящите планови проверки (за съществените субекти) или проверки след значителен инцидент (за важните субекти). При инциденти, които водят до нарушаване на сигурността на лични данни, проверки могат да бъдат осъществявани и от Комисията за защита на личните данни.

***