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

РАМКА НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА КИБЕРСИГУРНОСТ NIS 2

Готови ли сте за новите регулации?

С изменения и допълнения на Закона за киберсигурност (**„ЗКС“**) ще бъде транспонирана Директива NIS 2 (“**NIS 2**”) (Директива (ЕС) 2022/2555 относно мерки за високо общо ниво на киберсигурност в Съюза). NIS 2 е общоевропейско законодателство в областта на киберсигурността и модернизира и разширява съществуващата правна рамка, установена с Директива NIS от 2016 г. **Крайният срок за транспониране на NIS 2** е **17 октомври 2024 г.** като националните закони следва да се прилагат от 18 октомври 2024 г. .

На 13 септември 2024 г., в Народното събрание беше внесен проект на Закон за изменение и допълнение на ЗКС. Предвид предстоящите парламентарни избори, законопроектът ще бъде разгледан след повторното му внасяне от бъдещото 51-во Народно събрание.

***Защо** насочваме внимание към този проект на нормативен акт сега, преди той да е влязъл в сила?*

***Защото измененията в ЗКС** ще обхванат значително по-широк кръг от сектори и субекти в сравнение с действащия закон. Задължените субекти е необходимо да предвидят новите изисквания, така че дейността им да съответства на закона към момента на влизането му в сила.*

I. Какво ще регулират измененията в Закона за киберсигурност?

NIS 2 установява мерки, които имат за цел постигане на високо общо ниво на киберсигурност като изисква държавите членки на ЕС да приемат национални стратегии за киберсигурност и определят компетентни органи, органи за управление на киберкризи, единни звена за контакт по въпросите на киберсигурността и екипи за реагиране при инциденти с компютърната сигурност. Т.нар. съществени и важни субекти следва да въведат мерки за управление на риска в областта на киберсигурността и да докладват всеки значителен инцидент.

NIS 2 се допълва от Регламент (ЕС) 2022/2554 относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA) и Директива (ЕС) 2022/2557 за устойчивостта на критичните субекти (CER). Регламент DORA е специален закон спрямо ЗКС и предвижда правила за оперативна устойчивост на цифровите технологии във финансовия сектор като ще се прилага от 17 януари 2025 г. Критичните субекти, установени съгласно Директива CER, ще се считат за съществени субекти по изменения ЗКС. Крайният срок за транспониране на CER е същият като NIS 2 като към момента няма публикуван законопроект.

II. Кои са задължените лица?

Обхватът на задължените субекти ще бъде определен в зависимост от конкретната дейност и размера на предприятието или по преценка на компетентен орган. Размерът на предприятието се определя, съгласно Закона за малките и средните предприятия. Всички административни органи, а след въвеждане на Директива CER - и критичните субекти, ще се считат за съществени субекти по изменения ЗКС. Като съществени субекти ще бъдат определени по силата на закона и всички оператори на съществени услуги към датата на влизане в сила на измененията в ЗКС. Останалите категории задължени субекти ще бъдат определени като съществени или важни в зависимост от сектора и размера на предприятието:

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

<table>
<tr><th></th><th>Големи предприятия</th><th>Средни предприятия</th><th>Малки и микро-предприятия</th></tr>
<tr><td>Цифрова инфраструктура (квалифицирани удостоверителни услуги; DNS услуги; регистри на имената на домейни от първо ниво)</td><td colspan="3">Съществени субекти</td></tr>
<tr><td>Цифрова инфраструктура (доставчици на обществени електронни съобщителни мрежи или услуги)</td><td colspan="2">Съществени субекти</td><td>Важни субекти (съществени по изключение)*</td></tr>
<tr><td>Енергетика (електроенергия, топлоснабдяване, нефт, природен газ, водород, оператори на зарядни точки)</td><td rowspan="11">Съществени субекти</td><td rowspan="11">Важни субекти (съществени по изключение)*</td><td rowspan="11">Нямат задължения, освен ако по изключение са определени за съществени или важни*</td></tr>
<tr><td>Транспорт (въздушен, железопътен, воден, сухопътен)</td></tr>
<tr><td>Банков и финансов сектор (кредитни институции, места на търговия, централни контрагенти). DORA се прилага за мерките, докладването за инциденти и надзора.</td></tr>
<tr><td>Здравеопазване (здравно обслужване, референтни лаборатории, научноизследователска и развойна дейност за лекарства, производство на основни фармацевтични продукти и критично важни медицински изделия)</td></tr>
<tr><td>Питейна вода (доставка или дистрибуция, когато е съществена част от дейността)</td></tr>
<tr><td>Отпадъчни води (събиране и пречистване, когато е съществена част от дейността)</td></tr>
<tr><td>Цифрова инфраструктура (доставчици на точки за обмен в интернет; услуги за изчисления в облак; центрове за данни; мрежи за доставка на съдържание; неквалифицирани удостоверителни услуги)</td></tr>
<tr><td>Управление на услуги в областта на ИКТ и управлявани услуги за сигурност в ИКТ)</td></tr>
<tr><td>Космическо пространство (наземна инфраструктура, различна от електронни съобщителни мрежи)</td></tr>
<tr><td>Пощенски и куриерски услуги</td></tr>
<tr><td>Управление на отпадъци, когато е съществена част от дейността</td></tr>
<tr><td>Производство, изготвяне и дистрибуция на химикали (вещества и смеси или изделия от тях)</td><td colspan="2" rowspan="5">Важни субекти (съществени по изключение)*</td></tr>
<tr><td>Производство, преработка и разпространение на храни</td></tr>
<tr><td>Производство (медицински изделия, медицински изделия за инвитро диагностика; компютри, електронни и оптични продукти; електрически съоръжения; машини и оборудване; моторни превозни средства, ремаркета и полуремаркета; друго транспортно оборудване)</td></tr>
<tr><td>Доставчици на цифрови услуги (онлайн места за търговия; онлайн търсачки; платформи на услуги за социални мрежи)</td></tr>
<tr><td>Научноизследователски организации</td></tr>
</table>

* Малки и микро-предприятия могат да бъдат идентифицирани като съществени или важни. Средни предприятия могат да бъдат идентифицирани като съществени. Критериите са: 1) субектът е единствен доставчик на услуга, която е от съществено значение за поддържането на критични обществени и икономически дейности; 2) смущение (за определено време) в предоставяната от субекта услуга би могло да окаже значително въздействие върху обществената безопасност, обществената сигурност или общественото здраве, 3) смущение в предоставяната от субекта услуга би могло да предизвика значителен системен риск, по-специално за секторите, в които такова смущение би могло да има трансгранично въздействие; 4) субектът е критичен поради своята специфична значимост на национално или регионално равнище за конкретния сектор или вид услуга или за други взаимозависими сектори в Република България.

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

III. Как ще бъдат идентифицирани съществените и важните субекти?

Измененият ЗКС, също както и действащия закон, ще задължи националните компетентни органи по киберсигурност да определят субектите, които са задължени по NIS 2 и да уведомят Министъра на електронното управление. При определянето на субектите, компетентните органи ще прилагат методика, приета от Министерския съвет.

IV. Кои са основните задължения за съществените и важните субекти след влизане в сила на измененията на ЗКС?

Управителните органи на съществените и важни субекти ще одобряват мерките за управление на риска в областта на киберсигурността; следят за прилагането на одобрените мерки; преминават на всеки две години през обучение за придобиване на достатъчно познания и умения; предлагат и организират обучения и за своите служители.

Мерки за управление на риска, базирани на подход, обхващащ всички опасности

Анализ на риска като се отчита степента на излагане на риск, размер на субекта, вероятност от инциденти, тяхната значимост и въздействие

Определяне на подходящи и пропорционални, технически, оперативни и организационни мерки

Технологично неутрални, съобразно последните постижения и при отчитане на разходите

Цел: Да се гарантира ниво на сигурност, което съответства на риска

Минимални мерки, които обхващат всички опасности:

- политики
- действия при инцидент
- непрекъснатост
- сигурност на веригата за доставка
- сигурност при придобиването на системи
- оценяване на ефективността на мерките
- основни киберхигиенни практики и обучение
- криптография и, когато е целесъобразно, криптиране
- сигурност на човешките ресурси, контрол на достъпа и управление на активи
- многофакторни решения за удостоверяване, защитени комуникации
- управление на измененията
- мерки за управление на риска

Докладване на значителни инциденти

Съществените и важните субекти ще уведомяват Секторния екип за реагиране при инциденти с компютърната сигурност (**„СЕРИКС“**). Уведомленията ще се подават до СЕРИКС чрез образци, съгласно наредбите на Министерски съвет.

Сертифицирани ИКТ продукти, услуги или процеси. Стандартизация

Съответният национален компетентен орган ще може да изиска от съществените и важните субекти да използват конкретни, доказано подходящи в оперативно и икономическо отношение ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от тях или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност.

Уведомления за промяна в данните в регистъра на съществени и важни субекти

Министърът на електронното управление създава, води и поддържа регистър на съществените и важни субекти, който съдържа информация за идентифицираните съществени и важни субекти.

Доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, субектите, предоставящи услуги за регистриране на имена на домейни, доставчиците на компютърни услуги

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 облак, центрове за данни, мрежи за предоставяне на съдържание, управлявани услуги, управлявани услуги за сигурност, както и доставчиците на онлайн места за търговия, онлайн търсачки и платформи на услуги за социални мрежи ще бъдат задължени да предоставят на националните компетентни органи, информация за адреса на основното място на установяване в ЕС или неговия представител, до 2 месеца от възникването им.

Субектите, вписани е регистъра, ще следва да уведомяват съответния национален компетентен орган за всяка настъпила промяна в данните в срок до две седмици от датата на промяната.

V. Кои са компетентните органи за надзор за спазване на изискванията за киберсигурност?

Министерският съвет ще определи с решение административните органи, които изпълняват функциите на национални компетентни органи по киберсигурност за секторите и услугите, когато такива не са създадени със специален закон. Към компетентните органи се създават СЕРИКС.

Министерство на електронното управление (**„МЕУ“**) ще бъде национален компетентен орган за всички административни органи, както и за лицата осъществяващи публични функции или организациите, предоставящи обществени услуги, които не са съществени/важни субекти на друго основание, когато предоставят административни услуги по електронен път. Към МЕУ се създава Национален екип за реагиране при инциденти с компютърната сигурност.

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 ще може да бъде санкционирано с минимум 50 000 лева и максимум до 2% от световния оборот (но не по-малко от 20 млн. лв.). За важните субекти санкциите са в размер на минимум 25 000 лв. и максимум до 1,4% от световния оборот (но не по-малко от 14 млн. лв.). На управителите или членове на управителните органи на съществените и важните субекти ще може да се налага глоба в размер от 1 000 до 10 000 лв.

VII. Какви са препоръчителните първи стъпки?

Бихме препоръчали следните стъпки за привеждане в съответствие с предстоящите изменения на ЗКС:

- Направете оценка дали попадате в категориите на съществени и важни субекти или може да попаднете в краткосрочен период;
- Създайте вътрешен план за съответствие с измененията в ЗКС, планирайте въвеждането на мерки за управление на риска в съответствие с изменения закон;
- Въведете с вътрешни правила строго определен ред за подаване на уведомленията за значителни инциденти, отговорни лица за спазване на сроковете;
- Проведете подходящо обучение на персонала относно управление на риска в областта на киберсигурността, което позволява идентифициране на рисковете и оценка на въведените от Вас практики за управление на риска в областта на киберсигурността и въздействието върху услугите.

* * *