В срок до 17.10.2024 г. България следваше да въведе 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 (Директива МИС 2). За тази цел е необходимо да се измени Закона за киберсигурност, в който са транспонирани изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

Новата директива, чиито изисквания тепърва ще трябва да бъдат отразени в Закона за киберсигурност, предвижда различен подход при определяне на кръга лица, които имат задължения във връзка с осигуряването на мрежова и информационна сигурност. В Приложение I към Директива 2022/2555 са изброени редица сектори с висока степен на критичност за функционирането на държавите-членки – като енергетика, транспорт, банков сектор, здравеопазване, а в Приложение II са изброени други критични сектори като пощенски услуги, управление на отпадъците, производство, преработка и разпространение на храни. В рамките на тези сектори, субектите се разделят на съществени и важни, като се предвиждат различни задължения за тях.

Съществени са субектите, които извършват дейност в някои от секторите по Приложение I и надхвърлят таваните за средни предприятия по член 2, параграф 1 от приложението към Препоръка 2003/361/ЕО, както и доставчиците на квалифицирани удостоверителни услуги, регистратори на домейни от първо ниво и доставчиците на DNS услуги. В тази категория са и доставчици на обществено достъпни електронни съобщителни мрежи или обществено достъпни електронни съобщителни услуги, ако отговарят на изискванията за средни предприятия по член 2 1 от приложението към Препоръка 2003/361/ЕО. В нея попадат и органите на публична власт на централно ниво, както и други доставчици на услуги, за които държавата – членка е приела по един или друг ред, че са съществени – например съгласно Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 година за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета или съгласно вече отменената Директива 2016/1148.

Всички други субекти, действащи в секторите по Приложение I и Приложение II се дефинират като важни субекти.

CR legal DL 2018. Всички права запазени.

По отношение на субектите в двете групи – важни и съществени – са предвидени задължения за поддържане на мрежова и информационна сигурност, както и за докладване в рамките на 24 часа на инциденти, които са довели до смущаване на предоставяните услуги, финансова загуба или засяга други физически или юридически лица.

По отношение на съществените субекти Директива 2022/2555 предвижда предварителен надзор, както и контрол по време на осъществяване на дейността – а за важните само контрол по време на дейността. С оглед различната оценка за значението на субектите, има различни санкции за нарушение на изискванията на директивата. И за двете групи субекти се въвежда лична отговорност на управителни органи, както и задължения същите редовно да преминават през обучения за мрежова и информационна сигурност.

Предстои да се изясни как тези изисквания ще бъдат транспонирани в Закона за киберсигурност, като съществените и важните субекти следва да приведат дейността си в съответствие с изискванията на Директива 2022/2555, дори да не е транспонирана. Към момента има внесен законопроект в тази насока, но същият е приет на първо четене и предстои да бъде разгледан на второ четене от Народното събрание.

CR legal DL 2018. Всички права запазени.