Neues zur IT-Sicherheit: NIS-2-Richtlinie veröffentlicht

Zentrale Einrichtungen in der Privatwirtschaft und der öffentlichen Hand sind vulnerable Ziele für IT-Angriffe. Ihre Cybersicherheit ist daher von elementarer Bedeutung. Die Anforderungen daran schärft die kürzlich veröffentlichte NIS-2-Richtlinie, die „Network and Information Security-Richtlinie". Gegenüber der Vorgängerversion NIS-1 von 2016 haben sich der Anwendungsbereich, der Pflichtenkanon und gerade auch das Sanktionsrecht erheblich verschärft.

Harmonisierte IT-Sicherheit durch die NIS-2-Richtlinie

Mit der neuen NIS-2-Richtlinie hat die EU ihre Regularien zur IT-Sicherheit bestimmter Einrichtungen erneuert. Die am 27.12.2022 veröffentlichte Richtlinie tritt zum 16.01.2023 in Kraft und ist von den Mitgliedstaaten nun binnen 21 Monaten, also bis zum 16.10.2024, umzusetzen. Unternehmen mit einer Größe von mindestens 50 Mitarbeitern und einem Jahresumsatz bzw. einer Jahresbilanzsumme ab 10 Millionen Euro sollen Pflichten der IT-Sicherheit aus der Richtlinie treffen, wenn sie wesentliche oder zumindest wichtige Einrichtungen betreiben. Das sind nach wie vor insbesondere solche in Bereichen der Kritischen Infrastruktur (KRITIS), also etwa der Energieversorgung, dem Transport, dem Gesundheitswesen oder der Telekommunikationsnetze. Neu in Anhang II sind auch Sektoren gelistet, die bisher klassischerweise nicht als KRITIS eingestuft wurden, etwa solche aus der chemischen Industrie, dem Maschinenbau oder digitale Dienste, also Anbieter von Online-Suchmaschinen und sozialen Netzwerken. Der EU-Gesetzgeber trägt mit dieser Erweiterung dem Umstand Rechnung, dass auch diesen Sektoren eine herausragende Bedeutung für Gesellschaft und Wirtschaft zukommt – man denke etwa an die Folgen einer Fake-Berichterstattung im Vorfeld von Wahlen über die großen sozialen Netzwerke.

Erweiterter Pflichtenkreis und schärfere Sanktionen

Nicht nur der Adressatenkreis wurde erweitert, auch die materiellen Pflichten zur Implementierung eines hohen IT-Sicherheitsniveaus und die potentiellen Bußgelder wurden deutlich verschärft. Die Pflichten aus der NIS-2-Richtlinie sind umfassend: Pläne zur Prävention, Aufdeckung und Bewältigung von IT-Sicherheitslücken, interne Richtlinien zur Risikoabschätzung und Informationssicherheit, etc. müssen erstellt und gelebt werden. Die Sicherheit ist entlang der gesamten Lieferkette zu gewährleisten.

Zudem wurde erstmals ein Bußgeldrahmen für Verstöße gegen die Richtlinie auf EU-Ebene festgelegt. Unter der NIS-1-Richtlinie oblag es noch den Mitgliedsstaaten, dies rein national zu regeln. Der Bußgeldrahmen geht bis zu 10 Millionen Euro oder bis zu 2% des weltweiten Jahresumsatzes. Doppelstrafen nach NIS-2 und DSGVO sind ausgeschlossen.

Nationale Umsetzung notwendig

Die Richtlinie tritt am 16.01.2023 in Kraft und ist bis Oktober 2024 in nationales Recht umzusetzen. Bei der genauen Umsetzung und Ausgestaltung der Pflichten verbleibt den Mitgliedstaaten Spielraum. Wie genau die Ausgestaltung aussehen wird, ist daher noch abzuwarten.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de