الاتحاد الأوروبي

توجيه NIS2

(Directive EU 2022/2555)

تدابير لمستوى مشترك مرتفع من الأمن السيبراني عبر الاتحاد

ملخص بالعربية للمسؤولين عن أمن المعلومات ومسؤولي الامتثال

مرجع الوثيقة

الحقل	القيمة
الاسم الرسمي	Directive (EU) 2022/2555
تاريخ الاعتماد	14 ديسمبر 2022
تاريخ النشر	27 ديسمبر 2022 (OJ L 333/80)
تاريخ دخول النفاذ	16 يناير 2023
الموعد النهائي للنقل إلى التشريع الوطني	17 أكتوبر 2024
الصك الملغى	Directive (EU) 2016/1148 (NIS1)

> This document is an unofficial summary of the EU NIS2 Directive of 14 December 2022; it is not an authoritative translation. For binding interpretation, consult the official text at OJ L 333/80, 27.12.2022.

جدول المحتويات

1. الملخص التنفيذي
2. الغرض والأساس القانوني
3. من NIS1 إلى NIS2: لماذا تشريع جديد؟
4. النطاق والمجالات المستثناة
5. التعريفات الرئيسية
6. فئات الكيانات: الكيانات الأساسية والكيانات المهمة
7. القطاعات الخاضعة للتوجيه (Annex I وAnnex II)
8. التزامات الدول الأعضاء
9. تدابير إدارة مخاطر الأمن السيبراني (Article 21)
10. التزامات الإبلاغ عن الحوادث (Article 23)
11. أمن سلسلة التوريد
12. مسؤولية هيئة الإدارة
13. هياكل التعاون على مستوى الاتحاد الأوروبي
14. الإشراف والتنفيذ
15. الغرامات الإدارية
16. الجدول الزمني للتنفيذ والانتقال
17. التداعيات على الشركات غير الأوروبية
18. خارطة طريق الامتثال العملية (10 خطوات)
19. الخلاصة والتقييم

1. الملخص التنفيذي

يُعدّ **توجيه NIS2** (Directive EU 2022/2555)، الذي اعتمده البرلمان الأوروبي والمجلس في 14 ديسمبر 2022، التوجيه الأوروبي العام للحد الأدنى من معايير الأمن السيبراني. يلغي هذا التوجيه ويحلّ محلّ توجيه NIS1 السابق (2016/1148) اعتبارًا من 18 أكتوبر 2024.

خلصت المراجعات إلى أن NIS1، رغم إسهامه في رفع مستوى الصمود السيبراني عبر الاتحاد، أثبت عدم كفايته في مواجهة التهديدات السيبرانية الراهنة والمستقبلية. يوسّع NIS2 النطاق توسيعًا جوهريًا، ويُرسي معايير موحدة، ويُعزز التزامات إدارة المخاطر والإبلاغ عن الحوادث، ويُوفّر أحكامًا أكثر ردعًا في مجال التنفيذ.

الركائز الخمس للتوجيه

1. **النطاق الموسّع**: إخضاع قطاعات وشركات أكثر للتنظيم.
2. **إدارة المخاطر المشددة**: إلزامية 10 تدابير تقنية وتنظيمية حدّية بموجب Article 21.
3. **الإبلاغ السريع والمتدرج عن الحوادث**: إنذار مبكر خلال 24 ساعة، وإخطار بالحادث خلال 72 ساعة، وتقرير نهائي في غضون شهر واحد.
4. **مسؤولية هيئة الإدارة**: إمكانية مساءلة الإدارة العليا شخصيًا.
5. **عقوبات رادعة**: غرامات إدارية تصل إلى 2% من إجمالي المبيعات السنوية العالمية أو 10 ملايين يورو.

2. الغرض والأساس القانوني

يستند التوجيه قانونيًا إلى **Article 114 من معاهدة عمل الاتحاد الأوروبي (TFEU)**، الذي يُجيز اتخاذ تدابير لتقريب القواعد الوطنية بهدف إنشاء السوق الداخلية وضمان سيرها.

تتمثل الأهداف الرئيسية للتوجيه في:

- إزالة التفاوتات الكبيرة بين الدول الأعضاء ووضع قواعد حدّية مشتركة للأمن السيبراني؛
- إرساء آليات فعّالة للتعاون العابر للحدود وتبادل المعلومات؛
- تحديث قائمة القطاعات والأنشطة الخاضعة لالتزامات الأمن السيبراني لتعكس مشهد التهديدات الراهن؛
- توفير آليات التنفيذ والإنصاف التي تكفل التطبيق الفعّال للالتزامات؛
- تعزيز قدرات الصمود السيبراني لمشغّلي البنية التحتية الحيوية ومزوّدي الخدمات الرقمية.

يُطبّق التوجيه دون الإخلال بقانون الاتحاد الأوروبي المتعلق بحماية البيانات الشخصية (GDPR، Regulation EU 2016/679) والخصوصية في الاتصالات الإلكترونية (Directive 2002/58/EC)، وبما يتوافق معهما.

3. من NIS1 إلى NIS2: لماذا تشريع جديد؟

شكّل NIS1، الذي دخل حيّز النفاذ عام 2016، أول تشريع أفقي للأمن السيبراني في الاتحاد الأوروبي. كشفت عملية المراجعة عن تباينات جسيمة في التطبيق بين الدول الأعضاء، إذ تُرك تحديد النطاق إلى حدٍّ بعيد لتقدير كل دولة عضو مما أفضى إلى تجزئة السوق الداخلية.

أوجه القصور التي رُصدت في NIS1

مجال الإشكالية	وضع NIS1	حل NIS2
تحديد النطاق	متروك لتقدير الدولة العضو؛ تباين كبير في الممارسة.	قاعدة موحدة لـ "حجم الشركة" عبر الاتحاد (المؤسسات المتوسطة والكبيرة).
قائمة القطاعات	عدد محدود من القطاعات؛ استُثني جزء كبير من الاقتصاد الرقمي.	تغطية قطاعية أوسع بكثير؛ تشمل البنية التحتية الرقمية والإدارة العامة والفضاء وغيرها.
الإبلاغ عن الحوادث	أحادي المرحلة؛ تباينت المواعيد والمحتوى بين الدول الأعضاء.	إبلاغ متعدد المراحل: إنذار مبكر 24 ساعة + إخطار 72 ساعة + تقرير نهائي شهر.
إدارة المخاطر	صياغة عامة؛ غموض في الحد الأدنى من التدابير المحددة.	تُدرج Article 21 عشر فئات من التدابير الحدّية الإلزامية.
العقوبات	طُبّقت بمستويات متباينة جدًا بين الدول الأعضاء.	غرامات قصوى متناسقة على مستوى الاتحاد (10 ملايين يورو / 2% من رقم الأعمال).
مسؤولية الإدارة العليا	غير واضحة.	مسؤولية شخصية لهيئة الإدارة عن الامتثال؛ تدريب إلزامي.

لا يُعدّ NIS2 تحديثًا لـ NIS1؛ بل هو بديل صُمِّم لإرساء **إطار موحد قابل للتطبيق للأمن السيبراني** في جميع أنحاء الاتحاد.

4. النطاق والمجالات المستثناة

يُغطّي التوجيه في المقام الأول الكيانات العاملة في قطاعات **Annex I (عالية الأهمية الحيوية)** أو **Annex II (حيوية أخرى)** داخل الاتحاد الأوروبي والتي تستوفي تعريف المؤسسة المتوسطة على أقل تقدير. وفقًا لـ Article 2 من ملحق توصية المفوضية EC/2003/361، المؤسسة المتوسطة هي التي يقل عدد موظفيها عن 250 وتبلغ دورتها السنوية 50 مليون يورو كحدٍّ أقصى (أو لا يتجاوز إجمالي ميزانيتها العمومية 43 مليون يورو). يشمل NIS2 الكيانات التي تبلغ حجم المؤسسة المتوسطة أو تتجاوزه: الحد الفعلي الأدنى للكيانات الخاضعة للنطاق هو 50 موظفًا أو 10 ملايين يورو دورة (الحد الأعلى لـ "المؤسسة الصغيرة" بموجب التوصية ذاتها).

الكيانات المشمولة بصرف النظر عن الحجم

- مزوّدو شبكات الاتصالات الإلكترونية العامة ومزوّدو خدمات الاتصالات الإلكترونية المتاحة للعموم؛
- مزوّدو خدمات الثقة (بموجب eIDAS Regulation EU 910/2014)؛
- سجلات أسماء النطاقات من المستوى الأعلى (TLD) ومزوّدو خدمات DNS؛
- الكيانات التي تُعدّ المزوّد الوحيد لخدمة ما في دولة عضو أو التي قد يُلقي انقطاع خدمتها بظلاله الجسيمة على الأمن العام أو الصحة العامة أو السلامة العامة؛
- جميع كيانات الإدارة العامة المركزية (المعرَّفة وطنيًا من قِبل الدول الأعضاء).

المجالات المستثناة من النطاق

تُستثنى من نطاق التوجيه الكيانات العامة التي تنصبّ أنشطتها في معظمها على مجالات **الأمن الوطني أو الأمن العام أو الدفاع أو إنفاذ القانون** (الوقاية من الجرائم والتحقيق فيها وكشفها وملاحقتها قضائيًا). كما تُستثنى التمثيليات الدبلوماسية والقنصلية للدول الأعضاء في الدول الثالثة وخدمات الثقة المستخدمة في الأنظمة المغلقة.

5. التعريفات الرئيسية

ثمة مفاهيم أساسية ينبغي استيعابها بوضوح لتفسير التوجيه تفسيرًا سليمًا.

المصطلح	التعريف
شبكة ونظام معلومات	شبكات الاتصالات الإلكترونية، وأي جهاز أو مجموعة أجهزة تعالج البيانات الرقمية، وجميع البيانات الرقمية التي تُعالَج لتشغيل هذه الشبكات واستخدامها وحمايتها وصيانتها.
الأمن السيبراني	جميع الأنشطة اللازمة لحماية شبكات وأنظمة المعلومات والمستخدمين وغيرهم من الأشخاص من التهديدات السيبرانية.
حادث	حدث يُخلّ بتوافر البيانات المخزّنة أو المنقولة أو المعالَجة أو بأصالتها أو سلامتها أو سريتها، أو بخدمات مُقدَّمة عبر شبكات وأنظمة المعلومات أو يمكن الوصول إليها من خلالها.
حادث جسيم	حادث تسبّب أو قد يتسبّب في اضطراب تشغيلي حادٍّ للخدمات أو خسارة مالية للكيان المعني، أو أثّر أو قد يؤثّر في أشخاص آخرين طبيعيين أو اعتباريين بإلحاق ضرر مادي أو معنوي بالغ بهم.
تهديد سيبراني	أي ظرف أو حدث أو فعل محتمل قد يُلحق الضرر بشبكات وأنظمة المعلومات أو يعطّلها أو يُؤثّر فيها سلبًا بأي صورة أخرى.
تهديد سيبراني جسيم	تهديد سيبراني يمكن بناءً على خصائصه التقنية افتراض قدرته على إلحاق تأثير حادٍّ بشبكات وأنظمة معلومات كيان ما أو مستخدميه أو أشخاص آخرين، وذلك بإلحاق ضرر مادي أو معنوي بالغ بهم.
ثغرة أمنية	ضعف أو قابلية للتأثر أو خلل في منتجات أو خدمات تقنية المعلومات والاتصالات يمكن استغلاله من قِبل تهديد سيبراني.
حادث كاد يقع	حدث كان يمكن أن يُخلّ بتوافر البيانات المخزّنة أو المنقولة أو المعالَجة أو بأصالتها أو سلامتها أو سريتها، أو بالخدمات المقدَّمة عبر شبكات وأنظمة المعلومات، غير أنه جرى تفاديه بنجاح.
CSIRT	فريق الاستجابة لحوادث أمن الحاسوب، وهو الفريق التقني المنوط به التعامل مع الحوادث.
ENISA	وكالة الاتحاد الأوروبي للأمن السيبراني، تضطلع بدور استشاري وداعم محوري في تنفيذ التوجيه.

6. فئات الكيانات: الكيانات الأساسية والكيانات المهمة

يُقسّم التوجيه جميع الكيانات الخاضعة لنطاقه إلى فئتين رئيسيتين. يُحدد هذا التمييز كيفية تطبيق الالتزامات ونظام الإشراف والتنفيذ.

المعيار	الكيانات الأساسية	الكيانات المهمة
القطاع	Annex I، القطاعات عالية الأهمية الحيوية	Annex II، القطاعات الحيوية الأخرى (والمتوسطة الحجم في Annex I)
الحجم	المؤسسات الكبيرة (250 موظف فأكثر أو دورة 50 مليون يورو فأكثر)	المؤسسات المتوسطة (من 50 إلى 249 موظفًا)
نظام الإشراف	إشراف استباقي وإشراف لاحق معًا	إشراف لاحق فحسب، بناءً على دليل أو شكوى
الحد الأقصى للغرامة الإدارية	10 ملايين يورو أو 2% من إجمالي دورة الأعمال السنوية العالمية (أيهما أعلى)	7 ملايين يورو أو 1.4% من إجمالي دورة الأعمال السنوية العالمية (أيهما أعلى)
عقوبات الإدارة العليا	يجوز تطبيق حظر مؤقت على المديرين	لا يُطبَّق الحظر المؤقت على المديرين

ملاحظة مهمة: إذا كان كيان ما قد صُنِّف بوصفه "مشغّل خدمات أساسية" بموجب NIS1، جاز للدولة العضو أن تقرر اعتباره كيانًا أساسيًا مباشرةً بموجب NIS2. فضلًا عن ذلك، تُعدّ جميع الكيانات المصنَّفة "كيانات حيوية" بموجب Directive 2022/2557 (CER) تلقائيًا كيانات أساسية بموجب NIS2.

7. القطاعات الخاضعة للتوجيه (Annex I وAnnex II)

Annex I، القطاعات عالية الأهمية الحيوية

المؤسسات الكبيرة في هذه القطاعات كيانات أساسية؛ والمتوسطة منها كيانات مهمة.

القطاع	القطاع الفرعي / نوع الكيان
الطاقة	الكهرباء (التوليد والنقل والتوزيع والتوريد)؛ التدفئة والتبريد المحلي؛ النفط (خطوط الأنابيب والإنتاج والتخزين والنقل)؛ الغاز الطبيعي؛ إنتاج الهيدروجين وتخزينه ونقله
النقل	الجوي (شركات الطيران والمطارات وإدارة الحركة الجوية)؛ السكك الحديدية (مديرو البنية التحتية ومشغّلو القطارات)؛ المائي (مشغّلو النقل البحري والنهري)؛ البري (أنظمة النقل الذكية ومشغّلو الطرق)
الخدمات المصرفية	مؤسسات الائتمان بموجب Regulation (EU) 575/2013
البنية التحتية للأسواق المالية	أسواق التداول (البورصات) والأطراف المقابلة المركزية (CCP)
الصحة	مزوّدو الرعاية الصحية؛ المختبرات المرجعية الأوروبية؛ الكيانات التي تُجري أبحاثًا وتطويرًا للأدوية؛ شركات تصنيع الأدوية؛ شركات تصنيع الأجهزة الطبية المعتبَرة حيوية خلال حالات الطوارئ الصحية العامة (بموجب Regulation (EU) 2022/123)
مياه الشرب	موردو مياه الشرب البشري وموزّعوها
مياه الصرف	الكيانات التي تجمع مياه الصرف الحضرية أو المنزلية أو الصناعية أو تعالجها أو تتخلص منها
البنية التحتية الرقمية	نقاط تبادل الإنترنت (IXP)؛ مزوّدو خدمات DNS (باستثناء نظام أسماء النطاقات الجذري)؛ سجلات أسماء نطاقات المستوى الأعلى TLD؛ مزوّدو خدمات الحوسبة السحابية؛ مزوّدو خدمات مراكز البيانات؛ مزوّدو شبكات توصيل المحتوى (CDN)؛ مزوّدو خدمات الثقة؛ مزوّدو شبكات/خدمات الاتصالات الإلكترونية العامة
إدارة خدمات تقنية المعلومات والاتصالات (بين الشركات)	مزوّدو الخدمات المُدارة (MSP)؛ مزوّدو خدمات الأمن المُدارة (MSSP)
الإدارة العامة	كيانات الحكومة المركزية والإقليمية كما تُعرّفها الدول الأعضاء
الفضاء	مشغّلو البنية التحتية الأرضية التي تُديرها الدول الأعضاء أو القطاع الخاص

Annex II، القطاعات الحيوية الأخرى

القطاع	القطاع الفرعي / نوع الكيان
البريد والبريد السريع	مزوّدو الخدمات البريدية (بما تشمل خدمات البريد السريع)
إدارة النفايات	الكيانات التي تُقدّم خدمات جمع النفايات وإعادة تدويرها والتخلص منها
المواد الكيميائية	الكيانات العاملة في إنتاج المواد الكيميائية ومعالجتها وتوزيعها
الغذاء	المؤسسات الكبيرة العاملة في إنتاج الغذاء ومعالجته وتوزيعه بالجملة
التصنيع	الأجهزة الطبية وأجهزة التشخيص المختبري المعتمَدة في الجسم؛ المنتجات الحاسوبية والإلكترونية والبصرية؛ المعدات الكهربائية؛ الآلات والمعدات غير المصنفة في مكان آخر؛ المركبات الآلية والمقطورات ونصف المقطورات؛ تصنيع معدات النقل الأخرى
مزوّدو الخدمات الرقمية	الأسواق الإلكترونية؛ محركات البحث الإلكترونية؛ منصات الشبكات الاجتماعية
البحث العلمي	المنظمات البحثية التي تُجري أبحاثًا ذات طابع تجاري

8. التزامات الدول الأعضاء

يفرض التوجيه التزامات على الدول الأعضاء إلى جانب الكيانات الخاصة. يتعيّن على كل دولة عضو اتخاذ الخطوات التالية:

الاستراتيجية الوطنية للأمن السيبراني. اعتماد استراتيجية وطنية للأمن السيبراني تتضمن أهدافًا استراتيجية واضحة وأولويات وإطارًا للحوكمة. تتناول الاستراتيجية موضوعات من قبيل أمن سلسلة التوريد وبرامج الفدية ودعم المؤسسات الصغيرة والمتوسطة والمصدر المفتوح والدفاع السيبراني الاستباقي.

السلطة (السلطات) المختصة. تعيين سلطة أو أكثر من السلطات المختصة أو إنشائها لضمان تطبيق التوجيه والإشراف على تنفيذه.

نقطة الاتصال الواحدة (SPOC). تعيين نقطة اتصال واحدة مسؤولة عن التنسيق العابر للحدود على مستوى الاتحاد الأوروبي.

CSIRT. إنشاء CSIRT واحد أو أكثر أو تعيينه، مكلّف بالتعامل مع الحوادث والرصد الاستباقي والإفصاح المنسق عن الثغرات والتعاون الوطني والدولي.

قائمة الكيانات. مسك قائمة بالكيانات الأساسية والمهمة والكيانات المقدمة لخدمات تسجيل أسماء النطاقات، وتحديثها دوريًا وإرسالها إلى المفوضية.

الإفصاح المنسق عن الثغرات. تعيين CSIRT منسقًا؛ وتعزيز الوضوح القانوني للباحثين في مجال الثغرات الأمنية.

المساعدة المتبادلة. تقديم المساعدة المتبادلة للدول الأعضاء الأخرى في الإشراف والتنفيذ العابر للحدود.

دعم المؤسسات الصغيرة والمتوسطة. تقديم الإرشادات والأدوات المجانية ونقطة اتصال وطنية أو إقليمية للشركات الصغيرة والمتناهية الصغر.

9. تدابير إدارة مخاطر الأمن السيبراني (Article 21)

يُعدّ Article 21 أهم أحكام التوجيه التقنية. يُحدد الحد الأدنى من التدابير التقنية والتشغيلية والتنظيمية الواجب تطبيقها من قِبل الكيانات الأساسية والمهمة. يستند هذا النهج إلى **منظور "جميع المخاطر"**؛ لا تقتصر التغطية على الهجمات السيبرانية بل تمتد لتشمل التهديدات كالأضرار المادية والكوارث الطبيعية وأعطال المعدات والأخطاء البشرية.

Article 21: العشرة تدابير الحدّية

#	التدبير	الوصف
1	تحليل المخاطر وسياسات أمن نظام المعلومات	تحليل جميع المخاطر وإعداد سياسات عامة لأمن المعلومات كتابيًا.
2	التعامل مع الحوادث	عمليات الوقاية من الحوادث والكشف عنها والاستجابة لها والتعافي منها.
3	استمرارية الأعمال	إدارة النسخ الاحتياطية والتعافي من الكوارث وإدارة الأزمات.
4	أمن سلسلة التوريد	بما يشمل الممارسات الأمنية للموردين؛ وأحكام الأمن السيبراني في عقود الموردين المباشرين.
5	الأمن في اقتناء شبكات وأنظمة المعلومات وتطويرها وصيانتها	الأمن طوال دورة الحياة، بما يشمل التعامل مع الثغرات والإفصاح عنها.
6	تقييم فاعلية التدابير	تقييم دوري لفاعلية تدابير إدارة المخاطر.
7	ممارسات النظافة السيبرانية الأساسية والتدريب على الأمن	ممارسات النظافة السيبرانية وبرامج التوعية للموظفين.
8	التشفير والترميز	سياسات استخدام التشفير؛ والتشفير من طرف إلى طرف حيثما كان ذلك مناسبًا.
9	أمن الموارد البشرية والتحكم في الوصول وإدارة الأصول	فحص أمن الموظفين والتفويض وجرد الأصول.
10	المصادقة متعددة العوامل والاتصالات الآمنة	المصادقة متعددة العوامل (MFA) حيثما كان ذلك مناسبًا، والمصادقة المستمرة، والاتصالات الصوتية والمرئية والنصية الآمنة، وأنظمة الاتصالات الآمنة في حالات الطوارئ.

تُطبَّق هذه التدابير وفق **مبدأ التناسب**، مع مراعاة حجم الكيان ومستوى تعرّضه للمخاطر وأهميته القطاعية والأثر المحتمل للحوادث.

10. التزامات الإبلاغ عن الحوادث (Article 23)

أبرز ابتكار تشغيلي في التوجيه هو نظام الإبلاغ متعدد المراحل عن الحوادث. يتعيّن على الكيانات الأساسية والمهمة الإبلاغ عن **الحوادث الجسيمة**، وهي تلك التي تُسبّب اضطرابًا تشغيليًا حادًا أو خسارة مالية أو أثرًا بالغًا على أشخاص آخرين، إلى CSIRT أو السلطة المختصة ضمن الأطر الزمنية الآتية:

المرحلة	الموعد النهائي	المحتوى
الإنذار المبكر	خلال 24 ساعة من الإدراك بالحادث	الاشتباه في أن الحادث نتيجة عمل غير مشروع أو خبيث؛ احتمال وجود أثر عابر للحدود؛ معلومات أساسية تُمكّن CSIRT من الاطلاع على الحادث.
الإخطار بالحادث	خلال 72 ساعة من الإدراك بالحادث	تحديث للإنذار المبكر؛ الخطورة والأثر ومؤشرات الاختراق (IoCs) حين تتوافر.
التقرير المرحلي/ النهائي	في غضون شهر واحد على الأكثر من الإخطار بالحادث	وصف تفصيلي للحادث وخطورته وأثره؛ نوع التهديد المُستغَل؛ التدابير التخفيفية المتخذة والمخطط لها؛ الأثر العابر للحدود إن وُجد.
تقرير التقدم	إذا كان الحادث لا يزال قائمًا عند موعد التقرير النهائي	تقرير متابعة عن الوضع الراهن للحادث؛ تقرير نهائي بعد شهر من انتهاء التعامل مع الحادث.

الإخطار للمستفيدين من الخدمة: عندما يكون ثمة احتمال بوقوع تهديد سيبراني جسيم، يجب على الكيانات إخطار المستفيدين من خدماتها دون تأخير غير مبرر ومجانًا بالتدابير التخفيفية الممكنة، وبالتهديد ذاته حين يقتضي الحال، وذلك بلغة واضحة ومفهومة.

حوادث كادت تقع والإبلاغ الطوعي

علاوةً على الحوادث، **يجوز للكيانات طوعًا الإبلاغ عن حوادث كادت تقع والتهديدات السيبرانية الجسيمة** إلى CSIRT أو السلطة المختصة. كما يجوز للكيانات الواقعة خارج نطاق التوجيه الإبلاغ طوعًا. لا يُفضي الإبلاغ الطوعي إلى فرض التزامات إضافية على المُبلِّغ.

> **الأثر العملي:** يُلزم الإنذار المبكر خلال 24 ساعة الكيانات بالاستعداد المسبق لخطة للاستجابة لحوادث الأمن السيبراني وتدفق اتصالاتها قابلَين للتفعيل فور رصد الحادث. بالغ هو الصعوبة استيفاء هذا الموعد عبر عمليات يدوية ومتشعبة.

11. أمن سلسلة التوريد

في السنوات الأخيرة، وصلت معظم الهجمات السيبرانية الكبرى إلى المنظمات المستهدفة عبر الموردين ومزوّدي البرمجيات لا عبر الهجوم المباشر عليها. لذا يضع التوجيه مخاطر سلسلة التوريد في صميم التزامات إدارة المخاطر.

- يتعيّن على الكيانات تقييم **جودة الممارسات الأمنية وعمليات التطوير الآمن** لدى منتجات وخدمات مورّديها ومزوّدي خدماتها.
- **ينبغي إدراج متطلبات الأمن السيبراني في العقود** المبرمة مع الموردين المباشرين.
- ينبغي توخّي عناية خاصة عند اختيار **مزوّدي خدمات الأمن المُدارة (MSSP)** إذ يُعدّ هؤلاء المزوّدون أهدافًا عالية القيمة للمهاجمين.
- تُجري مجموعة التعاون، إلى جانب المفوضية وENISA، **تقييمات منسقة لمخاطر الأمن** لسلاسل التوريد الحيوية (على غرار ما جرى بشأن شبكات الجيل الخامس 5G).
- **عوامل المخاطر غير التقنية** مشمولة أيضًا في نطاق التقييم، بما فيها التأثير غير المشروع المحتمل لدول ثالثة على الموردين والثغرات/المداخل الخلفية المخفية والتبعية لمزوّد بعينه.

12. مسؤولية هيئة الإدارة

يكفل التوجيه انتقال الأمن السيبراني من كونه شأنًا محصورًا في الأقسام التقنية إلى **نطاق المسؤولية المباشرة للإدارة العليا**. وفقًا لـ Article 20، تلتزم هيئات إدارة الكيانات الأساسية والمهمة بما يلي:

- تحمّل مسؤولية **الموافقة على تدابير إدارة المخاطر** بموجب Article 21 والإشراف على تنفيذها؛
- إمكانية **مساءلتها شخصيًا** في حال الإخلال بهذه الالتزامات؛
- تلقّي تدريب دوري على الأمن السيبراني لاكتساب المعرفة والمهارات الكافيتين؛
- تشجيع موظفيها على الخضوع لتدريب مماثل.

> **ملاحظة مهمة:** في الكيانات الأساسية، يجوز للسلطة المختصة أن تطلب تطبيق **حظر مؤقت على الإدارة** على كبار المديرين (المدير التنفيذي أو الممثل القانوني). هذا إجراء أخير يُلجأ إليه فقط بعد استنفاد جميع خيارات التنفيذ الأخرى.

13. هياكل التعاون على مستوى الاتحاد الأوروبي

ينظّم التوجيه أو يعزز هياكل متعددة تكفل التعاون الفعّال بين الدول الأعضاء:

الهيكل	الوظيفة
مجموعة التعاون	تدعم التعاون على المستوى الاستراتيجي؛ وتُعِدّ برامج عمل كل سنتين؛ وتنشر وثائق إرشادية؛ وتُجري تقييمات منسقة للمخاطر في سلاسل التوريد الحيوية.
شبكة CSIRTs	تعاون على المستوى التشغيلي؛ وتبادل معلومات الحوادث؛ ومساعدة متبادلة؛ واستجابة مشتركة.
EU-CyCLONe	شبكة ارتباط أوروبية لإدارة الأزمات السيبرانية؛ تُجسّر الجانبين التقني والسياسي في الحوادث والأزمات الواسعة النطاق؛ وتُعِدّ تحليلات الأثر.
ENISA	تُنشئ قاعدة بيانات أوروبية للثغرات وتحافظ عليها؛ وتُقدّم الدعم التقني؛ وتُطوّر التوجيهات؛ وترصد سياسات النظافة السيبرانية للدول الأعضاء.
ترتيبات IPCR	ترتيبات الاستجابة المتكاملة للأزمات السياسية الأوروبية (Council Implementing Decision 2018/1993)، وإدارة الأزمات على مستوى الاتحاد في الأزمات الواسعة النطاق.
منسق EU-CSIRTs CVD	يُعيَّن CSIRT في كل دولة عضو منسقًا لإدارة الإفصاح المنسق العابر للحدود عن الثغرات.

التعاون مع الدول الثالثة: يجوز للاتحاد الأوروبي إبرام اتفاقيات دولية مع الدول الثالثة أو المنظمات الدولية بموجب TFEU Article 218. يجوز لهذه الاتفاقيات، مع صون مصالح الاتحاد وحماية البيانات، أن تُتيح لهذه الأطراف المشاركة في أنشطة مجموعة التعاون أو شبكة CSIRTs أو EU-CyCLONe.

14. الإشراف والتنفيذ

يُتيح التوجيه أنظمة إشراف مختلفة للفئتين. تخضع **الكيانات الأساسية** لكلا نوعَي الإشراف الاستباقي واللاحق، فيما تخضع **الكيانات المهمة** للإشراف اللاحق فحسب، بناءً على دليل أو شكوى.

صلاحيات الإشراف للسلطات المختصة

- إجراء عمليات تفتيش ميداني ورقابة عن بُعد؛
- طلب عمليات تدقيق أمني موجّهة (مع احتمال تحمّل الكيان التكاليف)؛
- الأمر بإجراء فحوصات أمنية؛
- طلب وثائق تُثبت الامتثال لتدابير إدارة المخاطر؛
- طلب معلومات حول أفعال يُشتبه في أنها تنتهك التوجيه؛
- طلب معلومات تستلزم الوصول إلى البيانات الشخصية وبيانات حركة المرور حين يكون ذلك ضروريًا.

تدابير التنفيذ المتاحة

- إصدار تحذيرات وتعليمات ملزمة؛
- الأمر باتخاذ تدابير بعينها أو معالجة ثغرات خلال مدة محددة؛
- الأمر بإجراء تدقيق مستقل للتحقق من تدابير إدارة المخاطر؛
- إلزام الكيانات بإعلام مستفيدي الخدمة بطبيعة الخرق؛
- الإصدار العلني للبيانات (الإفصاح عن اسم الكيان وطبيعة الخرق)؛
- للكيانات الأساسية (كملاذ أخير): التعليق المؤقت للشهادات أو التفويضات والحظر المؤقت على كبار المديرين؛
- فرض غرامات إدارية أو السعي لفرضها.

15. الغرامات الإدارية

يحدد التوجيه **حدودًا قصوى متناسقة على مستوى الاتحاد الأوروبي** للغرامات الإدارية التي تفرضها الدول الأعضاء. وهذه الحدود مرتبطة بإجمالي دورة أعمال الكيان العالمية، على غرار GDPR.

نوع الكيان	الحد الأقصى للغرامة (يُطبَّق أيهما أعلى)
الكيانات الأساسية	10,000,000 يورو أو 2% من إجمالي دورة الأعمال السنوية العالمية
الكيانات المهمة	7,000,000 يورو أو 1.4% من إجمالي دورة الأعمال السنوية العالمية

العوامل المؤثرة في تحديد الغرامات

- طبيعة المخالفة وجسامتها ومدتها؛
- الضرر المادي أو المعنوي المُلحَق؛
- ما إذا كانت المخالفة متعمدة أم ناجمة عن إهمال؛
- التدابير المتخذة للوقاية من الضرر أو التخفيف من حدته؛
- درجة المسؤولية والمخالفات السابقة؛
- درجة التعاون مع السلطة المختصة؛
- سائر العوامل المشددة أو المخففة.

يتعيّن أن تكون الغرامات **متناسبة**، وأن تُراعى في تطبيقها الحقوق الأساسية كحق الدفاع وقرينة البراءة وحق الانتصاف الفعّال. يجوز للدول الأعضاء أيضًا النص على عقوبات جنائية للمخالفات القانونية الوطنية؛ غير أنه لا يجوز معاقبة أي شخص مرتين على الفعل ذاته تطبيقًا لمبدأ **ne bis in idem**.

16. الجدول الزمني للتنفيذ والانتقال

التاريخ	الحدث
14 ديسمبر 2022	اعتماد التوجيه من البرلمان الأوروبي والمجلس
27 ديسمبر 2022	النشر في الجريدة الرسمية للاتحاد الأوروبي (OJ L 333/80)
16 يناير 2023	دخول التوجيه حيّز النفاذ (بعد 20 يومًا من النشر)
17 أكتوبر 2024	الموعد النهائي لنقل التوجيه إلى التشريعات الوطنية
18 أكتوبر 2024	بدء تطبيق التوجيه
18 أكتوبر 2024	إلغاء Directive (EU) 2016/1148 (NIS1)
17 أبريل 2025	الموعد النهائي لإرسال الدول الأعضاء قائمة الكيانات الأساسية والمهمة إلى المفوضية
17 أكتوبر 2027 فصاعدًا	المراجعة الدورية من قِبل المفوضية لتنفيذ التوجيه (كل 36 شهرًا)

ملاحظة مهمة: NIS2 توجيه ولا يُطبَّق مباشرةً. يتعيّن على كل دولة عضو نقل التوجيه إلى قانونها الوطني الخاص. لذا تتوقف الالتزامات والعقوبات المحددة المطبّقة على كيان ما على قانون النقل الوطني الذي اعتمدته الدولة العضو التي يعمل فيها.

17. التداعيات على الشركات غير الأوروبية

على الرغم من أن NIS2 توجيه أوروبي، تترتب عليه تداعيات جوهرية على الشركات غير الأوروبية، ولا سيما تلك التي تخدم السوق الأوروبية أو تُزوّد كيانات حيوية مقرّها الاتحاد الأوروبي:

الشركات غير الأوروبية المتأثرة مباشرةً

- يتعيّن على مزوّدي **DNS وخدمات الحوسبة السحابية ومشغّلي مراكز البيانات ومزوّدي CDN والخدمات المُدارة وخدمات الأمن المُدارة والأسواق الإلكترونية ومحركات البحث ومنصات الشبكات الاجتماعية** غير الأوروبيين الذين يُقدّمون خدمات داخل الاتحاد الأوروبي تعيين ممثل أوروبي والامتثال لالتزامات التوجيه؛
- قد تخضع الشركات غير الأوروبية التي لديها شركات تابعة أو فروع داخل الاتحاد للتوجيه من خلال هذه الوحدات؛
- سيخضع الموردون غير الأوروبيون الذين يُقدّمون منتجات وخدمات للكيانات الأساسية والمهمة الأوروبية **لمتطلبات تعاقدية خاصة بأمن سلسلة التوريد** يفرضها عملاؤهم (Article 21(2)(d))؛
- قد يقع MSPs/MSSPs غير الأوروبيون الذين يخدمون البنية التحتية الرقمية أو الكيانات المالية الأوروبية مباشرةً ضمن نطاق التوجيه.

التأثيرات غير المباشرة

- تُجبر تقييمات مخاطر سلسلة التوريد التي يُجريها العملاء الأوروبيون الموردين غير الأوروبيين على رفع معايير الأمن السيبراني لديهم؛
- باتت المعايير التي يُرسيها التوجيه (ISO/IEC 27001 وإرشادات ENISA وغيرها) **نقاط مرجعية فعلية** في السوق العالمي؛
- يستخدم المزيد من الدول خارج الاتحاد NIS2 مرجعًا عند صياغة تشريعاتها الخاصة بالأمن السيبراني.

18. خارطة طريق الامتثال العملية (10 خطوات)

تُشكّل خارطة الطريق ذات العشر خطوات التالية دليلًا عمليًا سواء للشركات العاملة داخل الاتحاد الأوروبي أو لتلك التي تسعى إلى التوافق الطوعي مع معايير NIS2.

الخطوة	النشاط
1. تحديد النطاق	تحديد ما إذا كانت الشركة تقع ضمن قطاعات Annex I أو Annex II وتستوفي معايير الحجم، وتحديد فئتها (أساسية/مهمة).
2. تحليل الفجوات	تقييم نظام إدارة أمن المعلومات القائم في مقابل العشر فئات من التدابير الواردة في Article 21؛ ورسم خريطة الفجوات.
3. هيكل الحوكمة	تحديد المسؤوليات وخطوط الإبلاغ وعمليات الموافقة على مستوى مجلس الإدارة والإدارة العليا؛ وإعداد برنامج تدريبي منتظم.
4. السياسات والتوثيق	إعداد سياسة أمن المعلومات وسياسة إدارة المخاطر وسياسة الاستجابة للحوادث وسياسة الاستخدام المقبول وغيرها من الوثائق أو تحديثها.
5. تقييم المخاطر	إجراء جرد للأصول وتحليل للتهديدات وتقييم للمخاطر بمنهجية جميع المخاطر؛ ووضع معايير قبول المخاطر.
6. تطبيق الضوابط التقنية	تطبيق المصادقة متعددة العوامل (MFA) والتشفير وتجزئة الشبكات وهندسة الثقة الصفرية وإدارة السجلات ونظم SIEM وEDR/XDR والنسخ الاحتياطي وحلول التعافي من الكوارث.
7. قدرة الاستجابة للحوادث	توثيق خطة الاستجابة للحوادث؛ وتحديد الأدوار والمسؤوليات؛ وإرساء تدفق اتصالات الإنذار المبكر خلال 24 ساعة؛ وإجراء تمارين محاكاة على الطاولة.
8. إدارة سلسلة التوريد	جرد الموردين؛ وتصنيفهم وفق مستوى المخاطر؛ وإضافة أحكام الأمن السيبراني إلى نماذج العقود؛ وإجراء عمليات تدقيق دورية.
9. التدريب والتوعية	تنفيذ تدريب سنوي على النظافة السيبرانية لجميع الموظفين؛ وتقديم تدريب متخصص لهيئة الإدارة؛ وإجراء محاكاة لهجمات التصيد الاحتيالي.
10. التحسين المستمر	إجراء عمليات تدقيق داخلية وخارجية؛ وتتبّع مؤشرات الأداء الرئيسية (KPIs)؛ والتعلم من كل حادث؛ وتحديث تقييم المخاطر سنويًا؛ والسعي للحصول على الشهادات (ISO/IEC 27001 وشهادة الأمن السيبراني الأوروبية).

19. الخلاصة والتقييم

يرفع توجيه NIS2 المعيارَ الأساسي للأمن السيبراني في الاتحاد الأوروبي رفعًا جوهريًا. لا يقتصر على فرض متطلبات تقنية؛ بل يجعل الأمن السيبراني **جزءًا لا يتجزأ من هيكل حوكمة الشركات وعملياتها التجارية**.

نقاط قوة التوجيه

- **النطاق الواسع**: نحو 18 قطاعًا وأكثر من 100,000 كيان خاضع للتوجيه في دول الاتحاد الأوروبي السبع والعشرين؛
- **التوحيد**: تكافؤ الفرص في السوق الداخلية من خلال معايير موحدة ونظام تنفيذ موحد عبر الاتحاد؛
- **التركيز على الحوكمة**: ضمان تغلغل الأمن السيبراني في جميع طبقات الشركة عبر إخضاع الإدارة العليا للمساءلة؛
- **التركيز على سلسلة التوريد**: الاستجابة لواقع أن غالبية الهجمات الحديثة تأتي عبر سلسلة التوريد؛
- **هياكل التعاون**: تنسيق متعدد المستويات على مستوى الاتحاد من خلال مجموعة التعاون وشبكة CSIRTs وEU-CyCLONe.

الانتقادات والتحديات

- تأخيرات وتباينات في نقل التشريع الوطني لدى الدول الأعضاء؛ والتطبيق الموحد عمليًا عبر الاتحاد الأوروبي السبع والعشرين غير منتظم؛
- تُشكّل تكلفة الامتثال وسدّ الفجوة في القدرات التقنية تحديًا جسيمًا، ولا سيما بالنسبة للمؤسسات المتوسطة؛
- قد يُفضي تطبيق موعد الإنذار المبكر خلال 24 ساعة قبل بلوغ قدر كافٍ من النضج إلى تدفقات إبلاغ سطحية أو مغلوطة؛
- قد تُشكّل مناطق التداخل مع اللوائح القطاعية (DORA في المجال المالي؛ وeIDAS في خدمات الثقة؛ ولوائح الطيران القطاعية وغيرها) تعقيدًا إضافيًا على الكيانات.

التقييم الشامل

يُعيد NIS2 تأطير الأمن السيبراني من مجرد شاغل تقني إلى **مسألة استمرارية أعمال وحوكمة مؤسسية وثقة للعملاء**. بالنسبة للكيانات العاملة داخل الاتحاد الأوروبي أو المتعاملة معه، يُمثّل الامتثال التزامًا قانونيًا ووسيلةً لتعزيز الصمود التشغيلي في آنٍ واحد.

بالنسبة للشركات غير الأوروبية، يُرسي NIS2 **معيارًا فعليًا جديدًا** للوصول إلى السوق الأوروبية ويرفع توقعات الأمن السيبراني على الصعيد العالمي. يُيسّر الامتثال المبكر استيفاء الالتزامات التعاقدية ويُحسّن الصمود السيبراني الكلي.

> **Final note:** This document summarises the directive's main provisions for English-speaking readers. For compliance requirements specific to your organisation, review the official text (OJ L 333/80, 27.12.2022), the national transposition act of your Member State, and sector-specific regulations; engage legal and cybersecurity counsel where appropriate.

المصادر

- Directive (EU) 2022/2555، EUR-Lex CELEX number 32022L2555
- Official Journal of the EU L 333/80، 27 December 2022
- ENISA، European Union Agency for Cybersecurity (www.enisa.europa.eu)
- بوابة الاستراتيجية الرقمية للمفوضية الأوروبية (digital-strategy.ec.europa.eu)

المزيد حول NIS2 من Rediacc

يرسم هذا الملخص هيكل التوجيه والتزاماته. تُترجم الأدلة المرافقة على rediacc.com تلك الالتزامات إلى قرارات تشغيلية وشرائية ملموسة.

ثلاثة أدلة مرافقة

- **Article 21(2)(d) والاستضافة الذاتية.** لماذا يتقلص سجل تقنية المعلومات الخارجية حين لا تغادر بيانات التشغيل بيئتك. موجّه إلى المسؤولين عن أمن المعلومات ومسؤولي الشراء الذين يُعيدون التفاوض على اتفاقيات معالجة البيانات في عام 2026.
- **فاعلية مستمرة بلا مسرحية.** Article 21(2)(e) وArticle 23(f) معًا. تفرّع الوقت الثابت الذي يجعل التدريبات الأسبوعية قابلة للتطبيق، والجدول الزمني للإبلاغ بموجب Article 23 الذي لا يمكنك استيفاؤه دون توفر مصنوعات ذات جودة جنائية رقمية. موجّه إلى مسؤولي هندسة الموثوقية والعمليات.
- **التكلفة الهيكلية للامتثال لـ NIS2.** المجموعة المؤلفة من خمس أدوات التي تُجمّعها هادئةً الكيانات الأساسية في السوق المتوسطة، وما يختزله مستوى التحكم المستضاف ذاتيًا، والبنود التي تظل لك في كلٍّ من الحالتين. موجّه إلى المدراء الماليين والمشترين المقبلين على دورة تجديد.

أين تجدها

الأدلة الثلاثة جميعها، إلى جانب هذا الملخص بصيغة PDF قابلة للتنزيل، متاحة على:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ منصة بنية تحتية مسجَّلة في إستونيا تعتمد الاستضافة الذاتية (رقم السجل التجاري 17363830، الرقم الضريبي VAT EE102920091). المنتج ليس بديلًا عن برنامج أمني؛ بل هو طبقة أدوات تُزيل مخاطر بيانات التشغيل الخاصة بالموردين التي لا تستطيع أدوات النسخ الاحتياطي والتعافي من الكوارث وبيانات الاختبار التقليدية إزالتها. تتوافر خطة مجتمعية مجانية وخطط مدفوعة تبدأ من 349 دولار شهريًا.

> This document and its companion guides are educational material. Compliance decisions specific to your organisation require legal counsel and reference to the national transposition act in your jurisdiction.