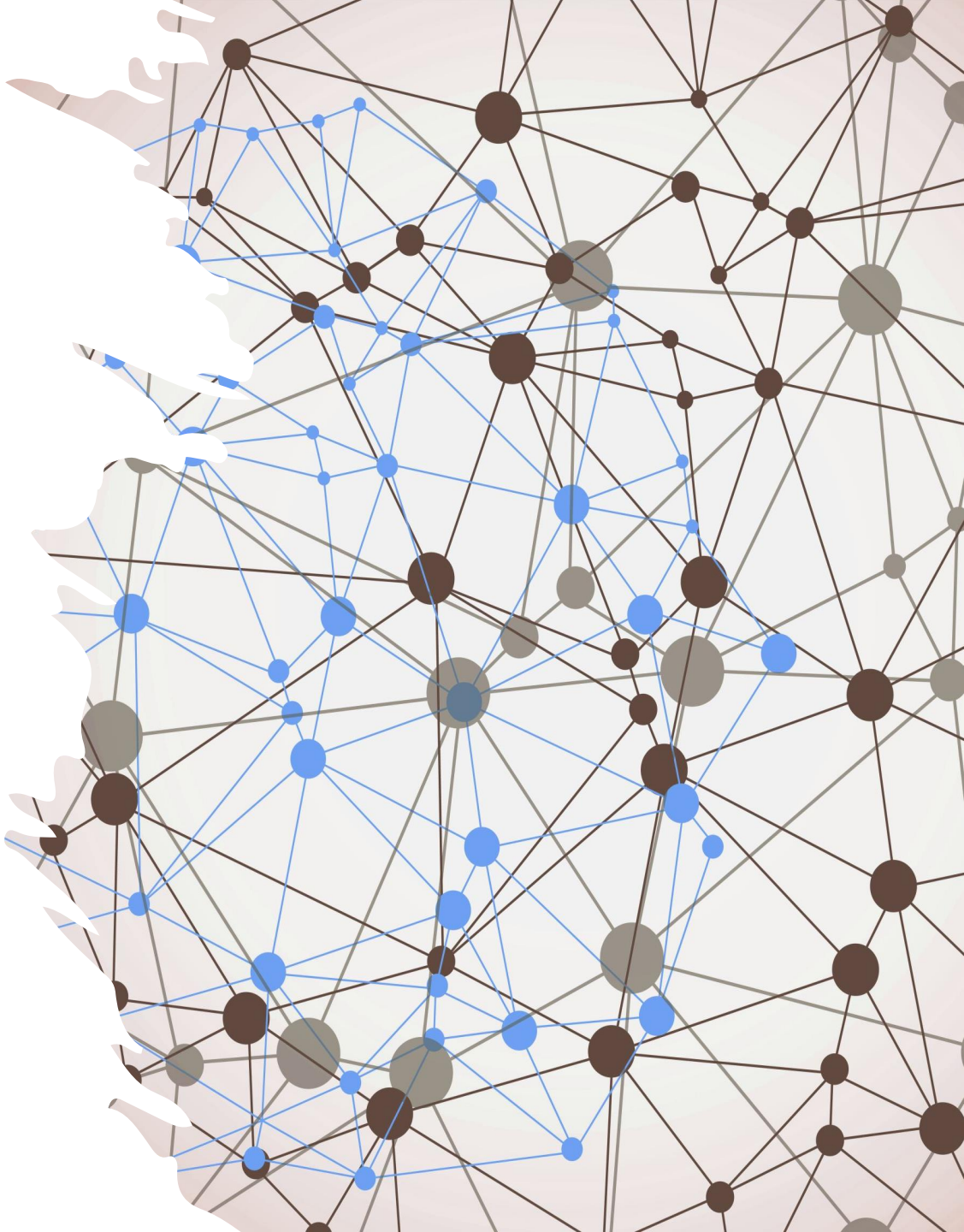
NIS2-FELKÉSZÜLÉS A GYAKORLATBAN

dr. Markó-Tichy Krisztián
Jambrik Ügyvédi Iroda

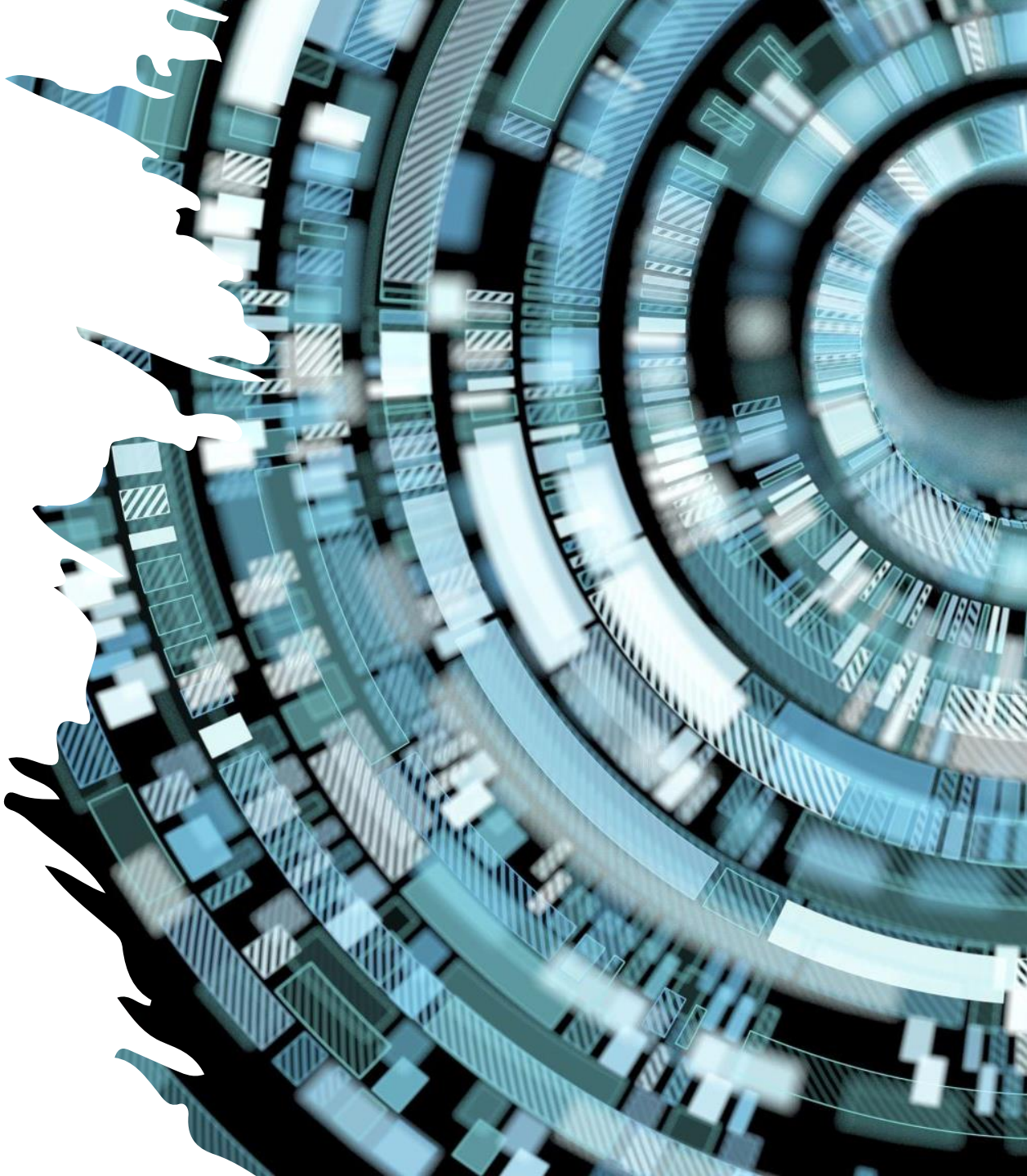
MELASZ ESIGN DAY

Budapest, 2024. június 28.



Bevezetés és előzmények:

- EU digitális jogalkotási csomagja
  Pl. DSA, DMA, AI A CT, NIS2
- NIS1 irányelv
- GDPR – Megelőző adatvédelmi jogszabályok, NAIH gyakorlat



Implementációs sarokkövek

- Jogszabályi követelmények azonosítása
- Belső folyamatok és ellenőrzések kialakítása -jogi elvárások vállalat belső működésére való „átfordítása
- Már meglevő eszközök, folyamatok felhasználása
- Képzések és tudatosságnövelés
- Kommunikáció a különböző érintettekkel
- A megfelelési folyamatok rendszeres felülvizsgálata
- A megfelelés ne kényszer legyen, hanem innováció é így versenyelőny

Feladatok priorizálása a jogi felkészülésben

- **Kockázatértékelés:** A legnagyobb kockázatot jelentő jogi kérdések azonosítása
- **Források allokálása:** Az erőforrásokat a prioritást élvező feladatokra súlyozni
- **Taktikai lépések:** Rövid távon megvalósítható intézkedéseket kell először hozni
- **Stratégiai tervezés:** Hosszú távú jogi stratégia tervezése a vállalat jövőbeli növekedési tervei és jogszabályi változások figyelembevételével
- **Monitoring, felülvizsgálat:** Kiberbiztonsági kockázatok ellenőrzése és értékelése, jogszabályi megfelelés állapotának figyelemmel kísérése

NIS 2 és a Kibertan tv. (2023. évi XXXIII. tv)

- **Kiemelten kockázatos ágazatokban** működő szolgáltatók és szervezetek, konkrét példa: digitális infrastruktúra, azon belül felhőszolgáltató és hírközlési szolgáltatás, azon belül **bizalmi szolgáltatók**
- **Kockázatos ágazatokban** működő szolgáltatók és szervezetek, konkrét példa: postai szolgáltatók, hulladékgazdálkodás
- Ide tartoznak a digitális (nem infrastruktúra) szolgáltatók is, például domainnév regisztrátor

NIS2 HATÓSÁGI NYILVÁNTARTÁSBA VÉTEL I.

- **Határidő: 2024.06.30.** (2024. január 1. után megkezdett működés esetén a határidő 2024. december 31.)
- **Önazonosítás alapján**, erre rendszeresített hatósági űrlapon cégkapun keresztül, ingyenes
- **Tevékenységek:** energetika, közlekedés, egészségügy, hírközlés, digitális infrastruktúra és szolgáltatások, gyártás, egyebek (posta, űr stb.)
- **Felelős személy (IBF):**

  Megbízott vagy foglalkoztatott

  Célszerűségi szempontok: kapcsolattartás magyar nyelven, informatikai ismeretek megléte
- **Szükséges adatok:**

  Szervezet alapadatai: név, cégjegyzékszám, adószám , székhely, alapítás dátuma

  További adatok (ha van ilyen): például nyilvános honlap, ügyfélportál, online ügyfélszolgálat, telefonos ügyfélszolgálat

NIS2 HATÓSÁGI NYILVÁNTARTÁSBA VÉTEL II.

Kkvtv. szerinti besorolás

Kibertan tv. főszabálya: több mint **50 alkalmazott** vagy több mint **10 millió euró** éves nettó árbevétel: középvállalkozásokat, nagyvállalkozásokat érinti

- **Középvállalkozás:**

  250 főnél kevesebb alkalmazott és éves nettó árbevétel **50 millió euró** / mérlegfőösszeg legfeljebb **43 millió euró**

- **Kisvállalkozás:**

  50 főnél kevesebb alkalmazott és éves nettó árbevétel / mérlegfőösszeg legfeljebb **10 millió euró**

- **Mikrovállalkozás:**

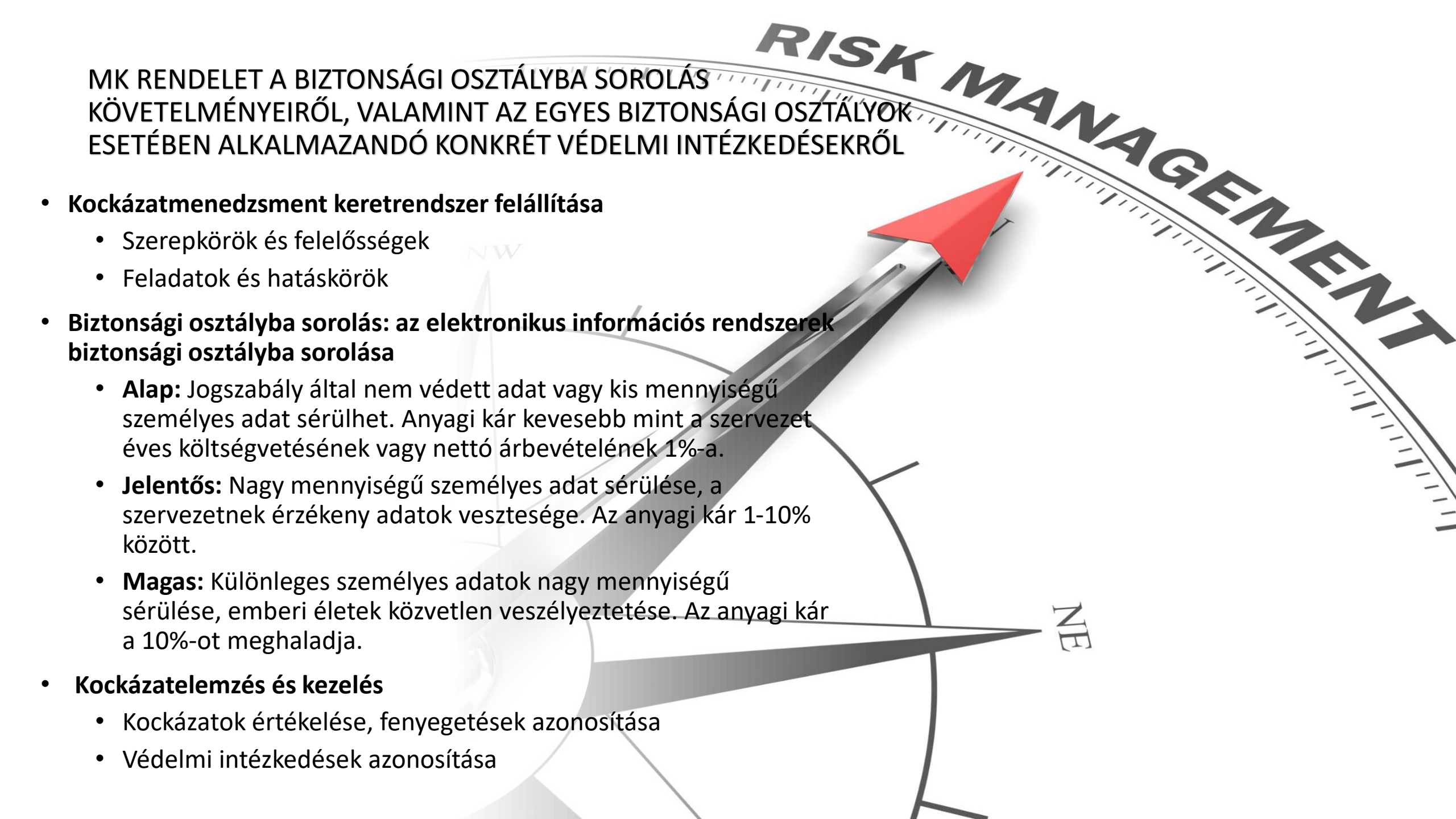
  10 főnél kevesebb alkalmazott és éves nettó árbevétele / mérlegfőösszege legfeljebb **2 millió eurónak** megfelelő forintösszeg

NIS2 HATÓSÁGI NYILVÁNTARTÁSBA VÉTEL III.

FŐSZABÁLY ALÓLI KIVÉTELEK

- Elektronikus hírközlési szolgáltató
- Bizalmi szolgáltató
- DNS-szolgáltatást nyújtó szolgáltató
- Legfelső szintű domainnév-nyilvántartó
- Domainnév-regisztrációt végző szolgáltató

MK RENDELET A BIZTONSÁGI OSZTÁLYBA SOROLÁS KÖVETELMÉNYEIRŐL, VALAMINT AZ EGYES BIZTONSÁGI OSZTÁLYOK ESETÉBEN ALKALMAZANDÓ KONKRÉT VÉDELMI INTÉZKEDÉSEKRŐL



- **Kockázatmenedzsment keretrendszer felállítása**
  - Szerepkörök és felelősségek
  - Feladatok és hatáskörök
- **Biztonsági osztályba sorolás: az elektronikus információs rendszerek biztonsági osztályba sorolása**
  - **Alap:** Jogszabály által nem védett adat vagy kis mennyiségű személyes adat sérülhet. Anyagi kár kevesebb mint a szervezet éves költségvetésének vagy nettó árbevételének 1%-a.
  - **Jelentős:** Nagy mennyiségű személyes adat sérülése, a szervezetnek érzékeny adatok vesztesége. Az anyagi kár 1-10% között.
  - **Magas:** Különleges személyes adatok nagy mennyiségű sérülése, emberi életek közvetlen veszélyeztetése. Az anyagi kár a 10%-ot meghaladja.
- **Kockázatelemzés és kezelés**
  - Kockázatok értékelése, fenyegetések azonosítása
  - Védelmi intézkedések azonosítása

Védelmi intézkedések és fenyegetések I.

Védelmi intézkedések katalógusa

1. Programmenedzsment

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	1.1. Információbiztonsági szabályzat	1.1. A szervezet: 1.1.1. Kidolgozza és kihirdeti az információbiztonsági szabályzatot, amely: 1.1.1.1. átfogó képet nyújt a biztonsági követelményekről, valamint a követelményeknek való megfelelés érdekében a szervezet által működtetett, vagy bevezetni kívánt védelmi intézkedésekről. 1.1.1.2. meghatározza a célkitűzéseket, a ható- és szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat. 1.1.1.3. Leírja az információbiztonságért felelös szervezeti egységek közötti együttműködést. 1.1.1.4. A szervezet vezetője által kerül jóváhagyásra, aki felelősséget vállal és elszámoltatható a szervezeti müveletek (beleértve a célkitüzéseket, funkciókat, imázst és hírnevet), a szervezeti eszközök, személyek, más szervezetek szempontjából számottevőnek tartott kockázatokért. 1.1.2. Felülvizsgálja és frissíti az információbiztonsági szabályzatot a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően. 1.1.3. Gondoskodik arról, hogy az információbiztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.	X	X	X

Védelmi intézkedések és fenyegetések II.

63.	2.62. Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz	2.62. A szervezet megköveteli, hogy a meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező fiókok felhasználói a nem biztonsági funkciók használatához ne privilegizált fiókot vagy szerepkört használjanak.	-	X	X

12.	Külső szolgáltatók hibája, vagy működési zavara	B, S, R

* Bizalmasság: B Sértetlenség: S Rendelkezésre állás: R

További feladatok

- **Védelmi intézkedések rangsorolása és végrehajtása**
  - Hatékonyság
  - Költségek
  - Kivitelezési kihívások
- **Döntéshozatal a rendszer üzembe helyezéséről** (vezető nem átruházható felelőssége)
  - Rendszerbiztonsági terv
  - Kockázatelemzés
  - Intézkedési terv
- **Folyamatos felügyelet és naprakészen tartás**

Felelősségi kérdések

- **Felügyeleti díj:** Előző évi árbevétel 0,015 %-a, de maximum 10 M Ft, határidő 2024. október 18.
- **Felügyeleti eszközök:** Hatósági ellenőrzés, Rendkívüli ellenőrzés elrendelése, Figyelmeztetés, Eltiltás (egyéb hatóságokkal együttműködve), Bírság
- **Szankciós lépcsőfokok:** SZTFH figyelmeztetés, határidő tűzése a megfelelő intézkedések meghozatalára, a szervezet eltiltása a veszélyeztető tevékenységtől, pénzbírság kiszabása
- **NIS2 pénzbírság mértéke:** 10.000.000. EUR de legfeljebb az éves árbevétel 2%-a
- **305/2023. (VII. 11.) Korm. Rendelet** a kiberbiztonsági bírságok mértékéről, a bírság kiszabásának és befizetésének részletes eljárási szabályairól

Kibertan tv. határidők

Határidő	Teendő
2024. június 30.	Az érintett szervezeteknek be kell jelenteniük az SZTFH részére az azonosításhoz szükséges adataikat (önazonosítás és biztonsági osztályba sorolás, házon belüli felkészülés), valamint az általuk kijelölt biztonságért felelős személyt.
2024. október 18.	Az irányadó védelmi intézkedéseket folyamatos megfelelőség mellett kell alkalmazni.
2024. december 31.	Szerződni kell egy akkreditált kiberbiztonsági auditorral.
2025. december 31.	Az első előírt kiberbiztonsági auditot el kell végeztetni, majd kétévente újból auditáltatni.

Köszönöm a figyelmet!

JAMBRIK ÜGYVÉDI IRODA

1095 Boráros tér 7. (Duna Ház)
j@mbrik.hu
www.jambrik.hu
+36 1 428 0028