GDPR
(2018-04-05)

1.1 A "személyes adatok" és a "személyes adatok kezelésére használt rendszerek és szolgáltatások" védelme

A 32. cikk és 5. cikk követelményeit többen többféleképpen értelmezik, viszont az egyes védelmi intézkedések között jelentős eltérések vannak, ezért nem mindegy, hogy pontosan milyen támadási esetekre kell felkészülni.

1.1.1 Mik a támadási esetek, amelyek ellen a személyes adatot védeni kell rejtjelezés révén?

Ha állományok (file system) szintjén fér hozzá a támadó a rendszerhez, ahol végrehajthat állomány kimásolási műveleteket, akkor az ellen tudunk készülni. (Pl. **adatbázis állomány rejtjelezése** TDE – Transparent Data Encryption – révén, ami egy telepítési, beállítási feladat az üzemeltetők oldalán.)

Ha külső kommunikációs felületen, anonim módon fér hozzá a támadó a rendszerhez (pl. SQL-injection), ahol végrehajthat adat kimásolási műveleteket, akkor az ellen tudunk készülni. (Pl. **az adatok az adatbázis tábláiban is rejtjelezetten kerülnek tárolásra**, ami egy kódolási feladat a fejlesztők oldalán, viszont ez minden erre épülő rendszert is érint, harmadik felek által fejlesztett alkalmazások továbbfejlesztését is indukálja, ezáltal növelve a költségeket és átfutási időket, azaz nem mindegy, hogy pontosan mely támadási esetek ellen kell felkészíteni a rendszert.)

Ha másféle támadási esetet is figyelembe kell venni, akkor kérünk iránymutatást!

1.1.2 Mik a támadási esetek, amelyek ellen a személyes adatok kezelésére használt rendszerek és szolgáltatások bizalmasságát biztosítani kell?

Ha állományok (file system) szintjén fér hozzá a támadó a rendszerhez, ahol végrehajthat állomány megnyitási, kimásolási műveleteket, akkor az ellen tudunk készülni. (Pl. rendszer állományaihoz és az általa tárolt adatokhoz való **hozzáférési szabályok érvényre juttatása és a hozzáférések monitorozása**, elektronikus aláírással ellátott naplóüzenetek létrehozása, **kimenő kommunikációs csatornákon védendő adatok figyelése, blokkolása**)

Ha másféle támadási esetet is figyelembe kell venni, akkor kérünk iránymutatást!

1.1.3 Mik a támadási esetek, amelyek ellen a személyes adatok kezelésére használt rendszerek és szolgáltatások sértetlenségét biztosítani kell?

Ha állományok (file system) szintjén fér hozzá a támadó a rendszerhez, ahol végrehajthat állomány törlési, módosítási műveleteket, akkor az ellen tudunk készülni. (Pl. rendszer állományaihoz való hozzáférések monitorozása, **elektronikus aláírással ellátott naplóüzenetek létrehozása**, a rendszer által használt **állományok kriptográfiai lenyomatainak, aláírásainak folyamatos ellenőrzése** DLL-injection megelőzése céljából.)

Ha másféle támadási esetet is figyelembe kell venni, akkor kérünk iránymutatást!

Article 5
Principles relating to processing of personal data
1. Personal data shall be:

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 32
Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

1.2 Az adathalmazok szintaktikai és szemantikai követelményei

Több olyan követelmény is megfogalmazásra kerül – ezek közül a 20. cikk egyértelműen előírja –, hogy a rendszerek közötti kommunikáció miatt az együttműködési képességet biztosítani kell az adathalmazok létrehozása, kezelése során. Ehhez szükséges az egyes adathalmazok műszaki szintű, részletes leírása.

1.2.1 Mi a pontos szintaktikai és szemantikai leírása a hozzájárulásnak (meghatalmazási rendelkezésnek)

A 7. cikk szerinti hozzájárulás (meghatalmazási rendelkezés) elektronikus változata ugyanolyan jellegű, mint a banki szektorban (ld. PSD2 irányelv) vagy a kormányzati szektorban (ld. eIDAS rendelet) már létező adathalmaz, viszont a pontos adattartalom, illetve az adatstruktúra nincs részletezve a GDPR rendeletben. A leírtak alapján meg kell jelennie annak egyértelműen beazonosítható módon, hogy ki az adatkezelő, ki az érintett, akinek személyes adatait kezelheti, mi az ügy, amely kapcsán kezelheti a személyes adatokat, illetve a hozzájárulás önkéntes-e és törekszik-e csak a szükséges adatokhoz való hozzáférésre (legkevesebb jogosultság elve adathozzáférés tekintetében).

A hozzájárulásnak (meghatalmazási rendelkezésnek) olyan egységes adattartalmú és egységes adatformátumú adathalmaznak kell lennie, amit minden fél fel tud dolgozni és ugyanúgy tud értelmezni, vagyis valamilyen szabványra, műszaki specifikációra van szükség.

> ***Article 7***
> ***Conditions for consent***
> 1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*
> 2. *If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*
> 3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*
> 4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

1.2.2 Mi a pontos szintaktikai és szemantikai leírása az exportált személyes adatnak?

A 20. cikk értelmében az "érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta". Az adathordozhatósághoz való jog alapján interoperabilis módon kell tudni adatokat exportálni, importálni, azonban a pontos adattartalom, illetve az adatstruktúra nincs részletezve a GDPR rendeletben.

Az exportált személyes adatnak olyan egységes adattartalmú és egységes adatformátumú adathalmaznak kell lennie, amit minden fél fel tud dolgozni és ugyanúgy tud értelmezni, vagyis valamilyen szabványra, műszaki specifikációra van szükség.

Article 20
Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: [...]

1.3 A személyes adatok egyes kategóriáira vonatkozó egyedi követelmények

1.3.1 Melyek az egyes országokban használt "nemzeti azonosító számok"?

A 87. cikk értelmében "a nemzeti azonosító számok, illetve az egyéb általános jellegű azonosító jelek felhasználására kizárólag az érintett jogainak és szabadságainak e rendelet szerinti megfelelő garanciái mellett kerülhet sor". A jogszabálynak való megfelelés érdekében szükség lenne az egyes országokban használt "nemzeti azonosító számok" egyértelmű megadására, tételes listájára (melyek azok, milyen okmányon találhatók, mik az alapértelmezett adathozzáférési szabályok)! Ez az egyértelműsítés az eIDAS rendelet által bevezetett egyedi és időben állandó azonosítók (természetes személyre vonatkozók és nem természetes személyre vonatkozók egyaránt) miatt is szükséges lenne. Magyarországon jelenleg a "Lakcímet igazoló hatósági igazolvány" okmányon található "Személyi azonosítót igazoló hatósági igazolvány" tartalmazza a "személyi azonosító" adatot, ami vélhetőleg a hazai nemzeti azonosító szám. Más EU tagállamokban ehhez hasonló jellegű adatok kezelése eltérő lehet. Pl. Észtország állampolgárainál az elektronikus azonosításhoz is használt tanúsítványokban megjelenik az ottani nemzeti azonosító szám ("Subject" mező "serialNumber" néveleme), azonban a tanúsítvány egy nyilvános adat (nem csak EU állampolgárai, hanem bárki számára), míg a magyar "személyi azonosító" alapértelmezetten nem (pl. külön engedély szükséges állampolgár részéről az okmány fénymásolásához). Szükséges tehát az EU tagállamokban használt nemzeti azonosító számok egyértelmű listájának összeállítása, illetve az ezekre vonatkozó alapértelmezett paraméterek (pl. nyilvános/titkos) megadása!

> ***Article 87***
> ***Processing of the national identification number***
> *Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.*