A GDPR

EGYSZERŰEN KIS- ÉS KÖZÉPVÁLLALKOZÁSOK
SZÁMÁRA

LINA JASMONTAITĖ-ZANIEWICZ / ALESSANDRA CALVI,
NAGY RENÁTA ÉS DAVID BARNARD-WILLS (SZERK.)

A GDPR
EGYSZERŰEN KIS- ÉS KÖZÉPVÁLLALKOZÁSOK SZÁMÁRA

A GDPR EGYSZERŰEN KIS- ÉS KÖZÉPVÁLLALKOZÁSOK SZÁMÁRA

A MAGYAR NYELVŰ FORDÍTÁS AZ ALÁBBI KIADÁS ALAPJÁN KÉSZÜLT:

'THE GDPR MADE SIMPLE(R) FOR SMES', VUBPRESS 2020

A KÉZIKÖNYV AZ EURÓPAI UNIÓ JOGOK, EGYENLŐSÉG ÉS POLGÁRSÁG 2014-2020 PROGRAMJÁNAK TÁRSFINANSZÍROZÁSÁBAN (REC-RDAT-TRAI-AG-2017), A 814775 AZONOSÍTÓSZÁMÚ STAR II (SUPPORT SMALL AND MEDIUM ENTERPRISES ON THE DATA PROTECTION REFORM II) PROJEKT KERETÉBEN KÉSZÜLT.

NYILATKOZAT: A KÖNYV TARTALMA NEM FELTÉTLENÜL TÜKRÖZI AZ EURÓPAI BIZOTTSÁG ÁLLÁSPONTJÁT.

ISBN 978-615-00-9975-0

A BORÍTÓT TERVEZTE © VUBPRESS - FRISCO
BELSŐ MEGJELENÉS © VUBPRESS – FRISCO

TÖRDELÉS ÉS NYOMTATÁS:
MAGYAR KÖZLÖNY LAP- ÉS KÖNYVKIADÓ KFT.

Tartalomjegyzék

Köszönetnyilvánítás

A kézikönyv az Európai Unió Jogok, Egyenlőség és Polgárság 2014-2020 programjának társfinanszírozásában (REC-RDAT-TRAI-AG-2017) a 814775 azonosítószámú STAR II (SupporT small And medium enterprises on the data protection Reform II) projekt keretében készült.

A STAR II projekt 2018 augusztusa és 2020 novembere között futott a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) (Koordinátor), a brüsszeli Vrije Egyetem LSTS kutatócsoportja és Trilateral Research Ltd partnerségében.

A kézikönyv szerkesztésében a STAR II Konzorcium tagjai vettek részt: az adatvédelem területén átfogó elméleti tapasztalattal rendelkező brüsszeli Vrije Egyetem Law Science Technology and Society (LSTS) interdiszciplináris kutatócsoportjának munkatársai, Lina Jasmontaite és Alessandra Calvi; az adatvédelem területén kutatási és tanácsadási szolgáltatásokat nyújtó Trilateral Research Ltd. multidiszciplináris kutatócsoportjának tagja, David Barnard-Wills, valamint a KKV-k tájékoztatására irányuló tevékenységekben aktív szerepet vállaló Nemzeti Adatvédelmi és Információszabadság Hatóság munkatársa, Nagy Renáta.

A projekt célja az Általános Adatvédelmi Rendelet (a továbbiakban GDPR vagy Rendelet) követelményeinek való megfelelés elősegítése az adatvédelmi hatóságok és a kis- és középvállalkozások kölcsönös kötelezettségeikben való támogatásával. Ennek érdekében a STAR II projekt keretében elkészült egy kézikönyv az adatvédelmi hatóságoknak a KKV-k számára működtetett információs vonalakról, valamint a személyes adatok kezelésére vonatkozó kötelezettségeket és legjobb gyakorlatokat bemutató kézikönyv az európai szabályozásról kis- és középvállalkozások számára.

A STAR II projekt a STAR I projektet követi, melynek keretében könnyen felhasználható képzési anyagokat dolgoztunk ki az adatkezelési tevékenységekben részt vevő munkatársak képzésének lebonyolításáért

felelős adatvédelmi szakemberek, különösen az adatvédelmi tisztviselők számára.

Köszönettel tartozunk Annika Linck-nek, az European Digital SME Alliance munkatársának az Előszóért. Köszönjük a STAR II projekt Külső Tanácsadó Testület tagjainak, és azoknak az adatvédelmi szakembereknek a közreműködését, akik javaslatokkal segítették a munkánkat a kézikönyv összeállítása során. Különösen szeretnénk megköszönni Jasmina Trajkovski (T&P Consulting), Denise Amram (LIDER Lab – DIRPOLIS Institute) és Erin Anzelmo munkáját.

Felelősség és jognyilatkozat

A kézikönyv nem feltétlenül tükrözi az Európai Unió álláspontját.

A kézikönyv a 2020. szeptember 30. napján érvényes jogszabályok figyelembevételével íródott.

A STAR II Konzorcium minden erőfeszítést megtett a kézikönyvben szereplő információk helyessége és pontossága érdekben, de nem vállal felelősséget az itt megjelenő információval összefüggésben. A kézikönyv nem minősül szakmai vagy jogi tanácsadásnak.

Rövidítések listája

AEPD (Agencia Española Protección de Datos)	spanyol DPA
APD-GBA (Autorité de protection des données Gegevensbeschermings-autoriteit)	belga DPA
CNIL (Commission nationale de l'informatique et des libertés)	francia DPA
CSIR(T) (Computer Security Incident Response (Team))	Számítógép-biztonsági incidenskezelő csoport
CSV (Comma Separated Values)	vesszővel tagolt adatfájl
DPA (Data Protection Authority)	adatvédelmi hatóság
DPbD (Data Protection by Design)	beépített adatvédelem
DPbDf (Data Protection by Default)	alapértelmezett adatvédelem
DPC (Data Protection Commission)	ír DPA
DPIA (Data Protection Impact Assessment)	adatvédelmi hatásvizsgálat
DPO (Data Protection Officer)	adatvédelmi tisztviselő
EDPB (European Data Protection Board)	Európai Adatvédelmi Testület
EDPS (European Data Protection Supervisor)	Európai Adatvédelmi Biztos
EGT	Európai Gazdasági Térség
EU	Európai Unió
GDPR (General Data Protection Regulation)	Általános Adatvédelmi Rendelet
ICO (Information Commissioner's Office)	brit DPA

IP (Informacijski pooblaščenec)	szlovén DPA
JSON	JavaScript Object Notation formanyelv
KKV	kis- és középvállalkozás
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
NGO	civil szervezet
NIS (Network and Information Security)	információs és hálózatbiztonság
PSD2 (Payment Service Directive) -	Pénzforgalmi Szolgáltatásokról szóló módosított EU-irányelv
PSI (public sector information) –	közszféra információ
RDF (Resource Description Framework)	Erőforrás Leíró Keretrendszer
SOP(s) (Standard Operating Procedure(s))	Szabványos működési eljárás(ok)
VDAI (Valstybinė duomenų apsaugos inspekcija)	litván DPA
WP29	WP29 munkacsoport
XML	kiterjeszthető jelölőnyelv

Előszó

A STAR II Konzorcium azzal a céllal állította össze ezt a kézikönyvet, hogy könnyebben érthetővé tegye az Általános Adatvédelmi Rendeletet a kis- és középvállalkozások számára. A részletes kézikönyv támogatja a KKV-kat a jogi kötelezettségeiknek való megfelelésben. A kézikönyv önmagában nem tudja könnyebben emészthetővé tenni a GDPR-t a KKV-k számára, ehhez az adatvédelmi hatóságok, a vállalkozások és a társadalom folyamatos elköteleződésére és munkájára is szükség van. Mindazonáltal a kézikönyv kiemelten fontos eszköze a KKV-k támogatásának, mert közérthető nyelven nyújt tájékoztatást a GDPR legfontosabb rendelkezéseiről (például a kockázatalapú megközelítésről, továbbá gyakorlati példákkal és jogesetekkel segíti a KKV-kat a GDPR-ból eredő kötelezettségeik megértésében).

A KKV-k az Európai Unióban működő vállalkozások közel 99 százalékát teszik ki, ezzel a foglalkoztatás és a gazdasági növekedés legnagyobb részéért ezek a vállalkozások felelősek. A GDPR-nak való megfelelés mégis problémát okozhat a KKV-knak, mert az esetleges meg nem felelésük jelentős következményekkel járhat bírságok vagy az ügyfeleik bizalomvesztése képében. Sajnos a nagyobb vállalkozásokkal szemben a legtöbb KKV nem rendelkezik megfelelő forrásokkal, amiket erre célra fordíthatna. A szükséges belső források és tapasztalatok hiányában a GDPR kockázatalapú megközelítésének értelmezése körüli jogi bizonytalanság is kihívás elé állítja a kisebb vállalkozásokat. Számos KKV kénytelen külső jogi tanácsadásra támaszkodni, ami pluszköltségeket jelent számukra. Továbbá a Rendelet formális előírásai, mint például a nyilvántartásvezetési-kötelezettség is további adminisztrációs terhet ró a KKV-kra.

Mindeközben a nagyobb csúcsvállalatok továbbra is megkérdőjelezhető adatkezelési gyakorlatot folytatnak. Amíg a GDPR több jogot garantál a természetes személyeknek és megteremti az uniós adatvédelmi

szabályozás keretét, nem képes szabályozni a nagyvállalatok személyes adatok kiaknázásán alapuló, hirdetésközpontú üzleti modelljét. A DIGITAL SME Alliance tagjainak nagy része nem támaszkodik a hirdetésalapú üzleti modellre, ezáltal kisebb veszélynek teszi ki a természetes személyek alapvető jogait. Mindazonáltal ezek a vállalkozások is kötelesek megfelelni a GDPR előírásainak, és végre kell hajtaniuk az uniformizált rendelkezéseit, miközben nem rendelkeznek a nagyvállaltokhoz hasonló anyagi és emberi erőforrásokkal (belső szakértők).

Az egységes uniós adatvédelmi jog területe még kialakulóban van, és jelentős kihívásokkal néz szembe a GDPR egységes alkalmazásának területén. Az adatvédelmi hatóságok feladata a KKV-k tájékoztatása, de a STAR II projekt keretében lefolytatott kutatás szerint csupán az uniós felügyeleti hatóságok kevesebb, mint egy harmada nyújt iránymutatást kifejezetten KKV-k számára. Az adatvédelmi hatóságokat különböző tényezők befolyásolhatják feladataik ellátásában, ezek a nemzeti sajátosságoktól is függenek (például a rendelkezésükre álló források és munkaerő). Ezek a körülmények bizonytalan környezetet teremtenek a KKV-k számára a személyes adatok kezelésével kapcsolatban, így nem képesek kihasználni az egységes adatvédelmi jogi szabályozás előnyeit. Az adatvédelmi hatóságok Európa-szerte más módon értelmezik és alkalmazzák a GDPR rendelkezéseit. Ez még egy adott tagállamon belül is előfordulhat, ha különböző szervek hajtják végre az adatvédelmi szabályokat. Ezért a vállalkozások gyakran nem tudják eldönteni, hogy megfelelnek-e a GDPR rendelkezéseinek vagy sem. Továbbá, ha a KKV a felügyeleti hatósághoz fordul tanácsért, csak javaslatokat és az esetleges következményekről szóló tájékoztatást kap, de a KKV-nak kell eldöntenie hogyan alkalmazza a felügyeleti hatóság javaslatát a gyakorlatban, és a jogi következményeket is a KKV viseli.

Az európai digitális térben működő kis-és középvállalkozások képviseletében a *DIGITAL SME Alliance* üdvözli a digitális egységes piacot megalapozó, könnyen érthető és uniformizált szabályozást, ami lehetővé teszi a vállalkozások- és különösen a kisebb vállalkozások számára –, hogy az EU határain belül és kívül is jogbiztonságban működhessenek és

fejlődhessenek. Ez a kézikönyv könnyen érthető és hasznos iránymutatást ad a KKV-knak, és elkíséri őket a jobb és egységesebb GDPR-megfelelés útján.

1. Bevezetés

Háttér

Az Általános Adatvédelmi Rendelet (GDPR, Rendelet) immáron több, mint két éve alkalmazandó az Európai Gazdasági Térség (EGT) tagállamaiban, ami magában foglalja az Európai Unió (EU) tagállamait, Izlandot, Liechtensteint és Norvégiát is. Az Európai Bizottság és az Európai Adatvédelmi Testület első értékelései jelentős sikernek tekintik GDPR-t[1]. A Rendelet harmonizált szabályrendszere egyértelműen hozzájárult az adatkezelési gyakorlatok javulásához és felhívta az érintettek figyelmét a jogaikra.[2] A GDPR-nak megfelelő adatkezelés versenyelőnyt jelenthet és erősítheti a vásárlói bizalmat, továbbá új üzleti lehetőségeket is rejt magában.

A megfelelés biztosítása és az ebből származó versenyelőny megszerzése az adatvédelmi alapelvek és az uniós adatvédelmi keretszabályozás megfelelő ismeretét igényli. Ez jelentős terhet ró a kisebb vállalkozásokra, különösen a kis- és középvállalkozásokra (KKV-k). Habár a legtöbb KKV fő tevékenységi körébe nem tartozik bele, nem tudja elkerülni a személyes adatok kezelését. A KKV-k nem rendelkeznek megfelelő emberi és anyagi erőforrásokkal, amit az adatvédelmi megfelelésre tudnának fordítani.[3]

1 Európai Bizottság: 'Communication – Two Years of Application of the General Data Protection Regulation | European Commission', 2020 **https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en**
Európai Adatvédelmi Testület: 'Contribution of the EDPB to the Evaluation of the GDPR under Article 97', 2020 **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf**

2 European Union, 'Special Eurobarometer 487a: The General Data Protection Regulation' (2019).

3 Például, ha a személyes adatokat a munkavállalók bérének kifizetése vagy az ügyfelekkel való kapcsolattartás céljából kezelik.

Az adatvédelmi hatóságok és adatvédelmi szakértők által összeállított iránymutatások és vélemények sokasága ellenére nem állnak a KKV-k rendelkezésére gyakorlatias, könnyen érthető és célzott iránymutatások. A Rendelet egyes rendelkezéseinek jogi értelmezése körüli bizonytalanságokat tovább erősíti, hogy egyes területeken a tagállamoknak lehetősége van eltérni a GDPR bizonyos rendelkezésitől (rendelkeznek némi mozgástérrel).

Az uniós szabályozók elismerik, hogy a GDPR-nak való megfelelés egyedülálló kihívás elé állítja a KKV-kat, ezért támogatják őket, amiben csak tudják. Azonban az adatvédelmi hatóságok a vállalkozás méretétől függetlenül számonkérik a GDPR-nak való megfelelést. Számos adatvédelmi hatóság (felügyeleti hatóság) foganatosított végrehajtási intézkedéseket KKV-kal szemben, ami Európa-szerte világossá teszi, hogy a KKV-k is kötelesek alkalmazni a Rendeletben foglaltakat. Egy belga vállalatnak 15.000 eurójába került, hogy nem felelt meg a Rendeletben foglalt tájékoztatási kötelezettségnek a cookie-k (sütik) alkalmazása során.[4] Egy másik KKV-t 20.000 euróra bírságolt meg a francia adatvédelmi hatóság, mert folyamatosan videofelvételt készített munkavállalóiról a munkaállomásukon.[5] Egy kis szállítmányozási cég 5.000 eurót fizetett azért, mert nem kötött adatkezelési szerződést az egyik üzleti partnerével.[6]

4 EDPB, The Belgian DPA has imposed a fine of €15000 on a website specialized in legal news.

5 CNIL, Délibération SAN-2019-006 du 13 juin 2019.

6 'Hessian DPA Fines Shipping Company For Missing Data Processing Agreement' (23 January 2019). https://www.jdsupra.com/legalnews/hessian-dpa-fines-shipping-company-for-76851/

Szerkezet

Fentiekre figyelemmel a STAR II Konzorcium azzal a céllal szerkesztette ezt a kézikönyvet, hogy támogassa a KKV-kat a GDPR-nak való megfelelésben. A kézikönyv összefoglalja a legfontosabb kötelezettségeket, melyeknek a KKV-knak meg kell felelniük a GDPR-nak megfelelő jogszerű adatkezelés érdekében.

Az I. fejezet *(Az adatvédelmi szabályozás térképe)* áttekintést nyújt az európai adatvédelmi terület főbb szereplőiről, bemutatja szerepüket és felelősségi körüket, és kitér arra, hogy milyen módon tudják segíteni a KKV-kat a GDPR-ból eredő kötelezettségeiknek való megfelelésben. Mivel a kézikönyv kifejezetten a KKV-kat érintő kérdéskörökre fókuszál, fontos, hogy az adatvédelmi megfelelést támogató források elérhetőségéről is tudomást szerezzenek a címzettek.

A II. fejezet *(Adatvédelmi alapismeretek)* ismerteti az adatvédelmi szabályozás hatályát és a KKV-kra vonatkozó rendelkezéseit. A fejezet a leggyakrabban felmerülő kérdések megválaszolásával bemutatja az adatvédelmi szabályozás középpontját jelentő fogalmakat és alapelveket. Az adatvédelmi megfelelési stratégia kidolgozásához elengedhetetlen ezek magas szintű ismerete. A gyakran ismételt kérdéseket a NAIH által üzemeltetett KKV- hotline-ra beérkező kérdések alapján állítottuk össze.

A III. fejezet *(A kockázatalapú megközelítés az elméletben és a gyakorlatban)* bemutatja a GDPR kockázatalapú megközelítést tartalmazó rendelkezéseit. A fejezet ismerteti az adatkezelő feladatait (GDPR 24. cikk), a beépített és alapértelmezett adatvédelem alapelvét (GDPR 25. cikk), a biztonsági követelményeket (GDPR 32. cikk), az adatvédelmi incidensre és az érintett tájékoztatására (GDPR 33. és 34. cikk), az előzetes adatvédelmi hatásvizsgálatra (GDPR 35. cikk), és az előzetes konzultációra (GDPR 36. cikk) vonatkozó szabályokat. A fejezet utolsó szakasza a magatartási kódexeket (GDPR 40. cikk) és a tanúsításokat ismerteti (GDPR 42. és 43. cikk).

Minden fejezet tartalmaz gyakorlati példákat, javaslatokat és további hasznos forrásokat is. Amennyiben elérhető, hivatkozik az adatvédelmi hatóságok döntéseire is. A kézikönyv elsősorban az uniós adatvédelmi hatóságok által kibocsátott iránymutatásokon alapul.

A IV. fejezet *(Sajátos adatkezelési tevékenységek)* a KKV-k munkavállalóira vonatkozó személyes adatok kezeléséről szól.

Módszertan

A fenti témaköröket a STAR II projekt[7] keretében azonosított, a KKV-kat leginkább foglalkoztató kérdéskörök alapján határoztuk meg. A projekt során interjúkat folytatottunk le 18 adatvédelmi hatóság képviselőjével, 22 KKV-szövetséggel és 11 KKV-val. További következtetéseket vontunk le 52-60 KKV által kitöltött online kérdőívből. A NAIH 2019. március 15. és 2020. március 15. között KKV-hotline-t (e-mailes információs vonal) működtetett, melyen a KKV-k GDPR-ral kapcsolatos kérdéseit válaszolta meg. A kézikönyvben meghatározott témakörök a KKV-hotline tapasztalatait követik.

A 2019-ben[8] lefolytatott interjúk során az adatvédelmi hatóságok és KKV-szövetségek képviselőitől kapott ajánlások alapján a kézikönyv:

- tartalmaz példákat és az uniós adatvédelmi hatóságok által kibocsátott sablonok és iránymutatások elérhetőségeit,
- bemutatja a kockázatalapú megközelítés hátterét és az elérhető jó gyakorlatokat,
- arra buzdítja a KKV-kat, hogy a GDPR-nak való megfelelésükkel szerezzenek versenyelőnyt,
- a KKV-k széles skáláját célozza meg (üzleti szektortól függetlenül),
- tisztázza a GDPR-ral kapcsolatos félreértéseket.

7 A STAR II projektről a NAIH honlapján talál további információt: **https://naih.hu/attekintes-1.html** (Főoldal/Egyéb projektek/STAR II).

8 A kutatás eredményei angol nyelven itt olvashatóak: **http://www.project-star.eu**, Deliverable D2.1 Report on DPA efforts to raise awareness among SMEs on the GDPR (Version 1.1; 2019); és STAR II, Deliverable D2.2 Report on the SME experience of the GDPR (2019).

A jogi hivatkozások a GDPR-ra vonatkoznak (ha nem jelöltük meg a pontos forrást.) A linkek a 2020. szeptember 21-én elérhető formájukban jelennek meg.

A kézikönyv hozzáadott értéke

Számos adatvédelmi hatóság bocsátott ki iránymutatásokat, némelyik kifejezetten KKV-knak szól.[9] Azonban az interjúk során a KKV-k bírálták ezeket a dokumentumokat, és arról számoltak be, hogy nem igazán használják őket. Az elérhető iránymutatásokkal szemben azt a kritikát fogalmazták meg, hogy ezek az anyagok túlságosan általánosak és csak a jogelméletre fókuszálnak. A válaszadók rámutattak, hogy a felhasználóknak kell levonniuk a következtetéseket, és feltételezések alapján kénytelenek alkalmazni a Rendeletet egy adott helyzetben.[10]

Célközönség

A kézikönyvet a KKV-k számára dolgoztuk ki. A KKV fogalma vállalkozások széles skáláját foglalja magában (például egyéni vállalkozók, családi vállalkozások, partnerségek és társulások stb.), melyek megfelelnek az alábbi kritériumoknak: 250 főnél kevesebb munkavállalót foglalkoztatnak, és éves árbevételük nem haladja meg az 50 millió eurót, és/vagy az éves mérlegfőösszegük a 43 millió eurót.[11] Természetesen a kisvállalkozások (50 főnél kevesebb munkavállalót foglalkoztatnak, és éves árbevételük és/vagy mérlegfőösszegük nem haladja meg a 10 millió eurót) és a mikrovállalkozások (10 főnél kevesebb munkavállalót foglalkoztatnak, és éves árbevételük és/vagy mérlegfőösszegük nem haladja meg a 2 millió eurót) is ebbe a kategóriába tartoznak.

9 Lásd az I. fejezetet.

10 STAR II, Deliverable D2.2 Report on the SME experience of the GDPR (2019)., p. 25.

11 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C (2003) 1422) Annex, Article 2.

2. Az adatvédelmi szabályozás térképe

Az adatvédelem területén dolgozó szakemberek gyakran úgy hivatkoznak a GDPR-nak való megfelelésre, mint egy utazásra: az egyik távoli helyről a másik távoli helyre, mely egyúttal egy hosszú és bonyolult személyes változás és fejlődés is.[12] Hasonlóan, a GDPR-nak való megfelelés sem egy egyszeri projekt, hanem egy kihívásokat rejtő folyamat. A szervezeteknek át kell tekinteniük az adatkezelési folyamataikat, és meg kell határozniuk, hogy ez milyen kockázatokat rejt magában a gyakorlatban. A folyamat során körültekintően értékelniük kell a vállalkozás egyedi jellemzőit és a működési környezetét is.

A GDPR alapelv-központú szabályozást tartalmaz, és minden vállalkozásnak lehetőséget biztosít arra, hogy a számára legmegfelelőbb megfelelési stratégiát dolgozza ki. A stratégia kialakítása, priorizálás és az intézkedések megtervezése során számos segítség áll a KKV-k rendelkezésére. Ezek közül néhányat a felügyeleti hatóságok, néhányat a magánszektor bocsátott ki. Az információgyűjtés során nagyon fontos, hogy megbízható forrásokra támaszkodjunk!

A fejezet bemutatja az uniós adatvédelmi terület legfontosabb szereplőit, ismerteti feladataikat és hatáskörüket, valamint azt, hogy milyen módon tudják támogatni a KKV-kat a GDPR-nak való megfelelésben. A fejezet szakmai szervezeteket is bemutat.

12 Oxford Dictionary, OUP 2020.

2.1. Nemzeti és regionális adatvédelmi hatóságok

A nemzeti és regionális felügyeleti hatóságok, adatvédelmi hatóságok (DPA) feladata a GDPR alkalmazásnak ellenőrzése az adott tagállamban. Minden tagállam felállít legalább egy felügyeleti hatóságot.[13] Egy adatvédelmi hatóság működik például Magyarországon, Franciaországban és Olaszországban. A szövetségi vagy decentralizált alkotmányos berendezkedésből adódóan a központi hatóság mellett regionális adatvédelmi hatóságok is működhetnek (például Németországban és Spanyolországban). Következésképpen ez azt jelenti, hogy a kompetenciák megoszlanak a központi és a regionális adatvédelmi hatóságok között.

Az adatvédelmi hatóságok emellett végrehajtó, ombudsman-jellegű, ellenőrző, konzultációs és tanácsadó szerepet is betöltenek.[14] Utóbbi a tájékoztatási tevékenységeket, és az adatkezelési tevékenységekkel összefüggő kockázatokra, szabályokra, garanciákra és jogokra vonatkozó információk megosztását jelenti. Az adatvédelmi hatóságok és az Európai Adatvédelmi Testület is bocsát ki követendő irányelveket a GDPR fogalmairól és rendelkezéseiről.

Néhány iránymutatás kifejezetten a KKV-knak szól. A STAR II projekt keretében az adatvédelmi hatóságokkal lefolytatott interjúk, valamint az EU-s adatvédelmi hatóságok honlapjának elemzése során szerzett információk alapján megállapítható, hogy jelenleg az adatvédelmi hatóságok alig egy harmada (a legutóbbi felmérés eredményeképpen csak

13 Az európai felügyeleti hatóságok listája az alábbi linken található: **https://edpb.europa.eu/about-edpb/board/members_en**

14 Bennett, Colin and Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, Cambridge MA & London, 2003, p.109–114. in David Barnard-Wills, Cristina Pauner Chulvi, and Paul De Hert, 'Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU', Computer Law & Security Review, 32.4 (2016), 587–98 (p. 587) <https://doi.org/10.1016/j.clsr.2016.05.006>.

Belgium (APD GBA)[15], Franciaország (CNIL)[16], Írország (DPC)[17], Litvánia (VDAI)[18], Szlovénia (IP)[19], Spanyolország (AEPD)[20], Svédország (Datainspektionen)[21], az Egyesült Királyság (ICO)[22] és Gibraltár (GRA) felügyeleti hatósága nyújt iránymutatást a GDPR-ról kifejezetten KKV-k számára. A magyar adatvédelmi hatóság kifejezetten KKV-k számára üzemeltetett e-mailes információs vonalat, amely különleges szereplő ebben a sorban. Az adatvédelmi hatóságok némelyike további megkülönböztetést tesz a mikrovállalkozások tekintetében is.[23]

15 Autorité de protection des données (APD) or Gegevensbeschermingsautoriteit (GBA) See 'RGPD Vade-Mecum Pour Les PME (January)' (2018)

16 Commission Nationale de l'Informatique et des Libertés (CNIL) See 'Guide Pratique de Sensibiliation Au RGPD (April)' (CNIL 2018) **https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf**

17 An Coimisiúm um Chosaint Sonrai/ The Data Protection Commission (DPC). See 'Guidance Note: GDPR Guidance for SMEs (July)' (Data Protection Commission 2019) **https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708 Guidance for SMEs.pdf**

18 Valstybinė duomenų apsaugos inspekcija (VDAI) Lásd: VDAI, 'Rekomendacija Smulkiajam Ir Vidutiniam Verslui Dėl Bendrojo Duomenų Apsaugos Reglamento Taikymo (September)' (2018) **https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_SVV_BDAR_2018.pdf**

19 Informacijski pooblaščenec (IP) Lásd: 'Varstvo Osebnih Podatkov' (Upravljavec, 2018) **https://upravljavec.si**

20 Agencia Española de Protección de Datos (AEPD). Lásd: 'Facilita RGPD' (AEPD) **https://www.aepd.es/herramientas/facilita.html**

21 Datainspektionen. Lásd: 'GDPR – Nya Dataskyddsregler' (Verksamt, 2018) **https://www.verksamt.se/driva/gdprdataskyddsregler**

22 Information Commissioner's Office (ICO). Lásd: 'Micro, Small and Medium Organisations' (ICO) **https://ico.org.uk/fororganisations/in-your-sector/business/**

23 Data Protection Commission, Guidance Note: Data Security Guidance for Microenterprises, 2019 **https://ico.org.uk/for-organisations/in-your-sector/** Information Commissioner's Office, 'How Well Do You Comply with Data Protection Law: An Assessment for Small Business Owners and Sole Traders', 2019 **https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/**

TIPP

Tekintve, hogy a GDPR az EU egész területén alkalmazandó, a KKV-k székhelyüktől függetlenül bármely uniós felügyeleti hatóság által kiadott sablont és eszközt felhasználhatják, feltéve, hogy az iránymutatást (amennyiben szükséges) hozzáigazították a nemzeti szabályozáshoz.

Az uniós adatvédelmi hatóságok listája, valamint a honlapjuk megtalálható az alábbi linken:

https://edpb.europa.eu/about-edpb/board/members_hu

2.2. Az Európai Adatvédelmi Testület

Az Európai Adatvédelmi Testület (EDPB) egy független uniós szerv, amely hozzájárul az adatvédelmi szabályok egységes alkalmazásához Európa-szerte, valamint elősegíti az adatvédelmi hatóságok közötti együttműködést. Az EDPB a nemzeti adatvédelmi hatóságok vezetőiből, az Európai Adatvédelmi Biztosból (EDPS), vagy az ő képviselőikből áll.

A GDPR hatálybalépésével átvette a független európai adatvédelmi munkacsoport, a WP29 helyét, amely a magánélethez való joggal, és az adatvédelemmel kapcsolatos kérdéskörökkel foglalkozott 2018. május 25-ig.[24] A WP29 által kibocsátott vélemények – habár nem kapcsolódnak közvetlenül a GDPR-hoz –, a mai napig hasznos eszközt jelentenek az európai adatvédelmi szabályozás kulcsfogalmainak megértéséhez.

Az EDPB rendszeresen bocsát ki véleményeket és (jogilag nem kötelező erejű) általános iránymutatásokat az európai adatvédelmi jog bizonyos területeinek tisztázása céljából. Habár az EDPB nem nyújt egyéni konzultációs szolgáltatást, az általános iránymutatásai hasznosak lehetnek a KKV-k számára.[25] Például az EDPB bocsátott ki iránymutatásokat az

24 A WP29 munkacsoportot a 95/46/EK adatvédelmi irányelv alakította meg.

25 További információk az EDPB-ről: **https://edpb.europa.eu/about-edpb/about-edpb_hu**

adatkezelő és az adatfeldolgozó fogalmának meghatározására, a hozzájárulásra, a beépített és alapértelmezett adatvédelemre vonatkozóan. Egyes iránymutatások konkrét adatkezelési tevékenységekre vonatkoznak, mint például a kamerás adatkezelések vagy a közösségi médiában történő adatkezelések.[26]

2.3. Az Európai Adatvédelmi Biztos

Az Európai Adatvédelmi Biztos (EDPS) az EU intézményeinek, szerveinek és ügynökségeinek felügyeleti hatóságaként működik.[27] Az EDPB-hez hasonlóan az EDPS is bocsát ki (jogilag nem kötelező erejű) véleményeket és általános iránymutatásokat a GDPR egyes vonatkozásaiban. Ezek elsősorban az uniós intézmények, szervek és ügynökségek számára szólnak (például az Európai Bizottság vagy Europol), de olyan gyakorlati tanácsokat fogalmaznak meg, melyeket a KKV-k is fel tudnak használni. Az EDPS bocsátott ki például egy iránymutatást az elektronikus hírközlésről (a személyes adatok kezelése és az elektronikus hírközlés az EU intézményeiben), valamint a felhő alapú szolgáltatásokról is. [28]

2.4. Európai Uniós Kiberbiztonsági Ügynökség

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) a hálózati- és információbiztonsági problémák kezelésében, megoldásában és megelőzésében támogatja az európai intézményeket, tagállamokat és vállal-

26 GDPR: Guidelines, Recommendations, Best Practices': **https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en**

27 Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

28 Az Európai Adatvédelmi Biztos iránymutatásai az alábbi linken érhetőek el: **https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en**

kozásokat.[29] Az ügynökség számos, kifejezetten KKV-k számára szóló iránymutatást bocsátott ki (például felhőbiztonsági iránymutatás KKV-k számára, KKV-nak szóló adatkezelés-biztonsági kézikönyv, iránymutatás KKV-k számára a személyes adatok biztonságos kezeléséről).[30] Ezek a források hasznosak lehetnek a GDPR technikai biztonsági előírásainak való megfeleléshez.

2.5. Az Európai Unió Alapjogi Ügynöksége (FRA)

Az Európai Unió Alapjogi Ügynöksége (FRA) tanácsokat nyújt az uniós szerveknek, intézményeknek, ügynökségeknek és a tagállami döntéshozóknak az alapvető jogokkal kapcsolatban. Az Európai Unió Alapjogi Chartájának 8. cikke alapjogként rögzíti a személyes adatok védelméhez való jogot. A FRA által kibocsátott adatvédelmi vonatkozású anyagok hasznosak lehetnek a KKV-k számára. Például a FRA kiadott egy kézikönyvet az európai adatvédelmi szabályozásról és egy iránymutatást a profilalkotásról.[31] Továbbá áttekintést nyújt a GDPR-t átültető nemzeti jogszabályokról is, például a szülői beleegyezésről.[32]

29 Az Európai Parlament és a Tanács (EU) 2019/881 számú Rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály).

30 Az ENISA iránymutatásai az alábbi linkeken érhetőek el: Cloud Security Guide for SMEs, **https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes**, Handbook on Security of Personal Data Processing specific for SMEs, **https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing** és Guidelines for SMEs on the security of personal data processing: **https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing**

31 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf** és 'Preventing unlawful profiling today and in the future (angol nyelven)': **https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide**

32 FRA, Consent to use data on children (angol nyelven): **https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/use-consent**

2.6. Uniós finanszírozású projektek

Az Európai Bizottság pénzügyi támogatást nyújt a GDPR-megfelelés elősegítését célzó projekteknek. Ezidáig három támogatási ciklusban került erre sor, 2020 májusáig 5 millió euró összegben. A két legutóbbi támogatást nemzeti felügyeleti hatóságok KKV-k és más érintettek tájékoztatására és támogatására irányuló projektje nyerte el. A projektek némelyike iránymutatásokat és képzési anyagokat dolgozott ki a tagállamok számára (ezek a hivatalos nyelvükön elérhetőek).[33] Iránymutatást bocsátottak ki például dán, holland, francia, izlandi, lett, litván és szlovén nyelven. Uniós finanszírozású projektek keretében angol nyelvű iránymutatások is készültek, például: "The DPO Handbook: Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation"[34] és a "GDPR in Your Pocket" mobil applikáció a SMEDATA Project keretében.[35]

2.7. Adatvédelmi Szakemberek Nemzetközi Szövetsége (IAPP)

Az Adatvédelmi Szakemberek Nemzetközi Szövetsége (IAPP) a világ legnagyobb globális információbiztonsági közössége, amely iránymutatásokat nyújt a tagjainak a személyes adatok kezelése során felmerülő kockázatok kezelésére vonatkozóan. Számos dokumentumot bocsátott ki a GDPR-megfelelés elősegítésére.[36] A szervezet képzési tevékenységet is folytat.

33 EC, An overview of EU funding supporting the implementation of the GDPR (angol nyelven): **https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en**

34 Marie Georges, Douwe Korff, The DPO Handbook: Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation (2019).

35 Az applikáció letölthető a Google Play Store-ban és Apple App Store-ban is: **https://smedata.eu/index.php/mobile-application/**

36 Az IAPP GDPR-ral kapcsolatos dokumentumai az alábbi linken érhetőek el: **https://iapp.org/resources/topics/eu-gdpr/**

3. Adatvédelmi alapismeretek

3.1. Mi a személyes adat és az adatkezelés?

A személyes adat és az adatkezelés fogalmának tisztázása alapvető fontosságú a GDPR-nak való megfeleléshez.[37] A GDPR csak a személyes adatok kezelésére vonatkozik, ami tehát azt jelenti, hogy ha a kezelt adatok nem személyes adatok, a GDPR nem alkalmazandó.

Személyes adatnak minősül az információ, ha közvetlenül vagy közvetetten egy egyénhez köthető, és az érintettet jogszabály védi a visszaéléssel szemben. Ezzel ellentétben, ha az információ nem köthető egy adott egyénhez, szabadon áramolhat.[38]

PÉLDA

Nem személyes adatok a műalkotások, a tudományos kutatás során előállított adatok, a statisztikai adatok, a közérdekű adatok és a környezeti adatok. [39]
Fontos:
Nem személyes adat a KKV info@cégnév.hu e-mail címe, kivéve, ha az e-mail cím tartalmaz személynevet.

37 Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) **https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679** és GDPR 4(1.).

38 Vö. például: Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról.

39 'Open Knowledge Foundation, What is open?' **https://okfn.org/opendata/**

Az úgynevezett háztartási célú adatkezelésre (a természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzett adatkezelése) nem vonatkozik a GDPR.

PÉLDA

Egy természetes személy családi fotót készít saját felhasználásra, vagy két munkatárs magántelefonszámot cserél munkán kívüli elfoglaltságok miatt (de ha telefonszámok cseréjére munkavégzés miatt kerül sor, már nem alkalmazható rá a háztartási kivétel). [40]

Ha egy vállalkozás csak kis számú személyes adatot kezel szakmai vagy üzleti tevékenysége során (például a szerződéses partnerek vagy a kapcsolattartóik adatait a szolgáltatásról szóló szerződéshez), az is személyes adatok kezelése. Mindaddig, amíg az adatkezelés a vállalkozás szakmai vagy üzleti tevékenysége vonatkozásában történik, az úgynevezett háztartási célú adatkezelésre vonatkozó kivétel nem alkalmazható.

Személyes adat az azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.[41] A fenti meghatározás nagyon tág keretet ad.

A **„bármely információ”** kitétel magában foglalja az objektív (például személyi szám és a TAJ, vérkép) és a szubjektív (az ügyfélről/munkavállalóról szóló vélemény vagy értékelés) információkat is.[42]

Személyes adat a név, azonosítószám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó adat.

40 GDPR 2(2)(c).

41 GDPR 4(1.).

42 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

Az információ természetes személyre **„vonatkozik”**, amennyiben természetes személyre *vagy* a természetes személyhez valamilyen módon köthető tárgyakra, eseményekre vagy folyamatokra vonatkozik.[43]

PÉLDA

Az autószerelő vagy a műhely által az autóról vezetett nyilvántartás információt tartalmaz az autóról, a kilométeróra állásáról, a műszaki ellenőrzések időpontjáról, a műszaki problémákról és az autó fizikai állapotáról. Ezek az információk a nyilvántartásban egy adott rendszámhoz és motorszámhoz vannak rendelve, amelyeket így a tulajdonossal össze lehet kötni. Amikor számlázás céljából a műhely összeköti a járművet és tulajdonosát, az információ a tulajdonosra vagy a jármű vezetőjére vonatkozik majd. Ha az adatokat az autót javító szerelővel kapcsolják össze (például a szerelő tevékenységének értékelése céljából), ez az információ a szerelőre is vonatkozni fog. [44]

A vállalati irodában található telefon hívásnaplózása információval szolgál több érintettről is, mint például a cég nevében hívásokat lebonyolító alkalmazottakról, az alkalmazottak által hívott ügyfelekről, bizonyos harmadik felekről (például a vállalkozás potenciális ügyfeleiről, a telefont esetleg használó biztonsági- vagy takarítószemélyzetről). [45]

Az okos energiamérő eszközök is személyes adatokat gyűjtenek a villanyfogyasztás rögzítése során. Ezek az adatok felfedhetnek

43 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

44 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

45 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

olyan szokásokat és viselkedési mintákat, melyek lehetővé tehetik a természetes személy azonosítását. [46]

Főszabály szerint egy vállalkozás (nem természetes személy) direkt marketing ajánlattal való megkeresésére nem vonatkozik a GDPR, mert a nem természetes személyek, így a vállalkozások személyes adatainak védelme nem esik a GDPR hatálya alá.[47] Ugyanakkor, amennyiben a jogi személy neve természetes személy nevéből ered, vagy a vállalati e-mail cím használata bizonyos alkalmazotthoz köthető, ezek az adatok személyes adatnak minősülnek és a GDPR hatálya alá esnek.[48]

A természetes személy azonosíthatóságának meghatározásához figyelembe kell venni minden olyan módszert, melyet felhasználhatnának az érintett azonosítására, figyelemmel az adatkezelés időpontjában rendelkezésre álló technológiákra és az azonosításhoz szükséges idő mennyiségére.[49]

A közvetlen azonosítás rendszerint név alapján történik. A közvetett azonosítás pedig számos információrészlet kombinációjával.[50]

Az érintett azonosíthatóságát álnevesítési vagy anonimizációs technikák alkalmazásával lehet befolyásolni.

46 Vagelis Papakonstantinou and Dariusz Kloza, 'Legal Protection of Personal Data in Smart Grid and Smart Metering Systems from the European Perspective' in Smart Grid Security. Springer Briefs in Cybersecurity. Springer (2015), **https://doi.org/10.1007/978-1-4471-6663-4_2**

47 Habár néhány tagállamban (például Olaszországban) a GDPR-t átültető nemzeti jogszabályok kiterjesztik a Rendelet egyes rendelkezéseinek alkalmazandóságát a jogi személyekre is.

48 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

49 GDPR (26) Preambulumbekezdés.

50 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

Az álnevesített adat további információ ismerete nélkül többé nem köthető az adott adatalanyhoz. Ezeket az adatokat elkülönítve kell tárolni, és megfelelő szervezési és technikai intézkedésekkel kell biztosítani, hogy az adatok nem köthetőek azonosított vagy azonosítható természetes személyhez.[51]

PÉLDA

Álnevesítés (pszeudonimizálás) esetén a személyes adatok, mint például a név, születési idő, nem, lakcím stb. álnévvel kerülnek helyettesítésre. Az álnevesítő technikák közé tartozik például a kulccsal történő titkosítás, a hash függvény, a tokenizálás stb.[52]

A GDPR nem tartalmazza az anonimizálás definícióját, de azt tisztázza, hogy az anonimizált adat fogalma mit jelent:

- az információ nem azonosított vagy azonosítható természetes személyre vonatkozik; vagy
- olyan személyes adatok, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.[53]

PÉLDA

Az anonimizációs technikák két fő megközelítéssel hajthatóak végre: randomizálás és generalizálás útján. Az előbbi azokat a módszereket (például zajhozzáadás és permutáció) foglalja magában, melyek az adatok pontosságát változtatják meg. Utóbbiak (például aggregálás, k-anonimitás, l-diverzálás, t-közelség) a

51 GDPR 4(5).

52 WP29 munkacsoport 05/2014. számú véleménye az anonimizálási technikákról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf**

53 GDPR (26) Preambulumbekezdés.

nagyságrendek módosításával általánosítják az adatalany tulajdonságait (például város helyett régiót adnak meg, hét helyett hónapot). [54]

Az álnevesített és anonimizált adatok között az a legfőbb különbség, hogy az álnevesített adatokra vonatkozik a GDPR[55], mert habár az anonimizált adat kiegészítő információ hiányában már nem köthető egy adott érintetthez, az adatalany közvetve azonosítható marad.[56]

Ezzel ellentétben, amennyiben minden azonosítást lehetővé tevő elemet felszámoltunk, azaz anonimizáltuk az adatot, a GDPR nem alkalmazandó.[57] A gyakorlatban azonban nehéz különbséget tenni az álnevesítés és az anonimizálás között, különösen, mert különböző szolgáltatások és technológiák „anonimizálásra" hivatkoznak, pedig valójában „álnevesítés" történt.

Egyes vélemények szerint az adatok anonimizációjának jelenlegi folyamatai kiteszik az érintetteket az újraazonosíthatóság veszélyének, mert a többi információtól függően az anonimizált adat és a személyes adat közti különbség könnyen átjárható lehet.[58]

54 A WP29 munkacsoport 05/2014. számú véleménye az anonimizálási technikákról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf**

55 WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

56 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

57 Vö. GDPR (26) Preambulumbekezdés és FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

58 Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models', NC (2019)10, 3069 https://www.nature.com/articles/s41467-019-10933-3 ,Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous data v. Personal data—A false debate: An EU perspective on anonymisation, pseudonymisation and personal data' (Brussels Privacy Symposium 2016): **https://fpf.org/wp-content/uploads/2016/11/16.10.29-A-false-debate-SSB_AK.pdf**

TIPP

Ha a KKV anonimizálás mellett dönt, meg kell bizonyosodnia róla, hogy az adatokat teljes egészében anonimizálta. Az érintettekre vonatkozó adatot kétség esetén kezeljük személyes adatként, mert ezzel biztosítani tudjuk az adatalanyok védelmét, valamint megelőzhetjük a GDPR előírásainak megszegését.

Az álnevesítés olyan technikai intézkedés, amely garantálja az adatkezelés biztonságát, és csökkenti az érintettekre leselkedő kockázatokat.

Adatkezelésnek minősül a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.[59]

PÉLDA

Adatkezelésnek minősül, ha

» egy fodrász ügyfelei nevét, keresztnevét, telefonszámait tartalmazó jegyzetet vezet;
» egy panzió tulajdonosa Excel táblázatban jegyzi fel a vendégek foglalásait és elérhetőségeit;
» a beteg alkalmazott munkaadója továbbítja az alkalmazott adatait a felelős hatósági szervnek;
» az állásra jelentkezők önéletrajzát átnézi a fejvadász;
» a KKV telefonszámokat és e-mail címeket gyűjt honlapokról direkt marketing üzenetek küldése céljából.

59 GDPR 4(2).

A GDPR magasabb szintű védelmet biztosít a személyes adatok különleges kategóriáinak:

- faji vagy etnikai származásra,
- politikai véleményre,
- vallási vagy világnézeti meggyőződésre,
- szakszervezeti tagságra utaló személyes adatok,
- a természetes személyek egyedi azonosítását célzó genetikai[60],
- biometrikus adatok[61],
- egészségügyi adatok[62],
- a természetes személyek szexuális életére, vagy
- szexuális irányultságára vonatkozó személyes adatok.[63]

Amennyiben különleges adatok kezelésére kerül sor, az adatkezelőnek a GDPR 9. cikkében felsorolt jogalapok valamelyikével rendelkeznie kell:

- az érintett kifejezett hozzájárulását adta;
- az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges;
- az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges;
- az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik;

60 Genetikai adat egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

61 Biometrikus adat egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

62 Egészségügyi adat egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

63 GDPR 9(1).

» az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
» az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges;
» az adatkezelés jelentős közérdek miatt szükséges;
» az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból szükséges;
» az adatkezelés a népegészségügy területét érintő közérdekből szükséges; vagy
» az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges.

TIPP

A különleges adatok kezelése során figyelembe kell venni az adatkezelés mértékét. Ha nagy számú különleges adat kezelése kerül sor, az adatkezelő köteles adatvédelmi hatásvizsgálatot lefolytatni.

Annak eldöntése érdekében, hogy az adatkezelés nagymértékűnek számít-e, az alábbi tényezőket kell figyelembe venni:

» az érintett adatalanyok száma (a kifejezett számuk vagy a népességhez viszonyított arányuk);

» a kezelt adatok mennyisége és/vagy köre, az adatkezelés időtartama vagy ismétlődő jellege, az adatkezelési tevékenység földrajzi kiterjedése;

» a kezelt személyes adatok nagy földrajzi területet fednek le vagy

» az adatkezelés jelentős hatással bírhat a természetes személyekre nézve.

Amennyiben az adatkezelés a fenti feltételek közül legalább egynek megfelel, feltehetően nagy mértékű adatkezelésnek minősül.

HASZNOS FORRÁSOK

» WP29 munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról: **https://ec.europa.eu/justice/https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf**

» WP29 munkacsoport 05/2014. számú véleménye az anonimizálási technikákról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf**

» ICO Anonymisation: managing data protection risk code of practice 2012 **https://ico.org.uk/media/1061/anonymisation-code.pdf**

3.2. Milyen szerepet tölthet be egy KKV az adatkezelési tevékenységekben?

A KKV-k GDPR-ból eredő kötelezettségei az adatkezelésben betöltött szerepüktől függően változnak.

Három lehetőség merülhet fel:

» a KKV lehet (önálló vagy közös) adatkezelő és saját maga végezheti az adatkezelési tevékenységet,
» megbízhat egy másik vállalkozást, az adatfeldolgozót, hogy a nevében dolgozzon fel személyes adatokat, vagy
» egy másik vállalkozás megbízásából kezel személyes adatokat, így adatfeldolgozóként jár el.

Az adatkezelők elsődleges felelősséggel bírnak az adatkezelés, valamint az adatvédelmi követelményeknek és alapelveknek való megfelelés tekintetében, és ők tehetők felelőssé az adatkezelésből eredő bármilyen

kár okozásáért, azonban a GDPR értelmében az adatfeldolgozóknak is teljesíteniük kell bizonyos jogi kötelezettségeket[64].

Az adatfeldolgozók csak akkor számoltathatóak el a GDPR-nak való megfelelésért, ha a kötelezettség kifejezetten rájuk vonatkozik, vagy az adatkezelő jogszerű utasításával ellentétesen vagy annak figyelmen kívül hagyásával jártak el.[65]

Az adatkezelési tevékenységben betöltött szerepe szerint tehát a KKV lehet:

1) **Adatkezelő**, amennyiben a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt határozza meg. Az adatkezelés célja meghatározza, hogy „miért" kezelünk személyes adatokat, az adatkezelés módja pedig azt, „hogyan" kezeljük a személyes adatokat.[66] Amennyiben a vállalkozás határozza meg a kezelt adatok körét, az adatkezelés jogalapját és időtartamát, valamint, hogy ki fér hozzá a személyes adatokhoz, akkor a vállalkozás adatkezelő.[67]

64 Például az adatfeldolgozóknak képesnek kell lenniük a GDPR-nak való megfelelésük bizonyítására, adatkezelési nyilvántartást vezetni, technikai és szervezési intézkedéseket hozni, adatvédelmi tisztviselőt kinevezni, valamint értesíteni az adatkezelőt az esetleges adatvédelmi incidensekről Lásd. FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf** A korábbi adatvédelmi irányelvhez képest a GDPR több kötelezettséget állapít meg az adatfeldolgozók számára. Lásd. Detlev Gabel and Tim Hickman, 'Chapter 11: Obligations of processors – Unlocking the EU General Data Protection Regulation' in White & Case LLP (ed.), Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law (5 April 2019): **https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection**

65 Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 (2016) JIPITEC 271 para 1. 282.

66 Data Protection Commission, 'Guidance Note: GDPR Guidance for SMEs' (July 2019): **https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708%20Guidance%20for%20SMEs.pdf**

67 A WP29 munkacsoport 1/2010. számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf**

PÉLDA

Egy gyógyfürdő és egy kozmetikus külön jogi személyek, de egy helyen nyújtanak szolgáltatást. Közös hűségprogramot indítanak (például a fürdőbelépő 5% kedvezményre jogosít a kozmetikusnál, és a kozmetikusnál 10.000 HUF feletti vásárlás esetén 5% kedvezmény jár a fürdőbelépő árából). A hűségprogramba való belépéshez az ügyfeleknek meg kell adniuk a nevüket, keresztnevüket és e-mail címüket. A közös hűségprogram során végzett adatkezelés tekintetében a kozmetikus és a fürdő közös adatkezelőnek minősül, ha együttesen határozták meg az adatkezelés lényeges kérdéseit, vagy ha külön-külön mindkét félnek érdemi ráhatása volt az adatkezelés kialakítására.

2) **Adatfeldolgozó**, amennyiben az adatkezelő nevében kezel személyes adatokat, annak utasításait követve. Az adatfeldolgozó felfogható az adatkezelő ügynökeként vagy delegáltjaként is, aki csak az adatkezelő utasításának megfelelően kezelheti a személyes adatokat.[68] Az adatfeldolgozó az adatkezelőtől különálló jogalany kell, hogy legyen.[69] Az adatkezelő írásos felhatalmazása alapján az adatfeldolgozók alkalmazhatnak alvállalkozókat.[70] Az adatkezelők eldönthetik, hogy maguk kezelik az adatokat, vagy kiszervezik ezt a tevékenységet egy adatfeldolgozónak.

PÉLDA

Egy kisállatkereskedés alkalmazottja a munkáltatója megbízásából e-mail útján küld ajánlatokat az ügyfeleknek. Ebben az esetben az adatkezelés házon belül történik, és nem kerül sor adatfeldolgozó

68 Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 (2016) 1

69 A WP29 munkacsoport 1/2010. számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf**

70 GDPR 28(2).

igénybevételére.[71] Azonban, ha a kisállatkereskedés döntést hoz arról, hogy az ügyfelei e-mail címét ajánlatok küldése céljából (is) felhasználja, és egy marketinges céget bíz meg ezzel a tevékenységgel – de a kisállatkereskedés határozza meg az adatkezelés célját –, akkor a kisállatkereskedés lesz az adatkezelő, a marketinges cég pedig az adatfeldolgozó. Az adatkezelő eldöntheti, hogy az adatkezelési műveleteket házon belül végzi vagy kiszervezi a tevékenységet egy adatfeldolgozónak.

3) **Címzett**[72]: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy **amellyel a személyes adatot közlik**, és a közlés nem az érintettől ered, függetlenül attól, hogy harmadik fél-e. A Rendelet nem határoz meg kifejezett kötelezettségeket vagy felelősségi kört a címzettekre vagy harmadik felekre vonatkozóan. Ugyanakkor, amennyiben a címzett a kapott adatokat saját célból kezelni kezdi, adatkezelőnek minősül minden saját célra történő adatkezelési tevékenység tekintetében.[73]

PÉLDA

Egy utazási iroda – amely számos eltérő úti célra szervez utazásokat – különböző szállodáknak továbbítja az érintett utasok személyes adatait, így biztosítva a más-más helyszíneken és időpontokban ügyfelei elszállásolását. A szállodák ebben a körben címzettnek minősülnek.[74]

71 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#:~:text=Employees%20of%20the%20controller%20are,data%20on%20the%20controller's%20behalf

72 GDPR 4(9).

73 Európai Adatvédelmi Testület: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (angol nyelven): https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

74 https://www.naih.hu/files/Adatved_allasfoglalas_NAIH-2018-4017-2-V_uzleti_titok.pdf

A szerepek megoszlását a tényleges helyzet határozza meg.[75] Amennyiben egy vállalkozás határozza meg az adatkezelés célját és eszközeit, adatkezelőnek minősül, függetlenül a hivatalos megnevezésétől (például a szerződésben). Egy KKV szerepe változhat az adatkezelési tevékenységektől függően, bizonyos adathalmazok tekintetében lehet adatfeldolgozó, más adathalmazok tekintetében adatkezelő.

PÉLDA

KKV1 reklámtevékenység és direkt marketing szolgáltatást nyújt KKV2 ügyfelei számára. Ebben az esetben KKV1 adatfeldolgozónak és KKV2 adatkezelőnek minősül. Azonban amennyiben KKV1 úgy dönt, hogy KKV2 ügyfélnyilvántartását más célokra használja (például harmadik KKV termékeit reklámozza nekik), akkor KKV1 ebben az adatkezelési tevékenységben adatkezelőnek minősül.

Egy ékszerész szerződést köt egy biztonsági céggel, és az ékszerüzlet több pontján kamerákat szereltet fel, melyet a biztonsági cég ellenőriz. Amíg a biztonsági cég alkalmazottai csupán figyelemmel követik a felvételeket és szükség esetén értesítik a rendőrséget, a biztonsági cég adatfeldolgozónak minősül, az ékszerész pedig adatkezelőnek.

A biztonsági cég minden olyan adatkezelési művelet tekintetében, amely meghaladja az ékszerész utasításait, és melyet saját önálló döntése alapján végez (például tárolja a felvételeket az ékszerész kérése nélkül), adatkezelőnek számít. Amennyiben a biztonsági cég csak technikai tevékenységet végez (beszereli a kamerákat), de a személyes adatokkal kapcsolatos műveleteket nem végez, még adatfeldolgozási tevékenységet sem folytat.

A GDPR előírja, hogy az adatkezelő és az adatfeldolgozó (vagy a közös adatkezelők, vagy az adatfeldolgozók és az alvállalkozók) írásos szerződést vagy egyéb uniós jogi aktusokat kötelesek kötni, ami részletezi a

75 A WP29 munkacsoport 1/2010. számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf

kölcsönös felelősségi köröket és jogokat, úgymint az adatkezelés tárgya, jellege, célja és időtartama, a kezelt személyes adatok köre és az érintettek köre.[76] Az adatfeldolgozási megállapodást az adatfeldolgozási tevékenység tényleges megkezdése előtt kell megkötni.

Ha az adatfeldolgozó alvállalkozót is bevon, az adatkezelő és az (eredeti) adatfeldolgozó között létrejött szerződésben foglalt kötelezettségek az alvállalkozóra is vonatkoznak.[77]

A közös adatkezelők adatkezelési megállapodásának meg kell határoznia az adatkezelők szerepét és kapcsolatát az érintettek vonatkozásában.[78]

PÉLDA

Az Európai Bizottság és az adatvédelmi hatóságok elfogadhatnak általános szerződési feltételeket az adatkezelők és adatfeldolgozók, valamint az adatfeldolgozók és alvállalkozók között kötött adatkezelési megállapodásokra vonatkozóan, melyeket az EDPB-nek jóvá kell hagynia.

Ezek alapvetően szolgálhatnának mintául az adatkezelő és az adatfeldolgozó közötti megállapodáshoz. Ha az adatkezelő vagy az adatfeldolgozó előzetesen jóváhagyott mintát használ a szerződéskötéshez, azt már csak kiigazítani lehet.

Mielőtt nekiállnánk a nulláról kidolgozni az adatfeldolgozási szerződést, érdemes megnézni a KKV működési helye szerinti tagállam adatvédelmi hatóságának a honlapját, hogy vajon az tett-e elérhetővé megállapodásmintákat a tagállam hivatalos nyelvén.

76 GDPR 28(3) és 28(9).

77 GDPR 28(4).

78 GDPR 26(2).

HASZNOS FORRÁSOK

» Európai Adatvédelmi Testület: Flowchart for applying the concepts of controller, processor and joint controllers in practice (in 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

» ICO: 'Controllers and processors', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

» A WP29 munkacsoport 1/2010. számú véleménye az „adatkezelő" és az „adatfeldolgozó" fogalmáról: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_hu.pdf

» FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (2. fejezet Adatvédelmi terminológia): https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf

Az adatkezelő és adatfeldolgozó közötti megállapodásra vonatkozó iránymutatások:

» ICO: 'Contracts' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

» DPC: 'Controller and Processor relationships – Guidance: A Practical Guide to Data Controller to Data Processor Contracts under GDPR' https://www.dataprotection.ie/en/organisations/know-your-obligations/controller-and-processor-relationships

» GDPR.EU: 'Data Processing Agreement (Template') https://gdpr.eu/data-processing-agreement/

» Dán adatvédelmi hatóság: 'Standard Contractual Clauses for the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)' https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf

» AEPD: 'Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas' in 'Directrices para la elaboración de contratos entre responsables y encargados del tratamiento' https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

» CNIL: 'Exemple de clauses contractuelles de sous-traitance' in the 'Guide du sous-traitant' (2017) https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

ADATVÉDELMI HATÓSÁGOK KKV-KAT ÉRINTŐ DÖNTÉSEI

A hesseni adatvédelmi hatóság egy kis hajózási vállalatot az üzleti partnereivel kötött adatkezelési megállapodás hiánya miatt bírságolt meg. A bírság hiányzó szerződésenként 5.000 euró volt. [79]

3.3. Az adatkezelés alapelvei

Az alapelveket felfoghatjuk a jogrendszer különösen fontos értékeit magukban foglaló általános normákként.[80] A GDPR hat alapelvet fogalmaz meg az adatkezelésre vonatkozóan, melyeknek az adatkezelők kötelesek megfelelni: [81]

79 'Hessian DPA Fines Shipping Company For Missing Data Processing Agreement' (23 January 2019): https://www.jdsupra.com/legalnews/hessian-dpa-fines-shipping-company-for-76851/

80 https://www.simone.it/newdiz/newdiz.php?action=view&id=149&dizionario=10 https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0063.xml

81 GDPR 5. cikk.

1. Jogszerűség, tisztességes eljárás és átláthatóság

A jogszerűség azt jelenti, hogy az adatkezelési tevékenység nem ütközhet semmilyen jogszabályba, és különösen, hogy megfelelő jogalappal kell rendelkeznie (lásd a *„Mi lehet az adatkezelés jogalapja?”* résznél).[82] A tisztességes eljárás az etikus adatkezeléssel hozható kapcsolatba, abban az értelemben, hogy a személyes adatokat oly módon kell kezelni, ahogyan azt az érintettek joggal elvárják, és nem használhatóak fel az érintetteket hátrányosan érintő jogtalan módon.[83]

Az átláthatóság azt jelenti, hogy az adatalanyokat világos és egyszerű nyelvezettel kell tájékoztatni arról, hogyan használják fel a személyes adataikat, valamint az adatkezeléssel járó kockázatokról, szabályokról, garanciákról és jogokról.[84]

2. Célhoz kötöttség

A célhoz kötöttség értelmében az adatkezelés csak az adatkezelést megelőzően meghatározott konkrét célból történhet. Minden további adatkezelésnek meg kell felelnie az eredetileg meghatározott célnak.[85] Ez az alapelv megakadályozza, hogy anélkül gyűjtsenek személyes adatokat, hogy meghatároznák a felhasználásuk módját.

3. Adattakarékosság

Az adattkarékosság értelmében a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és nem haladhatják meg a gyűjtésük és/vagy a további felhasználásuk céljához szükséges minimumot.[86]

---

82 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

83 ICO, ‚Principle (a): Lawfulness, fairness and transparency': **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/**

84 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

85 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

86 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

4. Pontosság

A pontosság azt jelenti, hogy a személyes adatokat rendszeresen ellenőrizzék és tartsák naprakészen, hogy a pontatlan adatokat haladéktalanul törölni vagy javítani tudják.[87]

5. Korlátozott tárolhatóság

A korlátozott tárolhatóság megköveteli, hogy a személyes adatokat töröljék vagy anonimizálják, ha már nincs rájuk szükség a gyűjtésük céljának eléréséhez.[88]

6. Integritás és bizalmasság

Az integritás és bizalmasság az adatbiztonsághoz kapcsolódik, és az adatvédelmi incidensek megelőzése érdekében megköveteli megfelelő technikai vagy szervezési intézkedések alkalmazását.[89]

Az adatkezelők elszámoltathatóak a hat adatvédelmi alapelvnek való megfelelésért. Ennek érdekében a KKV-k kötelesek megfelelő szervezési és technikai intézkedéseket hozni annak igazolására, hogy milyen intézkedéseket hoztak az alapelveknek való megfelelés érdekében, és ezek mennyire voltak hatékonyak.[90]

TIPP

Jogviták esetén a bíróság is hivatkozhat jogi alapelvekre, mint a jogszabályok értelmezését elősegítő vagy a joghézagokat kitöltő elvekre.[91] Hasonlóan, az adatvédelmi alapelvek is segíthetik a KKV-kat a GDPR többi rendelkezésének jobb megértésében.

87 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

88 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

89 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

90 Lásd „Az adatkezelő feladatairól, az elszámoltathatóság alapelve" című bekezdésben.

91 **https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0063.xml**

Például az adatkezelő tájékoztatási kötelezettsége[92] a jogszerűség, tisztességes eljárás és átláthatóság elvének gyakorlatba történő átültetésének egyik módja.

3.4. Mi lehet az adatkezelés jogalapja?

Háttér

A jogszerű adatkezelés érdekében a KKV-knak megfelelő jogalappal kell rendelkezniük a személyes adatok kezeléséhez.

A GDPR 6. cikke az alábbi lehetséges jogalapokat határozza meg:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Hogyan válasszuk ki a megfelelő jogalapot?

A megfelelő jogalap kiválasztása az adatkezelési tevékenységek körülményeitől függ.

92 Lásd „Az érintettek jogai" című bekezdésben.

Hozzájárulás

A hozzájárulás beszerezhető az érintettől nyilatkozat útján (írásos, szóbeli, képi vagy hang stb.) vagy megerősítő cselekedettel (kattintás, számjegy beírása stb.). A GDPR nem határozza meg a hozzájárulás formáját, így az elektronikusan is megadható, de az adatkezelőnek képesnek kell lennie a hozzájárulás megadásának bizonyítására.

A hozzájárulás érvényességének feltétele, hogy az az adatalany **önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű** kinyilatkoztatása legyen, amellyel hozzájárul személyes adatai kezeléséhez.

A gyakorlatban önkéntes hozzájárulásnak minősül, ha az adatalany arról szabadon dönthet, azaz a hozzájárulás megadását megtagadhatja vagy bármikor visszavonhatja anélkül, hogy bármilyen hátrány érné emiatt.[93] Ilyen hátrány például a megtévesztés, megfélemlítés, kényszerítés, vagy egyéb jelentős következmény.[94] Az adatalanyra nézve elhanyagolható negatív következmények nem veszélyeztetik a hozzájárulás érvényességét.

Feltehetően nem tekinthető önkéntesnek a hozzájárulás, ha az az általános felhasználási feltételekbe van beágyazva, és nem választás kérdése, valamint – főszabály szerint – kiegyensúlyozatlan erőviszonyokban sem (például munkaviszonyban).

PÉLDA

Egy kisbolt vásárlói kártyákat ad a vásárlóinak, hogy kedvezményeket gyűjthessenek. Ebben az esetben a kisbolt kezelheti a vásárlók adatait hozzájárulás alapján, mert a kedvezményektől való elesés nem jár jelentős negatív következménnyel a vásárlókra nézve.[95]

93 GDPR (42) Preambulumbekezdés.

94 Európai Adatvédelmi Testület: 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) 46. és 47. bekezdés (angol nyelven): **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf**

95 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

Egy munkáltató kamerákat szerel fel a munkahelyen, amelyhez a munkavállalók hozzájárulását kéri. A munkavállalók egyértelműen nincsenek abban a helyzetben, hogy a kamerák felszereléséhez szabadon hozzájárulást adjanak, illetve hátrányos következményekkel járna, ha a hozzájárulást megtagadnák. Az adatkezelőnek ebben az esetben más jogalapot kell választania.

Egy vállalkozás fitnesz applikációt fejleszt. Az applikáció felhasználási feltételei szerint a felhasználóknak meg kell adniuk nevüket, keresztnevüket, születési dátumukat, súlyukat, tápanyagszükségletüket és a földrajzi helymeghatározó adataikat. Ebben az esetben a hozzájárulásnak el kell különülni a felhasználási feltételektől. Továbbá a felhasználónak biztosítani kell a lehetőséget, hogy eldönthesse, az összes kért adatot meg kívánja-e adni, vagy csak néhányat közülük, tekintve, hogy az applikáció működéséhez nincs minden kért adatra szükség.

A megfelelő tájékoztatáson alapuló hozzájárulás azt jelenti, hogy az adatalanyok tisztában vannak azzal, mihez adják a hozzájárulásukat. Ennek érdekében az adatalanyokat tájékoztatni kell:

- az adatkezelő kilétéről és az adatkezelés céljáról,
- a kezelendő személyes adatok köréről,
- a hozzájárulás visszavonásának lehetőségéről.[96]

TIPP

A terjengős, szakkifejezésekkel telezsúfolt jogi nyelvezetű hozzájárulás nem tekinthető megfelelő tájékoztatáson alapulónak. A hozzájárulási nyilatkozat elkészítése során az adatkezelőnek az érintett helyébe kell képzelnie magát, és világos, közérthető nyelven kell fogalmaznia.

96 Európai Adatvédelmi Testület: 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) 64. és 65. bekezdés (angol nyelven): **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf**

A „kifejezett hozzájárulás” azt jelenti, hogy ha az adatkezelés több célt szolgál, a hozzájárulást minden egyes adatkezelési cél vonatkozásában be kell szerezni. Ezt nevezzük tagolt hozzájárulásnak.

PÉLDA

Egy sportközpont szeretné összegyűjteni a vásárlói e-mail címét, hogy havi hírlevelet küldhessen nekik az új edzésekről és képzésekről. A sportközpont a vásárlók e-mail címét további partnervállalataival is meg szeretné osztani (például fitnesz ruházatot gyártó vállalat, kiegészítőket forgalmazó vállalat). Ebben az esetben a sportközpontnak mindkét adatkezelési célhoz, azaz a hírlevél küldéséhez és az e-mail címek másik vállalatnak történő továbbításához is külön-külön be kell szereznie a hozzájárulást.

Az „egyértelmű” kritérium azt jelenti, hogy nyilvánvalónak kell lennie, az adatalany hozzájárult az adott adatkezeléshez. Egy honlap végiggörgetése nem tekinthető tevőleges cselekedetnek (kivéve, ha például a felhasználónak egy formát kell rajzolnia a kurzorral), mert ez nem különböztethető meg a honlap felhasználásának egyéb módjaitól.[97] Az adatkezelés „nem ellenzése”, azaz a hallgatás nem számít tevőleges cselekedetnek.

PÉLDA

Egy vendéglátóhely házhozszállítási szolgáltatásának igénybevételéhez a vásárlóknak online fiókot kell létrehozniuk. A regisztráció véglegesítésekor három jelölőnégyzet jelenik meg: „Egyetértek a felhasználási feltételekkel”, „Hozzájárulok személyes adataim kezeléséhez” és „Hozzájárulok, hogy számomra marketing célú üzeneteket küldjenek”. Abban az esetben, ha a jelölőnégyzetek előre ki vannak pipálva, a hozzájárulás nem érvényes.

97 Lásd fent, 8. bekezdés.

Ha az **információs társadalommal összefüggő szolgáltatásokat** (például szerződések vagy szolgáltatások online történő megkötése és megküldése) **kifejezetten gyermekeknek** nyújtják,[98] és az **adatkezelés jogalapja a hozzájárulás**, a gyermek törvényes képviseletét ellátó szülőnek kell hozzájárulnia az adatkezeléshez.[99] Magyarországon a 16. életév érvényesül.[100]

PÉLDA

Egyéb, a GDPR 8. cikkétől eltérő esetben a polgári jogi szabályozásból kell kiindulni.
A 14. életévét betöltött kiskorú személy jognyilatkozata (így hozzájáruló nyilatkozata) semmis, nevében törvényes képviselője tehet nyilatkozatot. A 14. életévét betöltött, de 18. életévét be nem töltött személy a Ptk.-ban felsorolt (kisebb jelentőségű, kisebb kockázattal járó) esetekben tehet önállóan jognyilatkozatot, így adott esetben adatkezeléshez megadott hozzájáruló nyilatkozatot, egyéb esetben nyilatkozata a törvényes képviselő jóváhagyásával érvényes.[101]

TIPP

Nem minden esetben megfelelő vagy célszerű a hozzájárulást választani az adatkezelés jogalapjának. Kihívást jelent annak bizonyítása, hogy a hozzájárulás önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű, ezért amennyiben lehetséges, ne féljünk másik jogalap alkalmazásától.

98 A GDPR előírja, hogy 16 évnél fiatalabb gyermek esetében szülői hozzájárulás szükséges, de a tagállamoknak lehetőségükben áll 13 évre csökkenteni a korhatárt.

99 Simone van der Hof, Eva Lievens and Ingrida Milkaite, 'The Protection of Children's Personal Data in a Data-Driven World: A Closer Look at the GDPR from a Children's Rights Perspective' in Ton Liefaard, Stephanie Rap and Peter Rodrigues (eds), Monitoring Children's Rights in the Netherlands. 30 Years of the UN Convention on the Rights of the Child (Leiden University Press, 2020).

100 FRA, Consent to use data on children (angol nyelven): **https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/use-consent**

101 Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) 2:11.-2:14. §.

HASZNOS FORRÁSOK

» ‘Európai Adatvédelmi Testület: ‘Guidelines 05/2020 on consent under Regulation 2016/679’ (4 May 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

» ICO: ‘Lawful basis interactive guidance tool’ https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/

Szerződéses jogviszony

Bizonyos esetekben az adatkezelés olyan szerződés teljesítéséhez szükséges, melyben az érintett az egyik fél.

PÉLDA

Egy online boltnak termékei kiszállításához kezelnie kell a vásárlók lakcímadatait. Ebben az esetben az adatkezelés jogalapja az eladó és a vevő között kötött adásvételi szerződés teljesítése, melynek érdekében szükséges a lakcím ismerete. Más információ is szükséges lehet a szerződés teljesítése érdekében: például alkoholos italok vásárlása esetén a vásárló kora, annak ellenőrzésére, hogy betöltötte-e már az előírt korhatárt.

Jogi kötelezettség teljesítése

Bizonyos esetekben az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. A jogi kötelezettség eredhet uniós vagy tagállami jogból is. A jogszabálynak ebben az esetben meg kell határoznia az adatkezelés célját, az adatkezelő kilétének megállapítását, a kezelendő adatok és érintettek, valamint azok körét, akikkel a személyes

adatokat közlik. Ha a KKV törvényi előírás alapján köteles személyes adatot kezelni, a GDPR jellemzően nem mentesíti ezen kötelezettsége alól.

PÉLDA

Az adatkezelés jogalapja a jogi kötelezettség teljesítése, ha egy vállalkozás a vásárlói adatait megküldi az adóhivatalnak, vagy ha az alkalmazottai társadalombiztosításhoz szükséges személyes adatait megküldi az illetékes nemzeti hatóságnak.

Az érintett vagy egy másik természetes személy létfontosságú érdeke

Bizonyos esetekben az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. Az adatvédelemhez való jog alapvető, de nem kizárólagos, élet-halál kérdésében a személyes adatok védelméhez való jogot természetesen felülbírálja az élethez való jog.

PÉLDA

Egy munkahelyi baleset esetén a munkaadó közölheti a munkavállaló személyes adatait a sürgősségi ellátást végző orvosokkal.

Közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges

Bizonyos esetekben az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Kivételes esetben egy KKV-t a rá vonatkozó jogi szabályozás értelmében megbízhatnak közérdekű vagy közhatalmi jogosítvány gyakorlásának

keretében végzett feladattal. Amennyiben ezen feladatok ellátásához a KKV-nak személyes adatokat kell kezelnie, közérdek vagy a közhatalmi jogosítvány gyakorlása lehet az adatkezelés jogalapja.

A „közérdek" nem azt jelenti, hogy általában jó lenne a köz számára, ha az adott adatkezelésre sor kerülne, hanem azt, hogy a közérdek azonosítható.

PÉLDA

Egy busztársaság biztosítja a közösségi közlekedést egy városban. A cég munkatársai a jegyellenőrzés során a bírság kiszabásához elkérhetik a jegy nélkül utazók elérhetőségét. A jogalap ebben az esetben közhatalmi jogosítvány gyakorlása.

A városi energiaszolgáltató a háztartások energiafogyasztásának és energiafelhasználásának feldolgozása során végzett adatkezelésének jogalapja a közérdekből végzett adatkezelés.

Az adatkezelő jogos érdeke

Bizonyos esetekben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, azonban ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek a személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A KKV-nak az alábbi elemeket kell megfontolnia a jogalap alkalmazásakor:

1. A KKV vagy harmadik fél jogos érdeke áll-e az adatkezelés mögött (a cél ellenőrzése)?

Ahhoz, hogy a KKV vagy harmadik fél érdeke „jogos" legyen:

» jogszerűnek kell lennie, ami azt jelenti, hogy összhangban kell állnia az alkalmazandó uniós és nemzeti joggal,
» eléggé meghatározottnak kell lennie, hogy lehetővé tegye az

adatalany jogainak és szabadságainak védelme érdekében az érdekmérlegelési teszt lefolytatását,

» az érdeknek valósnak és jelenlévőnek kell lennie, azaz nem lehet spekulatív[102] .

2. Az adatkezelés szükséges-e a céljának eléréséhez (a szükségesség ellenőrzése)?
3. Az adatalanyok jogai és szabadságai nem élveznek-e előnyt a jogos érdekkel szemben (érdekmérlegelés)?[103]

A jogos érdek alkalmazásának feltétele, hogy az adatalany az adatgyűjtés időpontjában a gyűjtött adatok vonatkozásában joggal számíthat arra, hogy az adatok kezelésére a meghatározott cél érdekében sor kerülhet.[104] Ha a személyes adatok kezelése egy csalás megelőzése érdekében feltétlenül szükséges, ez az adatkezelő jogos érdekének számít.[105]

PÉLDA

Egy vállalkozás ételházhozszállítási szolgáltatást nyújt. Az új vásárlók ajándék ételt kapnak házhozszállítással. Az ajánlatot egy háztartás csak egyszer veheti igénybe, ezért a vállalkozás a már meglévő ügyfeleiről vezetett nyilvántartását összeveti az új ügyfelek adataival, hogy ne történhessen visszaélés.

Egy online bolt hozzájárulás alapján e-mail címük megosztására kéri a vásárlóit, hogy tájékoztathassa őket a megrendelésük állapotáról. Ehhez az adatkezeléshez a vásárlók által megküldött e-mail címeket használja. Ha a bolt úgy dönt, hogy reklámokat küld a megadott email címekre, az adatkezelési tevékenység

102 WP29 munkacsoport 06/2014. számú véleménye az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf**

103 'A jogos érdek jogalapról (angol nyelven): **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/** és Rigas ügy (C13/16, 2017. május 4.).

104 GDPR (47) Preambulumbekezdés.

105 GDPR (47) Preambulumbekezdés.

vonatkozásában hivatkozhat a jogos érdekére. Következésképpen a boltnak rendelkeznie kell megfelelő jogalappal az új típusú adatkezelésre is. Amennyiben a fenti kritérium teljesül, a bolt hivatkozhat jogos érdekére.

Adatvédelmi hatóságok KKV-kat érintő döntései

Egy ellentmondásos példa direkt marketing célú adatkezelés vonatkozásában: Még akkor is, ha a GDPR szerint a direkt marketing lehet az adatkezelés jogalapja, ez nem minden esetben van így: Például a holland adatvédelmi hatóság megbírságolt egy teniszszövetséget, mert kiadta a tagjai személyes adatait egy szponzornak.[106] A holland felügyeleti hatóság álláspontja szerint[107] a pusztán profitszerzés miatti megosztás nem fogadható el jogos érdeknek, különösen annak fényében, hogy Hollandiában a rendszeres sporttevékenység kötelező egyesületi tagsághoz kötött.

HASZNOS FORRÁSOK

» FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

» Belga adatvédelmi hatóság: 'Direct Marketing Recommendations' **https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2020/02/Recommandation_01-2020_marketing_direct1-French.pdf**

106 GDPR (47) Preambulumbekezdés.

107 Lásd a holland felügyeleti hatóság döntését: **https://www.hldataprotection.com/2020/04/articles/international-euprivacy/dutch-dpa-imposed-a-controversial-fine-on-the-royal-dutch-tennis-association/**

» ICO: 'Direct Marketing' **https://ico.org.uk/media/for-organisations/documents/1555/directmarketing-guidance.pdf**

» DPC: 'Direct Marketing – What you need to know about direct marketing' **https://www.dataprotection.ie/en/dpc-guidance/blogs/direct-marketing-what-you-need-know-about-direct-marketing**

» CNIL: 'La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial' **https://www.cnil.fr/fr/la-reutilisation-des-donnees-publiquementaccessibles-en-ligne-des-fins-de-demarchage-commercial**

3.5. KKV-k és az adatalanyok jogai

Háttér

A GDPR számos joggal ruházza fel az érintetteket. Az érintetti kérelmek teljesítése az adatkezelőként eljáró KKV feladata[108], míg az adatfeldolgozó KKV-nak támogatnia kell az adatkezelőt az adatalanyok joggyakorlásának biztosításában.[109]

TIPP

Az adatkezelő és az adatfeldolgozó által kötött szerződés tisztázhatja, hogy az adatfeldolgozó hogyan tudja támogatni az adatkezelőt az érintetti kérelmek teljesítésében.

108 Ausloos, Jef and Mahieu, Rene and Veale, Michael, Getting Data Subject Rights Right (December 2019). (2019) 10 JIPITEC 283: **https://ssrn.com/abstract=3544173**

109 GDPR 28(3)(e).

Az adatkezelő indokolatlan késedelem nélkül, de legfeljebb 30 napon belül köteles megválaszolni az érintetti kérelmeket.[110] Ez a határidő szükség esetén meghosszabbítható, feltéve, hogy az érintettet erről 30 napon belül tájékoztatták, és a halasztás kellőképpen megindokolt (például a kérdéskörök összetettsége vagy a kérések nagy száma miatt).

Az érintettek a kérelmet benyújthatják szóban (például telefonon) vagy írásban (például e-mailen, postán, közösségi média).[111]

Nem minden érintetti kérelem feltétlenül indokolt. Ha az érintett kérelme egyértelműen megalapozatlan vagy túlzó (különösen annak ismétlődő jellege miatt), az adatkezelő – figyelemmel a kért intézkedés meghozatalával járó adminisztratív költségekre – ésszerű összegű díjat számíthat fel (a büntetés összegét nem lehet felszámítani) vagy megtagadhatja az intézkedést.

A kérelem megalapozatlanságát vagy túlzó jellegét az adatkezelő köteles bizonyítani. A kérelem teljesítését megelőzően az adatkezelő ellenőrzi az érintett személyazonosságát annak érdekében, hogy megakadályozza harmadik felek jogosulatlan hozzáférését az érintett személyes adataihoz.

Egyes esetekben az érintetti kérelem nem közvetlenül az érintettől, hanem harmadik féltől érkezik (például, ha az adatalany nevében egy képviselője vagy családtagja jár el felhatalmazás alapján vagy az érintett cselekvőképtelen).[112]

110 GDPR 12(3).

111 Hozzáférési jog (angol nyelven): **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/**

112 Adam Panagiotopoulos, Data subjects' requests made on behalf of others: Practical considerations on data subjects' requests and elected representatives': **https://www.trilateralresearch.com/dpo/data-subjects-requests-made-on-behalf-ofothers-practical-considerations-on-data-subjects-requests-and-elected-representatives/Z**

TIPP

» Ha kinevezünk egy adatvédelmi tisztviselőt, ő válaszolja meg az érintetti kérelmeket;

» Növelheti az érintetti kérelmek megválaszolásának hatékonyságát, ha kialakítunk egy részletes szabályzatot (a szerepek meghatározása, belső határidők stb.);

» A beérkezett érintetti kérelmek nyilvántartása (a szóban beérkezett kérelmek is ide tartoznak!) segíti a nyomonkövetési folyamatot, és a GDPR-megfelelés bizonyítását egy esetleges adatvédelmi hatósági ellenőrzés során.

HASZNOS FORRÁSOK

» ICO guide to data subjects rights **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/**

Az érintettek jogai

Átlátható tájékoztatáshoz való jog

Az érintetteket világos és közérthető nyelven tájékoztatni kell az alábbiakról:

» az adatkezelési tevékenység főbb elemei (például a kezelt adatok köre, az adatkezelés jogalapja és céljainak meghatározása, az adatmegőrzés ideje, esetleges adattovábbítások);
» az érintett felek elérhetőségei (például adatkezelők, adatvédelmi tisztviselő – ha van –, címzettek);
» az érintetti jogok érvényesítésének lehetőségei.

TIPP

A GDPR 13. és 14. cikke részletes listát tartalmaz az érintetteknek nyújtandó tájékoztatásról, valamint azokról az információkról, melyeknek a KKV-k adatvédelmi tájékoztatójában szerepelniük kell. A GDPR 12. cikke kiegészítő előírásokat tartalmaz arról, hogy a kérelmeket milyen módon és milyen határidőben kell teljesíteni. Amennyiben az adatvédelmi tájékoztató világos és közérthető, növeli az érintettek bizalmát, és ezáltal csökkenti az érintetti panaszok számát.

A tájékoztatásnak tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek kell lennie.

PÉLDA

Számos módon lehet tájékoztatást nyújtani:

» többszintű megközelítés (vagyis érdeklődés esetén bővebb információ is rendelkezésre áll);
» adatvédelmi beállítások menüpont;
» felugró tájékoztatás;
» ikonok;
» mobilos és okostelefonos alkalmazások;[113]
» ábrák, infógrafikák, folyamatábrák.[114]

113 A tájékoztatáshoz való jog (angol nyelven): **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/**

114 A 29. cikk szerinti munkacsoport Iránymutatása az (EU) 2016/679 rendelet szerinti átláthatóságról: **https://www.naih.hu/files/wp260rev01_hu.pdf**

HASZNOS FORRÁSOK

» A 29. cikk szerinti munkacsoport Iránymutatása az (EU) 2016/679 rendelet szerinti átláthatóságról **https://naih.hu/files/wp260rev01_hu.pdf**

» ICO: 'Right to information' **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/**

» Adatvédelmi szabályzat minta (angol nyelven): **https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf**

Az érintett hozzáférési joga

A hozzáférési jog (GDPR 15. cikk) keretében az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arról, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy a kezelt személyes adatokhoz hozzáférést, róluk másolatot kapjon.

A hozzáférési jog gyakorlására irányuló kérelmek érkezhetnek a szervezeten kívüli adatalanyoktól (például ügyfelektől) vagy szervezeten belüli adatalanyoktól (például munkavállalóktól).

A hozzáférési jog gyakorlásával az érintettek ellenőrizhetik az adatkezelő adatkezelési gyakorlatának jogszerűségét.

Amíg a GDPR 13. és 14. cikke szerinti tájékoztatáshoz való jog azt hivatott biztosítani, hogy az érintett általános és átfogó tájékoztatást kapjon személyes adatai kezelésének folyamatáról, a 15. cikk szerinti hozzáférési jog azt a célt szolgálja, hogy az érintett – erre irányuló kérése esetén – a saját személyes adatainak konkrét kezeléséről kapjon tájékoztatást a jogszerű adatkezelés és annak ellenőrzése érdekében.

A hozzáférési jog gyakorlására irányuló kérelem megválaszolása során az adatkezelő köteles:[115]

» tájékoztatni az érintettet arról, hogy kezeli-e a személyes adatait;
» az adatkezelés tárgyát képző személyes adatok másolatát az érintett rendelkezésére bocsátani (kivéve, ha ez mások jogait és szabadságait hátrányosan érinti);

PÉLDA

A hozzáférési jog gyakorlására irányuló kérelem olyan adatbázist is érinthet, ami nem csak a kérelmet benyújtó érintett adatait, hanem mások személyes adatait is tartalmazza (vagy üzleti titkot, szellemi tulajdont stb.). Ebben az esetben az adatkezelőnek egyensúlyt kell teremtenie a hozzáférési jog gyakorlása és azon érintettek jogainak védelme között, akiknek az adatait érintené az adatok érintett részére történő kiadása. Az adatkezelő nem teheti meg, hogy egyszerűen elutasítja minden releváns információ megosztását, hanem törekednie kell arra, hogy amennyire csak lehetséges eleget tegyen a hozzáférési jog gyakorlására irányuló kérelemnek, miközben biztosítja a többi érintett jogainak és szabadságainak megfelelő védelmét.[116] Például úgy, hogy biztosítja a nyilvántartáshoz való hozzáférést oly módon, hogy a többi érintett adatait kitörli belőle.

Ha a másolatok az érintett vagy más természetes személyek képét is tartalmazzák, javasolt elhomályosítani a többi személy képét, mielőtt a kérelmező rendelkezésére bocsátjuk a másolatot.

» tájékoztatást kell nyújtani:
  ⇨ az adatkezelés céljairól;
  ⇨ az érintett személyes adatok kategóriáiról (például a szerződés részletei, bankkártyaadatok);

115 Lásd GDPR 15. cikk.

116 A hozzáférési jog (angol nyelven): **https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information**

- a címzett(ek) kategóriáiról;
- a személyes adatok tárolásának tervezett időtartamáról, azaz, hogy meddig kívánja tárolni a személyes adatokat;
- a tárolás kritériumairól;
- az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat ezek kezelése ellen;
- valamely felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról;
- az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról, és az arról, hogy az ilyen adatkezelés milyen várható következményekkel jár;
- harmadik országokba vagy nemzetközi szervezet részére történő adattovábbítás esetén a megfelelő garanciákról (például adatkezelésre vonatkozó előírások, kötelező erejű vállalati szabályok, magatartási kódexek, tanúsítványok).

TIPP

Ha a hozzáférési jog gyakorlására irányuló kérelem túlságosan széles körű, javasolt megkérni az érintettet, hogy azt pontosítsa, mert ezzel jelentősen csökkenthető az adatok megküldésének terhe.

Érdemes megfontolni nyilvántartási szoftver alkalmazását, mert támogathatja az érintetti kérelmek megválaszolását és csökkentheti ennek költségeit.

HASZNOS FORRÁSOK

» ICO: Right to access **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/**

» DPC: The Right of Access **https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide**

A helyesbítéshez való jog

Az érintettek jogosultak arra, hogy kérésükre az adatkezelő helyesbítse a rájuk vonatkozó információt. A helyesbítéshez való jog az adatalanyok és a KKV-k számára is hasznos, mert utóbbiak így megbízhatnak a kezelt adatok minőségében. Az adatkezelő köteles minden olyan érintettet tájékoztatni a helyesbítésről, akivel korábban az adatokat közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.[117]

A törléshez való jog, azaz „az elfeledtetéshez való jog”

Az érintettek jogosultak arra, hogy kérésükre az adatkezelő törölje a rájuk vonatkozó személyes adatokat.

Az adatkezelő köteles törölni a személyes adatokat, ha:

» a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték (vagy más módon kezelték);

» gyermekek számára nyújtott információs társadalommal összefüggő szolgáltatásokkal összefüggésben gyűjtötték (ha közben ő elérte a törvényes korhatárt);

» a személyes adatokat jogellenesen kezelték (például megfelelő jogalap hiányában);

117 GDPR 19. cikk.

» az érintett visszavonja hozzájárulását vagy tiltakozik adatai kezelése ellen, és nincs más érvényes jogalap az adatkezelésre;
» uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez szükséges a törlés.[118]

Az elfeledtetéshez való jog gyakorlásának is vannak azonban korlátai, többek között: a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása; a személyes adatok kezelését előíró uniós vagy tagállami jog szerinti kötelezettség teljesítése; jogi igények előterjesztése, érvényesítése, illetve védelme stb.

Az adatkezelő köteles minden olyan érintettet tájékoztatni a törlésről, akivel az adatokat közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.[119]

PÉLDA

Az elfeledtetéshez való jog gyakorlására irányuló kérelem teljesítése során a másolati fájlokat is törölni kell (az adatkezelőnél, adatfeldolgozónál és a harmadik feleknél is). A törölt adatok visszaállításának lehetőségét minden elérhető technikai módszerrel meg kell akadályozni.

TIPP

Az elfeledtetéshez való jog gyakorlati alkalmazásának hatékonyságát elősegítendő az adatkezelő elérhetővé tehet a honlapján egy törlési kérelem formanyomtatványt.

118 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

119 GDPR 19. cikk.

HASZNOS FORRÁSOK

» Formanyomtatvány törléshez való jog gyakorlásához **https://gdpr.eu/right-to-erasure-request-form/**

Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

» vitatható a személyes adatok pontossága;
» az adatkezelés jogellenes és az érintett törlésük helyett a korlátozásukat kéri;
» az érintett jogi igényének gyakorlásához, vagy védelméhez szükséges;
» arra az időszakra, amíg megállapítása nem kerül, hogy az adatkezelő jogos érdekei elsőbbséget élveznek-e az érintett jogaival szemben.

Az adatkezelő köteles minden olyan érintettet tájékoztatni a korlátozásról, akivel az adatokat korábban közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.[120] Továbbá az adatkezelő köteles az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatni.[121]

PÉLDA

Hogyan lehet biztosítani az adatkezelés korlátozását?
» az éritett adatokat átmenetileg másik elkülönült adatbázisba továbbítjuk;
» az adatokat elérhetetlenné tesszük a felhasználók számára;
» átmenetileg eltávolítjuk a személyes adatokat.

120 GDPR 19. cikk.

121 GDPR 19. cikk.

Az adathordozhatósághoz való jog

Az adathordozhatósághoz való jog célja, hogy az érintettek könnyen magukkal vihessék a személyes adataikat, ha másik szolgáltatást vagy szolgáltatót kívánnak igénybe venni.

A GDPR 20. cikke értelmében az érintetteket megilleti az adathordozhatósághoz való jog, ha az általuk egy adatkezelő rendelkezésére bocsátott adatokat a hozzájárulásuk alapján vagy a szerződés teljesítéséhez szükséges jogalapon, automatizált módon kezelik. Ez nem jelenti azt, hogy az adathordozhatósághoz való jog ne vonatkozna olyan helyzetekre is, melyek esetében az adatkezelés jogalapja nem hozzájárulás vagy szerződés teljesítése.[122]

A gyakorlatban az adatalanyok jogosultak arra, hogy személyes adataikat egy adatkezelő közvetlenül továbbítsa egy másik adatkezelőnek, amennyiben ez technikailag kivitelezhető. Ennek elősegítése érdekében az adatkezelő köteles az adathordozhatóságot lehetővé tevő interoperábilis formátumokat kifejleszteni. A formátumoknak géppel olvashatónak, tagoltnak és széles körben használtnak kell lennie, de a GDPR nem írja elő kifejezetten, hogy melyik formátumot kell alkalmazni az adathordozhatóság biztosítása érdekében.

Az adathordozhatósághoz való jog biztosítása nem kötelezi az adatkezelőt, hogy olyan adatkezelési folyamatokat alakítson ki és alkalmazzon, melyek technikailag megfeleltethetők más szervezetek folyamatainak.

Az adathordozhatóság előnyös lehet a KKV-k számára, hiszen – ha jobb szolgáltatást nyújtanak a versenytársuknál –, a vásárlók könnyebben tudnak az ő szolgáltatásukra váltani.

122 GDPR 20. cikk.

PÉLDA

Az adathordozhatóság elvének megfelelő tagolt, széles körben használt, és géppel olvasható formátum többek között a CSV, XML, JSON, RDF[123].

A tiltakozáshoz való jog

Az adatalany jogosult arra, hogy tiltakozzon személyes adatainak kezelése ellen, ha azokat az adatkezelő:

- közérdek vagy jogos érdek alapján kezeli;
- közvetlen üzletszerzés céljából kezeli;
- az információs társadalommal összefüggő szolgáltatásokkal összefüggésben kezeli;
- tudományos és történelmi kutatási célból vagy statisztikai célból kezeli.[124]

Ha az érintett tiltakozik személyes adatainak kezelése ellen, az adatkezelő nem kezelheti tovább azokat, kivéve, ha bizonyítani tudja, hogy az érintettek jogai és szabadságai nem élveznek elsőbbséget a jogos érdekével szemben.

A tiltakozáshoz való jog automatizált eszközökkel is gyakorolható.

PÉLDA

A cookie-k (sütik) letiltása a tiltakozáshoz való jog érvényesítése.

123 Az adathordozhatósághoz való jog (angol nyelven): **https://ico.org.uk/your-data-matters/your-right-to-data-portability/**

124 GDPR 21. cikk.

Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

Az automatizált döntéshozatal azt jelenti, hogy technikai eszközökkel hozunk döntéseket emberi beavatkozás nélkül. Automatizált döntést bármilyen adat alapján lehet hozni:

- az érintett által rendelkezésre bocsátott adatok (például egy kérdőív kitöltésével) vagy
- az érintett megfigyelésével szerzett információ (például applikáció által gyűjtött helymeghatározó adat), vagy
- az érintett korábban megadott profiljából származó vagy abból kikövetkeztetett információ (például hitelbírálati minősítés) alapján.[125]

A profilalkotás a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

Amennyiben ezen döntések joghatás vagy jelentős egyéb hatás kiváltására alkalmasak (így komoly következményekkel járnak az adatalany életére), az érintettnek jogában áll, hogy tiltakozzon, és így ne terjedjen ki rá a kizárólag automatizált adatkezelésen alapuló döntés hatálya.

PÉLDA

Egy vállalkozás automatizált rendszert használ az alkalmazottak éves bónuszának kiszámítására. A bónusz kifizetése, pénzről lévén szó, minden alkalmazottat érzékenyen érint, ezért a végső döntést személyes döntéshozatallal kell meghozni.

125 WP29 munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához: **https://www.naih.hu/files/wp251rev01_hu.pdf**

Hacsak nem annyira népszerű egy vállalkozás, hogy állásjelentkezések ezrei érkeznek be hozzá, nem támaszkodhatnak kizárólag automatizált felvételi rendszerre, emberi erőforrást is alkalmazniuk kell, hiszen a kiválasztási folyamat jelentős hatással bír az érintettek életére.

HASZNOS FORRÁSOK

» WP29 munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához **https://www.naih.hu/files/wp251rev01_hu.pdf**

3.6. A KKV-k és az adatvédelmi tisztviselő

Háttér

A GDPR elfogadásával az adatkezelők és adatfeldolgozók is kötelesek adatvédelmi tisztviselőt kinevezni. Az adatvédelmi tisztviselő nem új elgondolás, a WP29 munkacsoport a GDPR-t megelőzően is az elszámoltathatóság sarokkövének tekintette.

A KKV-knak kötelező adatvédelmi tisztviselőt kinevezniük?

A széles körben elterjedt nézettel szemben az adatvédelmi tisztviselő kinevezésére vonatkozó jogi kötelezettség szempontjából nem a vállalkozás mérete, hanem az annak fő tevékenységéhez nélkülözhetetlen adatkezelési tevékenység nagysága a döntő. Ezek azok az adatkezelési tevékenységek, melyek alapvető fontosságúak a vállalkozás céljainak eléréséhez. Az adatvédelmi tisztviselő kinevezése ezért – bár nem gyakran fordul elő, de alapvetően – az adatkezelő és adatfeldolgozó KKV-kra is vonatkozik. Választhatnak, hogy belső (saját munkatárs) vagy külső (adatvédelmi tisztviselői szolgáltatás) adatvédelmi tisztviselőt neveznek ki.

Az adatvédelmi tisztviselő (DPO) legfontosabb feladata, hogy biztosítsa, a szervezete az adatvédelmi szabályozásnak megfelelően kezeli munkavállalói, ügyfelei és bárki más személyes adatait.[126]

Az alábbi feltételek fennállása esetén az adatkezelő és adatfeldolgozó KKV-k egyaránt kötelesek adatvédelmi tisztviselőt kinevezni:

1. **Az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat.**

Ez vonatkozhat KKV-kra is, amennyiben megfelelnek a közhatalmi szerv fogalmának: A közhatalmi szervek olyan – akár közjogi, akár magánjogi személyek –, melyeket a rájuk vonatkozó jogszabályok értelmében közérdekű feladatok ellátásával bíztak meg, és ezek ellátása során a magánjogi személyek közötti viszonyokban alkalmazandó szabályokhoz képest rendkívüli hatalommal – ún. közhatalommal – vannak felruházva.[127]

PÉLDA

A KKV köteles adatvédelmi tisztviselőt kinevezni, ha közösségi közlekedési szolgáltatást nyújt, víz- és energiaszolgáltatással, közúti infrastruktúrával, közszolgálati műsorszolgáltatással vagy szociális lakhatás biztosításával foglalkozik. Alapvető fontosságú annak meghatározása, hogy a KKV közfeladatot lát-e el, mert ettől függ az adatvédelmi tisztviselő kinevezésének szükségessége.

2. **A KKV fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé.**

126 Európai Adatvédelmi Biztos: 'Data Protection Officer': **https://edps.europa.eu/data-protection/eu-institutions-dpo/case-law-guidance_en**

127 Lásd C- 279/ 12 ügy (Fish Legal and Shirley, 52. bekezdés).

A KKV fő tevékenysége az adatkezelő vagy az adatfeldolgozó céljainak eléréséhez szükséges legfontosabb műveleteket jelenti. Előfordulhat, hogy a KKV fő tevékenysége elválaszthatatlanul összekapcsolódik személyes adatok kezelésével (például, ha a KKV applikációkat fejleszt). Ugyanakkor bizonyos adatkezelési tevékenységek bár az üzleti tevékenység érdekében elengedhetetlenek, járulékos tevékenységnek számítanak (például a munkavállalók bérének kifizetése vagy általános IT támogatás).

Megfigyelésnek számít, ha nyomon követik a természetes személy online tevékenységét.[128] A megfigyelés rendszeres és szisztematikus, ha az adatkezelési terv részeként folyamatosan vagy rendszeres időközönként sor kerül rá, valamint előre megszervezett vagy módszeres eszközökkel történik.

PÉLDA

Rendszeres és szisztematikus megfigyelésnek számítanak az alábbi tevékenységek:
telekommunikációs hálózat üzemeltetése, telekommunikációs szolgáltatások nyújtása, adatvezérelt marketing tevékenységek, kockázatelemzés céljából történő profilalkotás-, és elemzés (például hitelképesség elbírálása, biztosítási díj megállapítása, csalás megelőzése, pénzmosás felderítése), helymeghatározás (például mobiltelefonos applikációk), hűségprogramok, viselkedésalapú hirdetések, fitnesz és egészségügyi adatok megfigyelése applikációkon keresztül.

Annak eldöntéséhez, hogy az adatkezelés nagymértékűnek számít-e, az alábbi tényezőket kell figyelembe venni:

- az érintett adatalanyok száma (a kifejezett számuk vagy a népességhez viszonyított arányuk);
- a kezelt adatok mennyisége és/vagy köre; az adatkezelés időtartama

128 GDPR (24) Preambulumbekezdés.

vagy ismétlődő jellege; az adatkezelési tevékenység földrajzi kiterjedése.

PÉLDA

Nagymértékű adatkezelésnek minősül a közösségi közlekedést használók utazási adatainak kezelése (például a kártya formátumú jegyek követésével) vagy a valós idejű földrajzihely-meghatározás statisztikai célból.

Egy csempegyártó középvállalkozás munkaegészségügyi szolgáltatásait kiszervezi egy külső adatfeldolgozóhoz, amely nagy számú hasonló ügyféllel foglalkozik. Az adatfeldolgozó köteles adatvédelmi tisztviselőt kinevezni, mivel az általa végzett adatkezelés nagymértékű, de az adatkezelő számára ez nem kötelező.[129]

3. A KKV fő tevékenységei különleges adatok vagy bűncselekményekre és büntetőjogi felelősség megállapítására vonatkozó adatok nagy számban történő kezelésével járnak.

A személyes adatok különleges kategóriáit a GDPR 9. cikke tartalmazza. Különleges adatok a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

129 WP29 munkacsoport WP243 számú iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban: https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf

PÉLDA

Köteles adatvédelmi tisztviselőt kinevezni:
» a vérvizsgálatokat végző labor,
» a büntetőjogi ügyekkel foglalkozó ügyvédi iroda (ha nem egyéni ügyvédről van szó),
» egy klinika (ha nem egy adott szakorvos, egészségügyi szakember betegeiről van szó),[130]
» egy társkereső applikációt üzemeltető KKV.

Kit lehet adatvédelmi tisztviselőnek kinevezni?

Az adatvédelmi tisztviselő lehet a KKV alkalmazottja vagy külső szakértő is, de mindkét esetben alapvető fontosságúak a függetlenségét biztosító feltételek:

- Legyenek biztosítottak számára azok a források, amelyek feladatai végrehajtásához szükségesek, azaz pénz, munkaerő, (szakmai fejlődésre fordítható) idő;
- Az adatvédelmi tisztviselő feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el;
- Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el, és szankcióval nem sújthatja;
- Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel; valamint
- Az adatvédelmi tisztviselő feladataiból nem fakadhat összeférhetetlenség (például az adatkezelés tárgyának és céljainak meghatározása, a KKV képviselete jogi eljárásokban).

Amennyiben az adatvédelmi tisztviselő a vállalkozás alkalmazottja, függetlenségének biztosítása érdekében mindig tisztázni kell, hogy éppen adatvédelmi tisztviselői szerepében jár-e el.

130 A személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik. (GDPR (91) Preambulumbekezdés).

TIPP

A KKV-knál egy személy gyakran több szerepet is betölt egyszerre. Nem lehet adatvédelmi tisztviselőnek kinevezni az alábbi pozíciókat betöltő munkatársakat:

» ügyvezető
» operatív igazgató
» pénzügyi igazgató
» főorvos
» marketing osztály vezetője
» HR vezető
» IT vezető

Az adatvédelmi tisztviselőnek a vállalkozás által kezelt (különleges) adatokkal és az adatkezelési folyamatok összetettségével arányos tapasztalattal kell rendelkeznie. Például, ha az adatkezelési tevékenység különösen összetett, vagy nagy számú különleges adatot érint, az adatvédelmi tisztviselőtől elvárt a nagyobb szaktudás.

A GDPR nem ír elő az adatvédelmi tisztviselői tanúsítványra vonatkozó kötelezettséget.

Milyen feladatokkal bízhatja meg egy KKV az adatvédelmi tisztviselőt?

A GDPR alapján az adatvédelmi tisztviselő feladatai:

1. Szakmai tanácsot ad a KKV-nak a Rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeivel kapcsolatban;
2. Ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését is. Továbbá

támogatja az adatkezelési műveletekben részt vevő munkatársak tudatosságnövelését és képzését és részt vesz a kapcsolódó auditok lefolytatásában is;

PÉLDA

Az adatvédelmi tisztviselő azonosítja a KKV adatfeldolgozási tevékenységeit, elemzi és ellenőrzi az adatkezelés GDPR-nak való megfelelését, tájékoztatást nyújt, tanácsot ad és ajánlásokat bocsát ki az adatkezelő számára. [131]

Az adatvédelmi tisztviselőt nem terheli személyes felelősség, ha az adatkezelő vagy adatfeldolgozó nem teljesíti a GDPR előírásait.[132]

3. Szakmai tanácsokat ad az adatvédelmi hatásvizsgálatra vonatkozóan;

PÉLDA

A KKV kérheti az adatvédelmi tisztviselő tanácsát abban, hogy
» szükséges-e adatvédelmi hatásvizsgálatot lefolytatnia,
» milyen módszert alkalmazzon,
» külsős szakembert bízzon-e meg a lefolytatásával,
» a kockázatcsökkentő intézkedések alkalmazásának szükségességéről, valamint
» a hatásvizsgálat következményeiről (folytatható-e az adatkezelés, milyen biztonsági intézkedésekre van esetleg szükség).[133]

Az adatvédelmi tisztviselő egymaga nem tudja lefolytatni az adatvédelmi hatásvizsgálatot, mert összeegyeztethetetlen lenne a függetlenségére vonatkozó kritériummal: ha ő folytatná le a

131 WP29 munkacsoport WP243 számú iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban: **https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf**

132 Lásd fent.

133 Lásd fent.

hatásvizsgálati eljárást, az adatkezelési tevékenység értékelését és ellenőrzését egy személyben végezné. Mindazonáltal az adatvédelmi tisztviselő alapvető szerepet játszik az adatkezelő támogatásában.

4. Együttműködik a felügyeleti hatósággal;
5. Az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;

PÉLDA

Adatvédelmi incidens esetén az adatkezelő köteles tájékoztatni a felügyeleti hatóságot az adatvédelmi tisztviselő nevéről és elérhetőségéről.

A görög adatvédelmi hatóság véleménye szerint nem összeegyeztethető az adatvédelmi tisztviselő feladataival, ha egy esetleges eljárás során ő képviseli a KKV-t a felügyeleti hatóság vagy a bíróság előtt.[134]

6. Kezeli az érintettek kérelmeit és panaszait;
7. Egyéb feladatokat is elláthat, ha ezek nem összeférhetetlenek adatvédelmi tisztviselői feladataival.

PÉLDA

Az adatkezelő vagy adatfeldolgozó megbízhatja az adatvédelmi tisztviselőt, hogy vezesse az adatkezelési folyamatokról szóló nyilvántartást, de a nyilvántartási kötelezettségnek való megfelelés az adatkezelő felelőssége. Az adatkezelési nyilvántartások lehetővé

134 Judit Garrido-Fontova, 'The DPO cannot represent the controller in proceedings before the authority according to the Greek DPA' (31 January 2020).

teszik az adatvédelmi tisztviselő számára a megfelelés ellenőrzését, valamint az adatkezelő és adatfeldolgozó tájékoztatását és támogatását.[135]

Az adatvédelmi tisztviselő tanácsot adhat az adatkezelők és adatfeldolgozók, a (közös) adatkezelők, vagy adatfeldolgozók és alvállalkozók között kötött adatmegosztási megállapodások kapcsán is.

A DPO segítheti a KKV-t a magatartási kódexnek való megfelelésben, valamint az adatvédelmi tanúsítvány megszerzésében is.[136]

Kijelölhet a KKV más szervezetekkel közös adatvédelmi tisztviselőt?

Igen, a KKV-k számára praktikus lehet, ha közös adatvédelmi tisztviselőt neveznek ki. Erre a GDPR is biztosít lehetőséget azzal a kikötéssel, hogy az adatvédelmi tisztviselőnek minden érintett vállalkozás számára könnyen elérhetőnek kell lennie.

Biztosítani kell az adatvédelmi tisztviselő elérhetőségét az érintettek és a felügyeleti hatóság számára, valamint a szervezeten belül is.

Mit kell megfontolni az adatvédelmi tisztviselő kinevezése előtt?

» Habár nem minden KKV köteles adatvédelmi tisztviselőt kijelölni, hasznos lehet, ha rendelkezésre áll a szervezetnél egy adatvédelmi szakember, aki tud foglalkozni az érintettek kérelmeivel.
» Ha a KKV közszolgáltatást nyújt, javasolt adatvédelmi tisztviselőt kijelölnie (bár nem kötelező).[137]

135 Douwe Korff and Marie Georges, The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 152.

136 WP29 munkacsoport WP243 számú iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban: **https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztviselokkel-kapcsolatban.pdf** (Az adatkezelő feladatai).

137 WP29 munkacsoport WP243 számú iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban: **https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztviselokkel-kapcsolatban.pdf**

» Az adatvédelmi tisztviselő szaktudása legyen megfeleltethető az adatkezelési tevékenységek által jelentett kockázatok mértékének.

PÉLDA

Egy esetleges adatvédelmi hatósági ellenőrzés során a KKV számára hasznos lehet, ha írásos dokumentációval tudja alátámasztani, hogy miért (nem) nevezett ki adatvédelmi tisztviselőt, és mi alapján ítéli megfelelőnek az adatvédelmi tisztviselő szaktudását a feladat ellátásához, mert ezzel tudja bizonyítani a GDPR-nak és az elszámoltathatóság elvének való megfelelését.

Hasonlóan, ha egy KKV úgy dönt, hogy nem az adatvédelmi tisztviselő tanácsának megfelelően jár el, az elszámoltathatóság bizonyítása céljából célszerű dokumentálni ezen döntésének indoklását.

Az adatvédelmi előírásoknak való megfelelés érdekében önkéntes alapon akkor is nevezhetnek ki adatvédelmi tisztviselőt a vállalatok, ha az nem kötelező.[138]

138 GDPR képzési anyagok: 5. témakör: Az adatvédelmi tisztviselő: **https://naih.hu/eredmenyek.html** angol nyelven: Training materials: Topic 5 – Role of the DPO **http://www.project-star.eu/**

HASZNOS FORRÁSOK

» WP29 munkacsoport WP243 számú iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban **https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf**

» Douwe Korff and Marie Georges, The DPO Handbook – Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation **https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf/a5bfc9ba-8a0c-0f88-9874-71be40be6a6d?version=1.0**

ADATVÉDELMI HATÓSÁGOK KKV-KAT ÉRINTŐ DÖNTÉSEI

A német szövetségi adatvédelmi hatóság megbírságolt egy telekommunikációs szolgáltatást nyújtó KKV-t, mert többszöri felszólítás után sem jelölt ki adatvédelmi tisztviselőt, ahogyan azt a GDPR 37. cikke előírja. A felügyeleti hatóság a 10.000 eurós bírság megállapítása során tekintettel volt a KKV méretére is (mikrovállalkozás).[139]

139 'BfDI imposes Fines on Telecommunications Service Providers' (18 December 2019): **https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_es**

4. A kockázatalapú megközelítés az elméletben és a gyakorlatban

4.1. Háttér

A kockázatalapú megközelítés arra az elvre épül, hogy az adatvédelmi alapelvek tiszteletben tartása nem elegendő a természetes személyek alapjogainak biztosításához.[140] Személyes adatokat számtalan módon lehet kezelni, így az adatkezelés nagyon összetett is lehet, ezért az adatvédelmi alapelveknek való megfelelést össze kell kapcsolni a kockázatelemzéssel és a kockázatok kezelésével.[141] A kockázatalapú megközelítés lehetőséget teremt arra, hogy az adatvédelmi alapelveket az adott adatkezelési tevékenységhez igazítsuk.[142]

Az adatkezelők és az adatfeldolgozók kötelesek felmérni az adatkezelés természetes személyek jogaira és szabadságaira gyakorolt hatását, és fellépni a kockázatok ellen. Ez több tevékenység összehangolását igényli a kockázat felmérése, kontrollálása és csökkentése érdekében.[143]

---

140 A személyes adatok kezelésére vonatkozó alapelveket a GDPR 5. cikke sorolja fel: jogszerűség, tisztességes eljárás és átláthatóság, célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, integritás és bizalmas jelleg, és elszámoltathatóság.

141 Raphaël Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' (2016)2 EDPL 481, 482, 483, 484.

142 Lásd fent.

143 WP29 munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e: **https://www.naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf**

A kockázatkezelés négy alapvető lépése a következő:

1) a kockázatok azonosítása;
2) a kockázatok elemzése;
3) a kockázatok értékelése;
4) a kockázatok kezelése.[144]

4.2. Mi számít kockázatnak a GDPR szerint?

A kockázat jogi – különösen az európai adatvédelmi szabályozásban – fogalmának meghatározása még nem forrott ki. [145] A kockázat fogalmát eddig pénzügyi, technológiai, gazdasági szempontból vagy a természettudományok területén vizsgáltuk. A kockázat lehet szubjektív[146], objektív[147], önként vállalt[148], társadalmilag kirótt[149], önálló és átfogó[150] is. A kockázatot különböző szempontokból vizsgálhatjuk (technológiai, gazdasági, pszichológiai stb.)[151]

A kockázat meghatározása változatos lehet, többek között függ a különböző megközelítésektől; az érintett adott tevékenységre vonatkozó ismereteitől és az adott tevékenységben rejlő veszélyektől[152] vagy a tevékenységből származó előnyöktől, de szerepet játszhat benne az is, hogy

144 ISO 31000:2018(en), Risk management — Guidelines: **https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en**

145 Ulrich Beck, World at Risk (Polity, 2009).

146 A szubjektív kockázatelemzés a (nem szakmai) közvélekedésen alapul.

147 Az objektív kockázatokat szakértők tudományos értékelése alapján határozzák meg.

148 Például gyógyszeres kezelés (fogamzásgátló).

149 Például egy atomerőmű.

150 Azok a kockázatok, melyek „megtörténnek", például egy földrengés.

151 Robert Baldwin and Martin Cave, Understanding Regulation: Theory, Strategy, and Practice (Oxford University Press 1999) 139.

152 Paul Slovic, 'Perception of Risk' (1987) 236 Science 280–285.

az érintett önként tette-e ki magát a kockázatnak, és mennyire érzi úgy, hogy kézben tartja az eseményeket.[153]

A GDPR nem határozza meg a kockázat fogalmát, de a WP29 munkacsoport javaslata szerint a „kockázat" olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit.[154]

Az adatvédelmi szabályozásban az adatalanyok (érintettek) vagy természetes személyek jogaira és szabadságaira jelentett fenyegetéseket értjük alatta. Ezek más alapjogokat is érinthetnek, úgymint a szólásszabadság, gondolatszabadság, szabad mozgáshoz, szabadsághoz való jog, a diszkrimináció tilalma vagy lelkiismeret- és vallásszabadság.[155] A kockázat fenti értelmezése eltér a többi üzleti kockázattól, amelyeket a vállalkozás tekintetében vizsgálnak.

PÉLDA

A páciensek egészségügyi adatainak naprakészen tartása nem csak adatpontosság kérdése. A nem pontos vagy nem naprakész adatok élet-halál kérdése lehet a beteg számára.

4.3. Mi jelenthet kockázatot?

Az adatkezelési tevékenység járhat fizikai, anyagi vagy nem anyagi kárral a természetes személyek jogaira és szabadságaira nézve.[156]

153 Lásd fent.

154 WP29 munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e: **https://www.naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf**

155 WP29 munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e: **https://www.naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf**

156 GDPR (75) Preambulumbekezdés.

PÉLDA

» diszkrimináció, személyiséglopás, pénzügyi kár, jó hírnév megsértése, a személyes adat titkosításának feloldása, álnevesítés jogszerűtlen felfedése; vagy
» bármilyen egyéb jelentős gazdasági vagy társadalmi hátrány, ami megfosztja az érintetteket jogaiktól és szabadságaiktól vagy megakadályozza, hogy ellenőrzést gyakoroljanak személyes adataik kezelése felett;
» nyilvánosságra kerül a faji vagy etnikai származásra, politikai véleményre, vallási vagy filozófiai meggyőződésre, szakszervezeti tagságra vonatkozó adat.

Önmagában kockázatot rejt, ha:
» egészségügyi és genetikai, valamint a szexuális életre vagy bűncselekményekre vonatkozó adatok kezelésére kerül sor;
» az adatok alapján az érintett személyes jellemzőit értékelik, például a munkahelyi teljesítmény előrejelzése, gazdaság helyzet, egészségügyi állapot, érdeklődési kör, megbízhatóság és viselkedés, tartózkodási hely és mozgás, személyes profil megalkotása és felhasználása;
» sérülékeny csoportok, különösen gyermekek személyes adatait kezelik; vagy
» az adatkezelés nagy számú adat kezelésével jár vagy nagy számú adatalanyt érint.[157]

TIPP

A kockázatok azonosítása érdekében a KKV:

» kérhet tanácsot az adatvédelmi tisztviselőjétől (ha van),
» felhasználhat tudásbázisokat,[158] és/vagy
» interjúkat folytathat le vagy tanácskozhat érintett felekkel.[159]

157 GDPR (75) Preamulumbekezdés

158 Cnil, PIA, Knowledge Bases, 2018: Cnil, PIA, Knowledge Bases, 2018: **https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf**

159 Harri Ball, '7 Ways to Identify Risks': **https://projectriskcoach.com/7-ways-to-identify-risks/**

4.4. Hogyan kell értékelni a kockázatokat a GDPR szerint?

Az eltérő kockázatot jelentő helyzetek más jogi kötelezettségek alkalmazását keletkeztetik. A Rendelet három fokozatú kockázatot különböztet meg:

1) alacsony,
2) közepes, és
3) magas kockázat

Ha egy vállalkozás több adatkezelési tevékenységet is folytat egyszerre, ezek különböző kockázatot jelenthetnek.

PÉLDA

Adatvédelmi szempontból egyes üzletágak nagyobb kockázattal járnak:
» egészségügyi szolgáltatások,
» fizető- és hitelképesség megállapítása,
» profilalkotás,
» politikai, szakszervezeti vagy vallási tevékenységek,
» telekommunikációs szolgáltatások,
» biztosítások,
» banki és pénzügyi szolgáltatások,
» szociális szolgáltatások,
» reklámtevékenység,
» nagyobb infrastruktúrák kamerás megfigyelése (például vasútállomások).

Bizonyos adatkategóriák kezelése szintén nagyobb kockázattal jár:
» faji vagy etnikai származásra vonatkozó adatok,
» politikai vélemény és vallási meggyőződés,
» szakszervezeti tagság,
» genetikai adatok,
» a természetes személy egyedi azonosítását lehetővé tevő biometrikus adatok,
» fizikai és mentális egészségre vonatkozó adatok,

» szexuális életre vagy orientációra vonatkozó adatok,
» bűncselekményekre, büntetőítéletekre vonatkozó adatok,
» földrajzi helymeghatározási adatok.

Hasonlóan magasabb kockázatot jelentenek egyes adatkezelési tevékenységek is:
» profilalkotás- és elemzés,
» széleskörű reklámtevékenység,
» hálózatüzemeltetés vagy elektronikus hírközlési szolgáltatások nyújtása (internetszolgáltatók),
» politikai pártok, szakszervezetek, egyházak, vallási szervezetek vagy közösségek, jótékonysági szervezetek vagy más politikai, vallási vagy szakszervezeti célból működő civil szervezet tagjaira vonatkozó adatok kezelése,
» gyógyszerellátás, kórtörténet, egészségügyi szolgáltatások.[160]

A fentieken kívül más ágazatok vagy tevékenységek is jelenthetnek magas kockázatot, de mivel ismert, hogy ezek jellemzően magas kockázattal járnak, alapértelmezetten magas kockázatúnak tekintjük őket.

A kockázatot jellemzően annak valószínűsége és a súlyossága (a kockázat megvalósulásának következményei) egyidejű értékelésével mérjük fel.[161] A valószínűséget és a súlyosságot az adatkezelési tevékenységek jellege (jellemzői vagy típusa), hatóköre (mértéke), körülményei és céljai alapján kell meghatározni.[162]

A kockázat kvalitatív és kvantitatív módszerekkel vagy ezek kombinációjával is értékelhető. A kvantitatív kockázatelemzés nagyon pontos értékeket kíván meg, azaz minden egyes kockázati tényező előfordulásának

160 Facilita RGPD': **https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd**

161 Paolo Rossi, How to link the qualitative and the quantitative risk assessment'. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute.

162 GDPR (76) Preambulumbekezdés és Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): **https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en**

(0-1-es skálán kifejezve), és a súlyosságának kvantitatív meghatározását. Ehhez képest a kvalitatív kockázatelemzés abból a feltételezésből indul ki, hogy lehetetlen ilyen pontos értékeket megállapítani, és helyette valószínűségi és súlyossági szinteket használ (nagyságrendekben kifejezve). A természetes személyek jogaira és szabadságaira jelentett kockázat értékeléséhez a legtöbbször a kvalitatív módszer a megfelelő.[163]

PÉLDA

Kvalitatív kockázatelemzés esetében a súlyossági skála 1-5 között lehet:[164]

Érték	Az érintettek jogaira és szabadságaira gyakorolt hatás súlyossága
S1– Alacsony	Pusztán kényelmetlenséget / bosszúságot okoz.
S2– Mérsékelt	Az érintettek jogaira és szabadságaira nézve kisebb fizikai, anyagi vagy nem anyagi kárt okoz (például stressz, kisebb gazdasági veszteség, a személyes adatok feletti kontroll elvesztésének érzése stb.).
S3– Közepes	Az érintettek jogaira és szabadságaira nézve fizikai, anyagi vagy nem anyagi kárt okoz (például a jogok gyakorlásának korlátozása).
S4– Magas	Az érintettek jogaira és szabadságaira nézve jelentős fizikai, anyagi vagy nem anyagi kárt okoz, melyet nehézségek árán tudnak kiküszöbölni.
S5– Kritikus	Az érintettek jogaira és szabadságaira nézve visszafordíthatatlan fizikai, anyagi vagy nem anyagi kárt okoz.

163 Paolo Rossi, How to link the qualitative and the quantitative risk assessment'. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute. Kloza and others.

164 A CNIL Adatvédelmi hatásvizsgálat tudástára alapján: **https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf**

A valószínűségi skála 1-5 között:[165]

Érték	Az érintettek jogaira és szabadságaira jelentett kockázat valószínűsége
L1–Csekély	Nem valószínű, hogy a kockázat megvalósul.
L2–Valószínűtlen	A kockázat nehezen valósulhat meg.
L3–Lehetséges	Lehetségesnek tűnik a kockázat megvalósulása..
L4–Valószí-nűsíthető	Nagyon valószínű, hogy a kockázat megvalósul.
L5–Jelentős	Szinte biztos, hogy a kockázat megvalósul.

A megfelelő kockázati mátrix:

L5	5	10	15	20	25
L4	4	8	12	16	20
L3	3	6	9	12	15
L2	2	4	6	8	10
L1	1	2	3	4	5
	S1	S2	S3	S4	S5

A kockázat szintje (a valószínűség és a súlyosság szorzata adja)

Alacsony kockázat: ≤ 2;
Mérsékelt kockázat: 4 – 5
Közepes kockázat: 5 – 9
Magas kockázat: 10 – 16
Kritikus kockázat: ≥ 17

A fenti skála és a mátrix csak példaként szolgál, az adatkezelők használhatnak más skálát is (1-3, 1-4 stb.). A kockázati mátrixban megállapíthatnak más értékeket az alacsony, enyhe stb. kockázatokra. (Például alacsony kockázat ≤ 1, kritikus kockázat ≥ 25.).

165 A CNIL Adatvédelmi hatásvizsgálat tudástára alapján: **https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf**

Példa az adatvédelmi kockázatok nyilvántartására:[166]

Sorszám	A kockázat leírása	GDPR rendelkezése	Az érintettekre gyakorolt lehetséges hatások	Valószínűség	Súlyosság	A következmények súlyossága
1.	Jogtalan célú felhasználás	5. cikk	A személyes adatokat az eredetileg meghatározott céloktól eltérő célból kezelik.	2	4	8
2. stb.						

TIPP

Az adatkezeléssel járó kockázatokról javasolt nyilvántartást vezetni, mert ez felhívja a szervezet figyelmét az esetleges adatvédelmi problémákra, melyek azonosításával csökkenthető az adatvédelmi kockázat. Következésképpen segít a beépített és alapértelmezett adatvédelem elvének leginkább megfelelő szervezési és technikai intézkedések kiválasztásában, az adatvédelmi hatásvizsgálat lefolytatásában, és a felügyeleti hatóság esetleges ellenőrzése esetén is hasznos a megfelelés bizonyítására.[167]

HASZNOS FORRÁSOK

» ISO 31000:2018 kockázatkezelési iránymutatás **https://www.iso.org/standard/65694.html**

166 A spanyol adatvédelmi hatóság 'Practical Guide for DPIAs' című iránymutatása alapján.

167 Kockázatalapú megközelítés (angol nyelven): **https://dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach**

» Kockázatelemzés és tervezés **https://tietosuoja.fi/en/risk-assessment-and-dataprotection-planning**

» A spanyol adatvédelmi hatóság kockázatelemzési iránymutatása: Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD' **https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf**

4.5. A GDPR kockázatalapú megközelítést tartalmazó rendelkezései

A GDPR alábbi cikkeiben jelenik meg kockázatalapú megközelítés:

» 24. cikk az adatkezelő feladatairól (ezek szorosan kapcsolódnak az elszámoltathatóság alapelvéhez);
» 25. cikk a beépített és alapértelmezett adatvédelemről;
» 30. cikk az adatkezelési tevékenységek nyilvántartásáról;
» 32. cikk az adatkezelés biztonságáról;
» 33. és 34. cikk az adatvédelmi incidens kapcsán megjelenő bejelentési/tájékoztatási kötelezettségről;
» 35. cikk az adatvédelmi hatásvizsgálat lefolytatásáról;
» 36. cikk az előzetes konzultációról.

A kockázatalapú megközelítés alapelvének megfogalmazása bizonyos mértékben eltér a fenti cikkekben, de lényegében közös elvárás, hogy akármekkora kockázatot is rejt magában a személyes adatok kezelése, a természetes személyek jogait mindig tiszteletben kell tartani. A gyakorlatban ez azt jelenti, hogy az adatkezelők és adatfeldolgozók kötelesek az adatkezelési tevékenységük által jelentett kockázatokhoz igazítani az adatkezelési folyamatokat.[168]

168 Christopher Kuner, Lee Bygrave and Christopher Docksey, The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), 26

A GDPR a következő elemek alapján határozza meg a kockázatalapú megközelítést:

» a személyes adatok kezelésének jelenlegi eszközei (a szervezési intézkedések jelenlegi állapotának tekintetében);
» a megvalósítás költségei;
» az adatkezelés jellege, hatóköre és körülményei;
» az adatkezelés célja;
a természetes személyek jogait és szabadságait fenyegető különböző valószínűségű és súlyosságú kockázatok.[169]

A kockázat és értékelésének kritériumai azonosak:
» a védendő értékek (az érintettek),
» a kockázat (a személyek jogai és szabadságai),
» az értékelendő körülmények (az adatkezelés jellege, hatóköre, körülményei és céljai).[170]

4.6. Milyen előnyökkel jár a KKV-k számára a kockázatalapú megközelítés?

Az érintettek jogait veszélyeztető kockázat nem az adatkezelők számától, hanem az adatkezelés jellegétől, hatókörétől, körülményeitől és céljaitól függ.

A GDPR-nak való megfelelés kockázatalapú megközelítés szemszögéből történő vizsgálata különösen hasznos lehet a KKV-k számára:

» A KKV-k bizonyos mértékben szabadon határozhatják meg a kockázatelemzés lefolytatásának és az adatkezelésben rejlő kockázat

169 Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

170 Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

értékelésének módszerét. Továbbá szabadon választhatják ki a (magas) kockázat csökkentésére irányuló intézkedéseket is.

» A kockázatalapú megközelítés lehetővé teszi a KKV-k számára, hogy az adatvédelmi megfelelés keretét rugalmasan határozzák meg. A megközelítés nem konkrét intézkedések meghozatalát követeli meg, hanem az adatkezelési tevékenységek megértését célozza az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint az adatkezelés által a természetes személyek jogaira és szabadságaira jelentett kockázat valószínűségének és súlyosságának vizsgálata alapján. A gyakorlatban ez azt jelenti, hogy a GDPR mozgásteret biztosít a KKV-k számára, hogy az saját igényeikre szabják a technikai és szervezési intézkedéseket.[171]

» Bizonyos mértékig lehetővé teszi az uniformizált megközelítéstől való eltérést is. Az alacsony kockázattal járó adatkezelési tevékenységeket végző KKV-knak kevesebb intézkedést kell hozniuk a GDPR-megfelelés érdekében, mint a magas kockázattal járó adatkezeléseket végzőknek.

Habár a kockázatalapú megközelítés könnyen fellelhető a GDPR szövegében, a gyakorlati alkalmazása nehézségeket okozhat. Ahogyan az uniós döntéshozók számtalan alkalommal javasolták, a kockázatalapú megközelítés tartalmazhatna alapkövetelményeket, legjobb gyakorlatokat és standardokat is. Ezek hasznos eszköztárat jelentenének az adatkezelők számára a hasonló helyzetekben felmerülő, hasonló problémák (az adatkezelés természete, hatóköre, körülményei és célja szerint) kezelésére.

171 A belga adatvédelmi hatóság iránymutatása: 'RGPD vade-mecum pour les PME – Un guide pour préparer les petites et moyennes entreprises (PME) au Règlement général sur la protection des données' (January, 2018) 5. **https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf**

4.7. A kockázatalapú megközelítés a gyakorlatban

Az adatkezelő feladatairól, az elszámoltathatóság alapelve

Háttér

Az elszámoltathatóság alapelvének értelmében az adatkezelő felelős a GDPR többi adatkezelési alapelvének való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására is. Az adatfeldolgozóknak is meg kell felelniük az elszámoltathatóságnak, tekintve, hogy egyrészt teljesíteniük kell az elszámoltathatósághoz kötődő kötelezettségeiket, másrészt támogatniuk kell az adatkezelőt megfelelési kötelezettségei teljesítésében.[172] Ezért az elszámoltathatóságnak minden KKV-nak meg kell felelnie, függetlenül az adatkezelésben betöltött szerepétől.

Az adatvédelem és a magánélethez való jog területén az elszámoltathatóságot a szervezet GDPR-nak való megfelelés felelősségeként[173] vagy a megfelelési képesség proaktív bizonyításaként értelmezzük.[174] Az elszámoltathatóság növelheti az átláthatóságot és a szabályozók és adatalanyok bizalmát, továbbá biztosítja a vállalati működés nagyobb átláthatóságát is.[175]

Az elszámoltathatóság GDPR-ban való kifejezett megjelenése a korábbi reaktív megközelítést a proaktív megfelelés és adatkezelés irányába tolja

172 Az adatfeldolgozók kötelesek például nyilvántartást vezetni az adatkezelési tevékenységeikről (GDPR 30(2)), bizonyos esetekben adatvédelmi tisztviselőt kinevezni (GDPR 37. cikk), megfelelő szervezeti és technikai intézkedéseket hozni (GDPR 32. cikk). Lásd. FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

173 Colin Bennett, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats' in Daniel Guagnin et al. (eds.), Managing Privacy through Accountability (Springer 2012) 46.

174 Joseph Alhadeff, Brendan van Alsenoy and Jos Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', in Daniel Guagnin et al. (eds.), Managing Privacy through Accountability (Springer 2012).

175 Lásd fent.

el.[176] Amíg a megfelelés csupán azt írja elő, hogy a KKV-nak teljesítenie kell bizonyos kötelezettségeket, az elszámoltathatóság alapelve ennél tovább megy: a KKV-nak bizonyítania kell a személyes adatok védelme melletti elkötelezettségét.[177] Például a kockázatértékelést vagy a szervezeti és technikai intézkedések értékelését nem oldhatjuk meg ezek „egyszeri kipipálásával". [178]

Milyen intézkedéseket kell hozni a KKV-nak az elszámoltathatóság érdekében?

Az adatkezelő KKV köteles olyan szervezeti és technikai intézkedéseket végrehajtani – ideértve az adatkezelési szabályzatok megalkotását –, melyek biztosítják és igazolják az adatkezelési tevékenységek GDPR-nak való megfelelését.

Az intézkedéseket az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira jelentett különböző valószínűségű és súlyosságú kockázatok értékelésével hozza meg.[179]

Az adatfeldolgozó KKV-k is kötelesek garantálni, hogy meghozzák a szükséges intézkedéseket a GDPR-nak való megfelelés és a természetes személyek jogainak és szabadságainak védelme érdekében.[180]

176 Paul De Hert (2012) Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law. In: Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., Postigo H. (eds) Managing Privacy through Accountability. Palgrave Macmillan, London.

177 Lásd fent.

178 Dariusz Kloza et al., "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," (2017) d.pia.lab Policy Brief accessed 13 May 2020

179 GDPR 24. cikk.

180 GDPR 28(1).

TIPP

Az elszámoltathatóságnak és a jogszabályoknak való megfelelés igazolására javasolt írásos nyilvántartást vezetni a szervezeti és technikai intézkedésekről és a kiválasztásuk okáról.

További példák az elszámoltathatósági intézkedésekre

A GDPR-ban számos elszámoltathatósági intézkedés szerepel, többek között:

- adatvédelmi szabályzat kidolgozása és alkalmazása,
- az alapértelmezett és beépített adatvédelem elvének való megfelelés (25. cikk),
- a (közös) adatkezelők, az adatkezelők/adatfeldolgozók, az adatfeldolgozók/további adatfeldolgozók közötti, a kölcsönös felelősségi köröket meghatározó szerződés kidolgozása,
- az adatkezelési tevékenységek nyilvántartása (30. cikk),
- megfelelő technikai és szervezési intézkedések biztosítása (32. cikk),
- a hozzáférési jog gyakorlását támogató folyamatok alkalmazása,
- az adatkezelési szabályzat közzététele az interneten,
- incidenskezelési terv kidolgozása (35. cikk),
- az adatvédelmi incidensek nyilvántartása, és szükség esetén az adatvédelmi hatóság és az érintettek értesítése,[181]
- előzetes adatvédelmi hatásvizsgálat lefolytatása (35. cikk),
- az adott szektor és különböző vállalkozások magatartási kódexeinek alkalmazása,
- tanúsítási mechanizmusok, bélyegzők vagy jelölések alkalmazása, ami bizonyítja a szervezet GDPR-nak való megfelelését.[182]

181 GDPR 33. és 34. cikk.

182 Elszámoltathatósági eszköztár (angol nyelven): **https://edpb.europa.eu/our-work-tools/accountability-tools_en**

Az elszámoltathatósági intézkedéseket folyamatosan felül kell vizsgálni, és az adatkezelési tevékenység aktuális állapotának megfelelően frissíteni kell. Az elszámoltathatóságnak való megfelelés folyamatos erőfeszítést kíván az adatkezelőktől és adatfeldolgozóktól is.

Milyen előnyökkel jár az elszámoltathatóság a KKV-k számára?

Az elszámoltathatóság alapelve a valódi biztonságot elősegítő intézkedésekre fókuszál. Az elszámoltathatóság elősegíti a KKV-k megfelelő irányítását és a legjobb gyakorlatok alkalmazását, valamint a hatékonyságukat is növeli. Ösztönzőleg hat továbbá a KKV-kra, hogy rendben tartsák az adathalmazaikat,[183] ezáltal nagyobb rálátással rendelkezzenek a szervezet adatkezelési folyamataira. Az elszámoltathatóság elősegíti az innovatív technológiai és szervezési intézkedések végrehajtását, ideérte az adatkezelési szabályzatok megalkotását is.

Végül az elszámoltathatóság növeli a bizalmat a KKV-k és az ügyfeleik között, ami versenyelőnyt jelenthet a KKV-k számára.

HASZNOS FORRÁSOK

- WP29 munkacsoport WP 168 számú munkadokumentuma: The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data (WP 168, 1 December 2009) **https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2009/wp168_en.pdf**
- WP29 munkacsoport 3/2010 véleménye az elszámoltathatóság elvéről **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_hu.pdf**

183 Commissioner Vera Jourová 'Speech at the ‚Computers, Privacy and Data Protection' Conference 2019' SPEECH/19/787: **https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_19_787**

A beépített és alapértelmezett adatvédelem

Háttér

A GDPR hatálybalépésével a beépített és alapértelmezett adatvédelem elvének érvényesítése jogi kötelezettséggé vált az adatkezelők számára.

Adatvédelmi hatóságok KKV-kat érintő döntései

A baden-württembergi felügyeleti hatóság 20.000 eurós bírságot szabott ki egy KKV-ra, mert elmulasztotta a szükséges szervezési és technikai intézkedések meghozatalát, és felhasználóinak jelszavait egyszerű szöveges formátumban tárolta, nem pedig hash értékben. Ez a technikai megoldás 330.000 felhasználó adatainak ellopásához vezetett.[184]

A beépített és alapértelmezett adatvédelem elvének célja a magánélethez való jog védelmének beépítése a személyes adatokat kezelő technológiák és applikációk teljes életciklusába. A beépített és alapértelmezett adatvédelem elvének gyakorlati alkalmazása rendkívül összetett az alapelvek értelmezését övező bizonytalanság miatt.[185]

Ez a megközelítés ugyanakkor előnyt is jelent a KKV-k számára, mert nem kötelesek a beépített és alapértelmezett adatvédelem alapelvének való megfelelés érdekében előre meghatározott intézkedéseket hozni, hanem lehetőségük van testre szabni azokat.

Miből áll a beépített adatvédelem?

A beépített adatvédelem elvének értelmében az adatkezelő köteles már az adatkezelést megelőzően, valamint annak későbbi szakaszaiban is (például közbeszerzések, kiszervezés, fejlesztés, támogatás, fenntartás,

184 Lásd német nyelven: 'LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO'.

185 Michael Veale, Reuben Binns and Jef Ausloos, 'When data protection by design and data subject rights clash' (2018) International Data Privacy Law, ipy002,: https://doi.org/10.1093/idpl/ipy002

tesztelés, tárolás, törlés stb.) hatékony szervezési és technikai intézkedéseket hozni annak érdekében, hogy a GDPR által előírt követelményeket beágyazza az adatkezelési tevékenységeibe.[186] Az az elgondolás áll mögötte, hogy ne úgy tervezzünk meg egy adatkezeléssel járó eljárást, folyamatot, szolgáltatást vagy terméket, hogy majd utólag megpróbáljuk hozzáilleszteni a személyes adatok védelmét.

Az adatkezelőnek a technikai és szervezési intézkedések meghozatala során tekintettel kell lennie az alábbiakra:

- az adatkezelés jellege (az adatkezelési tevékenység sajátosságai), hatóköre (nagyságrendje és típusa: például, ha különleges adatok kezelésére is sor kerül), körülményei és céljai;[187]
- a technikai és szervezési intézkedések jelenlegi állása (ez nagyon változatos képet mutathat);
- a megvalósítás költségei, ideértve az anyagi költségeket, az idő és emberi erőforrások költségét;
- a változó valószínűségű és súlyosságú kockázat, amit az adatkezelési tevékenység a természetes személyek jogaira és szabadságaira jelent.

Az adatkezelő:

- az adatkezelési tevékenység során biztosítja a megfelelő technikai és szervezési intézkedéseket és a szükséges garanciákat (a GDPR egyetlen konkrét példát említ, az álnevesítést); valamint
- megvalósítja az adatvédelmi alapelveket,[188] és beépíti az adatkezelés folyamatába a Rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciákat.[189] A

186 Az Európai Adatvédelmi Biztos 5/2018 számú véleménye a beépített adatvédelemről (angol nyelven): **https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf** (10. bekezdés).

187 Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): **https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en**

188 GDPR 5. cikk.

189 GDPR III. fejezet.

beépített adatvédelem eszköze például az előzetes adatvédelmi hatásvizsgálat.[190]

» ezeket mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során (életciklus megközelítés);
» hatékony módon hajtja végre.

A GDPR 25. cikkében felsorolt technikai és szervezési intézkedések a munkatársak adatvédelmi tárgyú képzésétől (hogyan kezeljék az ügyfelek és a kollégák személyes adatait) a fejlett technikai megoldásokig terjedhetnek, bármilyen megoldás szóba jöhet. Néhány adatvédelmi hatóság mégis meghatározza a technikai intézkedések minimumát, és elvárja a személyes adatok titkosítását, ha ez lehetséges.

Amennyiben az intézkedések megfelelőek az adatvédelmi alapelvek hatékony alkalmazására, nincs szükség további fejlesztésükre.[191] Ez azt is jelenti, hogy nincsenek olyan kifejezett intézkedések, melyek garantálják a GDPR-nak való megfelelést.

A beépített és alapértelmezett adatvédelem elveinek való megfelelés érdekében javasolt megfontolni a magánélet védelmét erősítő technológiák (Privacy Enhancing Technologies, PETs) alkalmazását.

Ezek széles körben mozognak, magukban foglalják egyrészt a hagyományos adatbiztonsági technológiákat (anonimizálás, titkosítás, kriptográfia), másrészt a személyes adatok védelmét elősegítő általánosabb eszközöket (például webes böngészés követését megakadályozó eszközök, felhasználói interfészek alkalmazása a hozzájárulás beszerzéséhez vagy olyan eszközök biztosítása, melyekkel az érintettek nyomon tudják

190 Az Európai Adatvédelmi Biztos 5/2018 számú véleménye a beépített adatvédelemről (angol nyelven): **https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf**

191 Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): **https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en**

követni az adatvédelmi szabályzat alkalmazását vagy személyre tudják szabni az adatkezelési szabályzat feltételeit).[192]

A magánélet védelmét erősítő technológiák alkalmazása versenyelőnyt jelenthet a KKV-k számra, mert növelik az adatvédelem fontosságára hangsúlyt fektető ügyfelek bizalmát.

A magánélet védelmét erősítő újabb technológiák kidolgozása üzleti lehetőséget is jelenthet a KKV-k számára. Habár a beépített adatvédelem elve csak az adatkezelők számára jelent kötelezettséget, az adatkezeléssel járó szolgáltatást nyújtó vagy ilyen applikációt és termékeket előállító vállalkozásoknak is figyelemmel kell lenniük rá.[193]

Az ENISA jelenleg egy PETs adatbázis összeállításán, valamint az elérhető technológiák értékelésén dolgozik.[194]

Hogyan értékeljük, hogy megfelelőek és hatékonyak-e a beépített adatvédelemi intézkedések?

Az intézkedések megfelelősége szorosan összekapcsolódik a hatékonyságukkal. A hatékonyság azt jelenti, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy az adatkezelési tevékenység vonatkozásában a választott intézkedések megfelelőek a beépített adatvédelem céljainak eléréséhez.

Ezért nem elegendő általános intézkedéseket hozni csupán „papírozás" végett.[195] Az intézkedéseknek hatásosnak kell lenniük, és igazodniuk kell a kockázathoz, amit az alapelveknek való megfelelés elmulasztása okozhat.

192 Lásd például: Steve Kenny, 'An introduction to Privacy Enhancing Technologies' (1 May 2008), 'Privacy Enhancing Technologies – A Review of Tools and Techniques' and Yun Shen and Siani Pearson 'Privacy Enhancing Technologies: A Review'

193 GDPR (78) Preambulumbekezdés.

194 'ENISA PET maturity assessment repository': **https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository**

195 Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): **https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en**

Az alkalmazott intézkedések hatékonyságának igazolása céljából az adatkezelők teljesítménymutatókat alkalmazhatnak, így a KKV-k üzleti és adatvédelmi célkitűzéseiket párhuzamosan nyomon követhetik.

PÉLDA

A beépített adatvédelmi intézkedések vonatkozásában a KKV-knak az alábbiakat kell megfontolniuk a „smart" (Specific, Measurable, Attainable, Relevant, Time-bound) KPI (fő teljesítménymutató) felállítása érdekében:

1. Milyen céllal hozták ezeket az intézkedéseket? (Például az ügyfelek magánélethez való jogának megfelelőbb garanciája és a GDPR előírásainak való megfelelés igazolása.)
2. Miért fontos, hogy a vállalkozás elérje a meghatározott célokat? (Például versenyelőnyre tehet szert más, hasonló szolgáltatást nyújtó KKV-kkal szemben és elkerülheti a bírságokat.)
3. Hogyan értékeli a KKV az előrehaladást?

A KPI-k tartalmazhatnak mérőszámokat.
A mérőszám lehet kvantitatív és mérheti:

» az adatkezelési tevékenység által jelentett kockázat csökkenését (például magas kockázati szintről közepesre);
» az érintettek által benyújtott kérelmek számának csökkenését (például az intézkedések végrehajtását követően X százalékkal csökkent a benyújtott érintetti kérelmek száma);
» a benyújtott érintetti kérelmek válaszadási idejének csökkenését (például az intézkedések végrehajtását követően X százalékkal csökkent a benyújtott érintetti kérelmek válaszadási ideje).

Vagy lehet kvalitatív is, mint például a teljesítmény értékelése (végezheti az adatvédelmi tisztviselő vagy külsős auditáló cég is), osztályozási rendszer alkalmazása vagy szakértői értékelés. Az adatkezelők megindokolhatják, hogy milyen megfontolások alapján választották ki az intézkedések hatékonyságának értékelési módját, de elszámoltathatóak érte.

4. Milyen hatással bírhat a KKV az intézkedések kimenetelére? (Például PET elfogadása vagy további alkalmazottak felvétele.)
5. Az eredmények megvalósításáért felelős személyek kijelölése.

6. Milyen eredményt szeretnének elérni pontosan? (Például X%-kal szeretnénk csökkenteni az érintetti kérelmek számát.)
7. Milyen gyakran fogják ellenőrizni a folyamatot a kívánt cél eléréséig? [196]

A tanúsításoknak való megfelelés önmagában nem biztosítja a hatékonyságot, de felhasználható a megfelelés igazolásának támogatására.

Miből áll az alapértelmezett adatvédelem?

Az adatfeldolgozók kötelesek olyan megfelelő technikai és szervezési intézkedéseket hozni, melyek biztosítják, hogy csak azokat az adatokat kezelik, melyek szükségesek az adatkezelés kifejezett céljának eléréséhez.

Az „alapértelmezett", ahogyan azt az informatika tudománya általánosan meghatározza, egy szoftveralkalmazáshoz, számítógépes programhoz vagy eszközhöz kapcsolódó, konfigurálható beállítás már előre meghatározott vagy előre kiválasztott értéke. Ezeket a beállításokat gyári beállításnak is nevezik, különösen elektronikus eszközök esetén.[197] Ezért az alapértelmezett adatvédelem technikai értelemben arra utal, hogy az adatkezelő kiválaszthat szoftveralkalmazáshoz, számítógépes programhoz vagy eszközhöz kapcsolódó, előre meghatározott beállítást vagy adatkezelési opciót, amely hatással lehet – különösen, de nem kizárólag – a gyűjtött adatok mennyiségére, kezelésük mértékére és tárolásuk időtartamára stb.

Az az elgondolás áll mögötte, hogy az alapbeállítást választó érintettek személyes adatai is megfelelő védelemben részesüljenek.

196 Mohammed Badawya et al., 'A survey on exploring key performance indicators' (2016)1 FCIJ, 47-52;'What is a KPI?' **https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator**

197 Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről (angol nyelven): **https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en**

Milyen intézkedésekkel lehet megvalósítani az alapértelmezett adatvédelem elvét?

Az alapértelmezett adatvédelem gyakorlati megvalósítása érdekében javasolt intézkedések:

» Az igénybe vett szolgáltatáshoz igazítják a gyűjtött személyes adatok körét (kezelt adatok száma);

PÉLDA

Ha egy könyvesbolt úgy dönt, hogy hagyományos és e-book formátumban is árusít online, két különböző nyomtatványt kell a vásárlók rendelkezésére bocsátania, mert a hagyományos könyvek esetében a megrendelő címének ismerete szükséges a kiszállításhoz, azonban e-book rendelése esetén a postai cím kezelése felesleges.

» A személyes adatok törlésére vonatkozó átlátható szabályozás kialakítása;

PÉLDA

Egy sportközpont jogi kötelezettsége, hogy orvosi igazolást kérjen be az ügyfeleitől a szolgáltatás igénybevételéhez. Amennyiben jogszabály máshogyan nem rendelkezik, a tagság lejárta után ezeket az igazolásokat haladéktalanul meg kell semmisíteni.

» Kerüljük az előre „kipipált” négyzeteket, melyek arra sarkallják a vásárlókat, hogy további extra szolgáltatásokat vegyenek igénybe (az adatkezelés mértéke).

PÉLDA

Ha egy vállalkozás a honlapján cookie-kat (sütiket) alkalmaz, célszerű elkerülni az előre kipipált négyzeteket a nem szükséges cookie-k esetén.

Az alapértelmezett adatvédelem gyakorlati megvalósítása érdekében javasolt **szervezési** intézkedések:

» Hozzáférés-ellenőrzési szabályzat kialakítása (adathozzáférés);

A hozzáférés szükségességének értékelése alapján korlátozni kell azoknak az alkalmazottaknak a számát, akik hozzáférhetnek a személyes adatokhoz, egyúttal gondoskodni kell arról is, hogy azok viszont hozzáférhessenek, akiknek erre szüksége van. A hozzáférés-ellenőrzésnek az egész adatkezelési folyamatot végig kell kísérnie.

PÉLDA

Egy vállalkozás megfontolhatja, hogy korlátozza a HR osztály hozzáférését a személyes adatokhoz, amikor azok nem szükségesek feladataik ellátásához.

A hotel üzemeltetője nem közli a vendégek személyes adatait a takarítószemélyzettel vagy az étterem dolgozóival, ha ez nem szükséges a feladataik ellátásához.

HASZNOS FORRÁSOK

» ENISA PET maturity assessment repository
https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository

» Az Európai Adatvédelmi Biztos 5/2018 számú véleménye a beépített adatvédelemről **https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf**

» Az Európai Adatvédelmi Testület 4/2019 számú iránymutatása a GDPR 25. cikkéről a beépített és alapértelmezett adatvédelemről **https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en**

A GDPR 30. cikke az adatkezelési tevékenységek nyilvántartásáról

Háttér

Az adatkezelési tevékenységekről vezetett nyilvántartások hasznos eszközök a tervezett vagy már folyamatban lévő adatkezelések hatásainak elemzéséhez. A nyilvántartás támogatja az adatkezelőt vagy adatfeldolgozót az adatkezelési tevékenységeinek természetes személyek jogaira jelentett kockázatainak felmérésében, valamint a személyes adatok biztonságát garantáló megfelelő biztonsági intézkedések azonosításában és végrehajtásában.

Azoknak a mikro-, kis-, és középvállalkozásoknak, melyek alapvető üzleti tevékenysége nem jár személyes adatok kezelésével, az adatkezelési tevékenységekről vezetett nyilvántartás nem jelent különösebb terhet, de a KKV megfelelő irányítását erősítő eszközzé válhat.

Mire kell figyelni a dokumentáció vezetése során?

Az adatkezelők és az adatfeldolgozók is kötelesek nyilvántartást vezetni az adatkezelési tevékenységükről, de néhány különbséggel: az adatfeldolgozókat kevesebb kötelezettség terheli.

PÉLDA

Az adatkezelő KKV-k által vezetett nyilvántartásnak tartalmaznia kell az alábbiakat:

» az adatkezelő/az adatkezelő képviselője/az adatvédelmi tisztviselő neve és elérhetőségei;
» az adatkezelés célja(i);
» az érintettek (ügyfelek, alkalmazottak stb.) és a kezelt adatok kategóriái (elérhetőségek, egyedi azonosítók, társadalombiztosítási szám stb.);
» a címzettek kategóriái, akikkel a személyes adatokat közlik, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
» személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén az EGT-n kívüli ország vagy nemzetközi szervezet megnevezése;
» ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők; és
» ha lehetséges, a technikai és szervezési intézkedések általános leírása.

Az adatfeldolgozó KKV-k által vezetett nyilvántartásnak tartalmaznia kell az alábbiakat:

» az adatfeldolgozó/képviselője/az adatvédelmi tisztviselő neve és elérhetőségei, valamint az adatkezelő – akinek a nevében az adatfeldolgozó eljár – neve és elérhetőségei;
» az adatkezelő nevében végzett adatkezelési tevékenységek kategóriái;
» személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén az EGT-n kívüli ország vagy nemzetközi szervezet megnevezése;
» ha lehetséges, a technikai és szervezési intézkedések általános leírása.

TIPP

Habár nem kötelező, célszerű a nyilvántartásban rögzíteni az adatkezelési tevékenységek és esetleges harmadik országba történő adattovábbítások jogalapját is, valamint csatolni a (közös) adatkezelők, az adatkezelő és adatfeldolgozó, valamint az adatfeldolgozó és az alvállalkozó között létrejött adatmegosztási szerződést is.

A GDPR nem írja elő az adatkezelők számára, hogy részletes listát vezessenek minden adattovábbításról, azonban az elszámoltathatóság alapelvének értelmében az adatkezelőnek képesnek kell lennie az adatkezelés jogszerűségének igazolására. Ezen kötelezettségének könnyebben eleget tud tenni, ha az adatkezelés részleteit rögzíti a nyilvántartásban.

A nyilvántartási kötelezettség kapcsán felmerülnek további alternatív lehetőségek, többek között a jegyzékek, adatkezelési terv stb. A felügyeleti hatóság kérheti ezen dokumentumok benyújtását. A pontos dokumentáció vezetése hasznos lehet a vállalkozás számára, ha igazolnia kell a Rendeletnek való megfelelését.

Az adatkezelési tevékenységekről **írásos** formában kell dokumentációt vezetni.[198] Az adatkezelő (és az adatfeldolgozó) választhat, hogy papíralapon vagy elektronikus formában teszi ezt meg.

TIPP

Az elektronikus formában vezetett nyilvántartás előnye, hogy szükség esetén könnyen szerkeszthető, kiegészíthető és módosítható, de a KKV-k számára megfelelő a papíralapú nyilvántartás is.

198 A brit (ICO), ír és francia (CNIL) adatvédelmi hatóság véleménye és iránymutatásai alapján.

A KKV-k mentesülnek a nyilvántartási kötelezettség alól az alábbi feltételek fennállása esetén:

- az adatkezelés az érintettek jogaira és szabadságaira valószínűsíthetően nem jár kockázattal;
- az adatkezelés alkalmi jellegű (azaz nem rendszeres vagy folyamatos); vagy
- az adatkezelés nem terjed ki a személyes adatok különleges kategóriájának vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

A gyakorlatban csak kevés KKV felel meg teljesen ezeknek a feltételeknek.

PÉLDA

Ha a vállalkozásnak 250 főnél kevesebb alkalmazottja van, akkor is nyilvántartást kell vezetnie a munkavállalók adatainak kezeléséről, mert az adatkezelés nem alkalmi jellegű, és az alkalmazottak személyes adatai között különleges adatok is szerepelnek (például táppénz esetén).

Egy biztosítótársaság alkalmanként belső elégedettségi felméréseket végez az alkalmazottak részvételével. Mivel erre az adatkezelésre ritkán kerül sor, ezt nem kell feltüntetni az adatkezelésekről vezetett nyilvántartásban. Azonban amennyiben a vállalkozás hitelképesség megállapítása céljából alkalmanként profilalkotást végez az ügyféladatbázisban, ezt fel kell tüntetni a nyilvántartásban, mert a profilalkotás kockázattal járó adatkezelési tevékenység.[199]

199 A dokumentálási kötelezettségről (angol nyelven): **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/**

Egy tetoválószalon nyilvántartást vezet az ügyfelei egészségügyi adatival kapcsolatos adatkezelésekről.

A kereskedelmi tevékenységet folytató és legalább egy munkavállalót foglalkoztató vállalkozás (például étterem, pub, fodrász, kozmetikus) nyilvántartást vezet a munkavállalói személyes adatainak kezeléséről. [200]

TIPP

Ha a KKV mentesül is a nyilvántartás-vezetési kötelezettség alól, javasolt nyilvántartást vezetni az alkalmi jellegű adatkezelésekről, mert egy esetleges ellenőrzés során sokkal könnyebben együtt tud működni a felügyeleti hatósággal, és igazolni tudja a GDPR-nak való megfelelését.[201]

Az adatkezelők és adatfeldolgozók létrehozhatnak olyan egységes közös nyilvántartást, melyet szükség esetén a felügyeleti hatóság rendelkezésére tudnak bocsátani. Ha egy szervezet egy bizonyos adatkezelési tevékenység tekintetében egyszerre adatkezelőnek és adatfeldolgozónak is minősül, a nyilvántartást több részre lehet osztani, hogy megfeleljen a szervezet által betöltött különböző szerepeknek.[202]

Milyen egyéb dokumentációt ír elő a GDPR?

Az adatkezelési tevékenységekről vezetett nyilvántartás mellett az egyéb nyilvántartásokat is célszerű írásos formában vezetni, mert ezek segítsé-

200 FAQ sul registro delle attività di trattamento': **https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento**

201 A belga adatvédelmi hatóság n° 06/2017 számú ajánlása, 14 juin 2017 (angol nyelven): **https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/recommandation_06_2017.pdf**

202 A belga adatvédelmi hatóság n° 06/2017 számú ajánlása, 14 juin 2017 (angol nyelven): **https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/recommandation_06_2017.pdf**

gével az adatkezelők és adatfeldolgozók igazolni tudják, hogy megfelelnek a GDPR rendelkezéseinek.

Kifejezetten javasolt nyilvántartást vezetni az alábbiakról:

- adatvédelmi kockázatok;
- írásos szerződések megkötése a (közös) adatkezelők, az adatkezelők/adatfeldolgozók, valamint az adatfeldolgozók/alvállalkozók között, melyben meghatározzák a kölcsönös felelősségi köröket,
- az adatvédelmi tisztviselő javaslatai (írásos vélemények, e-mailek stb.),
- az adatvédelmi tisztviselő kinevezéséről (vagy ennek mellőzéséről) hozott döntés,
- az adatkezelési tevékenység különböző fázisaiban hozott technikai és szervezési intézkedések,
- az előzetes adatvédelmi hatásvizsgálat folyamatainak rögzítése,
- az adatvédelmi incidensek/ezek okai/hatása/orvoslásukra tett lépések,
- az érintettek jogait garantáló intézkedések,
- az adatkezelési alapelveknek való megfelelés érdekében hozott intézkedések,
- az adatkezelés joglapjai és azok felülvizsgálata.

HASZNOS FORRÁSOK

- Európai Adatvédelmi Biztos: Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies **https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en**

Minták adatkezelési tevékenységekről vezetett nyilvántartásokra:

- Az ICO (brit DPA) honlapján: **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/**
- A CNIL (francia DPA) honlapján: **https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement**
- Douwe Korff and Marie Georges, The DPO Handbook – Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation 158. oldaltól **https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf**

TIPP

A minta letöltése előtt a KKV-nak meg kell határoznia, hogy az adott adatkezelési tevékenység tekintetében adatkezelőként vagy adatfeldolgozóként jár el.

Az adatkezelés biztonságáról

Háttér

Az adatkezelők és adatfeldolgozók megfelelő technikai és szervezési intézkedéseket hajtanak végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantáljanak.

Ilyen intézkedések például:

- a személyes adatok álnevesítése vagy titkosítása;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének folyamatos biztosítása;

- fizikai vagy műszaki incidens esetén a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állásának kellő időben történő visszaállítási lehetősége;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás lefolytatása.

Hogyan kapcsolódnak a biztonsági kötelezettségek a GDPR más rendelkezéseihez?

A biztonsági előírások kötelezik az adatkezelőket, hogy amennyiben adatfeldolgozót kívánnak bevonni az adatkezelési tevékenységbe, a szerződés megkötésekor kellő gondossággal járjanak el, és mérjék fel, hogy az adatfeldolgozó megfelelő biztonsági szintet garantál-e.

Az adatkezelő csak akkor szerződhet az adatfeldolgozóval, ha megbízik abban, hogy az meg tud felelni a GDPR előírásainak.

Az adatfeldolgozóval való szerződéskötés során az adatkezelőnek javasolt megvizsgálnia, hogy az adatfeldolgozó megfelelő dokumentációt vezet-e a Rendelet követelményeinek való megfeleléséről (adatkezelési/információbiztonsági szabályzat, külső auditokról szóló jelentések, tanúsítványok stb.). Az adatkezelőnek meg kell győződnie az adatfeldolgozó szakértelméről (például az adatvédelmi incidensek kezeléséhez és a biztonsági intézkedések végrehajtásához szükséges szaktudás), megbízhatóságáról és a rendelkezésére álló forrásokról is. Kellő körültekintéssel végzett kiválasztási folyamat után elegendő bizonyíték áll az adatkezelő rendelkezésére, melyek alapján képes eldönteni, hogy megfelelő-e számára az adatkezelő és szerződhet-e vele.

Az átvilágítási folyamat nem egyszeri feladat, az adatkezelőnek folyamatosan ellenőriznie kell, hogy az adatfeldolgozó teljesíti-e a kötelezettségeit, és megfelel-e a Rendeletben foglalt előírásoknak. Ennek érdekében az adatkezelő saját alkalmazottai vagy külsős cég megbízásával vizsgálatot folytathat le.

Az adatkezelő az adatkezelési tevékenységet (például technikai támogatás vagy felhőszolgáltatás) részletes adatkezelési megállapodásban szervezheti ki szerződés, más jogi aktus vagy más kötelező erejű megállapodás útján, melyben egyértelműen és pontosan megfogalmazza az adatkezelés természetét és az azzal járó kötelezettségeket.

TIPP

Az átvilágítási folyamatról vezetett dokumentáció egy esetleges ellenőrzés során hasznos lehet annak alátámasztására, hogy az adatkezelő milyen megfontolás alapján ítéli megbízhatónak az adatfeldolgozót.

Milyen szervezési biztonsági intézkedéseket hozhat egy KKV?

- a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből eredő kockázatok elemzése,
- biztonságtudatos szervezeti kultúra kialakítása (például képzéseken),
- adatbiztonsági szabályzat kidolgozása, ami rögzíti minden felhasználó szerepét és az ahhoz szükséges hozzáférési szinteket (hozzáférés-ellenőrzés), ezáltal csak a felhasználó szerepéhez feltétlenül szükséges adatokra korlátozza a hozzáférést (például rendszergazda fiók). A szabályzat alátámasztja továbbá az adatkezelő felelős eljárását (24. cikk) és elősegíti a GDPR rendelkezéseinek való megfelelést is.

TIPP

Az adatvédelmi tisztviselő fontos szerepet tölthet be a szervezeti biztonsági intézkedések kialakítása során, például tájékoztatást nyújt, képzéseket tart vagy ellenőrzi a személyes adatokat kezelő munkatársak adatkezelési tevékenységét.

Milyen technikai biztonsági intézkedéseket hozhat egy KKV?

Technikai intézkedések alatt gyakran a számítógépen és hálózatokon tárolt személyes adatok védelmét értjük. Amíg ezek fontossága vitathatatlan, számos esetben az eszközök elvesztése vagy eltulajdonítása, régi számítógépek kidobása, adathordozók elvesztése, eltulajdonítása vagy helytelen felhasználása miatt következik be biztonsági incidens. A technikai intézkedéseknek ezért a fizikai és IT biztonságra is ki kell terjedniük.

A fizikai biztonság vonatkozásában az alábbiakra kell gondolnunk:

- az ajtók és zárak minősége, az üzlethelyiségek védelme (például riasztók, biztonsági világítás, kamerák);
- az üzlethelyiségbe belépők és látogatók ellenőrzése;
- a papír- és elektronikus hulladék kezelése; és
- az IT eszközök biztonságos tárolása, különös tekintettel a mobil eszközökre.

Informatikai megközelítéssel a technikai intézkedésekre gyakran kiberbiztonságként hivatkozunk. Ez egy folyamatosan fejlődő összetett technikai terület, melyen újabb és újabb veszélyek és fenyegetések jelennek meg.

Kiberbiztonsági szempontból az alábbi tényezőket érdemes megvizsgálni:

- rendszerbiztonság – a hálózatok és információs rendszerek biztonsága, különös tekintettel azokra, melyek személyes adatokat kezelnek;
- adatbiztonság – a rendszerekben kezelt személyes adatok biztonsága (például megfelelő hozzáférés-ellenőrzés és az adatok biztonságos kezelése megfelelő titkosítási technikák alkalmazásával);
- online biztonság (például a vállalkozás által használt honlap és online szolgáltatások biztonsága); és
- az eszközök biztonsága (ideértve a „Hozd a saját eszközödet (BYOD)” szabályozást).

Milyen biztonsági szintet kell garantálni?

A GDPR nem határozza meg, hogy milyen biztonsági intézkedéseket kell a KKV-knak megvalósítaniuk. Az adatkezelők és adatfeldolgozók „megfelelő" biztonsági szintet kötelesek biztosítani, az adatkezelés természetes személyek jogaira és szabadságaira gyakorolt hatását, a tudomány és technológia állását és a megvalósítás költségét, valamint az adatkezelés jellegét, hatókörét, körülményeit és céljait figyelembe véve.

Ez reflektál egyrészt a GDPR kockázatalapú megközelítésére, másrészt arra, hogy az adatbiztonság tekintetében nincs uniformizált megoldás. Az adatkezelő és adatfeldolgozó „megfelelősége" minden esetben a sajátos körülményeik, valamint az adatkezelési tevékenységük, és annak szervezetükre és természetes személyek jogaira gyakorolt hatásának függvénye. Amennyiben különleges adatok (például egészségügyi) vagy kiskorúak személyes adatainak kezelésére is sor kerül, magasabb biztonsági szintet kell garantálni.

A megfelelő intézkedések kiválasztása előtt a KKV-nak értékelnie kell az információbiztonsági kockázatokat. Át kell tekintenie a személyes adatok kezelését és felhasználásuk módját annak érdekében, hogy fel tudja mérni, az esetleges sérülésükből származó károkat vagy, hogy a kezelt adatok különleges adatok-e.

További megfontolandó körülmények:

- a vállalkozás üzlethelyiségeinek és számítógépes rendszereinek típusa és nagysága;
- az alkalmazottak száma és a személyes adatokhoz való hozzáférésük mértéke;
- az adatfeldolgozó által kezelt és használt adatok köre.

HASZNOS FORRÁSOK

» European Union Agency For Network and Information Security, Handbook on Security of Personal Data Processing **https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing**
» ENISA On-line tool for the security of personal data processing **https://www.enisa.europa.eu/risk-level-tool/**
» ISO/IEC 27001:2013: **https://www.iso.org/standard/54534.html**

Az adatvédelmi incidens

Háttér

Az „adatvédelmi incidens" a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.[203] Amennyiben a GDPR rendelkezései más módon sérülnek (például az adatkezelésnek nincs megfelelő jogalapja vagy az érintettek nem kapnak megfelelő tájékoztatást), nem vonatkoznak rájuk az adatvédelmi incidensekhez kapcsolódó kötelezettségek. Ha az információbiztonság sérülése nem érint személyes adatokat, szintén nem vonatkoznak rá az adatvédelmi incidensre vonatkozó kötelezettségek.[204] Ezért nem minden biztonsági incidens számít adatvédelmi incidensnek. Az adatvédelmi incidensek oka lehet hanyagság, baleset vagy technikai hiba, valamint belső vagy külső munkatársak szándékos cselekedete is.[205]

Ha az adatvédelmi incidens valószínűsíthető kockázattal jár a termé-

203 GDPR 4(12.).

204 Európai Adatvédelmi Biztos:, 'Guidelines on Data Breach notifications for the European Union Institutions and Bodies' (angol nyelven) 25. bekezdés: **https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf**

205 Lásd fent (29. bekezdés).

tes személyek jogaira és szabadságaira nézve, az adatkezelő köteles bejelenteni az illetékes felügyeleti hatóságnak. Ha az adatvédelmi incidens valószínűsíthetően **magas kockázattal** jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő az érintettet is köteles tájékoztatni az adatvédelmi incidensről.

Az adatvédelmi incidens bejelentése egyrészt elszámoltathatósági, másrészt arra vonatkozó kötelezettség, hogy adott kockázat azonosítása esetén meg kell tenni a szükséges intézkedéseket.[206] Amellett, hogy elszámoltathatósági követelmény, az adatvédelmi incidens bejelentése az adatkezelőre vonatkozó jogi kötelezettség is, ami az adatkezelési tevékenységektől és az érintettekre jelentett kockázattól függően változik.[207] Az adatvédelmi incidens kockázatának adatvédelmi hatásvizsgálat során történő azonosítása arra kötelezi az adatkezelőket, hogy a kockázat kezelése érdekében hozzanak olyan megfelelő intézkedéseket, melyek enyhítik, megszüntetik vagy megosztják a kockázatot.

Mikor kell bejelenteni az adatvédelmi incidenst a felügyleti hatóságnak?

A GDPR előírja, hogy az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak.[208]

A bejelentésben ismertetni kell legalább:

- az adatvédelmi incidens jellegét (például szándékos vagy véletlen, elveszett vagy tönkrement eszköz stb.);
- az incidensben érintett adatalanyok hozzávetőleges számát (ha ismert);
- az adatvédelmi tisztviselő (kapcsolattartó) nevét és elérhetőségeit;

206 WP29 munkacsoport állásfoglalása a kockázatalapú megközelítésről (angol nyelven): **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf**

207 WP29 munkacsoport állásfoglalása a kockázatalapú megközelítésről (angol nyelven): **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf**

208 GDPR 33(1).

» az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
» az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket.

TIPP

Ha nem áll rendelkezésre minden információ, a bejelentést meg lehet tenni több részletben is.

Az adatvédelmi incidens kezeléséhez az adatkezelőnek először is tudnia kell róla, hogy incidens történt. Ez azt jelenti, hogy az adatkezelőnek rendelkeznie kell olyan belső folyamatokkal, melyek segítségével meg lehet állapítani, hogy adatvédelmi incidens történt. A GDPR nem határozza meg ezen folyamatok gyakorlati elemeit.

Ezzel párhuzamosan a személyes adatokat kezelő vállalkozásnak a zökkenőmentes működés érdekében megfelelő irányítási és szervezeti struktúrával kell rendelkeznie, melyben az egyéni szerepeket és felelősségi köröket belső szabályzatok és stratégiai dokumentumok szabályozzák.

Ezek a dokumentumok összeállíthatóak külső forrásokból származó előírások, iránymutatások és modellek alapján is, de figyelembe kell venni a vállalkozáson belüli kapcsolatrendszert, a vállalkozási kultúrát és értékeket, valamint a szerződéses kapcsolatokat is. Az információbiztonsági incidens kezelési tervének kidolgozása során fokozottan fontos a kockázattudatosság. Az incidenskezelési tervnek tartalmaznia kell a GDPR-ból, és egyéb szabályozási keretrendszerből eredő kötelezettségeket (például a NIS és a PSD 2 irányelv).

TIPP

Az incidenskezelési tervnek már az incidens bekövetkezte előtt rendelkezésre kell állnia, hogy szükség esetén használhassuk.

A GDPR előírja, hogy minden adatvédelmi incidensről, annak hatásáról és az orvoslására tett lépésekről nyilvántartást kell vezetni akkor is, ha a felügyeleti hatóságot vagy az érintetteket nem tájékoztatták róla.

Hogyan tud felkészülni a KKV egy esetleges adatvédelmi incidensre? Milyen dokumentáció segíthet?

Egy esetleges adatvédelmi incidens esetén az alábbi dokumentumok lehetnek a KKV-k segítségére:

1) **szabályzat:** magasabb szintű dokumentum, amely meghatározza az incidenskezelési terv részleteit (célja, szervezeten belüli hatálya, szerepe, hatásköre és az incidens kommunikálásának és bejelentésének módja);
2) **terv**: a szabályzat szervezeten belüli végrehajtására vonatkozó hivatalos dokumentum. A biztonsági sérülés kezelési tervének központi eleme a kommunikációs terv, ami arra vonatkozik, hogy az incidenssel kapcsolatos információkat és fejlemények hogyan kell megosztani a szervezeten belüli és az azon kívüli szereplőkkel. A terv tartalmazza továbbá a hatékonyság mérésére alkalmazott mérőszámokat, azokat a tényezőket, melyek szükségessé teszik a terv módosítását, valamit a terv fejlesztésére és javítására vonatkozó startégiát.
3) **szabványműveleti előírások (SOPs):** a CSIRT (Cyber Security Incident Response Team) listája az incidensek elhárítását célzó technikai intézkedésekről. A szabványműveleti előírások minimalizálják az incidensek kezelésének hibáit, biztosítják a folyamatos és megismételhető incidenskezelési képességet. A szabványműveleti előírások a CSIR Team által használt ellenőrzőlistát is tartalmazzák.[209]

Mikor kell tájékoztatni az érintetteket az incidensről?

Az érintetteket akkor kell tájékoztatni, ha az incidens valószínűsíthetően

209 Kevvie Fowler, Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not (2016) Kindle edition.

magas kockázattal jár a jogaikra és szabadságaikra nézve. Az érintettek értesítésére vonatkozó küszöbérték azért magasabb, hogy ne terheljük őket feleslegesen.[210]

Az adatvédelmi incidens súlyossága az alábbi faktorok alapján állapítható meg:

» Az incidens típusa

A WP29 munkacsoport iránymutatása szerint az incidens által jelentett kockázat mértéke attól függ, hogy az incidens érinti-e a bizalmasság, integritás és rendelkezésre állás elvét.[211] Az iránymutatás nem tér ki arra, hogy az adatvédelmi incidensek oka változatos lehet: pénzügyi motivációból elkövetett számítógépes bűncselekmény, kiberkémkedés (nemzetbiztonság vagy gazdasági érdek) vagy mások anyagi nyereséggel nem járó nyilvános megalázása.[212]

» A személyes adat mennyisége, jellege és különleges kategóriája

A kockázatelemzés nagyban függ attól, hogy az adatvédelmi incidens érintett-e különleges adatokat. Összefüggéseikben kell vizsgálni a különleges adatokat (például az örökbefogadó szülő neve vagy lakcíme különleges adat is lehet) és az érintett adatok számát. Amíg a nagyobb adathalmaz sérülése általában súlyosabb hatással jár, kis számú különleges adat sérülése is járhat súlyos következményekkel az egyénre nézve.[213] Világos, hogy az egészségügyi adatokat, személyazonosító okmányokat és bankkártya-adatokat érintő incidensek kockázattal járnak, de ezen információk kombinációja magasabb kockázatot jelent, mint külön-külön, mert elősegítheti a személyazonosság-lopást is.[214]

210 WP29 munkacsoport WP250 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről: **https://www.naih.hu/files/wp250rev01_hu.pdf**

211 WP29 munkacsoport WP250 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről: **https://www.naih.hu/files/wp250rev01_hu.pdf**

212 Josephine Wolff, You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches (Kindle, MIT Press 2018) Location 2743 of 6938.

213 WP29 munkacsoport WP250 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről: **https://www.naih.hu/files/wp250rev01_hu.pdf**

214 WP29 munkacsoport WP250 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről: **https://www.naih.hu/files/wp250rev01_hu.pdf**

» A természetes személyek azonosítása

Az adatvédelmi incidens által okozott kockázat felmérése során az adatkezelőknek fel kell mérniük, hogy könnyen azonosíthatóak-e az incidensben érintettek. Az adatkezelőnek meg kell győződnie arról, hogy a sérült adatok összeköthetőek-e más adathalmazokkal, és azokat milyen biztonsági intézkedések védik (például álnevesítés, titkosítás).

» Az érintettekre gyakorolt hatás súlyossága

A WP29 munkacsoport véleménye szerint az adatkezelők az incidensben érintett személyes adatok természete alapján (például különleges adat, pénzügyi információ) meg tudják jósolni, hogy az incidens milyen kockázattal jár az érintettekre nézve.

» Az érintett egyéni sajátosságai

Az adatvédelmi incidens érintettekre gyakorolt hatásának vizsgálata során az adatkezelőnek ellenőriznie kell, hogy az incidens sérülékeny csoportok személyes adatait is érintette-e. A sérülékeny adatalanyok lehetnek gyermekek (szándékosan és tudatosan nem képesek megtagadni a hozzájárulást), munkavállalók (alá- fölérendeltségi viszony a munkaadójukkal) és más sérülékeny csoportok (szellemi fogyatékossággal küzdők, menedékkérők, idős korúak, betegek stb.). Még, ha a természetes személyek nem is tartoznak sérülékenynek tartott csoporthoz, az adatkezelővel fennálló alá- fölérendeltségi viszonyuk okozhatja adatvédelmi sérülékenységüket, ha bármilyen hátrány éri őket személyes adataik kezelése vagy ennek elmulasztása miatt.

» Az adatkezelő egyéni sajátosságai

A WP29 munkacsoport szerint az adatkezelő természete, szerepe és adatkezelési tevékenysége is hatással lehet az incidens által jelentett kockázat mértékére. [215]

215 WP29 munkacsoport WP250 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről **https://www.naih.hu/files/wp250rev01_hu.pdf**

PÉLDA

Ha egy magánklinika által kezelt különleges adatokhoz jogosulatlanul férnek hozzá, ezeket a páciensek zsarolására is használhatják.

» Az érintett természetes személyek száma

Az adatkezelőnek fel kell mérnie az incidensben érintett személyes adatok mennyiségét. Általában úgy véljük, hogy a nagyobb számú adatot érintő adatvédelmi incidensek sokkal nagyobb hatással járnak, de ahogyan azt már korábban megállapítottuk, az is járhat súlyos következménnyel, ha az adatvédelmi incidens egyetlen személy különleges adatait érinti.[216]

Az adatvédelmi hatóságok eltérő küszöbértékeket állapítanak meg az adatvédelmi incidensek bejelentési kötelezettségére vonatkozóan.

Az ír adatvédelmi hatóság iránymutatása részletes példákat mutat be az adatvédelmi incidens bejelentési kötelezettségére vonatkozóan.[217]

HASZNOS FORRÁSOK

» DPC: 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (2019) **https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide**
» WP29 munkacsoport WP250 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről **https://www.naih.hu/files/wp250rev01_hu.pdf**
» Európai Adatvédelmi Biztos: 'Guidelines on Data Breach notifications for the European Union Institutions and Bodies': **https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf**

216 Amíg jellemzően a nagymértékű incidensek járnak súlyosabb következményekkel, az az incidens is jelenthet komoly veszélyt, ami csak egy személyt érint.

217 Az ír adatvédelmi biztos iránymutatása (angol nyelven): 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (2019).

Az adatvédelmi hatásvizsgálat és az előzetes konzultáció

Háttér

Az előzetes adatvédelmi hatásvizsgálatot más területeken végzett hatásvizsgálatok (például magánélet-védelmi, környezeti, szabályozási hatásvizsgálat) tapasztalataira támaszkodva vezette be az új adatvédelmi keretszabályozás.

A hatékonyság érdekében a hatásvizsgálatokat a projekt korai, tervezési szakaszában kell lefolytatni (proaktív kezdeményezés) a projekt lehetséges előnyös vagy hátrányos hatásainak azonosítása céljából. A hatásvizsgálatok támogatják a döntéshozókat a fejlesztések és új kezdeményezések legjobb és leghasznosabb megoldásainak azonosításában.[218] Ahhoz, hogy hasznos legyen, a hatásvizsgálatnak rugalmasnak, és a szervezetek méretétől függetlenül alkalmazhatónak kell lennie. **A hatásvizsgálat lefolytatása nem egyszeri feladat, rendszeresen felül kell vizsgálni annak biztosítása érdekében, hogy megfeleljen a projekt aktuális állapotának.**

Fentieknek megfelelően az adatvédelmi hatásvizsgálatot is az adatkezelési tevékenység megkezdése előtt kell lefolytatni, ideális esetben már a tevékenység tervezésének időpontjában. Az adatvédelmi hatásvizsgálat semmilyen esetben sem használható a döntések visszamenőleges igazolására (például drón vásárlása, kamerarendszer beüzemelése). Éppen ellenkezőleg, az előzetes adatvédelmi hatásvizsgálat módszerét azzal a céllal dolgozták ki, hogy az adatkezelők az adatkezelési tevékenységek tervezése során figyelemmel legyenek azok hatásaira, és a leginkább adatbiztonság-barát megközelítést alkalmazzák a természetes személyek jogaira és kötelezettségeire gyakorolt negatív következmények minimalizálása céljából.

---

218 A környezeti hatásvizsgálat például a 60-as években jelent meg az aktivistáknak köszönhetően (lásd: International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice), a szociális hatásvizsgálat pedig a 80-as években.
A szociális hatásvizsgálat célja annak biztosítása, hogy a fejlesztések vagy a tervezett beavatkozások maximalizálják a fejlesztések előnyeit és minimalizálják a költségeket, különösen a közösség által viselt költségekre (további információ: The Interorganizational Committee on Guidelines and Principles for Social Impact Assessment: Guidelines and Principles for Social Impact Assessment: **https://www.iaia.org/pdf/IAIAMemberDocuments/Publications/Guidelines_Principles/SIA%20Guide.PDF**

A többi hatásvizsgálathoz hasonlóan az adatvédelmi hatásvizsgálat is a legjobb erőfeszítést követeli meg. A negatív hatásokat lehetetlen nullára csökkenteni, de a KKV-k kötelesek a legjobb képességük szerint kezelni a kockázatokat a rendelkezésükre álló forrásoknak és a technológia jelenlegi állásának megfelelően.[219] A GDPR-nak való megfelelést mindenképpen biztosítani kell.[220]

Kinek kell adatvédelmi hatásvizsgálatot lefolytatnia?

Az adatvédelmi hatásvizsgálat lefolytatása csak az adatkezelő KKV-k számára, és csak bizonyos adatkezelési tevékenységek esetén kötelező. Az adatfeldolgozó és az adatvédelmi tisztviselő köteles segíteni az adatkezelőt a hatásvizsgálati eljárás lefolytatásában, de utóbbit terheli minden felelősség.

TIPP

Adatkezelési tevékenységük és a rendszereik fejlesztése érdekében az adatfeldolgozó KKV-k is lefolytathatnak adatvédelmi hatásvizsgálatot önkéntes alapon, ezzel biztosítva a szervezeti előírásoknak való megfelelésüket, erősíthetik megbízhatóságukat, valamint kifejezhetik az adatvédelem melletti elköteleződésüket, egyúttal biztosíthatják az adatkezelőket, hogy képesek megfelelő biztonsági szintet garantálni.

Az adatvédelmi hatásvizsgálat egy új technológiai eszköz által okozott hatások felmérésére is alkalmas lehet (például új hardver vagy szoftver kifejlesztése, felhőalapú tárolási szolgáltatás).[221]

219 Dariusz Kloza et al., "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," (2017) d.pia.lab Policy Brief: **https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf**

220 GDPR 35(7)(d).

221 WP29 munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e: **https://naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf**

Az adatkezelő döntése, hogy az adatvédelmi hatásvizsgálatot a „házon belül" elérhető szakértőkre támaszkodva, vagy külső szakértők bevonásával folytatja le.

Mikor kötelező adatvédelmi hatásvizsgálatot lefolytatni?

Nem minden adatkezelési tevékenység esetén szükséges, csak akkor, ha valószínűsíthető, hogy az adatkezelési műveletek magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve. A GDPR nem csak az érintettek, hanem „a természetes személyek jogait és szabadságait" említi, mivel az adatkezelési tevékenység kockázatot jelenthet az adatalanyokon kívüli körben is.

PÉLDA

Önvezető járművek esetén a gyalogos adatait ugyan nem kezeli az autó (nem adatalany), az adatkezelés mégis hatással lehet az egészségére vagy akár az életére is.

Az adatkezelési tevékenységek az alábbi jogokra és szabadságokra lehetnek hatással:

- a GDPR-ban felsorolt érintetti jogok (hozzáférési jog, törléshez, adattovábbításhoz való jog);
- egyéb alapjogok, például:
    - a magán- és családi élet tiszteletben tartása;
    - gondolatszabadság, lelkiismereti és vallásszabadság;
    - véleménynyilvánítási és információszabadság;
    - a vállalkozás szabadsága;
    - hatékony jogorvoslathoz és a tisztességes eljáráshoz való jog;
    - kulturális, vallási és nyelvi sokféleséghez való jog;
    - egyenlő bánásmódhoz való jog;
    - menedékjog;
    - a dokumentumokhoz való hozzáféréshez való jog;

- foglalkozás megválasztásának szabadsága;
- oktatáshoz való jog;
- tulajdonhoz való jog;
- férfiak és nők közti egyenlőség;
- idősek joga stb.[222]

A GDPR biztosít bizonyos fokú mérlegelési jogkört az adatkezelők számára a tervezett adatkezelési tevékenységek által jelentett kockázatok súlyosságának értékelésében[223], de az adatkezelési tevékenységek bizonyos elemei automatikusan valószínűsítik a magas kockázatot.

PÉLDA

Egyes adatkezelési tevékenységek elkerülhetetlenül magas kockázattal járnak:
1) értékelés és pontozás, ideértve a profilalkotást és az előrejelzéseket;
2) jogi vagy hasonlóan jelentős hatással járó automatizált döntéshozatal;
3) szisztematikus megfigyelés;
4) különleges vagy különösen személyes természetű adatok (például pénzügyi, földrajzi helymeghatározási adatok) kezelése;
5) nagymértékű adatkezelés;
6) adathalmazok összekapcsolása;
7) sérülékeny csoportok személyes adatainak (például gyermekek, menedékkérők, idősek, betegek stb.) kezelése;
8) új szervezeti és technológiai eljárások alkalmazása (például mesterséges intelligencia, testen viselt eszközök);
9) az adatkezelés önmagában akadályozza az érintettet jogainak

222 További példákat az alapjogokra az Európai Unió Alapjogi Chartája **https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN**, Az Emberi Jogok Európai Egyezménye: **https://www.echr.coe.int/Documents/Convention_HUN.pdf** és Magyarország Alaptörvénye tartalmaz **https://www.parlament.hu/irom39/02627/02627.pdf**

223 Dariusz Kloza et al., "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," (2017) d.pia.lab Policy Brief 3.

gyakorlásában vagy egy szolgáltatás igénybevételében (például egy lehetséges ügyfelet kizárnak a szolgáltatásból a profilja alapján).

Az adatkezelők az adatvédelmi hatásvizsgálat során a fent felsorolt körülményeket mérlegelve felmérhetik, hogy az adatkezelési tevékenységük magas kockázattal jár-e.[224]

A GDPR három esetet taglal a természetes személyek jogaira és szabadságaira nézve **magas kockázattal** járó adatkezelési tevékenységekkel összefüggésben:

a) a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;

PÉLDA

Köteles adatvédelmi hatásvizsgálatot lefolytatni:
» Egy biztosítótársaság, ha ügyfelei hitelképességének megállapításához vagy a prémiumok megállapításához profilalkotást folytat,
» A pályázók önéletrajzát automatizált rendszer alapján kiválasztó vállalkozás,
» A vállalkozás, ha automatikus munkaerőértékelési-rendszert alkalmaz a bónuszok kiszámítására.

b) személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelésére kerül sor; vagy

224 WP29 munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e: **https://naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf**

PÉLDA

Kötelesek adatvédelmi hatásvizsgálatot lefolytatni:
» A magánklinikák,
» A társkereső applikációt (adatot gyűjt a felhasználók szexuális irányultságáról) üzemeltető vállalkozás,
» A cikluskövető alkalmazást fejlesztő vállalkozás, amely egyéni naptáralapú cikluskövetést tesz lehetővé, és előrejelzéseket, emlékeztetőket és értesítéseket küld.

c) nyilvános helyek nagymértékű, módszeres megfigyelése.

PÉLDA

Köteles adatvédelmi hatásvizsgálatot lefolytatni:
» Egy bevásárlóközpontban vagy állomáson kamerarendszert üzemeltető biztonsági cég,
» Egy szellemi fogyatékosok számára fenntartott otthon, mely olyan nagy felbontású kamerarendszert üzemeltet, amely egy szoftver segítségével képes a bentlakók normálistól eltérő viselkedését azonosítani,
» A vállalkozás, ha a szolgáltatás fejlesztése érdekében ellenőrzi az általa fejlesztett applikáció használatának metaadatait (az applikáció adataira vonatkozó információt vizsgálja),
» A gluténérzékenyek számára applikációt kifejlesztő vállalkozás, ha az applikáció helymeghatározó adatuk alapján megmutatja, hol van a legközelebbi gluténmentes élelmiszert árusító bolt.

Abban az esetben is kötelező adatvédelmi hatásvizsgálatot lefolytatni, ha az adatkezelési tevékenység szerepel a nemzeti adatvédelmi hatóság kötelező hatásvizsgálati listáján.[225] További támpontot jelenthetnek a magatartási kódexek.

225 GDPR 35(4).

TIPP

A kötelező hatásvizsgálati lista megtalálható a NAIH honlapján:
https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

PÉLDÁUL

az alábbi adatkezelési tevékenységek kapcsán indokolt adatvédelmi hatásvizsgálatot lefolytatni:

» Egy ékszerész ujjnyomat- és arcfelismerő eszközt alkalmaz a széfhozzáférés ellenőrzésére,
» Egy biotechnológiai vállalkozás genetikai tesztelési szolgáltatást nyújt ügyfelei számára, amivel előre tudja jelezni az egészségügyi kockázatokat;
» Egy vállalkozás a közösségi médiában megosztott adatok alapján végez profilalkotást ügyfelei és alkalmazottjai tekintetében;
» Egy vállalkozás eHealth applikációt fejleszt;
» Egy biztosítótársaság osztályozza ügyfeleit a szolgáltatásai igénybevételéhez;
» Egy magánnyomozó iroda bűncselekményekre, büntetőítéletekre vonatkozó adatokat kezel.

Mikor nem kell adatvédelmi hatásvizsgálatot lefolytatni?

A GDPR értelmében **nem** kell adatvédelmi hatásvizsgálatot lefolytatni:

» ha a személyes adatok kezelésére jogi kötelezettség teljesítése, közérdek, uniós vagy nemzeti jogszabály alapján kerül sor, és a GDPR követelményeinek megfelelő adatvédelmi hatásvizsgálatot a jogalap alkalmazhatóságának vizsgálata során korábban már lefolytatták (ez csak ritkán fordul elő KKV-k esetén);
» ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik (nem tekinthető nagymértékűnek).

Az adatkezelő akkor is köteles megfelelő intézkedéseket hozni a természetes személyek jogainak és szabadságainak biztosítása érdekében, ha az adatkezelési tevékenység nem indokolja adatvédelmi hatásvizsgálat lefolytatását. A kockázatok valószínűségének és súlyosságának csökkentése érdekében hozott szervezési és technikai intézkedések megjelennek az adatkezelő általános kötelezettségei között, a beépített és alapértelmezett adatvédelem elvében, továbbá az adatbiztonsági előírásokban is. Ezeknek a horizontális előírásoknak meg kell felelni, akár szerepelnek az adatvédelmi hatásvizsgálati listán, akár nem.

Ha kétely merül fel az adatvédelmi hatásvizsgálat szükségességével kapcsolatban, javasolt lefolytatni a vizsgálatot.

Mikor kell felülvizsgálni (újra lefolytatni) az adatvédelmi hatásvizsgálatot?

A kockázatalapú megközelítés alapján az adatkezelők kötelesek folyamatosan értékelni, hogy az adatkezelési tevékenységük valószínűsíthetően kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve.[226] A gyakorlatban ez azt jelenti, hogy az adatvédelmi hatásvizsgálat eredményét rendszeresen felül kell vizsgálni. Az adatvédelmi hatásvizsgálat ismételt lefolytatása nem csak a folyamatos fejlődés szempontjából fontos, hanem az adatbiztonság megfelelő szintjének biztosításában is.

Új adatvédelmi hatásvizsgálat (azaz a korábbi felülvizsgálata) akkor szükséges, ha az adatkezelési tevékenység által jelentett kockázatok változtak (például egy új technológiát vagy szervezési megoldást vezettek be vagy a személyes adatokat új célból kezelik).[227] Az adatkezelési tevékenységek gyorsan fejlődnek, ezért új sérülékenységek merülhetnek fel. Az adatvédelmi incidensek és egyéb biztonsági sérülések felhívhatják a figyelmet az adatkezelési tevékenységből származó kockázatokra és az adatvédelmi hatásvizsgálat felülvizsgálatának szükségességére.

226 WP29 munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e: **https://www.naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf**

227 Lásd fent, 13-14. bekezdés.

Új adatvédelmi hatásvizsgálat lefolytatására akkor is szükség lehet, ha az adatkezelési tevékenység szervezeti vagy társadalmi szerkezetében következett be változás, például az adatkezelő székhelye szerinti tagállamban új szabályozást fogadtak el az adatvédelemre vagy az adatvédelmi hatásvizsgálatra vonatkozóan; az automatizált döntéshozatali eljárás nagyobb hatással jár az érintettekre nézve vagy az adatkezelés miatt diszkrimináció fenyegeti az érintetteket.

A fenti példák mindegyike vezethet a kockázat szintjének megváltozásához, de bizonyos változások – éppen ellenkezőleg – csökkenthetik is az adatkezelési tevékenységgel járó kockázatok mértékét. Például az adatkezelési tevékenység fejlesztése eredményezheti, hogy többé már nincs szükség automatizált döntéshozatalra, vagy a megfigyelési tevékenység már nem szisztematikus. Ebben az esetben a kockázatértékelés juthat arra konklúzióra, hogy nem szükséges adatvédelmi hatásvizsgálatot lefolytatni.

Hogyan folytassuk le az adatvédelmi hatásvizsgálatot?

A GDPR rugalmasságot biztosít az adatkezelőknek az adatvédelmi hatásvizsgálat lefolytatásában. Számos hatásvizsgálati módszer létezik.[228]

A csillaggal jelölt lépéseket nem követeli meg kifejezetten a GDPR, ezek a legjobb gyakorlatokon vagy gyakorlati megfontolásokon alapulnak.

228 A bemutatott módszer Dariusz Kloza, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) „Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals" című könyvén alapul (d.pia.lab Policy Brief 1/2017. VUB: Brussels). A minták Dariusz Kloza, Alessandra Calvi, Simone Casiraghi, Sergi Vazquez Maymir, Nikolaos Ioannidis, Alessia Tanas and Niels van Dijk (2020) „Data protection impact assessment in the European Union: developing a template for a report from the assessment process" című tanulmányából származnak (d.pia.lab Policy Brief No. 1/2020. VUB: Brussels).

1. lépés	*Átvilágítás (a küszöbérték elemzése).*	A) Az érdekelt felek bevonása	B) Dokumentáció	C) Minőség-ellenőrzés
2. lépés*	*Alkalmazási kör meghatározása*			
3. lépés *	*Tervezés és előkészítés*			
4. lépés	*Helyzetleírás*			
5. lépés	*Hatások felmérése*			
6. lépés	*Javaslatok*			
7. lépés	*Előzetes konzultáció az adatvédelmi hatósággal*			
8. lépés	*Felülvizsgálat*			

Az első hat lépést egymás után kell végrehajtani; az utolsó két lépésre csak bizonyos körülmények fennállása esetén kerül sor. Az A, B és C lépéseket pedig folyamatosan kell végrehajtani (az érintettekkel való konzultációnak, a dokumentációnak és a minőség-ellenőrzésnek minden másik lépésben is meg kell jelennie). Az utolsó két lépésre csak bizonyos körülmények fennállása esetén kerül sor.

1. lépés: Átvilágítás (a küszöbérték elemzése)

Ebben a lépésben az adatkezelő az adatvédelmi tisztviselő (ha van) segítségével felvázolja a tervezett adatkezelési tevékenységeket. Ennek alapján megállapítható, hogy szükséges-e adatvédelmi hatásvizsgálatot lefolytatni (például az adatkezelési tevékenységek valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve) vagy sem (mert az adatkezelési tevékenységek valószínűsíthetően nem járnak magas kockázattal a természetes személyek jogaira és szabadságaira nézve, vagy az adatkezelő egyéb okból kifolyólag mentesül). Utóbbi esetben jó gyakorlat, ha a KKV egy nyilatkozatban dokumentálja, miért mellőzi az előzetes adatvédelmi hatásvizsgálat lefolytatását (például, mert az adatkezelés nem jár jelentős hatással a természetes személyek jogaira vagy szabadságaira).

2. lépés: Alkalmazási kör meghatározása*
Ebben a lépésben az adatkezelő meghatározza az alábbiakat:

(a) a referenciaértéket: a személyes adatok védelméhez való jog mely aspektusait (például érintetti jogok gyakorlása, a hozzájárulás feltételei) vagy milyen más alapjogot érinthet a tervezett adatkezelés;

(b) az érintettek körét: az adatalanyok és az ő képviselőik (például civil szervezetek)[229], adatvédelmi tisztviselő[230] és adatfeldolgozó[231], esetleg címzettek, más természetes személyek;

(c) milyen módszerekkel értékeli az adatkezelés hatásait: A GDPR csupán az adatkezelés természetes személyek jogaira és szabadságaira jelentett kockázatainak, valamint az adatkezelés szükségességének és arányosságának felméréséről rendelkezik. Például a különböző kockázatcsökkentő intézkedések hatása az adatkezelési tevékenység által jelentett kockázatra vagy költség-haszon elemzés (az adatkezelő rendelkezésére álló pénzügyi forrásoknak megfelelő kockázatcsökkentő intézkedések kiválasztása).;

(d) az alkalmazható egyéb kockázatelemzési technikák: Például, ha a vállalkozás tevékenysége hatással van a környezetre is, az adatvédelmi hatásvizsgálattal párhuzamosan egy környezeti hatásvizsgálat lefolytatására is kötelezheti jogszabály. Hasonlóan, ha a tevékenység hatással lehet természetes személyek egészségére, egészségügyi vagy etikai hatásvizsgálat szükségesége is felmerülhet.

3. lépés: Tervezés és előkészítés*
Az adatkezelő meghatározza:

(a) a hatásvizsgálati eljárás célját;

(b) a kockázat meghatározásának kritériumait és az adatkezelési tevékenység szükségességét és arányosságát igazoló kritériumokat;

229 GDPR 35(9).
230 GDPR 39(c).
231 GDPR 28(f).

(c) a hatásvizsgálat lefolytatásához szükséges forrásokat: idő, pénz, munkaerő, tudás, hely és infrastruktúra;

(d) a hatásvizsgálat eljárási- és időkeretét, a hatásvizsgálati eljárás szereplőinek (kölcsönös) feladatait, a mérföldkövek időzítését;

(e) a hatásvizsgálatot végzők kiválasztásának kritériumait, a szerepüket és felelősségi körüket;

(f) azokat a részletes szabályokat, melyek bármilyen zavar (a kockázatértékelésben részt vevők összetételének változása vagy természeti katasztrófák) ellenére garantálják a hatásvizsgálati eljárás folyamatosságát;

(g) azokat a körülményeket, melyek szükségessé teszik a folyamat felülvizsgálatát. A kockázat szintjének változása[232] mellett más körülmények is felmerülhetnek.

4. lépés: Leírás

Ebben a szakaszban a tervezett adatkezelési tevékenységek leírását ki kell bővíteni a technikai részletekkel. Tisztázni kell az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint meg kell határozni az adatkezelő jogos érdekét.[233]

5. lépés: A hatások felmérése

Ebben szakaszban a tervezett adatkezelési tevékenységek szükségességét és arányosságát, valamint a természetes személyek jogaira és szabadságaira gyakorolt hatását kell értékelni. A szükségességi és arányossági teszt során értékelni kell az adatkezelési tevékenységek adatvédelmi alapelveknek (jogszerűség, tisztességes eljárás és átláthatóság, célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, integritás és bizalmas jelleg, és elszámoltathatóság) való megfelelését.

A kockázatelemzési folyamat jellemzően az alábbi lépésekből áll:

- A kockázat azonosítása (felismerése és leírása),
- A kockázat jellegéből adódó kockázati szint értékelése (például a következmények súlyossága hatással van-e a valószínűségükre),

232 GDPR 35(11).

233 GDPR 35(7)a).

» A kockázat kiértékelése (például a kockázat meghatározásának kritériumait (lásd 3. lépés b pont) összevetjük kockázatelemzés eredményével annak megállapítása érdekében, hogy a kockázat mértéke kezelhető-e vagy további intézkedéseket kell hoznunk a csökkentésére.

6. lépés: Javaslatok

Ebben a szakaszban határozzuk meg a korábban azonosított kockázat csökkentésére és az adatvédelmi szabályozásnak való megfelelés biztosítására tett lépéseket. Az adatkezelő azonosítja azokat az intézkedéseket, melyeket az adatvédelmi alapelveknek való megfelelés érdekében kell hoznia (például az adattakarékosság elve értelmében nem gyűjt bizonyos adatokat; csökkenti az adattárolási időt). A kockázat csökkenthető egyrészt a valószínűség (a kockázatnak való kitettség csökkentése), a súlyosság vagy mindkettő egyidejű mérséklésével.

A kockázatok elkerülhetőek, csökkenthetőek, áthelyezhetőek (másik szervezethez, például kiszervezés útján) vagy elfogadhatóak (de csak az első esetben kerülhetjük el az alapjogok sérülését). Ha a fennmaradó kockázatot nem tudjuk enyhíteni, előzetes konzultációra van szükség a felügyeleti hatósággal (lásd 7. lépés). A kockázat enyhítésére tett lépések lehetnek szervezeti vagy technikai intézkedések, ideértve az adatvédelmi folyamatok és szabályzatok kialakítását, az adatkezelési tevékenységben részt vevők szerepének és felelősségi körének meghatározását, hozzáférés-ellenőrzési szabályzat kialakítását, incidenskezelési-terv és üzletfolytonossági terv kidolgozását, valamint az adathozzáférés ellenőrzését és az adatok törlését biztosító eszközök alkalmazását.[234]

TIPP

A legjobb gyakorlatok szerint a megfelelőség igazolására javasolt nyilvántartást vezetni az azonosított kockázatokról, értékelésükről

234 European Union Agency For Network and Information Security, Handbook on Security of Personal Data Processing (December 2017) Annex A: **https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing**

és az enyhítésükre tett intézkedésekről. Előzetes konzultáció esetén ezt a nyilvántartást meg lehet küldeni a felügyeleti hatóságnak.

7. lépés: Előzetes konzultáció a felügyeleti hatósággal

Ha az adatkezelési tevékenységek által jelentett kockázat a mérséklésére tett intézkedések ellenére is fennáll, de az adatkezelő mégis folytatni kívánja a személyes adatok kezelését, javasolt előzetes konzultációt kérni az adatvédelmi hatóságtól. Az előzetes konzultáció eredményeképpen az adatvédelmi hatóság jogilag nem kötelező erejű írásos javaslatot bocsát ki. Mindazonáltal a GDPR kilátásba helyezi, hogy a felügyeleti hatóság gyakorolhatja hatósági jogkörét is (például vizsgálatot indít vagy figyelmeztet).

TIPP

A felügyeleti hatóságok honlapján általában elérhetőek az előzetes konzultációs formanyomtatványok.

8. lépés: Felülvizsgálat

Kötelező ismételten lefolytatni az adatvédelmi hatásvizsgálatot, ha változik az adatkezelési tevékenységgel járó kockázat mértéke.

***A* lépés: Az érdekelt felek bevonása**

A döntéshozatali folyamat teljessége érdekében az érdekelt feleket minden hatásvizsgálati folyamatba be kell vonni. Az adatkezelő köteles megismerni az adatvédelmi tisztviselő, az adatfeldolgozók, és ha *szükséges,* az érintettek és képviselőik véleményét. Ebben az esetben a *szükségesség* nem opcionális: csak akkor lehet kivételt tenni, ha a velük történő konzultáció aránytalanul nagy erőfeszítést kívánna vagy nem lenne hozzáadott értéke. Mindazonáltal további érintetteket is lehet találni (példá-

ul IT szakember). Az érdekelt felek véleményét ki kell kérni, és mérlegelni kell a javaslatukat, de a végleges döntést az adatkezelő hozza meg.

***B* lépés: Dokumentáció**

A hatásvizsgálati folyamatról vezetett áttekinthető, írásos vagy más tartós formátumban vezetett dokumentáció a legmegfelelőbb módszer a jogszabályoknak való megfelelés bizonyítására. Alkalmazható legjobb gyakorlat, ha az érintettek (például adatvédelmi tisztviselő) javaslatairól és azok követéséről vagy elutasításáról is nyilvántartást vezetünk.

***C* lépés: Minőség-ellenőrzés**

Az adatvédelmi tisztviselő feladata az adatvédelmi hatásvizsgálat ellenőrzése.[235]

TIPP

A hatásvizsgálati eljárás szabályainak való megfelelés érdekében a KKV ezen túl folyamatellenőrzési-eszközöket is alkalmazhat.

HASZNOS FORRÁSOK

- European Union Agency For Network and Information Security, 'Handbook on Security of Personal Data Processing' **https://www.enisa.europa.eu/publications/handbook-onsecurity-of-personal-data-processing ISO 31000:2018**
- Risk management — Guidelines **https://www.iso.org/standard/65694.html**

NAIH hatásvizsgálati lista: **https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf**

Sablonok adatvédelmi hatásvizsgálat lefolytatásához:

- A francia felügyeleti hatóság honlapján: **https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf**

235 GDPR 39(c).

» A spanyol felügyeleti hatóság honlapján: **https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepdpublica-un-modelo-de-informe-para-ayudar-las-empresas**

» A brit felügyeleti hatóság honlapján: **https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-d-dpia-template/?q=media**

» Dariusz Kloza, Alessandra Calvi, Simone Casiraghi, Sergi Vazquez Maymir, Nikolaos Ioannidis and Niels van Dijk (2020) Data protection impact assessment in the European Union: developing a template for a report from the assessment process. d.pia.lab Policy Brief No. 1/2020. VUB: Brussels (draft)

Adatvédelmi hatásvizsgálati szoftver

» NAIH – **https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html**

» CNIL – **https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil**

A magatartási kódexek

Háttér

A tagállamok, a felügyeleti hatóságok, az EDPB és az Európai Bizottság a GDPR megfelelő alkalmazásának érdekében bátorítja az adott szektor jellegzetességeinek és tipikus adatkezelési tevékenységének megfelelő magatartási kódexek kidolgozását. A magatartási kódexek tartalmazzák az adott szektorra jellemző adatkezelési tevékenységek legjobb gyakorlatait, így javítani tudják az adatkezelők és adatfeldolgozók adatkezelési tevékenységének színvonalát.

A magatartási kódexek önkéntesen alkalmazható szabályokat tartalmaznak, melyeket egy adott szektorba tartozó szervezetek vagy adatkezelők/adatfeldolgozók adott kategóriái állítanak össze (például szövetkezetek, kereskedelmi kamarák). A magatartási kódexnek való megfelelést az illetékes felügyeleti hatóság által akkreditált testületnek kell ellenőriznie,

amely megfelelő tapasztalattal rendelkezik a kódex szabályozási területén.[236]

Az Európai Szerencsejáték és Fogadási Szövetség (EGBA) az elsők között hozta nyilvánosságra adatvédelmi magatartási kódexét, amely elfogadását követően a GDPR-nak való megfelelést biztosító szektorspecifikus szabályokat és legjobb gyakorlatokat tartalmaz a szerencsejáték szektorra vonatkozóan.[237] Az EGBA az összeállított magatartási kódexet megküldte a máltai felügyeleti hatóságnak jóváhagyásra. Akár két évet is igénybe vehet, mire a többi uniós adatvédelmi hatóság és az Európai Adatvédelmi Testület átnézi és elfogadja a magatartási kódexet.

A magatartási kódexeknek meg kell haladniuk a GDPR alapelveit.

Az adott szektor vagy adatkezelési tevékenység vonatkozásában kell meghatározniuk és elősegíteniük az adatvédelmi szabályozás gyakorlati alkalmazását.[238] A gyakorlatban ez azt jelenti, hogy a felügyeleti hatóság (az adott tagállam a területén alkalmazandó), az EDPB (több tagállamban alkalmazandó) és az Európai Bizottság (harmadik országokba történő adattovábbításokra alkalmazandó) által elfogadott magatartási kódexeknek a GDPR alábbi rendelkezéseinek alkalmazását kell meghatároznia:

- tisztességes és átlátható adatkezelés;
- az adatkezelők jogos érdekei meghatározott körülmények között;
- adatgyűjtés;
- személyes adat álnevesítése;
- a nyilvánosság és az érintettek tájékoztatása;
- az érintettek jogainak gyakorlása;
- a gyermekek tájékoztatása és védelme, valamint a szülői felügyelet gyakorlójától származó hozzájárulás kikérésének módja;
- a 24. és a 25. cikkben említett intézkedések és eljárások, valamint a 32. cikkben említett, az adatkezelés biztonságát szolgáló intézkedések;

236 Ezekről a testületekről az EDPB honlapján található bővebb információ angol nyelven.

237 EGBA Demonstrates Commitment To GDPR With Sectoral Code Of Conduct For Data Protection **https://www.egba.eu/news-post/egba-demonstrates-commitment-to-gdpr-with-sectoral-code-of-conduct-for-data-protection/**

238 DPC 'Codes of conduct' **https://www.dataprotection.ie/en/organisations/codes-conduct**

» a felügyeleti hatóságok értesítése, valamint az érintettek tájékoztatása az adatvédelmi incidensekről;
» a személyes adatok harmadik országok vagy nemzetközi szervezetek részére történő továbbítása; vagy
» az adatkezelő és az érintettek között az adatkezeléssel kapcsolatban felmerülő vitás ügyek megoldására irányuló, nem bírósági útra tartozó eljárások és egyéb vitarendezési eljárások, az érintettek 77. és 79. cikk szerinti jogainak sérelme nélkül.

Milyen előnyökkel jár a magatartási kódex alkalmazása?

A magatartási kódexhez való csatlakozás hasznos lehet a KKV-k számára, mert megkönnyíti a GDPR előírásainak való megfelelést, és költséghatékony módja a meg nem felelés, és ezáltal a bírságok kockázatának csökkentésének.

Hogyan válasszuk ki a megfelelő magatartási kódexet?

A magatartási kódex kiválasztása során a KKV-nak nagy körültekintéssel kell eljárnia, különösen annak értékelése során, hogy kódex megfelel-e a KKV adatkezelési tevékenységeinek.

TIPP

Továbbá, a KKV-nak ellenőriznie kell, hogy a magatartási kódexet jóváhagyta-e a felügyeleti hatóság vagy adott esetben az EDPB vagy az Európai Bizottság. A nemzeti magatartási kódexek megjelennek az adatvédelmi hatóság által jóváhagyott magatartási kódexek nyilvántartásában a felügyeleti hatóságok honlapján, az EDPB vagy a Bizottság honlapján.

HASZNOS FORRÁSOK

» Európai Adatvédelmi Testület 1/2019. számú iránymutatása az (EU) 2016/679 rendelet szerinti magatartási kódexekről és ellenőrző szervezetekről https://www.naih.hu/files/edpb_guidelines_201901_v2.0_codesofconduct_hu.pdf

A tanúsítás

Háttér

A tagállamok, a felügyeleti hatóságok, az Európai Adatvédelmi Testület, valamint az Európai Bizottság – különösen uniós szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek a Rendelet előírásainak.

A tanúsítás GDPR-kompatibilitásának értékelése során az alábbiakat kell megvizsgálni:

1. A tanúsítás adatkezelési tevékenységekre vonatkozik-e?

Az adatkezelési tevékenység felmérése során meg kell vizsgálni a személyes adatokat (a GDPR tárgyi hatálya); a technikai rendszereket (infrastruktúra, úgymint az adatkezelés során használt hardverek és szoftverek); és az adatkezelési tevékenységekhez kapcsolódó folyamatokat.

2. A tanúsítás tágabb értelemben vonatkozik személyes adatokra és adatvédelemre?

3. A tanúsítás önkéntes-e?

4. A harmadik fél megfelelőségének vizsgálata. Tanúsítást csak az illetékes a felügyeleti hatóság által megnevezett nemzeti akkreditáló testület vagy a nemzeti adatvédelmi hatóság vagy az

EDPB bocsáthat ki. Ez azt jelenti, hogy a GDPR 42. cikke nem vonatkozik az öntanúsítási mechanizmusokra.[239]

Milyen előnyökkel jár a tanúsítás a KKV-k számára?

Az adatkezelő és adatfeldolgozó KKV-k számára is hasznos a tanúsítás.

Először is, a tanúsítás növeli az érintettek és az ügyfelek bizalmát a vállalkozás és az ügyfelek, valamint a vállalkozások közti kapcsolatokban is, mert átláthatóbbá teszi a személyes adatok kezelését.[240]

Másrészt a tanúsítások motiválják az adatvédelem-tudatos technológiák kidolgozását és alkalmazását.[241] A fentiek alapján megállapítható, hogy a tanúsítások alkalmazása versenyelőnyhöz juttathatja a KKV-kat.[242]

Továbbá, az EU-n kívüli adattovábbítások esetében a tanúsítás garantálhatja a megfelelő biztonságot a GDPR hatálya alá nem tartozó adatkezelő és adatfeldolgozó számára is, így a tanúsítás szolgálhat az adattovábbítás jogalapjaként is.[243]

A tanúsítások önmagukban nem bizonyítják a GDPR-nak való megfelelést, de lehetővé teszik az adatkezelők és adatfeldolgozók számára a megfelelő technikai és szervezési intézkedések végrehajtásának, valamint a megfelelő garanciák biztosításának igazolását az adatkezelők / adatfeldolgozók, és az adatfeldolgozók /alvállalkozók között.[244]

239 Lásd fent.

240 Európai Bizottság adatvédelmi tanúsítási mechanizmusokról szóló tanulmánya (angol nyelven): Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report – Study: **https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en**

241 Termékek és szolgáltatások nem szerezhetnek GDPR megfelelőségi tanúsítást, de az adatkezelési tevékenység értékelése során ezeket is meg kell vizsgálni. **https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/**

242 Lásd fent.

243 Lásd fent.

244 Az Európai Adatvédelmi Testület 1/2018. számú iránymutatása a rendelet 42. és 43 cikkével összhangban történő tanúsításról és a tanúsítási szempontok meghatározásáról: **https://www.naih.hu/files/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_hu.pdf**

Hogyan válasszuk ki a megfelelő tanúsítási mechanizmust?

A kézikönyv szerkesztésének időpontjában még nem érhető el uniós adatvédelmi bélyegző vagy a GDPR szerinti jóváhagyott nemzeti tanúsítási mechanizmus. Léteznek nemzeti és nemzetközi tanúsítási rendszerek, de nem tekinthetők GDPR szerinti tanúsításnak, mert habár adatvédelmi témájú tanúsításokról van szó, nem igazították őket a GDPR követelményeihez.[245]

Az elérhető nemzeti és nemzetközi tanúsítások különböznek. Némelyek teljes egészükben az adatvédelemre, mások csak részben, egyes tanúsítások pedig az adatvédelem egy kifejezett területére (kiberbiztonság) vonatkoznak. A tanúsítások lehetnek multiszektorálisak (nem tesznek különbséget az egyes üzleti tevékenységek között) vagy egy szektorra vonatkozóak (kifejezett üzleti tevékenységre vonatkoznak, mint például a felhőalapú számítástechnika). A több szektorra vonatkozó tanúsítások között is számos modell található, amely megfelelő a KKV-k számára: néhány a vállalkozás méretének megfelelő árat állapít meg, mások minden vállalkozás számára ingyenesen vagy kedvezményes áron biztosítják a tanúsítást.[246]

Ha elfogadott nemzeti vagy uniós tanúsítási mechanizmust alkalmazunk, meg kell különböztetnünk átfogó (a teljes GDPR szabályozásra vonatkozó) és egyetlen kérdéskörre fókuszáló (a GDPR egy kifejezett témakörére, például a beépített adatvédelemre vagy a gyermekek hozzájárulására vonatkozó) mechanizmusokat.[247]

A KKV-k számára könnyebb és költséghatékonyabb megoldás az átfogó megközelítésű tanúsítási mechanizmus alkalmazása. Figyeljünk arra, hogy minden tanúsítás korlátozott időre szól. A tanúsításokat felül kell vizsgálni, ha módosítják azokat a jogszabályokat, amelyekre a tanúsítás hivatkozik vagy a nemzeti előírásokra és rendelkezésekre vonatkozó íté-

245 Lásd fent.

246 Európai Bizottság adatvédelmi tanúsítási mechanizmusokról szóló tanulmánya (angol nyelven): Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report – Study: **https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en**

247 Lásd fent.

letet bocsátanak ki vagy fejlődik a technika jelenlegi állása.[248] A GDPR maximum 3 évben határozza meg a GDPR-hoz kapcsolódó mechanizmusok érvényességét.

HASZNOS FORRÁSOK

» Az Európai Adatvédelmi Testület 1/2018. számú iránymutatása a rendelet 42. és 43 cikkével összhangban történő tanúsításról és a tanúsítási szempontok meghatározásáról **https://www.naih.hu/files/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_hu.pdf**

» Az elérhető tanúsítások listáját az Európai Bizottság adatvédelmi tanúsítási mechanizmusokról szóló tanulmánya sorolja fel: Data protection certification mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report – Study **https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en**
https://ec.europa.eu/info/sites/info/files/certification_study_annexes_publish_0.pdf

248 Az Európai Adatvédelmi Testület 1/2018. számú iránymutatása a rendelet 42. és 43 cikkével összhangban történő tanúsításról és a tanúsítási szempontok meghatározásáról: **https://www.naih.hu/files/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_hu.pdf**

5. Sajátos adatkezelési tevékenységek

5.1. KKV-k és a munkavállalók adatai

Adatvédelmi szempontból a munkakapcsolatokban a munkaadó általában az adatkezelő, a munkavállaló pedig az adatalany szerepét tölti be.

A foglalkoztatás során számos, a munkavállalók személyes adatainak kezelésével járó tevékenységet végzünk rutinszerűen, ezek némelyike a GDPR 9. cikkében felsorolt különleges adatok kezelését is magában foglalja (például szakszervezeti tagság, egészségügyi adatok).

PÉLDÁK MUNKAHELYI ADATKEZELÉSRE

Jelentkezési lapok és ajánlások kezelése, bérszámfejtés, adó- és társadalombiztosítási információk megosztása az illetékes hatósággal, táppénz, szabadságok nyilvántartása, fizetés nélküli/egyéb szabadságok nyilvántartása, éves teljesítményértékelés, előléptetések nyilvántartása, képzések, fegyelmi ügyek, munkahelyi balesetek nyilvántartása vagy az e-mailek és telefonhívások biztonsági okból történő ellenőrzése és rögzítése stb.[249]

A GDPR biztosít némi rugalmasságot a munkahelyi adatkezelés szabályozásában. A tagállamoknak lehetőségük van egyedi szabályokat elfogadni – ideértve a kollektív és munkaszerződéseket – például a munkavállaló

249 WP29 munkacsoport 2/2017. számú véleménye a munkahelyi adatkezelésről: **https://www.naih.hu/files/wp249_hu_munkahelyi_adatkezelesek.pdf**

hozzájárulására, a toborzás céljaira vagy a munkaszerződés teljesítésére vonatkozóan.[250]

TIPP

Célszerű, ha a KKV-k a GDPR-t nemzeti jogba átültető jogszabályra vagy a nemzeti adatvédelmi hatóság által kiadott iránymutatásra hivatkoznak.

A munkahelyi adatkezelés lehetséges jogalapjai

A munkavállalók adatainak kezeléséhez a KKV-knak megfelelő jogalappal kell rendelkezniük. A munkahelyi adatkezelések esetén általában megkérdőjelezhető a hozzájárulás érvényessége az alá-fölérendelt viszonyrendszer miatt A GDPR szerint a hozzájárulás érvényességének feltétele, hogy az önkéntes legyen, de a követelmény teljesülését befolyásolhatja a munkáltató és a munkavállalók közti gazdasági egyensúlytalanság.[251] A hozzájárulást azokban az esetekben lehet alkalmazni, ha az a munkavállaló valóban szabad akaratán alapul, és bármikor visszavonhatja anélkül, hogy emiatt bármilyen hátrány érné.[252]

A leginkább megfelelő jogalap lehet:

» szerződés teljesítése, melyben a munkavállaló a szerződő fél;

PÉLDA

A munkaszerződésben foglalt kötelezettségek teljesítése, például a munkavállaló bérének kifizetése.[253]

250 GDPR 88. cikk és (155) Preambulumbekezdés.

251 FRA/ECtHR/EDPS Európai adatvédelmi jogi kézikönyv 2018. évi kiadás (magyar nyelven): **https://www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf**

252 WP29 munkacsoport 2/2017. számú véleménye a munkahelyi adatkezelésről: **https://www.naih.hu/files/wp249_hu_munkahelyi_adatkezelesek.pdf**

253 WP29 munkacsoport 2/2017. számú véleménye a munkahelyi adatkezelésről: **https://www.naih.hu/files/wp249_hu_munkahelyi_adatkezelesek.pdf**

» az adatkezelőre vonatkozó jogi kötelezettség teljesítése;

PÉLDA

A munkáltató a munkavállaló személyes adatait társadalombiztosítás, segély vagy adózási célokból továbbítja.

A munkáltató jogi kötelezettsége a (leendő) munkavállaló erkölcsi bizonyítványának vagy megfelelő végzettségének ellenőrzése.

» a munkáltató jogos érdeke, kivéve, ha elsőbbséget élveznek az érintett érdekei vagy alapvető jogai és szabadságai.

PÉLDA

Egy munkaerőtoborzó nyilvánosan elérhető adatbázisban keres (például LinkedIn), és kapcsolatba lép valakivel, hogy állásinterjúra hívja.

Egy ingatlanügynök kapcsolatba lép az ügyféllel, és időpontegyeztetés céljából megadja az egyik alkalmazottja elérhetőségét.

Meddig terjedhet a munkavállalók megfigyelése?

A modern technológia lehetővé teszi a munkavállalók különböző eszközökkel (okostelefonok, számítógépek, tabletek, járművek és testen hordozható eszközök) történő megfigyelését.[254]

A megfigyelési tevékenységekre sor kerülhet a kiválasztási folyamatban (a munkáltató utánanéz a jelentkező személyes adatainak a közösségi médiában), a szerződéses jogviszony során (kamerás megfigyelés vagy GPS-t helyeznek el a munkavállalók által használt járművekben) és a munkaviszony megszűnése után is (a munkáltató ellenőrzi a korábbi al-

254 Lásd fent.

kalmazottainak LinkedIn profilját, hogy ellenőrizze, nem sérti-e meg a versenytilalmi kikötéseket).[255]

Egyes esetekben a munkáltató jogi kötelezettsége, hogy bizonyos módon megfigyelje az alkalmazottait (például nyomonkövetési technológiákat alkalmaz a járművekben, hogy ellenőrizhesse, az alkalmazottak nem lépik-e túl a jogszabályban meghatározott napi vezetési idejüket).

Más esetekben a munkáltató jogos érdeke a munkavállalók megfigyelése (például biztonsági megfontolásból, a munkavállalók jogellenes magatartásának bizonyítása céljából), de ez a tevékenység kockázatos lehet alapjogi szempontból. A munkavállalók szisztematikus vagy alkalmi megfigyelése nem csak sértheti a munkavállalók magánélethez való jogát, de korlátozhatja őket abban is, hogy tájékoztassák a munkaadót feletteseik és/vagy kollégáik esetleges szabálytalanságairól és jogtalan tevékenységeiről, ezzel kárt okozva az üzleti érdekeknek vagy a munkahelynek.[256]

PÉLDA

A munkáltató GPS eszközt helyez el a céges autókban a munkavállalók munkájának és munkakörülményeinek ellenőrzése céljából. Ebben az esetben az adatkezelés jogalapja lehet a munkáltató jogos érdeke. Még akkor is, ha a munkáltatónak jogos érdeke fűződik a nyomkövető rendszer alkalmazásához, elsőként azt kell megvizsgálnia, hogy az adatkezelésre mindenképpen szükség van-e az általa megjelölt célok eléréséhez, és hogy a tényleges megvalósítás, azaz a GPS berendezés használata általi jogkorlátozás arányos-e ezzel.
A munkáltató köteles egyértelműen tájékoztatni a munkavállalókat a nyomkövető berendezés beszereléséről az általuk vezetett vállalati járműbe, és arról, hogy amíg az adott járművet használják, addig mozgásuk rögzítésre kerül. Más a helyzet, ha a munkavállalók a céges autót magáncélokra is használhatják, ebben az esetben a munkáltató – a magáncélú használat ideje alatt – nem hivatkozhat a jogos érdekére, mert a GPS eszköz alkalmazása aránytalan lenne.

255 Lásd fent.

256 Lásd fent.

TIPP

Bár a munkavállalók megfigyelésének lehetőségére vonatkozó nemzeti szabályozások különböznek, fellelhetők közös vonások:

» A jogszerű megfigyelésre vonatkozó szabályzatok és szabályozások legyenek egyértelműek, könnyen hozzáférhetőek, és ideális esetben a munkáltató a munkavállalók képviselőivel közösen dolgozza ki ezeket.

» Részesítsék előnyben a magánélet-barát megoldásokat a munkavállalók megfigyelésével szemben.

Például célszerűbb, ha a munkáltató korlátozza a munkahelyről elérhető honlapok hozzáférését, mint ha megfigyelné a munkavállalók minden online tevékenységét.

6. Nemzeti adatvédelmi jogszabályok

2018. május 25-én az Általános Adatvédelmi Rendelet a 95/46/EC adatvédelmi irányelv helyébe lépett. A GDPR közvetlenül alkalmazandó az EU/EGT területén, és összehangolta a nemzeti adatvédelmi szabályozásokat, de néhány különbség mégis van a nemzeti szabályozások között. Ezért az adatvédelmi szabályok alkalmazása során tekintettel kell lenni a GDPR-t végrehajtó nemzeti jogszabályokra is.[257]

2018. május 25-től az Európai Unió tagállamaiban kötelező alkalmazni a 2016-ban elfogadott uniós adatvédelmi norma, az általános adatvédelmi rendelet – a GDPR – szabályait. 2018-ban megtörtént az adatvédelmi csomag részét képező másik jogi aktus, a bűnügyi adatvédelmi irányelv magyar jogba való átültetése is, és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 2018-as novellája megteremtette a felügyeleti hatóság működésének, eljárásának és jogértelmezésének megfelelő jogi alapjait. További információkat a NAIH honlapján[258] talál.

257 A VUB-LSTS által összeállított lista az alábbi linken megtalálható: **https://lsts.research.vub.be/en/specifying-the-gdpr/**

258 **https://naih.hu/**

7. Biográfia

Lina Jasmontaitė-Zaniewicz a brüsszeli Vrije Egyetem (VUB) doktorjelöltje. PHD kutatásának témája a GDPR adatvédelmi incidens bejelentésére vonatkozó rendelkezéseinek és a hálózati és információs rendszerek biztonságáról szóló irányelv (IS irányelv) kölcsönhatásának vizsgálata. IAPP tanúsítással rendelkező információbiztonsági szakember (CIPP/E, IAPP). Európai projektekben is közreműködött a személyes adatok kezelésének etikai megfontolásai kapcsán. Jog és technológia szakjogászi képesítését a Tilburg Universityn szerezte meg (cum laude), ezt követően az Európai Adatvédelmi Biztos Hivatalánál folytatta szakmai gyakorlatát. 2013-ban jogi gyakornokként dolgozott egy brüsszeli székhelyű adatvédelmi és adatbiztonsági irodánál. 2014 és 2016 között jogi kutató a Leuven Universityn (CiTiP).

Alessandra Calvi a brüsszeli Vrije Egyetem (VUB) doktorjelöltje. Európai és uniós jogi, valamint adatvédelmi szakjogász (Summa cum laude) végzettségét a VUB Institute of European Studies-nál szerezte. 2015-ben a milánói Università Cattolica del Sacro Cuore-ban szerezte meg jogi képesítését, 2016-2017 között a paviai törvényszék munkajogi osztályán dolgozott. Szakmai gyakorlatát az Európai Adatvédelmi Biztos Hivatalánál és egy büntetőjogi irodánál töltötte. Kutatási területe a jog és a technológia kapcsolata, különös tekintettel az adatvédelem és a körkörös gazdaság kapcsolatára.

Nagy Renáta 2018 óta a Nemzeti Adatvédelmi és Információszabadság Hatóság munkatársa. A STAR II projekt adminisztratív irányításáért felelős, emellett aktív szerepet vállalt a 2019. március 15. – 2020. március 15. között üzemeltetett KKV-hotline működésében és a beérkező kérdések megválaszolásában. A NAIH által szervezett konferenciákon tartott előadásokat a KKV-k számára a GDPR alkalmazásáról.