Adatvédelmi Szabályzat

EX-ON Mérnökiroda Kft.

2018.

1. BEVEZETŐ RENDELKEZÉSEK

A szabályzat célja, hogy összefoglalja az EX-ON Mérnökiroda Kft. (székhelye: 1183 Budapest, Örs utca 3., cégjegyzékszáma: 01-09-875445, statisztikai számjele: 13829632-7112-113-01, adószáma: 13829632-2-43, képviseli: Zsarnovszki Attila ügyvezető, a továbbiakban: Vállalkozás) által a Vállalkozás működése és szolgáltatásának nyújtása során gyűjtött, rendelkezésre bocsátott vagy egyéb módon tudomására jutott személyes adatok kezelésével kapcsolatos teendőket. Továbbá a szabályzat célja annak biztosítása, hogy a Vállalkozás valamennyi adatkezelése során a kötelezően alkalmazandó európai uniós jogi aktusokban foglaltaknak, a hatályos magyar jogszabályok rendelkezéseinek, valamint az adatvédelem terén kialakult bírósági gyakorlatnak megfelelően járjon el.

2. ÁLTALÁNOS RENDELKEZÉSEK

2.1. A szabályozás hatálya

A szabályzat tárgyi hatálya kiterjed a Vállalkozás tulajdonában lévő vagy általa üzemeltetett összes informatikai rendszerében, eszközén és azok környezetén (a továbbiakban együtt: informatikai rendszer) végzett valamennyi adatkezelési tevékenységre, melyek tekintetében további részletes szabályokat állapít meg a Vállalkozás Informatikai Biztonsági Szabályzata.

Az utasítás tárgyi hatálya kiterjed továbbá a nem informatikai rendszerekben végzett (manuális, papíralapú) adatkezelési tevékenységekre is. Jelen szabályzat személyi hatálya kiterjed a Vállalkozás minden munkavállalójára és tisztségviselőjére.

A szabályozás hatálya kiterjed a Vállalkozás számára adatfeldolgozási tevékenységet végző személyekre, partnerekre, és a Vállalkozás adatkezelési tevékenységéhez eszközöket, számítástechnikai programokat szállító más személyekre is. A szabályzat elvárásait a felsoroltakkal kötött szerződésekben kell érvényre juttatni.

2.2. Alapelvek

A Vállalkozás a személyes adatok kezelésével járó tevékenysége során érvényre juttatja az európai uniós Általános Adatvédelmi Rendeletben (2016/679/EU, General Data Protection Regulation, a továbbiakban: GDPR) foglalt alapelveket, így különösen:

Jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;

Célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat a Vállalkozás nem kezeli ezekkel a célokkal össze nem egyeztethető módon;

Adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;

Pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;

Korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;

Integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;

Beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;

Alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedések végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége, kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé arra illetéktelen személyek számára.

Az alapelvek érvényesítésére munkavégzésük során a Vállalkozás minden munkavállalója és tisztségviselője kötelesek.

3. ÉRTELMEZŐ RENDELKEZÉSEK

3.1. Fogalommeghatározások

Adat: az adatfajta értéke egy adott személy esetén; az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

Adatcsoport: azonos ismérvekkel jellemezhető több adat együttesen (pl. személyazonosító adatok, jövedelmi adatok, stb.);

Adatfajta: a kezelt személyes adatok típusának legkisebb egysége (pl. név, születési név, lakcím, telefonszám, havi jövedelem, stb.).

Adatfeldolgozó: az a természetes, vagy jogi személy, közhatalmi szerv, ügynökség, vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

Adathordozhatóság: hozzájáruláson vagy szerződésen alapuló, automatizált módon történő adatkezelés [GDPR 6. cikk (1) bek. a) és b) pont, 9. cikk (2) bek. a) pont] esetén az érintett azon joga, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá azokat egy másik adatkezelőnek továbbítsa;

Adatkezelés: 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, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

Adatkezelési cél: az a pontosan meghatározott, jogszerű cél, amelynek elérése érdekében a személyes adatokon az adatkezelő az adatkezelési műveleteket végzi;

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség, vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. A Vállalkozás által ellátott adatkezelések vonatkozásában a Vállalkozást kell adatkezelőnek tekinteni.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele. A Vállalkozás munkavállalói között, illetve az adatfeldolgozónak történő adatátadás nem minősül adattovábbításnak;

Adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi- és Információszabadság Hatóság, illetve a GDPR 56. cikke szerinti fő felügyeleti hatóság;

Adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet a Vállalkozás köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti;

Adatvédelmi incidens: az adatvédelmi előírások 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;

Adatvédelmi tisztviselő: az adatvédelmi jog és gyakorlat szakértői szintű ismeretével bíró személy, akit az adatkezelő és az adatfeldolgozó köteles kijelölni a GDPR 37. cikkében nevesített esetekben (így pl. abban az esetben, ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé, vagy különleges adatok kezelését foglalják magukban), aki feladatai ellátása körében nem utasítható, és munkaviszony vagy szolgáltatási szerződés keretén belül végzi tevékenységét;

Munkavállaló: a Vállalkozással munkavégzésre irányuló jogviszonyban álló személy;

Érdekmérlegelési teszt: jogos érdeken alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést

megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását;

Érintett: azonosított vagy azonosítható természetes személy; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

Harmadik ország: minden olyan állam, amely nem tagja az Európai Gazdasági Térségnek (EGT). Az EGT államai: az EU tagállamai, valamint Izland, Lichtenstein és Norvégia;

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

Hozzájárulás: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

Jogosultságkezelés: a személyes adatokhoz, informatikai rendszerekhez vagy egyéb erőforrásokhoz való hozzáférés kezelésének folyamata és módszere, beleértve különösen a jóváhagyásokat, szerepköröket, összeférhetetlenségi kontrollokat;

3.2. Dokumentálási kötelezettség

A Vállalkozásnak képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések, az érintetteknek szóló tájékoztatások és nyilatkozatok, valamint az érintettől származó nyilatkozatok megfelelő dokumentálásával történik.

3.3. Az adatkezelés bevezetéséhez, módosításához, megszüntetéséhez kapcsolódó dokumentálási kötelezettség

A Vállalkozás az adatkezelést érintő minden tevékenységről, beleértve az adatkezelés megkezdésére, megváltoztatására irányuló bármely és valamennyi igényt, szándékot, az adatkezelést érintő valamennyi és bármely döntést írásban, dokumentálható és visszakereshető formában rögzíti és tárolja.

Ha az adatkezelésre érdekmérlegelési teszt elvégzését követően jogos érdek alapján kerül sor, a Vállalkozás azt írásban, dokumentálható és visszakereshető formában rögzíti és tárolja.

Ha az adatkezelésre hatásvizsgálat elvégzését követően kerül sor, a Vállalkozás azt írásban, dokumentálható és visszakereshető formában rögzíti és tárolja.

3.4. A hozzájárulások dokumentálása és tárolása

A Vállalkozásnak képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Ennek érdekében az érintetteknek a Vállalkozás egyes adatkezelési tevékenységeihez hozzájáruló valamennyi – írásban, online felületen, elektronikus üzenet, illetve egyéb úton tett – nyilatkozatát a Vállalkozás dokumentálható és visszakereshető formában rögzíti, nyilvántartja és tárolja.

Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy a hozzájárulás visszavonása esetén a Vállalkozás a hozzájárulás alapján kezelt adatokat a GDPR 17. cikke figyelembe vételével törli.

3.5. Az érintettek tájékoztatásának dokumentálása

A Vállalkozás megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi szükséges információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében.

Az érintettnek címzett tájékoztatás megtörténtét és annak az érintett általi megismerését dokumentálható és visszakereshető formában rögzíteni kell.

3.6. Az adatkezelések nyilvántartása

A Vállalkozás valamennyi adatkezelési tevékenységéről és adatfeldolgozási tevékenységéről nyilvántartást vezet.

3.7. Az adatvédelmi tisztviselő

A Vállalkozás adatvédelmi tisztviselőjének feladatait a Vállalkozás Ügyvezetője látja el.

Az adatvédelmi tisztviselő feladatai:

+ ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezéseknek, való megfelelést;
+ elősegíti a Vállalkozás munkavállalóinak az adatvédelmi tudatosságának növelését;
+ irányítja az érintettől származó kérelmek, panaszok megválaszolását;
+ kapcsolatot tart az adatvédelmi felügyeleti hatósággal.

3.8. Adatkezelés bevezetésével kapcsolatos feladatok

Új adatkezelés bevezetése esetén, amennyiben az természetes személyek adatainak kezelésével (meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik személynek továbbításával, stb.) jár. Az adatvédelmi tisztviselőt az

új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelési gyakorlat kialakításába.

Az új adatkezelés kialakításával kapcsolatosan meg kell határozni az adatkezelés (természetes személyek adatainak kezelésével járó termék bevezetése) célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, meg kell határozni az érdekmérlegelési teszt és a hatásvizsgálat elkészítésének szükségességét amennyiben ez indokolt. (GDPR 4. cikk 7. és 16. pont);

3.9. Adatkezelés megszüntetésével kapcsolatos feladatok

Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni.

Ebben az esetben vizsgálni szükséges az adatkezelés megszüntetésének mértékét az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére, nyilvántartási rendszer egészének vagy egyes adatfajták, illetve adatok törlésére vonatkozóan.

Az adatkezelés megszüntetését követően az adatok megtarthatóságára vonatkozó elévülési idő leteltét követően az adatokat az informatikai rendszerekből törölni, a papír alapú nyilvántartásban kezelt adatokat pedig selejtezni kell.

3.10.Az érdekmérlegelés teszt elvégzésének módszertana

Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a társadalom származtathat – az adatkezelésből.

Érdekmérlegelési tesztet kell elvégezni, ha a tervezett adatkezelés jogalapja jogos érdek. Az érdekmérlegelési tesztet a tervezett adatkezelésről az adatvédelmi tisztviselő végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. A jogos érdeken alapuló tervezett adatkezelés kizárólag az érdekmérlegelési teszt elvégzését követően kezdhető meg.

Az érdekmérlegelési tesztre az alábbiakban javasolt módszertan opcionális. A teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembe vételével kell megválasztani, a kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.

3.11.Az érdekmérlegelési teszt részei

A tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása. Ezen belül a következőket kell megvizsgálni:

+ A tervezett művelethez, folyamathoz valóban szükség van-e a személyes adatok kezelésére?

+ Van-e olyan alternatív megoldás, ami nem jár személyes adatok kezelésével?

+ Az adatkezelő vagy harmadik fél, akinek az adatkezelés érdekében áll, jogos érdekének azonosítása (Miért szükséges az adatkezelés? – Szükségességi teszt):

+ Mi a célja az adatkezelésnek?

+ A Vállalkozás mely céljaihoz szükséges az adatkezelés?

+ Valamely harmadik fél céljaihoz szükséges az adatkezelés?

+ A GDPR vagy valamelyik hazai jogszabály jogos érdek alapján végzendő adatkezelésnek tekinti-e az adatkezelést? Ha jogszabály nem rendelkezik az adatkezelésről, mely jog által elismert, védett (pl. üzleti, munkáltatói) érdek, jogszabályból következő feladat áll az adatkezelés mögött?

+ Más módon elérhető-e az adatkezelés célja?

+ Az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával – Arányossági teszt):

+ Az adatkezelés annak az érintettnek az érdekében áll, akinek a személyes adatai kezelésére kerül sor?

+ Az adatkezelés az érintett jogát hátrányosan érinti?

+ Az érintett számíthat-e arra, hogy személyes adatai kezelésére kerül sor?

+ Az érintett számíthat-e arra, hogy az adatait a kívánt célra felhasználják?

+ Korlátozza, befolyásolja az adatkezelés az érintett jogait?

+ A felhasználni kívánt adatot közvetlenül az érintettől vagy valaki mástól szerezte meg az adatkezelő?

+ Az adatkezelés módosítható annak érdekében, hogy csökkenthető vagy elkerülhető legyen a magánszférát érintő veszély?

+ Az érintett megfelelő tájékoztatást kapott az adatkezelésről?

+ Az érintett, akinek adatait az adatkezelés érinti, ellenőrizheti az adatkezelést vagy tiltakozhat ellene?

+ Az adatkezelés nyújt valamilyen hozzáadott értéket ahhoz a termékhez vagy szolgáltatáshoz, melyet az érintett igénybe vesz?

+ Az adatkezelőt kár érné, ha az adatkezelésre nem kerül sor?

+ Harmadik felet kár érné, ha az adatkezelésre nem kerül sor?

+ Az érintett jogos érdeke egyensúlyban van az adatkezelő jogos érdekével?

+ Mi a kapcsolat az érintett és az adatkezelő között? (meglévő, korábbi vagy érdeklődő ügyfél, munkavállaló, partner, stb.)

+ Milyen típusú a kapcsolat az érintett és az adatkezelő között? (folyamatos, visszatérő vagy alkalmi)

+ Milyen típusú adatokat érint az adatkezelés?

+ Az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése az adatkezeléssel járó előnyök (az adatkezelő vagy harmadik fél érdekének) és hátrányok (az érintett érdekeinek) összevetése.

+ Az adatkezelés során alkalmazott biztosítékok leírása, amelyek alkalmasak arra, hogy a személyes adatok biztonságos kezelését, vagyis a véletlen vagy jogellenes megsemmisítést, elvesztést, megváltoztatást, jogosulatlan nyilvánosságra hozatalt vagy az adatokhoz való jogosulatlan hozzáférést kizárják. Ilyen biztosíték (technikai és szervezési intézkedés) lehet többek között az adatminimalizálás, adatrejtés (pl. titkosítás, álnevesítés), korlátozott hozzáférés (jogosultságkezelés) szabályozása, lehetőség az opt-outra (kilépés az adatkezelésből) és az adatkezelési műveletek nyilvántartása (pl. naplózás).

+ Az érdekmérlegelési teszt eredményeként annak összefoglalása, hogy a jogos érdek alkalmazható-e az adatkezelés jogalapjaként. Amennyiben nem (pl. az érdekmérlegelési teszt eredményeként az adatkezelés vagy egyes adatfajták kezelése nem szükséges és/vagy nem arányos), az adatkezelés feltételeit felül kell vizsgálni.

3.12.Az adatvédelmi hatásvizsgálat elvégzésének módszertana

Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, az adatkezelést megelőzően hatásvizsgálatot kell végezni. Olyan egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (továbbiakban hatásvizsgálat) keretei között is értékelhetők.

A hatásvizsgálat elvégzésének szükségességéről a tervezett adatkezeléssel kapcsolatosan az adatvédelmi tisztviselő dönt.

A hatásvizsgálat megállapításait írásban kell rögzíteni. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

A Vállalkozás esetében ilyen esetek különösen:

+ ha személyes adatok különleges kategóriáinak, így különösen egészségügyi adat vagy a természetes személyek egyedi azonosítását célzó biometrikus adatoknak a kezelésére kerül sor;

+ ha a munkavállalók munkahelyi teljesítményére, megbízhatóságára, viselkedésére vonatkozó módszeres elemzésre vagy értékelésére kerül sor;

+ ha video-megfigyelő rendszer bevezetésére vagy az alkalmazott technológia megváltoztatására kerül sor;

+ ha új, innovatív technológiai megoldások bevezetésére kerül sor (pl. felhőszolgáltatás igénybe vétele).

A felsorolt eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az érintettre tekintettel jelentős joghatással bír vagy jelentős mértékben érinti.

A hatásvizsgálatra javasolt alábbi módszertan opcionális. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembe vételével kell megválasztani.

A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:

+ a tervezett adatfeldolgozó megjelölését, ha van ilyen;

+ az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét;

+ az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,

+ azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik;

+ az adatkezelés folyamatának a leírása.

+ milyen célból szükségesek az egyes adatkezelési műveletek a cél eléréséhez. Ha ugyanazon cél elérése többféle adatkezelés, adatkezelési művelet vagy adatkezelési módszerrel lehetséges, annak indoklása, hogy miért az adott adatkezelés mellett döntött az adatkezelő.

A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni az adatkezelés szükségességének és arányosságának garanciáit, különösen:

+ a tervezett adatkezelés célját/céljait: mennyiben felelnek meg annak a követelménynek, hogy a cél legyen meghatározott, egyértelmű és jogszerű;

+ a tervezett adatkezelés jogalapját/jogalapjait: melyik jogalap jöhet számításba és miért. Különösen a „jogos érdek” jogalapot kell megindokolni;

+ azt, hogy a tervezett adatkezelés mennyiben felel meg az adatminimalizálás elvének;

+ azt, hogy a tervezett adatkezelés hogyan biztosítja a pontosság követelményét;

+ az adattárolás tervezett időtartamát, illetve azt, hogy az adattörlést hogyan biztosítják az adatkezelési időtartam lejártakor;

+ amennyiben az értékelés hiányosságokat tár fel, milyen intézkedések szükségesek a GDPR-nak való megfelelés érdekében;

+ az érintett jogait biztosító garanciák érvényesülését, azt, hogy hogyan biztosítja az adatkezelő, az érintett hozzájárulásának megszerzését, az érintett tájékoztatáshoz való jogát, hozzáféréshez és/vagy adathordozhatósághoz való jogát, helyesbítéshez, illetve törléshez való jogát, tiltakozáshoz és az adatkezelés zárolásához való jogát, az adatfeldolgozóval kapcsolatos kötelezettségek érvényesülését, amennyiben az értékelés hiányosságokat tár fel, milyen intézkedések szükségesek a GDPR-nak való megfelelés érdekében;

A hatásvizsgálatban továbbá azonosítani és értékelni kell az adatkezelés potenciális kockázatait, különösen a fenyegető eseményeknek vagy veszélyeknek, kockázatoknak a típusát, a lehetséges forrását, előfordulásának valószínűségét és súlyosságát az érintettek magánszférájára gyakorolt lehetséges hatását.

A kockázatok enyhítésére tervezett, elfogadott intézkedések, megoldások bemutatása és értékelése abból a szempontból, hogy azok megfelelőek-e a kockázatok kiküszöbölésére, mérséklésére, illetve, hogy milyen kiegészítő intézkedésekre van szükség a GDPR-nak való megfelelés érdekében. A kockázatok mérséklésére szolgáló jogi intézkedések, szervezési intézkedések, logikai biztonsági és általános biztonsági intézkedések ismertetése.

Az esetleges adatvédelmi incidensek elemzése és értékelése és a hatások mérséklésére alkalmazható eszközök.

A hatásvizsgálat végén a tervezett adatkezelést kell értékelni és egyértelmű rögzíteni kell, hogy a tervezet adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

A hatásvizsgálatot legalább háromévente felül kell vizsgálni, szükség esetén újra el kell végezni.

4. AZ ÉRINTETTŐL SZÁRMAZÓ KÉRELMEK, PANASZOK MEGVÁLASZOLÁSÁRA VONATKOZÓ SZABÁLYOK

Az érintettől a következő a személyes adatai kezelésével kapcsolatos kérelmek, panaszok érkezhetnek:

Bejelentheti a Vállalkozás által nyilvántartott adatok megváltozását.

Tájékoztatást kérhet személyes adatai kezeléséről milyen személyes adato(ka)t milyen célból, milyen jogalapon, milyen forrásból szerezve meddig kezeli a Vállalakozás. (GDPR 16. cikk)

Kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát.– helyesbítéshez való jog (GDPR 16. cikk).

Kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk);

Kérheti személyes adatai kezelésének korlátozását – az adatkezelés korlátozásához való jog (GDPR 18. cikk);

Kérheti, hogy a rá vonatkozó, általa a Vállalkozás rendelkezésére bocsátott és elektronikus adatbázisban kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk);

Tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke (pl. direkt marketing célú adatkezelés), illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk);

Panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintően [GDPR 38. cikk (4) bek.];

A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi tisztviselő intézkedik a panaszt kiváltó okok orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására.

Az adatvédelmi bejelentéseket indokolatlan késedelem nélkül, de legfeljebb az adatvédelmi bejelentésnek a Vállalkozáshoz történő beérkezésétől számított egy hónapon belül kell megválaszolni. Az olyan összetett és/vagy több típusú kérelmet is tartalmazó adatvédelmi bejelentés esetén, amelynek egyes elemei egymástól függetlenül nem válaszolhatóak meg, az érintett előzetes tájékoztatása mellett az adatvédelmi tisztviselő a válaszadási határidőt legfeljebb további két hónappal meghosszabbíthatja.

5. BEÉPÍTETT ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK ÉRVÉNYYESÜLÉSE

A beépített és alapértelmezett adatvédelem elveinek egy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése az adatvédelmi tisztviselő feladata.

Az adatbiztonsági intézkedések mindennapi működésben történő betartása a Vállalkozás minden alkalmazottja, valamint a Vállalkozás informatikai rendszereihez hozzáférő személy kötelessége.

6. A KÖZÖS ADATKEZELŐI ÉS AZ ADATFELDOLGOZÓI SZERZŐDÉSEK MEGKÖTÉSÉNEK SZABÁLYAI

6.1. Közös adatkezelés

Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit a Vállalkozás egy vagy több másik adatkezelővel közösen határozza meg (GDPR 26. cikk).

A közös adatkezelésről szóló megállapodásban meg kell határozni az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit.

Azt, hogy a közös adatkezelésben érintett egyes adatkezelők, mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása, stb.) végzik, az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek

rendelkezésére, stb.), az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat, stb.), az esetleges jogellenes adatkezelés következményeit milyen arányban viselik.

Az adatvédelmi rendellenesség vagy incidens észlelése esetén követendő eljárást, különösen azt, hogy az adatvédelmi rendellenesség vagy incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről, egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában, az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség.

Kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani.

A megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

A közös adatkezelői megállapodás megkötését követően a Vállalkozás a vele közös adatkezelő adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelések Nyilvántartásában.

6.2. Adatfeldolgozói szerződések

Adatfeldolgozó igénybe vétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket.

Az adatfeldolgozóval kötendő szerződésben a kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (aladatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint a Vállalkozás által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait.

Rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködését.

Rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi rendellenesség vagy incidens észlelése esetén, így különösen, hogy adatvédelmi incidens tudomásra jutása esetén a Vállalkozás adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről.

Köteles együttműködni a Vállalkozás adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában, az adatvédelmi incidens bejelentésének teljesítésében.

Rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának

figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

A Vállalkozás az adatfeldolgozói szerződés megkötését követően az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelések Nyilvántartásában.

7. AZ ADATKEZELÉSEK NYILVÁNTARTÁSA

A Vállalkozás GDPR 30. cikke szerinti nyilvántartást vezet. (Adatkezelések Nyilvántartása).

Az Adatkezelések Nyilvántartása külön tartalmazza az adatkezelések adatait és a Vállalkozás által ellátott adatfeldolgozói tevékenységek adatait.

Az Adatkezelések Nyilvántartásának adattartalma adatkezelésenként a következő:

+ Az adatkezelés főbb adatai: az adatkezelő neve, az adatkezelő elérhetősége (címe), az adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége, az adatkezelés elnevezése, az adatkezelés kezdete, az adatkezelés célja(i), közös adatkezelés esetén e tény, és a további adatkezelő(k) adatai: név és cím, kapcsolattartó neve és elérhetősége, az adatbiztonsági intézkedések leírása (technikai és szervezési intézkedések).

+ Az adatfeldolgozók adatai, az adatfeldolgozó(k) neve és címe, az adatfeldolgozónak az adatkezeléssel kapcsolatos tevékenységének leírása.

+ Az érintettek körének megjelölése az adatfajták, az adatkezelés jogalapja, az adat forrása, az a tény, hogy adathordozhatóságban érintett-e, az a tény, hogy különleges adat-e, az adat megőrzési idejének jogalapja, az adat megőrzésének időtartama.

8. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

8.1. Az adatvédelmi incidens

Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés.

Az adatok véletlen vagy jogellenes megsemmisítésének az adatok helyreállíthatatlan megváltoztatása vagy az adatokat tartalmazó adathordozó fizikai megsemmisítése, használhatatlanná tétele adatvédelmi incidensnek minősül.

Az adatok elvesztésének az adatoknak, illetve az adatot tartalmazó adathordozónak a Vállalkozás birtokából való időleges vagy végleges kikerülése adatvédelmi incidensnek minősül.

Jogosulatlan közlésnek az adatoknak olyan harmadik személy tudomására hozása minősül (akár szóban, akár írásban, elektronikus vagy bármely más úton), aki az adatokat nem ismerhette volna meg.

Jogosulatlan hozzáférésnek minősül minden olyan eset, amikor arra nem jogosult személyek megismerik a személyes adatot (pl. személyes adatot tartalmazó dokumentum felügyelet nélkül hagyása, vagy más által is látható módon történő elhelyezése, vagy nyilvános internetes felületen, stb.)

A Vállalkozásnál bekövetkezett adatvédelmi incidensekről az adatvédelmi tisztviselőt soron kívül tájékoztatni szükséges.

Az adatvédelmi incidenst az adatvédelmi tisztviselő – ha lehetséges – a tudomásszerzést követő 72 órán belül bejelenti az adatvédelmi felügyeleti hatóság felé.

Amennyiben a bejelentés megtétele 72 órán belül nem lehetséges, az adatvédelmi tisztviselő összegyűjti a késedelem alapjául szolgáló indokokat, bizonyítékokat az adatvédelmi incidensek kivizsgálásával kapcsolatosan.

A bejelentést az adatvédelmi tisztviselő adatvédelmi felügyeleti hatóság – alábbi linken keresztül elérhető – online felületén teszi meg: www.naih.hu.

A bejelentésnek tartalmaznia kell:

+ az adatvédelmi tisztviselő nevét és elérhetőségét,
+ az adatvédelmi incidens bekövetkezésének időpontját,
+ az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és nagyságát,
+ az adatvédelmi incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
+ az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
+ az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Amennyiben a fenti információk egyidejű közlése nem lehetséges, úgy azokat az adatvédelmi tisztviselő indokolatlan késedelem nélkül később részletekben közli a hatósággal.

8.2. Az érintettek tájékoztatása az adatvédelmi incidensekről

A Vállalkozás az érintettet az adatvédelmi tisztviselő által hozott döntése alapján írásban/e-mail útján, telefonon/SMS útján közvetlenül tájékoztatja az adatvédelmi incidensről az érintett által korábban megadott elérhetőségeken.

A tájékoztatásnak tartalmaznia kell az adatvédelmi incidens jellegét.

9. AZ ADATVÉDELMI FELÜGYELETI HATÓSÁGOKKAL VALÓ KAPCSOLATTARTÁS

9.1. Az adatvédelmi tisztviselő feladata:

+ az adatvédelmi felügyeleti hatóságtól érkező, a GDPR, illetve az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) hatálya alá tartozó ügyre vonatkozó megkeresésekre (vagyis az adatvédelmi felügyeleti hatóság vizsgálati, illetve korrekciós hatáskörében hozott intézkedésekre –a továbbiakban együtt: adatvédelmi hatósági megkeresés) adandó válasz koordinált előkészítése [GDPR 58. cikk (1)-(2) bek.], továbbá a felügyeleti hatóság által folytatott helyszíni vizsgálat esetén a felügyeleti hatósággal való együttműködés koordinálása;

+ a felügyeleti hatóság értesítése az adatvédelmi incidensről a szabályzatba foglaltak szerint;

+ az érintettek által a Vállalkozásnak megküldött adatkezeléssel kapcsolatos kérelmek, panaszok megválaszolásának a koordinálása;

+ előzetes konzultáció kezdeményezése a felügyeleti hatósággal, amennyiben az adatvédelmi hatásvizsgálat elvégzését követően megállapítható, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár [GDPR 36. cikk (1) bek. és 58. cikk (3) bek. a) pont].

10.ZÁRÓ RENDELKEZÉS

Ez a szabályzat 2018. május 25-én lép hatályba.

A szabályzatban hivatkozott jogszabályok:

+ az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet; a továbbiakban: GDPR);

+ az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.).