Az Aon Magyarország Kft. Adatvédelmi és Adatbiztonsági Szabályzata

Hatályos: 2020.01.01

1. A Szabályzat célja

A jelen helyi adatvédelmi és adatbiztonsági szabályzat („Szabályzat”) az Aon Globális Adatvédelmi Szabályzatát („Globális Szabályzat") egészíti ki, és ebben a kontextusban olvasandó és értendő. Amennyiben az Általános Adatvédelmi Rendelet („GDPR”) és a jelen Szabályzat, vagy a Globális Szabályzat rendelkezései közötti eltérés, vagy bizonytalanság merül fel, a GDPR és a jelen Szabályzat rendelkezései e sorrendben elsőbbséget élveznek a Globális Szabályzat rendelkezéseivel szemben. A jelen rendelkezések a magyar helyi sajátosságokra utalnak, amelyek a Globális Szabályzatban meghatározott minimális követelmények mellett és azok pontosításaként veendők figyelembe.

Az Aon Magyarország vállalja, hogy kizárólag olyan személyes adatot és információt gyűjt és tárol, amely az üzleti követelményeknek, a lentiekben összefoglalt tevékenységéhez való megfeleléshez észszerűen szükséges, és amely a hatályos helyi törvényeknek és rendeleteknek, különösen a GDPR-nak, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek („Infotv.”), valamint a munka törvénykönyvéről szóló 2012. évi I. törvénynek („Mt.”) megfelel.

A jelen Szabályzat az alkalmazandó jogszabályokhoz képest járulékos kötelezettséget nem keletkeztet, azok kötelező érvényű rendelkezéseit nem korlátozza.

2. Hatály

A jelen Szabályzatot a magyarországi székhellyel rendelkező Aon Magyarország Kft. használja. A jelen szabályzatban meghatározott követelmények egy része hatással lehet külső szolgáltatókra és egyéb szerződéses partnerekre is, ezért ezeket figyelembe kell venni a harmadik felekkel kötött szerződések megfogalmazásakor és jóváhagyásakor.

A GDPR által meghatározott tárgyi hatályt (ti. amely alapján a GDPR-t alkalmazni kell a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni) az Infotv. úgy szélesíti ki, hogy az nem csak a teljesen vagy részben automatizált eszközzel, hanem az olyan manuális módon végzett adatkezelésre és adatfeldolgozásra is kiterjed, amely nem valamely nyilvántartási rendszer részét képezi, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

3. Az Aon Magyarország Kft. adatvédelmi rendszere

Az Aon Magyarország Kft. mindenkori vezető tisztségviselője ellátja az Aon Magyarország Kft. adatvédelmi rendszerének felügyeletét egy általa kinevezett adatvédelmi tisztviselő útján.

Az adatvédelmi tisztviselő a szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői ismerete alapján kerül kiválasztásra.

Az Aon Magyarország Kft. az adatvédelmi tisztviselő nevét és elérhetőségét közzéteszi a honlapján, valamint bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) részére.

Az Aon Magyarország vezető tisztviselője az adatvédelemmel kapcsolatban:

a) Felelős az érintettek Infotv-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
b) Felelős az Aon Magyarország Kft. által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
c) Felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok és jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
d) Felügyeli az adatvédelmi tisztviselő tevékenységét;
e) Vizsgálatot rendel el;
f) Kiadja az Aon Magyarország Kft. adatvédelemmel kapcsolatos belső szabályzatait.

Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

g) Segítséget nyújt az érintett jogainak biztosításában;
h) Kezdeményezi a NAIH felé az Info.-tv-ben meghatározott nyilvántartásba vételi eljárás lefolytatását;
i) Minden év január 15-ig jelentést készít a vezető tisztségviselő részére az Aon Magyarország Kft. adatvédelmi feladatainak végrehajtásáról;
j) Jogosult a szabályzat betartását ellenőrizni;
k) Vezeti az adattovábbítási nyilvántartást;
l) Részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
m) Figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;
n) Közreműködik a NAIH-tól az Aon Magyaroság Kft-hez érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
o) Általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
p) Tájékoztatást és szakmai tanácsot ad az Aon Magyarország Kft. adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
q) Ellenőrzi az adatvédelmi jogszabályoknak, valamint az Aon Magyarország Kft. belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság- növelését és képzését, valamint a kapcsolódó auditokat is;
r) Kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
s) Együttműködik a NAIH-al;
t) Az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le.
u) Nyomon követi az Aon Globális Szabályzatának megfelelően a („OneTrust) rendszerben történő adatnyilvántartást.

4. Érintettek jogai

Hozzáféréshez való jog

Az Aon Magyarország Kft. birtokában lévő személyes adatokat illetően az érintettek hozzáférési jog illeti meg.

Helyesbítéshez való jog

Az érintettnek jogában áll az Aon Magyarország Kft-t arra kérni, hogy az érintettről vezetett pontatlan vagy elavult személyes adatokat helyesbítse.

Az elfeledtetéshez való jog (a törlés joga)

Bizonyos körülmények esetén az érintettnek jogában áll a személyes adatait kitöröltetni. Az adatokat csak akkor lehet azonban törölni, ha azok nem szükségesek arra a célra, amely a gyűjtésüket indokolta, és az Aon Magyarország Kft-nek nincs jogalapja a kezelésére.

Az adatkezelés korlátozásához való jog

Az érintettnek jogában áll a személyes adatok kezelésének korlátozására, de csak akkor:

- ha az adatok pontossága vitatott, és lehetőséget kíván teremteni azok pontosságának igazolására; vagy
- ha az adatkezelés jogszabályellenes, de nem kívánja az adatokat töröltetni, vagy
- ha az adatokra a gyűjtéskor megjelölt cél eléréséhez már nincs szükség, az Aon Magyarország Kft. viszont jogi követelések megállapításához, érvényesítéséhez vagy az ellenük való védelemhez szüksége van rájuk; vagy
- az érintett élt a tiltakozáshoz fűződő jogával, de a felülbírálat jogalapjának igazolása még folyamatban van.

Az *adathordozhatósághoz fűződő jog*

Az érintettet megilleti az adathordozhatósághoz fűződő jog, amelynek alapján az Aon Magyarország Kft. az érintettnek, illetve egyéb adatkezelőknek általánosan használt, gépileg olvasható formában köteles a személyes adatokat átadni, amely azonban csak abban az esetben érinti a Társaságot, ha az adott információ feldolgozása (i) hozzájáruláson vagy (ii) olyan szerződés teljesítésén alapul, amelyeknek az érintett is részese.

Az adatkezelés elleni tiltakozáshoz fűződő jog

Az érintettnek jogában áll a személyes adatainak kezelése ellen bármikor tiltakozni, de csak olyan esetben, ahol az adatkezeléshez az Aon Magyarország Kft. legitim érdekünk szolgáltat alapot. Ha az érintett tiltakozással él, az érintettnek lehetőségünk van annak igazolására, hogy az érintett jogait és szabadságait felülíró cáfolhatatlan jogos társasági érdekek léteznek.

Az adatok nemzetközi továbbítása

Az érintett másolatban vagy hivatkozás formájában kérhet tájékoztatást arról, milyen óvintézkedések mellett történik az érintett személyes adatainak a továbbítása az Európai Unión kívülre.

Az Aon Magyarország Kft. minden munkavállalója – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles bármely beérkező érintetti megkeresést haladéktalanul jelenteni az üzletág vezetőjének. Az üzletág vezető az értesítést követően haladéktalanul tájékoztatja az adatvédelmi tisztviselőt is. A jelentés tartalmazza az érintett nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, jogi személy nevét (ha van ilyen), valamint a bejelentés tárgyát, rövid leírását és azt, hogy az érintetti megkeresés érinti az Aon Magyarország Kft. informatikai rendszerét.

Az érintett a fentieknek megfelelően tájékoztatást kérhet tehát a személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését, korlátozását az Aon Magyarország Kft. feltüntetett elérhetőségein.

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Aon Magyarország Kft. rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

Az Aon Magyarország Kft. a beérkezett megkeresést, illetve tiltakozást köteles a beérkezéstől számított három napon belül áttenni az adatkezelés szempontjából releváns üzletág vezetőjéhez.

Az üzletág vezetője az érintett személyes adatának kezelésével összefüggő kérelmére az érkezésétől számított legkésőbb 25 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban, közérthető formában választ ad.

A tájékoztatás kiterjed az Infotv. 16. § (1) bekezdésében meghatározott információkra, amennyiben az érintett tájékoztatása törvény alapján nem tagadható meg. A tájékoztatás főszabály szerint ingyenes.

Az Aon Magyarország Kft. kérelmet csak az Infotv-ben meghatározott okokból utasít el, erre csak indoklással, az Infotv. 16. § (3) bekezdésében meghatározott tájékoztatással, írásban kerül sor.

A valóságnak nem megfelelő adatot az adatot kezelő üzletág vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, az Infotv. 20. § szakaszában meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törlése iránt.

Az érintett személyes adata kezelése elleni tiltakozásának elbírálásának időtartamára – de legfeljebb 5 napra – az adatkezelést az adatkezelést végző szervezeti egység vezetője felfüggeszti, a tiltakozás megalapozottságát megvizsgálja és döntést hoz, amelyről a kérelmezőt az Infotv. 21. § (2) bekezdésében foglaltak szerint tájékoztatja.

Amennyiben a tiltakozás indokolt, az adatot kezelő üzletág vezetője az Infotv. 21. § (3) bekezdésében meghatározottak szerint jár el.

Amennyiben az érintett jogainak gyakorlása során az ügy megítélése nem egyértelmű, az adatot kezelő üzletág vezetője az ügy iratainak és az ügyre vonatkozó álláspontjának megküldésével állásfoglalást kérhet az adatvédelmi tisztviselőtől, aki azt három napon belül teljesíti. Az adatkezeléssel érintett üzletág vezetője az érintett jogára irányuló tevékenységet az arról való értesítést követően összefoglalja az adatvédelmi tisztviselő részére, aki a Compliance vezetővel együtt jelzi az érintetti megkeresést a OneTrust rendszeren keresztül.

5. Adatvédelmi incidens

Az adatvédelmi incidens a GDPR 4. cikk 12. pontja alapján a biztonság olyan sérülése, amely a továbbított, tárolt, vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, vagy az adatokhoz való jogosulatlan hozzáférést eredményezi.

Az Aon Magyarország Kft. minden munkavállalója -beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles az Aon Magyarország Kft-n belül történt adatvédelmi incidenst haladéktalanul jeleneti az üzletág vezetőjének, valamint az adatvédelmi tisztviselőnek a jelen Szabályzathoz mellékelt Data Incident Notification Form kitöltésével és megküldésével.

Amennyiben az adatvédelmi incidens érinti az Aon Magyarország Kft. informatikai rendszerét is, akkor a bejelentést az informatikai vezetőnek (a továbbiakban: IT vezető) is meg kell küldeni.

A munkavállaló köteles a Data Incident Notification Form-ot a kitöltést követően az üzletág vezetőjével és a compliance vezetővel egyeztetve megküldeni a Global Emergency Operation Centre-nek a global.eoc.mailbox@aon.com e-mail címre.

Ezt követően az Aon Magyarország Kft comliance vezetője felel az ún. Incident Response Team (csoport) felállításáért, mely csoport a helyi compliance vezetőt, az adatvédelmi tisztségviselőt, és regionális compliance vezetőt feltétlenül magában foglalja. Az Incident Response Team feladatait a mindenkor hatályos Data Privacy Incident Playbook tartalmazza.

Az adatvédelmi incidens kivizsgálása és értékelése

Az Incident Response Team - informatikai rendszert érintő incidens esetén az IT vezetővel együttműködve -megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az Incident Response Team bármely tagjának felhívására a bejelentő köteles a Data Incident Notification Form-on meghatározottak mellett további adatok és információk megadására. A bejelentő az adatszolgáltatást haladéktlanul teljesti az Incident Response Team bármely tagja felé.

Amennyiben az adatvédelmi incidens vizsgálatot igényel, az adatvédelmi tisztviselő az IT vezetővel valamint az egyéb, vizsgálat lefolytatásához szükséges további munkatársasak,bevonásával lefolytatja a vizsgálatot. A vizsgálat tartalmazza, hogy a vizsgálat magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatokról van szó továbbá hogy szükséges-e az érintettek tájékoztatása az incidensről.

A vizsgálat eredményeként – az Incident Response Team álláspontja, valamint a GEOC-tól kapott utasítások alapján az adatvédelmi tisztségviselő javaslatot tesz az incidens kezeléséhez szükséges intézkedések megtételére.

A vizsgálatot legkésőbb 72 órán belül be kell fejezni, melyen belül az adatvédelmi tisztviselő a vezető tisztségviselőt még a bejelentési határidőt megelőzően tájékoztatja.

A megvalósítható további intézkedésről az adatvédelmi tisztségviselő javaslatára a vezető tisztségviselő - dönt.

Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet.

A nyilvántartás tartalmazza:

- Az érintett személyes adatok körét,
- Az adatvédelmi incidenssel érintettek körét és számát,
- Az adatvédelmi incidens időpontját,
- Az adatvédelmi incidens körülményeit és hatásait,
- Az elhárítására megtett intézkedéseket,
- Egyéb jogszabályban rögzített adatokat.

Adatvédelmi incidens bejelentése a hatóság felé

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezésétől számítottan 72 órán belül bejelenti a hatóság részére a hatóság erre a célra rendszeresített felületén, kivéve, ha a saját, illetve a GEOC megállapításai alapján az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a hatóság részére. Annak megítélése, hogy az incidenst be kell jelenteni a hatóság felé, az adatvédelmi tisztviselő feladata és felelőssége a GEOC valamint az Incident Response Team javaslatainak figyelembevételével.

A hatósági bejelentésnek tartalmaznia kell:

- Az az adatvédelmi incidenssel érintett személyes adatok körét, és hozzávetőleges számát,
- Az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- Az adatvédelmi incidens jellegét, körülményeit,
- Az adatvédelmi tisztviselő nevét és elérhetőségét,
- Az adatvédelmi incidens valószínűsíthető következményeit,
- Az adatvédelmi incidens orvoslására megtett intézkedéseket.

Az érintettek tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi tisztségviselő, az Incident Response Team valamint a GEOC álláspontja alapján az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket az Aon Magyarország Kft. vezető tisztségviselője utasítására.

Nem kell az érintetteket tájékoztatni:

- ha az Aon Magyarország Kft. olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét.
- ha az adatvédelmi incidens bekövetkezését követően az Aon Magyarország olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg.
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

6. Hatásvizsgálat

Amennyien valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve az adatkezelés megkezdését megelőzően, akkor az Aon Magyarország Kft. hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelés a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatvédelmi műveletek, amelyek hasonló kockázatot jelentenek egyetlen egy hatásvizsgálat keretben is elvégezhetők.

A hatásvizsgálatot főszabály szerint az adatvédelmi tisztviselő - az Aon Magyarország Kft érintett munkatársainak bevonásával -végzi. Amennyiben nem ő végzi, úgy az Aon Magyarország Kft. köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén gondoskodik a hatásvizsgálat felülvizsgálatáról, mely során a kockázatok értékelését újra elvégzi. A kockázatok felülvizsgálatát legalább 3 évente el kell végezni.

A személyes adatok kezelésével kapcsolatosan az Adatkezelő kötelezettsége továbbá a kockázatelemzés, amelynek lépései a következők:

- a személyes adatok kezelésével kapcsolatos kockázatok azonosítása,
- kockázati lista felállítása,
- az egyes kockázatok valószínűsíthető fő okainak és várható negatív hatásainak meghatározása és
- ezek alapján a preventív és a korrektív kockázatkezelési folyamatok kidolgozása.

Szükséges a kockázatforrások feltárása, melyen belül meg kell határozni a kockázati preventív és korrektív célkezelés elemeit, az erőforrás-kezelés rendszerét, és el kell különíteni az objektív és szubjektív kockázati elemeket.

Az elemzés során el kell jutni a teljes kockázatértékelésig, amelyben teljes kockázatpotenciál és kockázat prioritási sorrend (nem az intézkedési rendszerrel azonos) megállapítása kell, hogy megtörténjen. Az elemzés menetét és eredményeit írásba kell foglalni.

A kockázatpotenciálnál meg kell határozni a valószínűség szempontjából

- kicsi
- közepes

és nagy bekövetkezésű kockázatokat, illetve horderő szempontjából

- kicsi
- közepes
- és nagy horderejű kockázatokat.

Ez a meghatározás alapozza meg a későbbi kockázatkezelési eljárás módját mind a preventív, mind a korrektív eljárás tekintetében. A kockázatelemzés végrehajtásáért az adatvédelmi tisztviselő felel.

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az Aon Magyarország Kft. az adatvédelmi tisztviselő útján konzultál a NAIH-al.

7. Érdekmérlegelés

Az Infotv. rendelkezései szerint lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy az Aon Magyarország Kft. eleget tesz tájékoztatási kötelezettségének. Az adatkezelés jogalapjának vizsgálata során a GDPR 6. cikk (1) bekezdése a)-f) pontjai az irányadók.

Amennyiben a jogalapot a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben 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.

Az adatkezelés jogszerűségének vizsgálatához az Aon Magyarország Kft. elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során az Aon Magyaroság Kft. azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja az Aon Magyarország Kft. Az Aon Magyarország Kft. a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is elvégzi az Aon Magyarország Kft., amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján az Aon Magyarország Kft. megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy az Aon Magyarország Kft. az érintett beleegyezése nélkül kezeli a személyes adatot, tehát az Aon Magyarország Kft adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait. Az Aon Magyarország Kft. tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé az Aon Magyarország Kft. az adott eset sajátos körülményeire tekintettel, ezért az Aon Magyarország minden egyes esetben külön érdekmérlegelési tesztet végez el.

Lehetséges forgatókönyv, melytől való eltérés jogát az Aon Magyarország Kft. fenntartja:

1. lépés: az Aon Magyarország Kft. a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

2. lépés: az Aon Magyarország Kft. a jogos érdekét a lehető legpontosabban meghatározza.

3. lépés: az Aon Magyarország Kft. meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.

4. lépés: az Aon Magyarország Kft. meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben).

5. lépés: az Aon Magyarország Kft. elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e. Az Aon Magyarország Kft.

meghatározza, hogy miért korlátozza arányosan az jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat.

6. lépés: az Aon Magyarország Kft. meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát más garanciális intézkedések is alkalmazhatók).

8. A megvalósuló adatkezelések

Az Aon Magyarország Kft., mint adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységekről a OneTrust elektronikus rendszerben „*RPA with evergreen principle"* néven nyilvántartást vezet. E nyilvántartás üzletágakra lebontva írja le az adatkezelési folyamatokat, valamint a következő információkat tartalmazza:

- Adatkezelő neve;
- Adatkezelés célja és jogalapja;
- Érintettek kategóriáinak, és a személyes adatok kategóriájának ismertetetése;
- Olyan címzettek kategóriái, akikkel a személyes adatokat közlik;
- Adott esetben a személyes adatok harmadik országba, vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk;
- Adatkategóriák törlésének határidei, amennyiben van ilyen;
- Ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések leírása.

Az adatkezelési tevékenységről végzett nyilvántartás szükség esetén, de félévente legalább egyszer felülvizsgálatra kerül. A *RPA with evergreen principle* dokumenum a jelen Szabályzat 1. számú melléklete.

9. Munkaviszonnyal kapcsolatos adatkezelés

A munkaviszonnyal kapcsolatos adatkezelés szabályait a jelen Szabályzat 2. számú melléklete az alábbi eltérésekkel tartalmazza.

Személyazonosító igazolványok fénymásolása

Az Aon Magyarország Kft.– összhangban a NAIH álláspontjával – nem készít fénymásolatot személyazonosító igazolványokról. A hatósági okmányról készített fénymásolat nem alkalmas a természetes személyek azonosítására, mivel az egyén személyes jelenléte elengedhetetlen a hatósági igazolvány alapján történő személyazonosításhoz. Az arcképes hatósági igazolvány értelemszerűen csak akkor rendelkezik bizonyító erővel, ha annak alapján az Aon Magyarország Kft. megbizonyosodhat arról, hogy az igazolványon szereplő személy képmása és az igazolványt felmutató személy megegyeznek. Egy hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági igazolványnak.

Az adatrögzítés és az adatminőség elvének megtartása céljából az Aon Magyarország Kft. azonban az újonnan belépő vagy adatot módosító munkavállalók azonosító igazolványairól fénymásolatot (vagy szkennelt képet – együtt: fénymásolat) készíthet. A fénymásolás során az Aon Magyarország Kft. az igazolvány csak azon részeit hagyja fénymásolásra alkalmas, a továbbiakban olvasható állapotban, amely adatokat a munkavállaló a belépése során egyébként is köteles magáról megadni. A fénymásolat ebben az esetben az adategyeztetés céljából készül. A fénymásolatot az Aon Magyarország Kft. azonnal és visszavonhatatlanul törli vagy megsemmisíti a munkavállaló által kitöltött belépőpapírokon és

igazolvány-fénymásolatokon szereplő adatok az Aon Magyarország által kijelölt munkatársa általi összehasonlítását, de legkésőbb a fénymásolat készültét követő 30 nap elteltével.

Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése

Az egészségügyi alkalmassággal kapcsolatos adatokat az Aon Magyarország Kft. nem ismeri meg, és nem kezeli egyetlen érintett adatát a célon túlterjeszkedő mértékben. Az Aon Magyarország Kft. az egészségügyi alkalmasság eldöntése céljából egészségügyi szolgáltatótól származó alkalmassági eredmény alapján dönt az adott (leendő) munkavállaló egészségügyi alkalmasságáról. Az Aon Magyaroszág Kft. csak az egészségügyi alkalmasság tényét bizonyító adatot kezeli.

Amennyiben a munkaszerződés megkötésének folyamata során derül ki, hogy az adott érintett alkalmatlan a munkakör betöltésére, ezért a munkaviszony nem jön létre vagy ennek hatására szűnik meg, úgy az adatkezelés határideje és módja is ezzel párhuzamos.

10. Munkára jelentkezők adatkezelése

A munkára jelentkezők személyes adatai kezelésének szabályait a jelen Szabályzat 3. mellékleteként szereplő Személyes Adatokat Tartalmazó Pályázati Anyagok, önéletrajzok kezelése a GDPR szabályainak megfelelően című ügyvezető utasítás tartalmazza.

11. Munkavállalók technikai eszközeinek ellenőrzése

Az Aon Magyarország Kft. a munkavállalóit a munkaviszonnyal összefüggésben jogosult ellenőrizni azzal, hogy amennyiben erre sor kerül, az Aon Magyarország Kft. az ellenőrzi eszközéről és módjáról a munkavállalókat előzetesen tájékoztatja.

12. Információ az adatkezelőről

- Adatkezelő neve: Aon Magyarország Kft.
- Adatkezelő címe: 1138 Budapest, Váci út 121-127.
- Vezető tisztségviselő: Gerendai Károly, ügyvezető
- Adatkezelő telefonszáma: +36-1- 815-9800
- Adatkezelő faxszáma: +36-1- 815-9807

13. Információ az adatvédelmi tisztviselőről

- Az adatvédelmi tisztviselő neve: Balogh Bertalan
- Az adatvédelmi tisztviselő telefonszáma: +36-1 815-9845
- Az adatvédelmi tisztviselő e-mail címe: bertalan.balogh@aon.hu

14. Jogorvoslat és Tájékoztató

Az érintettek adatkezeléssel kapcsolatos kérdései, észrevételei vagy panaszai esetén, vagy ha bármely vonatkozó jogukkal élni kívánnak, (úgy mint a tájékoztatáshoz való jog, helyesbítéshez való jog, korlátozáshoz vagy elfelejtéshez való jog), ezt az info@aon.hu címre történő e-mail küldése útján tehetik meg.

Amennyiben az érintettnek a személyes adatok feldolgozásával kapcsolatos olyan panaszai vannak, amelyeket nem sikerült megoldani, az érintett Budapesten, Magyarországon kapcsolatba léphet a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH, https://naih.hu/).

15. Oktatás

Az adatvédelmi tisztviselő gondoskodik az adatvédelmi tudatosság növelése céljából az adatvédelmi oktatásról, mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi. Az adatvédelmi oktatás a globális Training and Awareness Standards dokumentummal összhangban kerül megszervezésre.

Kiemelt területként kell kezelni a munkavállalók kapcsán a biztonságtudatossági képzést a szervezet informatikai és nem informatikai alkalmazottai részére. A biztonságtudatos magatartás komoly üzleti károkat okozó hibák és támadások megelőzésében játszhat szerepet.

II. IT /Adatbiztonsági Szabályzat

1. Védelem

A papír alapon kezelt személyes adatok biztonsága érdekében az Aon Magyarország Kft. az alábbi intézkedéseket alkalmazza:

- Az adatokhoz csak az arra jogosultak férhetnek hozzá, más számára fel nem tárhatók.
- A dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezik el.
- Folyamatos kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá.
- A munkavállaló iratokat a munkavégzés végeztével a papír alapú iratokat és az adathordozókat elzárja.
- Amennyiben a papír alapon tárolt személyes adat kezelésének célja megvalósult, úgy az Aon Magyarország Kft. intézkedik azok megsemmisítéséről.

Az adatkezelésre a Physical Security Policy dokumentummal, valamint a Clear Desk and Clear Screen Policy dokumentummal, Global Information Security Policy dokumentummal összhangban kerül sor.

2. Informatikai védelem

A számítógépeken, illetve a hálózaton tárolt személyes adatok biztonsága érdekében az Aon Magyarország Kft. az alábbi biztonsági intézkedéseket alkalmazza:

- Az adatkezelés során használt számítógépek az Aon Magyarország Kft. tulajdonát képezik.
- Az adatokkal történő minden számítógépes rekord rögzítésre kerül.
- A hálózaton tárolt adatok biztonsága érdekében csak megfelelő jogosultsággal rendelkező és csakis az arra kijelölt személyek férhetnek hozzá.
- A számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről az Aon Magyarország Kft. rendszeresen, illetve indokolt esetben gondoskodik;
- A szerveren tárolt adatokhoz, megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- Az Aon Magyarország Kft. a mentésekkel és a Global IT Policy szabályzattal összhangban archiválással kerüli el az adatvesztést;

- Az Aon Magyarország Kft. gondoskodik a személyes adatokat kezelő hálózatok vírusvédelméről;
- Az Aon Magyarország Kft. megakadályozza illetéktelen személyek hálózati hozzáférését. (felhasználó, jelszóvédelem, hálózati hozzáférés szabályozása útján)
- Amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül.

3. Szerverek biztonsága és jogosultságkezelés

Az Aon Magyarország Kft. által kezelt személyes adatok áramlását elektronikus módon szerverek segítségével valósítják meg, tárolásuk pedig adattárolók segítségével történik.

A szerverszobába kizárólag az arra jogosultak léphetnek be. A szerverszoba hozzáférés szabályozása a Physical Security Policy, a Physical Access Control és a Global IT Security Policy szabályzattal összhangban történik.

Az informatikai rendszerekhez történő hozzáférés jogosultságkezelés a Global IT Security Policy szabályzattal összhangban történik. A szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti az Aon Magyarország Kft-t a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A jogosultságkezelés az Identity and Data Access Policy szabályzattal és a Global IT Security Policy dokumentummal összhangban történik.

4. Eszköz menedzsment

Az adatvédelmi szabályozás szempontjából az eszköz menedzsment területén az Aon Magyarország Kft. üzletmenetéhez fontos szolgáltatások informatikai biztosítása mellett adatvédelmi szempontból fontos kötelezettség keletkezik, azaz biztosítani kell az Aon Magyarország Kft. birtokába kerülő adatok titkosságát, sérthetetlenség és a biztonságos rendszerben történő működését.