Adatvédelmi és Adatbiztonsági Szabályzat

DUAL GLASS Korlátolt Felelősségű Társaság

Utolsó módosítás:	2022. május 12.
Dokumentum verziója:	1.0
Dokumentumgazda:	Lakatos Rita
Felülvizsgálat gyakorisága:	1 év

Jóváhagyta:

Gárgyán Zsolt

Tartalomjegyzék

1. Bevezető rendelkezések

1.1. A szabályzat célja

Az Adatvédelmi és Adatbiztonsági Szabályzat (továbbiakban: Szabályzat) célja, hogy meghatározza a DUAL GLASS Kft-nél zajló adatkezelések törvényes kereteit, biztosítsa az adatvédelem alkotmányos elveinek és az információs önrendelkezési jognak az érvényesítését, elősegítse az adatbiztonság követelményeinek való megfelelést, továbbá megakadályozza a jogosulatlan adatkezelést. Az Adatvédelmi és Adatbiztonsági Szabályzat kialakítja az adatvédelem szempontjából fontos feladatokat, felelősségi viszonyokat, különös tekintettel a munkavállalók szerepére az adatbiztonságban.

1.2. A szabályzat hatálya

A Szabályzat **személyi hatálya** kiterjed a DUAL GLASS Kft. valamennyi szervezeti egységére, minden alkalmazottjára, valamint a vele szerződéses vagy egyéb kapcsolatban álló, személyes adat kezelését vagy feldolgozását végző személyre.

A Szabályzat **tárgyi hatálya** kiterjed a DUAL GLASS Kft. szervezeti egységei által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

1.3. Jóváhagyás és felülvizsgálat

Jelen Szabályzatot az ügyvezető hagyja jóvá és tárolja. A Szabályzatot jelentős szervezeti vagy informatikai változás esetén, de legalább évente felül kell vizsgálni.

1.4. Felelősség és jelentés

A Szabályzat végrehajtatásáért az ügyvezető felelős. Valamennyi munkavállaló kötelezettsége annak bejelentése, ha a Szabályzat megkerüléséről vagy megsértéséről szerez tudomást, vagy ennek gyanúja merül fel. Bejelentés elsődlegesen a szokásos bejelentési csatornákon teendő, vagyis az ügyvezető igazgató vagy az adatvédelmi felelős írásbeli megkeresésével. Sürgős esetben a bejelentés telefonon is történhet, azonban a bejelentést legkésőbb a következő munkanapon írásban is meg kell tenni.

1.5. Jogszabályi hivatkozások

Jelen Adatvédelmi és Adatbiztonsági Szabályzat jogszabályi alapját a következő jogszabályok jelentik:

- Magyarország Alaptörvénye;
- 2011. évi CXII. törvény - (Infotv.);
- 679/2016. EU rendelet - (GDPR);
- 2018. évi XXXVIII. törvény (Módtv.);
- 2005. évi CXXXIII. törvény - (Szvtv.);
- 2012. évi I. törvény - (Mt.);
- 2013. évi V. törvény - (Ptk.).

1.6. Kapcsolódó szabályozások és dokumentumok

Jelen Adatvédelmi Szabályzat az Adatkezelő alábbi belső dokumentumaihoz kapcsolódik, azokkal együttesen értelmezendő:

- Információbiztonsági Szabályzat - (IBSZ);
- Üzletmenet folytonossági és Katasztrófa elhárítási terv – (BCP-DRP);
- Kamera Szabályzat;
- kockázatelemzés és kockázatkezelés;
- hatásvizsgálatok-érdekmérlegelések;
- adatkezelési tájékoztatók.

1.7. Értelmező rendelkezések

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik;

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés;

adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy;

harmadik ország: minden olyan állam, amely nem EGT-állam;

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 és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez;

különleges adat: a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, az egészségi állapotra, a kóros szenvedélyre, a szexuális irányultságra és szokásokra vonatkozó adat, valamint a bűnügyi személyes adat;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

személyes adat: az érintettel kapcsolatba hozható adat (különösen az érintett neve, azonosító jele, egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret), valamint az adatból levonható, az érintettre vonatkozó következtetés;

tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

üzleti titok: a gazdasági tevékenységhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a jogosult jogos pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli;

1.8. Az adatkezelő adatai

megnevezés: ***DUAL GLASS Korlátolt Felelősségű Társaság,***

székhely: 2241 Sülysáp, Ipar utca 14/A.,

cégjegyzékszám: 13-09-119143,

adószám: 14262807-2-13,

weboldal: dualglass.hu

1.9. Az adatvédelmi felelős adatai

Adatkezelő a jogszabályi előírások alapján adatvédelmi felelőst nevezett ki, akihez az adatkezeléssel kapcsolatban az alábbi elérhetőségeken lehet fordulni:

Név: ***Lakatos Rita,***

Üzenet: info@dualglass.hu,

Telefon: +36 20 211 5151

2. Szerepkörök, felelősségek

2.1. Általános felelősségi szabályok

A DUAL GLASS Kft. valamennyi foglalkoztatottja és alvállalkozója köteles gondoskodni a személyes adatok védelméről, valamint az adatok és az adatkezelés biztonságáról.

Tevékenységi körén belül mindenki felelős az adatkezelés jogszerűségéért. A vonatkozó jogszabályokban és a belső szabályozó eszközökben foglaltaknak nem megfelelő adatkezelés az adott mulasztás vagy egyéb cselekmény jellegétől függően fegyelmi, illetve polgári jogi, büntetőjogi felelősséget von maga után.

Az adatkezelő foglalkoztatottja és alvállalkozója a kötelezettsége megszegésével okozott kárért köteles helytállni.

A vonatkozó jogszabályokban meghatározott felelősség terheli azt, aki tudomást szerez a nem megfelelő adatkezelésről, de erről az adatvédelmi felelőst vagy az ügyvezetőt nem tájékoztatja.

A foglalkoztatott köteles megtagadni az olyan utasítás végrehajtását, amelynek teljesítésével bűncselekményt követne el, és megtagadhatja az olyan utasítás végrehajtását is, amelynek végrehajtása jogszabályba ütközne. Ez utóbbi esetben a foglalkoztatott köteles az utasítást adó figyelmét felhívni arra, hogy az utasítás végrehajtása jogszabályba ütközne.

Adatkezelőnél a személyes adatokat érintő adatkezelést végző foglalkoztatott köteles a tudomására jutott személyes adatokat titokként megőrizni, ilyen munkakörben csak az foglalkoztatható, aki titoktartási nyilatkozatot tett.

2.2. Ügyvezető igazgató

Az ügyvezető irányítja és felügyeli a DUAL GLASS Kft. egészére nézve az adatvédelmi feladatok ellátását, az adatvédelemre vonatkozó rendelkezések betartását.

Az adatvédelmi szempontok maradéktalan érvényesítése érdekében...

- kiadja az Adatvédelmi Szabályzatot;
- kinevezi az adatvédelmi felelőst;
- az adatvédelmi feladatokat érintő kérdésekben képviseli Adatkezelőt az egyes hatóságok, ellenőrző szervek előtt, vagy erre megbízást ad;
- ha a NAIH jogellenes adatkezelés észlelése esetén Adatkezelőt az adatkezelés vagy annak jogszerűtlensége megszüntetésére hívja fel, haladéktalanul megteszi a szükséges intézkedéseket és erről 30 napon belül tájékoztatja a NAIH-ot, vagy erre megbízást ad;
- folyamatosan ellenőrzi az adatvédelemre vonatkozó rendelkezések betartását, ennek keretében szükség esetén vizsgálatot rendel el;
- gondoskodik az adatvédelmi tevékenységek ellátásához szükséges feltételek folyamatos biztosításáról.

2.3. Adatvédelmi felelős

Az adatvédelmi felelős közvetlenül az ügyvezetőnek beszámolva látja el feladatait, szakmailag felügyeli és ellenőrzi a DUAL GLASS Kft. adatvédelmi tevékenységét. Ezen feladataival összefüggésben az adatvédelmi felelős...

- szakmai tanácsot ad;
- véleményezi, rendszeresen felülvizsgálja, szükség esetén módosíttatja az Adatvédelmi Szabályzatot;
- kérésre közreműködik az adatkezelő belső szabályozó eszközeinek megalkotásában, adatvédelmi szempontból véleményezi azok tervezeteit, szükség esetén javaslatot tesz az egyes rendelkezések módosítására;
- véleményt ad az adatvédelmi tárgyú kérdésekben;
- adatvédelmi szempontból javaslattétellel, véleményezéssel támogatja az induló projekteket;
- kérésre tanácsot ad az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- kivizsgálja a hozzá érkezett bejelentéseket és jogosulatlan adatkezelés észlelése esetén annak haladéktalan megszüntetésére hívja fel az adatkezelőt vagy adatfeldolgozóit;

- a hozzá külső szervektől és személyektől érkező adatvédelmi tárgyú megkereséseket véleményezi, majd intézkedik vagy további intézkedésre megküldi egy, az adat kezelésére és átadására jogosult személynek;
- nyilvántartást vezet a személyes adataik kezelésével kapcsolatban az érintettektől érkezett, teljesített vagy elutasított kérelmekről, valamint az esetleges elutasítások indokairól a munkavállalóktól vagy adatfeldolgozóktól kapott kimutatások alapján;
- szakmailag ellenőrzi a vonatkozó jogszabályokban és belső szabályozó eszközökben foglaltaknak megfelelő adatkezeléseket;
- az adatvédelmi szempontok érvényesülése céljából javaslatot tesz az egyes feltárt jogszerűtlenségek kiküszöbölésének módjára;
- vezeti az incidens nyilvántartást;
- adatvédelmi szempontból figyelemmel kíséri az adatvagyonleltár elkészítését, kérésre véleményt ad, illetve amennyiben ennek szükségét látja, javaslattal él;
- évente legalább egy alkalommal gondoskodik az adatvédelmi ismeretek oktatásáról.

2.3.1. Állásfoglalás, véleményezés

Az adatvédelmi felelős állásfoglalását minden esetben írásban kell kikérni, aki az írásbeli állásfoglalást alapvetően 5 munkanap alatt köteles kiadni. Amennyiben további információ beszerzése vagy a Hatósággal történő konzultáció szükségessége ezt nem teszi lehetővé, úgy az adatvédelmi felelős ennek tényét és az állásfoglalás kiadásának várható időpontját köteles 3 napon belül írásban jelezni a kérelmező felé.

2.4. Informatikáért felelős vezető

Amennyiben adatkezelő az adatkezelési vagy adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, akkor az elektronikus információs rendszerek biztonságáért felelős vezető jogosult a közreműködőtől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához jogosult bekérni a közreműködői tevékenységgel kapcsolatos adatokat, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

2.5. Adatkezelést végző személy

- kezeli és megőrzi a feladata ellátása során birtokába került adatokat;
- ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására;
- gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá;
- betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat;
- haladéktalanul jelzi vezetője felé, amennyiben az adatvédelmi ügyben a felettes vagy az adatvédelmi felelős segítségére szorul;
- részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon.

A DUAL GLASS Kft. szervezetében adatkezelést végző személy a tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért.

Aki bizalmas információ, illetve személyes adat birtokába jut, köteles azt titokként időbeli korlátozás nélkül megtartani. A bizalmas információt, személyes adatot nem lehet visszaélésszerűen felhasználni, így különösen tilos a DUAL GLASS Kft. feladatkörén kívül a munkavállaló vagy harmadik fél személyes, illetve üzleti céljainak, közvetlen vagy közvetett előnyök elérésére, valamint adatkezelő vagy az állampolgárok megkárosítására használni.

3. Adatkezelési szabályok

3.1. Az adatvédelem alapelvei

A személyes adatok:

1. *a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság'');*

   b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség");

   c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság");

   d) 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 („pontosság");

   e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság");

   f) 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 („integritás és bizalmas jelleg").

(2) Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek, kell lennie e megfelelés igazolására („elszámoltathatóság").

5. cikk

A törvényesség elve alapján az információs önrendelkezési jog az érintett hozzájárulásának hiányában kizárólag törvényi felhatalmazás alapján korlátozható. Ennek megfelelően adatkezelőnél személyes adat kizárólag az érintett hozzájárulásával, jogos érdekből, szerződés vagy jogi kötelezettség teljesítéséhez, illetve létfontosságú érdek védelmében kezelhető. A kezelt személyes adatok magáncélra való felhasználása tilos.

A célhoz kötöttség elve alapján kizárólag olyan személyes adatot lehet kezelni, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas, továbbá csak olyan mértékben és ideig, amely mértékben és amely ideig ez a cél eléréséhez feltétlenül szükséges. Ezen elv alapján a foglalkoztatottak kizárólag a munkaköri leírásukban meghatározott feladataik ellátása céljából kezelhetnek személyes adatot. Amennyiben az adatkezelés célja megszűnt, az adatot haladéktalanul – legkésőbb az előírt megőrzési idő leteltével – törölni kell. A konkrét célhoz nem köthető adatkezelés tiltott.

Az adatminőség elve alapján adatkezelő köteles az érintett jelzése vagy más, hitelt érdemlő információ alapján a valóságnak nem megfelelő (hibás, hiányos, pontatlan vagy időszerűtlen) adatot helyesbíteni. A helyesbítés módjára az adatkezelést szabályozó jogszabály előírásait kell alkalmazni.

Az érintett előzetes tájékoztatásának kötelezettsége alapján az érintettel az adat felvétele előtt közölni kell az adatkezelés célját, valamint azt, hogy az adatszolgáltatás önkéntes vagy kötelező. Utóbbi esetben a tájékoztatáskor meg kell jelölni az adatkezelést elrendelő jogszabályt.

Az adatbiztonság elve alapján az adat kezelése során biztosítani kell, hogy a személyes adat illetéktelen harmadik személy tudomására ne jusson (bizalmasság), az adat illetéktelen harmadik személy által ne legyen módosítható (sértetlenség), az adat elérhető legyen a feljogosított személyek vagy szervezetek számára (rendelkezésre állás), valamint védeni kell az adatot sérülés és megsemmisülés ellen a megőrzési idő végéig.

3.2. Az adatok kezelésének jogalapja

A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

1. *a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;*

   b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

   c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

   d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

   e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

   f) 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 16 éven aluli gyermek.

GDPR 6. cikk (1)

1. *a) Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.*

   b) Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat, bármely olyan része, amely sérti e rendeletet, kötelező erővel nem bír.

   c) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

   d) Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett, hogy a szerződés teljesítésének - beleértve a szolgáltatások nyújtását is - feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

GDPR 7. cikk

1. *a) Ha a 6. cikk (1) bekezdésének a) pontja alkalmazandó, a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.*

A tagállamok e célokból jogszabályban ennél alacsonyabb, de a 13. életévnél nem alacsonyabb életkort is megállapíthatnak.

1. *a) Az adatkezelő - figyelembe véve az elérhető technológiát - észszerű erőfeszítéseket tesz, hogy ilyen esetekben ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte.*

   b) Az (1) bekezdés nem érinti a tagállamok általános szerződési jogát, például a gyermek által kötött szerződések érvényességére, formájára vagy hatályára vonatkozó szabályokat.

GDPR 8. cikk

Felhatalmazás hiányában adatkezelőnél az adatkezelés alapjául kizárólag az érintett megfelelő tájékoztatásán alapuló, önkéntes és határozott, írásban kifejezett hozzájárulása szolgálhat, amelyben félreérthetetlen beleegyezését adja a szükséges személyes adatok meghatározott célból, meghatározott körben és ideig történő kezeléséhez. A hozzájárulás megszerzése során az érintettet kifejezetten figyelmeztetni kell a beleegyezés önkéntességére.

3.3. Az adatkezelés megkezdésének feltételei

Jogviszony létesítését megelőzően az adatkezelő jelen Szabályzatot és az Adatvédelmi tájékoztatót átadja az új belépő részére, melynek megismerését és titoktartási kötelezettségét nyilatkozat aláírásával igazolja.

Az adatvédelemre vonatkozó jogszabályi környezet megváltozásakor, továbbá, ha adatkezelő adatvédelmét vagy adatbiztonságát, illetve, ha e Szabályzat tartalmát érintő jelentős változás következik be, adatvédelmi továbbképzés tartandó.

Az évente tartandó (rendszeres) oktatásról az adatvédelmi felelős gondoskodik. Az oktatást végző személy az oktatáson részt vett személyekről – a részvétel bizonyíthatósága érdekében – azok aláírásával ellátott jelenléti ívet készít, amelynek 3 évig történő megőrzéséről adatkezelő gondoskodik.

3.3.1. Adatkezelési folyamatok megváltozása, új adatkezelés bevezetése

Adatkezelő az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően köteles az adatvédelmi felelőshöz fordulni a változtatás, illetve az új adatkezelés jogszerűségének, megfelelőségének, célszerűségének és hatékonyságának vizsgálata tárgyában. Az adatvédelmi felelős véleményezési jogkörrel vesz részt a folyamatban.

Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően szükséges azok jelen Szabályzatnak való megfelelőségét vizsgálni és azok csak abban az esetben vezethetők át a gyakorlatba, ha nem ütköznek jelen Szabályzat előírásaiba.

Az adatkezelési folyamatok megváltoztatása esetén vizsgálni kell, hogy az eredeti adatkezelés keretein belüli-e a változás, vagy egy más, új adatkezelés jön létre általa.

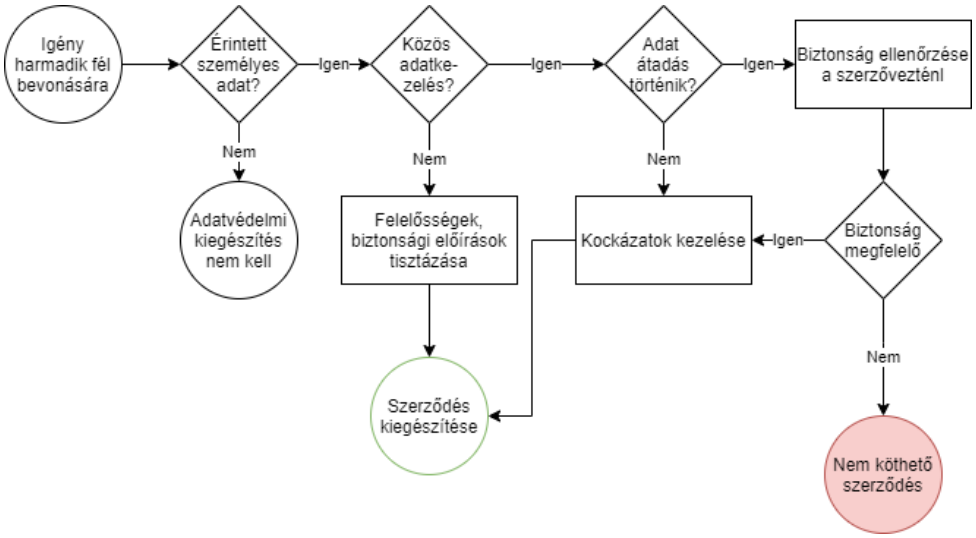
Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően az alábbiakat kell megvizsgálni:

- az adatkezelés célját;
- az adatkezelés jogalapját;
- az érintettek körét;
- az érintettekre vonatkozó adatok leírását;
- az adatok forrását;
- az adatok kezelésének időtartamát;
- a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is;

- az adatkezelő, valamint az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;
- az alkalmazott adatfeldolgozási technológia jellegét;
- az adatvédelmi hatásvizsgálat szükségességét, illetve annak eredményét.

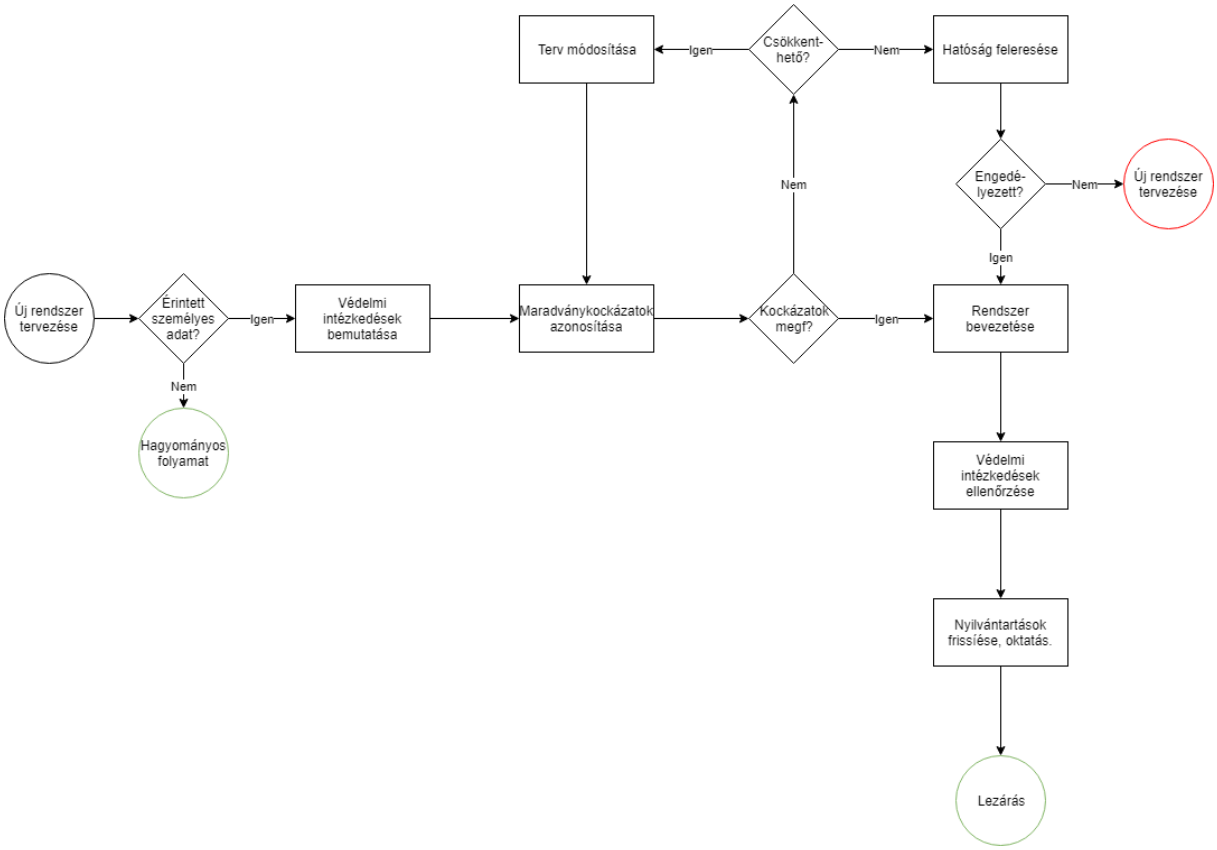
Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően meg kell határozni az azzal érintett munkavállalók körét és el kell végezni a szükséges dokumentummódosításokat.

Szerződéskötés Új szerződés kötése esetén meg kell vizsgálni az adatvédelmi felelős bevonásával, hogy történik-e személyes adat átadása a felek között. Amennyiben igen, akkor ki kell egészíteni a szerződést az adatvédelmi előírásoknak megfelelően, vagy adatfeldolgozási szerződést is kell kötni.



1. ábra. Új szerződéskötés folyamata

Új rendszer bevezetése Új informatikai rendszer bevezetése esetén meg kell vizsgálni az adatvédelmi felelős bevonásával, hogy az tárol-e személyes adatot. Amennyiben igen, a rendszer használatának megkezdése előtt (az adatkezelést megelőzően) az adatvédelmi felelős véleményét ki kell kérni arra vonatkozóan, hogy a rendszer megfelel-e a beépített adatvédelem (Privacy by design) követelményének.



2. ábra. Új rendszer bevezetésének folyamata

3.3.2. Adatvédelmi érdekmérlegelés és hatásvizsgálat

A kockázat forrását, jellegét, egyediségét és súlyosságát felmérő adatvédelmi hatásvizsgálatot kell végezni a bevezetendő adatkezeléssel kapcsolatban, ha a következők legalább egyike teljesül:

- valószínűsíthető, hogy az adatkezelés magas kockázattal jár az érintettekre nézve;
- új technológián alapul az adatkezelés;
- az adatkezelés profilalkotás célját szolgálja;
- az adatkezelés tárgya a személyes adatok különleges kategóriájába tartozik;
- az adatkezelés nyilvános helyek nagymértékű, módszeres megfigyelése;
- az első adatkezelés óta eltelt időre tekintettel szükséges.

A hatásvizsgálat kiterjed legalább...

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára;
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek jogait figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

Ha az adatvédelmi hatásvizsgálat szerint az adatkezelési műveletek olyan magas kockázattal járnak, amelyet Adatkezelő nem képes a rendelkezésre álló technológia és a végrehajtási költségek szempontjából

is megfelelő intézkedésekkel mérsékelni, az adatkezelést megelőzően az adatvédelmi hatósággal konzultálni kell.

A hatásvizsgálat alapját a NAIH oldalán elérhető, nyílt forráskódú szoftver képezi:
`https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html`

A hatásvizsgálat elvégzésébe be kell vonni az adatkezelésben részt vevő részleg legalább egy olyan munkavállalóját, aki a folyamatban tevékenyen részt vesz (felhasználó), valamint egy olyan személyt, aki a technikai (informatikai) oldalt képviseli. Amennyiben szükséges, további résztvevők is bevonhatók a vizsgálatba.

Adatkezelő az adatvédelmi érdekmérlegelés és hatásvizsgálat elvégzésekor az adatvédelmi felelős szakmai tanácsát is köteles kikérni.

3.4. Az adatkezelések összekapcsolásának tilalma

Az egyes adatkezelések főszabályként sem egymással, sem más adatkezelésekkel nem kapcsolhatók össze. Összekapcsolhatók az adatkezelések, ha ezt jogszabály megengedi vagy ahhoz az érintett hozzájárult. Ilyenkor további követelmény, hogy az adatkezelés feltételei minden egyes személyes adatra nézve teljesüljenek. Az adatkezelések jogosulatlan összekapcsolásáért az adattovábbító és a címzett adatkezelő egyaránt felelős.

Az összekapcsolást célzó adatkezelési művelet, amelynek eredményeképpen az egyes adatok együttesen sem válnak személyessé, azaz együtt sem köthetők egy konkrét személyhez, és a személyre következtetni sem lehet, nem minősül a személyes adatok összekapcsolásának.

3.5. Tájékoztatási kötelezettség új adatkezelésekről

Amennyiben adatkezelő új adatkezelést kíván végezni, az adatkezelést végző szervezeti egység vezetője írásban tájékoztatja az adatvédelmi felelőst. A tájékoztatás az adatok felvétele és az adatkezelés megkezdése előtt 30 nappal, kötelező adatkezelés esetén az adatkezelést előíró jogszabály hatályba lépésétől számított 10 napon belül kell végrehajtani.

4. Adatközlések

4.1. Az adatközlések típusai

Személyes adat harmadik személlyel való közlése adattovábbítás vagy nyilvánosságra hozatal formájában valósulhat meg.

Adattovábbításnak minősül, ha az adatot meghatározott harmadik személy tudomására hozzák. A továbbítás történhet egyedi megkeresésre, harmadik személlyel kötött szerződés, illetve jogszabályi előírás alapján.

Az adat nyilvánosságra hozatala esetén az adat bárki számára hozzáférhetővé válik.

4.2. Az adattovábbítás rendjére vonatkozó általános szabályok

Adatkezelő adatkezeléseiből személyes adatot továbbítani az érintett önkéntes, az adatkezelés körülményeit illetően tájékozott hozzájárulása hiányában csak jogszabály felhatalmazása alapján, a jogszabályban meghatározott szerv vagy személy részére, és csak jogszabályban meghatározott adatkörben, a célhoz kötöttség elvének maradéktalan érvényesítésével lehet.

Abban az esetben, amikor valamely adattovábbítási kérelem olyan személyes adatra vonatkozik, amely esetében adatkezelő csak adatfeldolgozásra jogosult, a kérelmet – jogszabály kifejezett eltérő rendelkezése hiányában – el kell utasítani és a kérelmezőt tájékoztatni kell arról, hogy a kért adatokat kitől igényelheti.

Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása, az adattovábbítási feltételeik fennállásának vizsgálata az adatvédelmi felelős hatáskörébe tartozik.

A teljesíthetőség feltételei körében minden esetben meg kell vizsgálni, hogy megvan-e az adatkérés teljesítéséhez szükséges jogalap, a megkeresés megfelel-e a célhoz kötöttség és a szükségesség elvében megfogalmazott kívánalmaknak, teljesül-e az adatminőségre, az adatbiztonságra és az érintett tájékoztatására vonatkozó törvényi követelmény. Ezen feltételeknek minden egyes továbbítandó személyes adat vonatkozásában fenn kell állniuk függetlenül attól, hogy az érintett hozzájárulásán vagy jogszabály alapján történik az adatközlés.

Az adattovábbításra irányuló kérelem abban az esetben teljesíthető, ha az tartalmazza az adattovábbítás célját, jogalapját, a kért adatok pontos körének meghatározását, az érintett személy azonosításához szükséges adatokat.

A személyes adatok személyazonosításra alkalmatlan módon feldolgozott (anonimizált) statisztikai célú továbbítása megengedett.

A személyes adatok külön megkeresésre történő továbbításáról az adatvédelmi felelős adattovábbítási nyilvántartást köteles vezetni.

4.3. Adattovábbítás a szervezeten belül

A DUAL GLASS Kft. szervezetén belül a kezelt személyes adatok kizárólag olyan szervezeti egységhez, illetve munkavállalóhoz továbbíthatók, amelynek vagy akinek feladatai ellátásához azok feltétlenül szükségesek. A személyes adatok adatkezelő egyes szervezeti egységei között is csak a meghatározott feladat elvégzéséhez szükséges mértékben és ideig továbbíthatók, illetve tárolhatók.

Az adattovábbításra vonatkozó iratkezelési, eljárási szabályokat az adathordozótól vagy az adatátvitel módjától függően adatkezelő vonatkozó belső szabályozó eszközei tartalmazzák.

4.4. Adattovábbítás külső megkeresésre

A DUAL GLASS Kft. szervezetén kívüli, személyes adat közlésére irányuló megkeresés csak akkor teljesíthető, ha az érintett ehhez előzetesen hozzájárulását adta, vagy azt jogszabály elrendeli. Az érintett valamely időtartamra és a potenciálisan megkereséssel élő szervek meghatározott körére is adhat előzetes hozzájárulást.

A jogszabályi előírás vagy felhatalmazás alapján történő adattovábbításokat az azokban foglalt rendelkezések alapján és azoknak megfelelően, továbbá az egyéb vonatkozó jogszabályi előírásoknak megfelelően kell teljesíteni.

Az érintett nyilatkozattételétől függetlenül a – amennyiben annak jogszabályi feltételei fennállnak – teljesíteni kell az adattovábbítást az alábbi esetekben:

- a bíróságnak, ügyészségnek, a törvényben meghatározott feladatkörében eljáró nyomozóhatóságnak, a bírósági végrehajtónak, valamint az államigazgatási szerveknek az egyes konkrét ügyek eldöntéséhez szükséges adatokra irányuló megkeresése;
- a nemzetbiztonsági szolgálatok bármely adatra vonatkozó megkeresése;
- jogszabály által az előbbi pontokon kívül elrendelt adattovábbítások.

Az adatkezelő szervezeti egység vezetője az adattovábbítás teljesítése előtt ki kell kérje az adatvédelmi felelős véleményét. Ebben az esetben az adatvédelmi felelős az adattovábbítás feltételeinek fennállását megvizsgálja, majd az adatszolgáltatás teljesíthetőségéről a kérdés hozzá való megérkezésétől számított 3 munkanapon belül véleményt ad.

A nemzetbiztonsági szolgálatoktól érkező megkeresésekre, adatbetekintésekre vonatkozó adatokat – ideértve a megkeresés, betekintés tényét is – és a megtett intézkedésre vonatkozó információkat bizalmasan kell kezelni, ezekről az érintett, illetve más személy vagy szervezet nem tájékoztatható.

Nem teljesíthető olyan adatigénylés, amelynek törvényessége nem állapítható meg.

4.5. Adattovábbítás külföldre

Személyes adat külföldre csak akkor továbbítható, ha ahhoz az érintett kifejezetten hozzájárul vagy azt jogszabály elrendeli.

Utóbbi esetben vizsgálni kell, hogy a címzett ország biztosítja-e az átadott adatok megfelelő védelmét. A személyes adatok megfelelő szintű védelme akkor biztosított, ha az Európai Unió kötelező jogi aktusa azt megállapítja, vagy a harmadik ország és Magyarország között az érintettnek az Infotv. 14. §-ban meghatározott jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban.

Amennyiben az adatkezelés jellegéből adódóan számolni kell a külföldre való adattovábbítással, az érintett figyelmét erre külön fel kell hívni, még személyes adatainak felvétele előtt.

Az Európai Unió tagállamaiba irányuló adattovábbításokat úgy kell tekinteni, mintha azok belföldi adattovábbítások lennének.

4.6. Személyes adatok nyilvánosságra hozatala

A DUAL GLASS Kft-nél kezelt személyes adatok nyilvánosságra hozatala – kivéve, ha azt jogszabály rendeli el, vagy ha az érintett ehhez kifejezetten hozzájárul – tilos.

5. Az érintettek jogainak érvényesítése

5.1. Az érintett jogai

Általános szabály, hogy joggyakorlási kérelmet csak az érintett vagy képviselője nyújthat be.

5.1.1. Tájékoztatás

Az érintett tájékoztatást kérhet személyes adatainak kezeléséről, melyet az adatot ténylegesen kezelő szervezeti egységnek kell megadnia az alábbi szabályok szerint.

A kérelmet minden esetben az adatvédelmi felelős 2 munkanapon belül véleményezi és dokumentálja a kérés teljesíthetőségére vonatkozóan.

A DUAL GLASS Kft-nél az érintettre vonatkozóan kezelt adatokról, adatkezelő által megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről, az adatkezeléssel összefüggő tevékenységekről és az adattovábbítás részleteiről (adatigénylő megnevezése, adattovábbítás célja, adattovábbítás jogalapja, érintettről továbbított adatok köre, adattovábbítás időpontja) szóló tájékoztatást a lehető legrövidebb idő alatt, de legfeljebb a kérelem benyújtásától számított 30 napon belül, írásban, közérthető formában kell megadni az érintett részére.

A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozó tájékoztatási kérelmet adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték vagy a tájékoztatás kérése helyesbítéshez vezetett.

Az érintett személyes adatainak kezelésébe betekinthet, a róla kezelt adatokról feljegyzést készíthet. A betekintés lehetőségét úgy kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg.

A tájékoztatás, valamint a betekintés biztosítása csak akkor tagadható meg, ha a kért adatokat illetékes szerv a megfelelő eljárás keretében előzetesen minősített adattá nyilvánította vagy ha a tájékoztatás megadása, a betekintés biztosítása mások jogait sértené. A megtagadás indokait az érintettel minden esetben írásban, közérthető formában közölni kell.

A tájékoztatást abban a formában szükséges megadni az érintettnek, ahogy azt igényelte, hacsak másképpen nem rendelkezett a kérelemben.

5.1.2. Helyesbítés

Az érintett írásban kérheti a valóságnak nem megfelelő személyes adatainak helyesbítését. Az adat téves mivoltáról az adatkezelőnek meg kell győződni. A kérelmet minden esetben az adatvédelmi felelős 2 munkanapon belül véleményezi és dokumentálja a kérés teljesíthetőségére vonatkozóan.

Teljesíthetőség esetén a téves adatot az azt kezelő szervezeti egység 8 napon belül köteles helyesbíteni.

5.1.3. Törlés

Az érintett – a törvényben elrendelt, kötelező adatszolgáltatáson alapuló adatkezelések kivételével – indoklás nélkül kérheti személyes adatainak törlését. A kérelmet minden esetben az adatvédelmi felelős 2 munkanapon belül véleményezi és dokumentálja a kérés teljesíthetőségére vonatkozóan.

Törölni kell a személyes adatot, ha…

- kezelése jogellenes;
- az érintett azt – kötelező adatkezelés kivételével – kéri;
- az adat hiányos vagy téves és ez az állapot jogszerűen nem korrigálható – feltéve, hogy jogszabály nem zárja ki a törlést;
- az adatkezelés célja megszűnt;
- az adatok tárolásának ideje lejárt;
- azt bíróság vagy a NAIH elrendelte.

5.1.4. Zárolás

Amennyiben az érintett kéri, vagy ha a rendelkezésre álló információk alapján feltételezhető, hogy a törlés sértené az érintett, illetve harmadik személy jogos érdekeit, az adatkezelést végző szervezeti egység vezetője törlés helyett zárolja az adatot. A kérelmet minden esetben az adatvédelmi felelős 2 munkanapon belül véleményezi és dokumentálja a kérés teljesíthetőségére vonatkozóan.

Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta. Törlés helyett zárolásra kerül a sor abban az esetben is, amennyiben joggal feltételezhető, hogy az érintett adat törlése harmadik fél személyes adatához fűződő érdekeit sértheti.

5.1.5. Tiltakozás

Az érintett tiltakozhat személyes adatának kezelése ellen, ha…

- a személyes adat kezelése vagy továbbítása kizárólag az adatkezelő vagy az adatátvevő jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést jogszabály rendelte el;
- a tiltakozás jogának gyakorlását egyébként jogszabály lehetővé teszi.

A kérelmet minden esetben az adatvédelmi felelős 2 munkanapon belül véleményezi és dokumentálja a kérés teljesíthetőségére vonatkozóan, majd döntéséről a kérelmezőt írásban tájékoztatja.

Az érintett tiltakozása elbírálásának időtartamára az adatkezelést fel kell függeszteni. A felfüggesztés ideje alatt az adat az elbírálással összefüggő eljáráson kívül nem használható fel, nem továbbítható, a tároláson kívül azzal egyéb adatkezelési művelet nem végezhető.

Amennyiben megállapításra kerül az érintett tiltakozásának megalapozottsága, az adatkezelést végző szervezeti egység vezetője gondoskodik az adatkezelés – beleértve a korábbi adatfelvételt és adattovábbítást is – megszüntetéséről és az adatok zárolásáról.

Megalapozott tiltakozás megállapítása esetén az adatkezelő szervezeti egység vezetője írásban értesíti mindazokat – így az adatkezelő más szervezeti egységeit is –, akiknek a részére a tiltakozással érintett személyes adatot korábban továbbították. Ennek alapján utóbbiak szintén kötelesek az adatkezelés megszüntetéséről az előző bekezdésben foglaltak szerint gondoskodni.

Ha az érintett az adatkezelőnek a tiltakozás megalapozottsága kérdésében hozott döntésével nem ért egyet vagy ha adatkezelő a tiltakozás iránti kérelem elbírálására rendelkezésre álló határidőt elmulasztja, az érintett a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül bírósághoz fordulhat. E lehetőségre az érintett figyelmét a döntésről való tájékoztatásban fel kell hívni.

5.2. Az érintetti jogok érvényesítésének közös szabályai

A DUAL GLASS Kft. valamennyi foglalkoztatottja és alvállalkozója köteles az érintettek fenti jogainak gyakorlását előmozdítani, abban minden lehetséges segítséget megadni.

A helyesbítésről, a zárolásról és a törlésről értesíteni kell az érintettet, továbbá mindazokat, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára tekintettel az érintett jogos érdekét nem sérti.

Ha adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 30 napon belül adatvédelmi tisztviselője írásban közli a kérelem elutasításának ténybeli és jogi indokait.

A helyesbítés, zárolás vagy törlés iránti kérelem elutasítása esetén az adatvédelmi felelősnek tájékoztatni kell az érintettet a bírósági jogorvoslat, továbbá a NAIH-hoz fordulás lehetőségéről.

Az érintettek jogait kizárólag jogszabály korlátozhatja az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is – továbbá az érintett vagy mások jogainak védelme érdekében.

Az adatvédelmi felelős az érintett jogainak érvényesítésével kapcsolatosan teljesített és elutasított kérelmekről (betekintés, törlés, helyesbítés, tiltakozás tárgyában), valamint az elutasítás részleteiről nyilvántartást vezet és ezekről a jogszabályban meghatározott módon tájékoztatja az adatvédelmi hatóságot (NAIH).

6. Adatfeldolgozó, adatfeldolgozói felelősség

Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

28. cikk (1)

Az adatfeldolgozók jogait és kötelezettségeit, továbbá a vállalt garanciákat az adatfeldolgozóval kötött szerződés rögzíti, melynek kötelező mellékleteként szerepelnek az alábbiak:

Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is -, kivéve

akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza a 32. cikkben előírt intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a (2) és (4) bekezdésben említett feltételeket;

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett III. fejezetben foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az adatkezelőt a 32-36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az első albekezdés a) pontjával kapcsolatban az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti ezt a rendeletet vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

28. cikk (2), (3)

Az adatkezelő határozza meg az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit. Az írásban rögzített adatfeldolgozásra vonatkozó szerződésnek ezeket tételesen tartalmaznia kell. Adatfeldolgozásra nem köthető szerződés olyan személlyel vagy vállalkozással, aki vagy amely érdekelt a feldolgozandó személyes adatokat felhasználó egyéb üzleti tevékenységben.

A szerződésnek a következő elemeket kell tartalmaznia:

- az adatkezelő és az adatfeldolgozó megnevezését;
- az adatfeldolgozási tevékenység megnevezését;
- az átadandó személyes adatok körét;
- automatizált adatfeldolgozás esetén az alkalmazott módszert és lényegét;
- az adatkezelő szavatolását az adatbázis, az átadott személyes adatok jogszerű kezeléséért;
- az adatfeldolgozó nyilatkozatát, hogy kizárólag az adatkezelő utasítása alapján végzi az adatok feldolgozását;
- az adatfeldolgozónak a saját és a szerződésben foglaltaktól eltérő célú adatfelhasználásának tilalmát;
- azt az előírást, hogy az adatfeldolgozó tevékenysége ellátása során más adatfeldolgozót az adatkezelő rendelkezése szerint vehet igénybe;
- az adatfeldolgozó kötelezettségvállalását az adatbiztonsági szabályok megtartására;
- az adatok sorsára vonatkozó rendelkezést a szerződés megszűnésének eseteire;
- a mindezekért való anyagi felelősségvállalást.

Az adatfeldolgozó részére csak olyan személyes adatok adhatók át, amelyek szerepelnek...

– az adatfeldolgozói szerződésben

vagy

– a konkrét adatkezelésre vonatkozó tájékoztatásban.

Az adatfeldolgozói feladat teljesítését követően, illetve a szerződés megszűnésekor az adatfeldolgozó a birtokában lévő személyes adatokat vissza kell szolgáltassa az adatkezelőnek. Az átadott adatok adatfeldolgozó számítástechnikai rendszerében található másolatait visszavonhatatlan módon töröltetni kell, melynek megtörténtéről az adatfeldolgozónak nyilatkoznia kell.

Az adatfeldolgozó tevékenységi körén belül, illetve az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért, zárolásáért és nyilvánosságra hozataláért. Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót adatkezelő írásbeli engedélye nélkül nem vehet igénybe.

Adatfeldolgozó igénybevétele esetén dokumentáltan gondoskodni kell arról, hogy az adatfeldolgozásra irányuló szerződésekben jelen szabályzat ismerete és betartása, továbbá a titoktartás mint kötelezettség a szerződő félre és munkavállalóira is kiterjedjen.

7. Az adatkezelésekkel kapcsolatos nyilvántartások

Az adatkezelő vagy az adatfeldolgozó az a rendeletnek való megfelelés bizonyítása érdekében nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Minden adatkezelő és adatfeldolgozó köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.

Preambulum (82)

Az adatvédelmi nyilvántartás naprakész kimutatás adatkezelő által folytatott, személyes adatokat érintő adatkezelésekről, azok legfontosabb adatairól. Az adatvédelmi nyilvántartás tartalmazza adatkezelő által kezelt, valamennyi személyes adatra vonatkozó adatkezelést.

A nyilvántartásokat elektronikusan olyan mappában kell elhelyezni, amelynek rendszeres mentése biztosított.

Az adatvédelmi nyilvántartást az adatvédelmi felelős vezeti, az adatkezelő szervezeti egységek vezetői által megküldendő nyilvántartások alapján. A nyilvántartást Adatkezelő 5 évig megőrzi.

Adatkezelőnél az adatkezelést végző szervezeti egység vezetőjének a szervezeti egység adatkezelését érintő jogszabályi változásokról és az adatkezelések változásairól írásban tájékoztatni kell az adatvédelmi felelőst.

7.1. Adatkezelési nyilvántartás

Minden adatkezelő szervezeti egység – vagy ha van ilyen, az adatkezelő szervezeti egység adatvédelmi felelőse – az egység által végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:

– *az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;*

– *az adatkezelés céljai;*

– *az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;*

– *olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;*

– *adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet*

azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;

- *ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;*
- *ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.*
- *Az (1) és (2) bekezdésben foglalt kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 11). cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.*

30. cikk

7.2. Adatfeldolgozási nyilvántartás

Minden adatkezelő szervezeti egység – vagy ha van ilyen, az adatkezelő szervezeti egység adatvédelmi felelőse – nyilvántartást vezet a más adatkezelő nevében végzett adatkezelési tevékenységek (adatfeldolgozások) minden kategóriájáról.

A nyilvántartás a következő információkat tartalmazza:

- az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi felelősnek a neve és elérhetőségei;
- az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák, leírása;
- ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.
- Az (1) és (2) bekezdésben említett nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is.
- Az adatkezelő vagy az adatfeldolgozó, valamint – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselője megkeresés alapján a felügyeleti hatóság részére rendelkezésére bocsátja a nyilvántartást.
- Az (1) és (2) bekezdésben foglalt kötelezettségek nem, vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 11). cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

30. cikk

7.3. Adattovábbítási nyilvántartás

A szervezeti egységeknek saját nyilvántartást kell vezetniük az általuk kezelt személyes adatok jogszabály alapján vagy megkeresésre történő továbbításáról.

Az adattovábbítási nyilvántartás célja az érintett tájékozódási jogának érvényesíthetősége, illetve az adatátadások ellenőrizhetősége, ezért a nyilvántartást úgy kell vezetni, hogy abból megállapíthatók legyenek az adattovábbítás részletei. E részletek alapján kell kérésre tájékoztatni az adatvédelmi felelőst arról, hogy mely személyes adatot, kinek a részére, milyen célból és mely jogalapon továbbította a szervezeti egység.

Az Adattovábbítási nyilvántartásban nem kell rögzíteni azon adattovábbításokat…

- amelyeket adatkezelő jogszabályban kötelezően előírtan végez (pl. adatszolgáltatások Nyugdíjbiztosító Igazgatóságnak, Nemzeti Adó és Vámhivatalnak stb.);
- amelyeket az érintett kérelmére indult eljárásban az érintett kérelmében foglaltak megvalósítása érdekében kell teljesíteni (pl. az érintett adatkezelő adatbázisban szereplő személyes adatairól kért adatszolgáltatást, igazolást stb.).

Amennyiben informatikailag megoldható, az adattovábbító szervezeti egység az adattovábbítások jellemzőit kinyerheti az általa kezelt elektronikus rendszerből is, ha az így előállított adatokból megállapíthatók az adattovábbítás tekintetében az érintett tájékoztatásához szükséges információk (adatigénylő megnevezése, adattovábbítás célja, adattovábbítás jogalapja, érintettről továbbított adatok köre, adattovábbítás időpontja). Erről a technikai megoldásról tájékoztatni kell az adatvédelmi felelőst, és a megoldás jellegétől függetlenül az adatszolgáltatási kötelezettségnek eleget kell tenni.

Az érintett tájékoztatásra vonatkozó jogosultsága – miszerint az adattovábbítási nyilvántartás információiból megismerheti, hogy adatszolgáltatás alanya volt-e – a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében a rendőrség, a nemzetbiztonsági szolgálatok részére történt adatszolgáltatás esetén korlátozható vagy kizárható.

Az adattovábbítási nyilvántartásból adatigénylésre jogosult az érintetten kívül a NAIH, az adatvédelmi ellenőrzésre feljogosított személy, bűncselekmény gyanúja esetén az eljárásra hatáskörrel rendelkező nyomozó hatóság és az ügyész; az adatkezelő szerv vezetője és a nemzetbiztonsági szakszolgálatok. Az adattovábbítási nyilvántartásba az arra jogosultak által történő betekintést és az abból történő adattovábbítást dokumentálni kell.

Az adattovábbítási nyilvántartást az adott év folyamán az adattovábbítást végző szervezeti egységnek elektronikusan kell vezetni, év végén az adott évre vonatkozóan ki kell nyomtatni és az adatvédelmi felelős aláírásával kell ellátni. A papíralapú, adott évre vonatkozó adattovábbítási nyilvántartásokat 5 évig meg kell őrizni. Ezen időszakon belül a benne szereplő adatok nem törölhetők.

7.4. Megkeresések nyilvántartása

Az érintettektől saját adataikkal kapcsolatosan érkezett kérelmekre vonatkozó információkat a szervezeti egységeknek is nyilván kell tartani. Az elutasított kérelmeket az elutasítás indoka szerinti bontásban külön szükséges részletezni.

A nyilvántartásban kizárólag az érintett saját személyes adatai kezeléséről történő tájékoztatása, személyes adatainak helyesbítése, illetve – a jogszabály által elrendelt kötelező adatkezelések kivételével – törlése, zárolása iránti megkeresésekre vonatkozó jellemzőket kell feltüntetni.

Az érintett kérelmére adatkezelő tájékoztatást ad az érintett adatainak vonatkozásában az általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről az adatkezeléssel összefüggő tevékenységéről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.

Az érintett tájékoztatásának és egyéb, az információs önrendelkezési jogának érvényesítésével összefüggő kérelmének teljesítését adatkezelő csak a jogszabályokban szabályozott esetekben tagadhatja meg.

Az elutasítás indokai között a törvényi korlátozáson kívül főként olyan okok fordulhatnak elő, amelyek miatt a kérelem gyakorlatilag nem teljesíthető, pl. az adatkezelő a kérelmezővel kapcsolatban adatot nem kezel, az érintett adatainak helyesbítésére irányuló kérelem azért nem teljesíthető, mert a kezelt adatok helyesek, az adat törlése jogszabály által elrendelt kötelező adatkezelés miatt nem lehetséges, a megkeresés illetékesség hiányában nem teljesíthető, illetve a kérelmező nem saját vagy képviseltje adatának megismerésére irányuló kérelmet nyújtott be.

Az adatkezelő szervezeti egységek az érintettek megkereséséről tájékoztatják az adatvédelmi felelős, aki a teljesített és elutasított kérelmekről szintén nyilvántartást vezet. A nyilvántartást 5 évig meg kell őrizni.

7.5. Adatvagyon leltár

Az adatvagyon leltár a személyes adatok kezelésére vonatkozó nyilvántartásoknál szélesebb körű nyilvántartás, melynek célja az, hogy naprakész információval szolgáljon adatkezelő teljes védendő adatvagyonáról, azok tulajdonosairól (adatgazdák) és az egyes vagyonelemek értékéről. Mindezen információk birtokában lehet kialakítani adatkezelő teljes adatkezelésére vonatkozó hatékony és megfelelő szintű védelmet.

A tételes adatvagyon leltárnak tartalmaznia kell adatkezelő teljes információvagyonát (adatok, adatbázisok, ezek biztonsági osztálya, oktatási-, üzemeltetési-, biztonsági segédletek és nyilvántartások, hozzáférési- és kezelési jogosultságok) és szoftvervagyonát (rendszerszoftverek, alkalmazói szoftverek, fejlesztőeszközök, szolgáltatások).

A tételes adatvagyon leltár felvételéről és aktualizálásáról a szervezeti egységek vezetői gondoskodnak, azok másolatát az adatvédelmi felelősnek továbbítják. Az összegyűjtött tételes adatvagyon leltárak az egyéb, adatvédelemmel kapcsolatos dokumentumokkal együtt megőrzendők. Az adatvédelmi felelős számára megengedett a szervezeti egységektől érkező tételes adatvagyon leltárak összefésülve tárolása.

8. Az adatbiztonság általános szempontjai

Adatkezelő köteles gondoskodni az általa kezelt adatok biztonságáról. A kezelt adatokat védeni kell az egyes veszélyeztető tényezőktől, így különösen a jogosulatlan hozzáféréstől, megváltoztatástól, továbbítástól, nyilvánosságra hozataltól, törléstől, bármely sérüléstől, valamint a megsemmisítéstől és a véletlen megsemmisüléstől, továbbá az alkalmazott technika megváltozásából adódó hozzáférhetetlenné válástól.

Az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelent az adatkezelőnek.

Adatbiztonsági szempontból a személyes adatok érzékeny, védendő adatnak minősülnek. Az egyes szükséges adatbiztonsági intézkedések meghatározása céljából adatkezelő kezelésében lévő minden egyes adatállományt a védelmi igény szempontjából értékelni kell és a megfelelő biztonsági osztályba kell sorolni.

8.1. Automatizált adatkezelés

Az egyes adatkezelések biztonsági fokozatának megállapításához az adatok minősítésének figyelembevételén kívül elemezni kell...

- az adatkezelésnek adatkezelő munkája során betöltött szerepét;
- a kezelt személyes adatok jogosulatlan megismerésével, megváltoztatásával, törlésével, a hardver- és szoftvereszközök megrongálásával járó kockázatot és a várható kárt figyelemmel arra, hogy az adatkezelés hiánya vagy az abban bekövetkezett sérülés milyen mértékben akadályozza adatkezelő munkavégzését;
- azt, hogy helyreállítható-e a sérült adatállomány, valamint az esetleges helyreállítás ráfordítási igényeit;

- a személyes adatok reprodukálásához szükséges adatforrások rendelkezésre állását, a manuális háttérnyilvántartásokból az elveszített adatok pótlásának lehetőségét;
- azt, hogy a kezelt személyes adatok jellegére tekintettel indokolt-e megkülönböztetett biztonsági előírásokat alkalmazni;
- az adatbiztonságot veszélyeztető más kockázati elemeket;
- azt, hogy a védelemhez szükséges feltételrendszer megteremtéséhez és fenntartásához biztosítottak-e a szükséges erőforrások.

A szükséges biztonsági intézkedéseket meg kell tenni a papíralapú, valamint a számítógépen tárolt és feldolgozott adatok védelméért is. A számítógépen, hálózaton, illetve adathordozón tárolt személyes adatok biztonságának megteremtése és fenntartása céljából különös figyelmet kell fordítani az információbiztonság megteremtésére és folyamatos szinten tartására (pl. biztonsági mentések, archiválás, tűzvédelem, áramellátás szünetmentessége, vírus- és hozzáférés-védelem, adathordozók biztonságos tárolása).

Számítógépen tárolt személyes adatok kezelése során adatkezelőnek biztosítania kell...

- a jogosulatlan adatbevitel megakadályozását;
- az automatikus feldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
- annak ellenőrizhetőségét és megállapítását, hogy mely személyes adatokat, mikor és ki vitt be az automatikus adatfeldolgozó rendszerbe;
- a megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával kinek továbbították vagy továbbíthatják;
- a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát;
- jelentés készítését a fellépő hibákról.

Az Üzletmenet folytonossági és katasztrófaelhárítási tervben (BCP-DRP) foglaltakat jelentősebb változás esetén, de legalább évente szükséges felülvizsgálni, illetve aktualizálni.

A fizikai biztonság megteremtéséhez az alábbi intézkedéseket szükséges megtenni:

- Az adathordozó eszközök elhelyezésére szolgáló helyiségeket, épületeket, épületrészeket úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűzkár, vízkár vagy természeti csapás ellen.
- Azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését – a minősítéstől függően – korlátozni és ellenőrizni kell. A belépésre adott felhatalmazásnak összhangban kell lennie az adott személy munkaköri feladataival, illetve az ott kezelt adatokhoz történő hozzáférési jogosultságával.
- A számítástechnikai eszközzel olvasható és a manuális adathordozók tárolását, hozzáférését és felhasználását ellenőrizni kell. Különös figyelmet kell fordítani arra, hogy a biztonságos területről kivitt eszközök maradványadatokat ne tartalmazzanak.
- Az adathordozókról és mozgásukról, azok tartalmáról és felhasználásáról nyilvántartást kell vezetni.
- Annak érdekében, hogy lecsökkenjen a jogosulatlan hozzáférés, az információvesztés és információrongálás kockázata, mind munkaidőben, mind azon kívül bevezetésre kerül az „üres asztal” szabály a papíralapú anyagokra és a hordozható adattárolókra, valamint a „zárolt képernyő” szabály az információfeldolgozó eszközökre. E szabályok részletesen:
  - a papíranyagokat és a számítógépek adathordozóit megfelelő, zárható szekrényben vagy más, hasonlóan biztonságos bútorban kell tárolni, amikor éppen nincsenek használatban, különösen a munkaidőn kívüli időszakokban;
  - személyi számítógépeket, munkaállomásokat, nyomtatókat és fénymásolókat nem szabad „bejelentkeztetve” hagyni, amikor felügyelet nélkül maradnak, illetve használaton kívül

kulcsreteszekkel, jelszavakkal vagy más óvintézkedésekkel legyenek védve (munkanap végén kikapcsolás).

Az üzemeltetési biztonság kialakítására az alábbi intézkedéseket szükséges megtenni:

- Az adatkezelő eszközöket üzemeltető személyek feladatait egyértelműen meg kell határozni. Egyéb, a feladatoktól eltérő tevékenységet csak külön, erre irányuló egyedi vezetői felhatalmazás alapján lehet végezni.
- Az adatkezelő eszközök előre nem látható üzemzavara esetére olyan tervet kell kidolgozni, amellyel annak hatása ellensúlyozható.
- Az adatkezelést végző eszközök felhasználói kötelesek...
  - az aktív keresési folyamatok lezárására, ha a munka befejeződött, hacsak alkalmas reteszelő mechanizmussal nem tehetők biztonságossá (pl. jelszóval védett képernyővédővel);
  - az adathordozó eszközöket a jogosulatlan használattal szemben biztonságossá tenni úgy, hogy elzárják azokat.

A technikai biztonság érdekében szükséges intézkedések:

- Az adatok és programok véletlen vagy szándékos megrongálását meg kell akadályozni.
- Az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell.
- Az adatbevitel során a bevitt adatok helyességét ellenőrizni kell.
- Közvetlen adathozzáférés kezdeményezésének jogosultságát ellenőrizni kell.
- Pontosan meg kell határozni (munkakörönként, ill. személyenként) az egyes adatokhoz való hozzáférést.

8.2. Papíralapú adatkezelés

A manuális kezelésű adatok biztonsága érdekében tűz- és vagyonvédelmi szempontból biztosítani kell, hogy a papíralapú dokumentumok (iratok) jól zárható, száraz, tűz- és vagyonvédelmi riasztóberendezéssel ellátott helyiségben legyenek elhelyezve. Hozzáférés-védelmi szempontból gondoskodni kell arról, hogy a folyamatos, aktív kezelésben lévő iratokhoz csak az illetékes, illetve titoktartási nyilatkozatot tett alkalmazottak férhessenek hozzá.

A manuális kezelésű iratok archiválását rendszeres időközönként el kell végezni. A megőrzési időt jól látható formában szükséges feltüntetni az iratokat tároló mappán, illetve dobozon. Az iratokat a meghatározott adatkezelési határidő elteltével haladéktalanul át kell adni megsemmisítésre. A személyes adatokat tartalmazó iratok megsemmisítéséről jegyzőkönyvet kell készíteni és azt megőrzés céljából át kell adni az adatvédelmi tisztviselőnek. A megőrzés elektronikus (szkennelt) formában is végezhető.

Az archiválást és a megsemmisítést az információbiztonsági rendszerben (IBR vagy IBIR) foglaltaknak megfelelően kell végrehajtani. Az egyes szükséges biztonsági intézkedésekre vonatkozó részletes szabályok több, különböző szabályzásban kerültek rögzítésre, melyeket a „Kapcsolódó szabályozások és dokumentumok” című fejezet tartalmazza.

9. A jogellenes adatkezelés következményei

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) a személyes adatok kezelésével kapcsolatos jogsérelem esetén felszólíthatja adatkezelőt a jogsérelem orvoslására a szükséges intézkedések megjelölésével. Amennyiben a jogsérelem orvoslására a felszólítás alapján nem került sor, a hatóság jelentést készíthet és adatvédelmi hatósági eljárást indíthat. A hatóság jelentése bíróság vagy más hatóság előtt nem támadható meg.

9.1. Szankciók

Az adatvédelmi hatósági eljárásban hozott határozatában a Hatóság...

- elrendelheti a személyes adatok helyesbítését, zárolását, törlését, megsemmisítését;
- megtilthatja az adatok jogellenes kezelését, feldolgozását, külföldre történő továbbítását vagy átadását;
- elrendelheti az érintett tájékoztatását;
- akár húszmillió euróig vagy az előző pénzügyi év cégcsoportra vetített teljes éves világpiaci forgalmának 4 %-át kitevő (amelyik magasabb) összegig terjedő közigazgatási bírságot szabhat ki.

A bírság akár ismételten, jogsértésenként is kiszabható. A Hatóság a határozatát az adatkezelő azonosító adataival együtt nyilvánosságra hozhatja. Ha a Hatóság eljárása során fegyelmi vétség, szabálysértés vagy bűncselekmény elkövetésének alapos gyanúját észleli, fegyelmi-, szabálysértési- vagy büntetőeljárást köteles kezdeményezni.

A Ptk. 2:51. § (1) bekezdése alapján az érintett fél a fentieken felül a következő igényeket is támaszthatja:

- *a jogsértés megtörténtének bírósági megállapítását;*
- *a jogsértés megszüntetését és a jogsértő eltiltását a további jogsértéstől;*
- *azt, hogy a jogsértő adjon megfelelő elégtételt, és ennek biztosítson saját költségén megfelelő nyilvánosságot;*
- *a sérelmes helyzet megszüntetését, a jogsértést megelőző állapot helyreállítását és a jogsértéssel előállított dolog megsemmisítését vagy jogsértő mivoltától való megfosztását;*
- *azt, hogy a jogsértő vagy jogutódja a jogsértéssel elért vagyoni előnyt engedje át javára a jogalap nélküli gazdagodás szabályai szerint.*

Sérelemdíj a személyiségi jog megsértésével okozott nemvagyoni sérelem miatt követelhető a kártérítési felelősség szabályai szerint. A sérelemdíj megállapításához csak a jogsértés tényét kell bizonyítani, egyéb hátrányt nem.

Ptk. 2:52. §

- *Akit személyiségi jogában megsértenek, sérelemdíjat követelhet az őt ért nem vagyoni sérelemért.*
- *A sérelemdíj fizetésére kötelezés feltételeire – különösen a sérelemdíjra köteles személy meghatározására és a kimentés módjára – a kártérítési felelősség szabályait kell alkalmazni, azzal, hogy a sérelemdíjra való jogosultsághoz a jogsértés tényén kívül további hátrány bekövetkeztének bizonyítása nem szükséges.*
- *A sérelemdíj mértékét a bíróság az eset körülményeire – különösen a jogsértés súlyára, ismétlődő jellegére, a felróhatóság mértékére, a jogsértésnek a sértettre és környezetére gyakorolt hatására – tekintettel, egy összegben határozza meg.*

A személyiségi jogok megsértése esetén a jogsértőtől kártérítés követelhető.

Ptk. 2:53. §

Aki személyiségi jogainak megsértéséből eredően kárt szenved, a jogellenesen okozott károkért való felelősség szabályai szerint követelheti a jogsértőtől kárának megtérítését.

A büntetőeljárás az egyéni felelősségre vonást célozza, tehát a szabályokat megsértő munkatárs, illetve a vezető kerül közvetlenül felelősségre vonásra.

Btk. 219. §

Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva...

- *jogosulatlanul vagy a céltól eltérően személyes adatot kezel;*
- *az adatok biztonságát szolgáló intézkedést elmulasztja, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.*

Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti. A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges személyes adatra követik el.

A Munka Törvénykönyve (2012. évi I. tv.) rendelkezései alapján a munkáltató a Szabályzat és az adatkezelésre vonatkozó jogszabályok be nem tartását akár rendkívüli felmondással is szankcionálhatja, illetve a vétkesség függvényében a bekövetkezett teljes kár megfizetésére is igényt tarthat.

10. Incidensek kezelése

10.1. Az adatvédelmi incidens bejelentése

Az a munkavállaló, aki az adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst vagy annak gyanúját, azaz a személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen kiszivárgást, megsemmisülést vagy sérülést észlel, azt köteles haladéktalanul (közvetlenül vagy az ügyvezető igazgatón keresztül) az adatvédelmi felelősnek jelenteni. Az adatvédelmi felelős feladata incidens esetén azt 72 órán belül a NAIH-nak bejelenteni, megadva a nevét, telefonszámát és emailcímét, a cég elérhetőségeit, az incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e. A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából a hatóság lényegesnek ítél.

Amennyiben az adatvédelmi incidens informatikai rendszert érintően következett be, akkor a rendszergazdát is tájékoztatni kell.

10.2. A bejelentés megvizsgálása és az incidens kezelése

Az adatvédelmi felelős – informatikai rendszert érintő incidens esetén a rendszergazdával együttműködve – a bejelentést megvizsgálja, a bejelentőtől adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb egy napon belül teljesíteni.

Az adatszolgáltatásnak tartalmaznia kell:

- az incidens bekövetkezésének időpontját és helyét,
- az incidens leírását, körülményeit, hatásait,
- az incidens során kompromittálódott adatok körét, számosságát,
- a kompromittálódott adatokkal érintett személyek körét,
- az incidens elhárítása érdekében tett intézkedések leírását,
- a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Amennyiben az adatszolgáltatás alapján az adatvédelmi incidens vizsgálatot igényel, annak végrehajtására az adatvédelmi felelős felkéri a ügyvezetőt, informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazdát is bevonva. Az adatvédelmi felelős szaktanácsadóként közreműködik a vizsgálat lefolytatásában.

Az adatszolgáltatás alapján és az adatvédelmi felelős – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazda segítségével – javaslatot tesz az adatvédelmi incidens

elhárításához szükséges intézkedésekről az adatok kezelését vagy feldolgozását végző területnek, továbbá – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében – az adatgazdának.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző terület vezetője dönt.

Az adatvédelmi incidens elhárítása érdekében megvalósított egyes intézkedésekről az adatok kezelését vagy feldolgozását végző terület vezetője az intézkedések végrehajtását követő egy munkanapon belül köteles az adatvédelmi felelőst tájékoztatni.

10.3. Az incidensek nyilvántartása

Az adatvédelmi incidensekről az adatvédelmi felelős nyilvántartást vezet.

A nyilvántartásba rögzíteni kell:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens elhárítására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatvédelmi felelős a nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 10 évig köteles megőrizni.

11. Oktatás

Az új belépő munkatársak az adatkezelésben csak a belépést követő oktatás megtörténte és titoktartási nyilatkozat aláírása után vehetnek részt.

A személyes adatok kezelésében részt vevő munkavállalók számára az adatvédelmi tudatosság növelése érdekében évente oktatást kell tartani. Az oktatás megtartható az éves információbiztonsági oktatással egyidőben is. Az oktatásról jegyzőkönyvet kell készíteni, amit a személyi anyagban vagy az adatvédelemmel kapcsolatos iratmappában szükséges tárolni.

Új rendszer bevezetése vagy jelentős változás esetén az adatkezelésben részt vevők, illetve a hosszabb távollétről visszatérő munkavállalók számára rendkívüli oktatást kell tartani.

Amennyiben az oktatást nem az adatvédelmi felelős tartja meg, a tematikával kapcsolatban írásban ki kell kérni a véleményét.