

TRUPLAST HUNGÁRIA Műanyagtechnikai KFT

Adatvédelmi Tájékoztató és Adatvédelmi Szabályzat

Jakabszállás, 2018. május 24.

I. Adatvédelmi Tájékoztató és Adatvédelmi Szabályzat (egységes szerkezetben)

1. Bevezető

1.1. Az adatvédelmi tájékoztató célja:

A TRUPLAST KFT (székhely: 6078 Jakabszállás, Petőfi Sándor u. 44.) mint adatkezelő az adatkezelési tájékoztatókban részletezettek szerint a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendeletnek („Általános Adatvédelmi Rendelet”), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek („Infotv.”), továbbá az egyéb jogszabályoknak megfelelően kezeli.

Az adatvédelmi tájékoztató célja, hogy a mindenkor hatályos adatvédelmi jogszabályokban foglaltaknak megfelelően és az Érintettek adatait megfelelő szinten kezelje, védje.

A TRUPLAST KFT (továbbiakban: KFT) a rendelkezésére álló, a rendelkezésére bocsátott természetes személyek személyes adatait bizalmasan, a hatályos jogszabályi előírásokkal összhangban kezeli, gondoskodik azok biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket, valamint kialakítja azokat az eljárási szabályokat, amelyek a vonatkozó jogszabályi rendelkezések és más ajánlások érvényre juttatásához szükségesek.

Jelen Tájékoztató meghatározza a személyes adatok védelmével kapcsolatos politikát és mindennapos gyakorlatot, továbbá lefekteti azt, hogy milyen célokra, és hogyan használja fel a rendelkezésére bocsátott adatokat.

1.2. Az adatkezelő adatai, az adatvédelemért felelős munkatárs elérhetősége:

Cégnév: TRUPLAST HUNGÁRIA Műanyagtechnikai KFT

Székhely (levélcím): 6078 Jakabszállás, Petőfi Sándor u. 44.

Cégjegyzékszám:

Internet: www.truplast.de

Adatvédelemért felelős munkatárs neve, elérhetősége: Tóthné Szlovák Marianna

Telefon: +36 30 438 - 2545

E-mail: szlovak.m@truplast.hu

1.3. Az adatkezeléshez kapcsolódó gazdasági tevékenység bemutatása:

A TRUPLAST KFT egy nemzetközi cégcsoport magyarországi tagjaként műanyag-gyártással, elsősorban porszívó gégecsövek és porszívófejek előállításával foglalkozik, az alkalmazott technológia elsősorban extrudálás, valamint fröccsöntés.

Főtevékenység: Műanyag lap, lemez, fólia, cső, profil gyártása

A KFT 2002 óta működik Magyarországon, méretei alapján jelenleg a KKV szektorba tartozik.

A KFT személyes adatokat elsősorban a munkavállalói körében kezel, továbbá a leginkább céges vevői és beszállítói oldali kapcsolattartók (természetes személyek) vonatkozásában.

2. A Tájékoztatásban érintett alapelvek, az adatkezelés elvei

2.1. Jogszerűség, tisztességes eljárás és átláthatóság:

Az adatok kezelését **jogszerűen** és **tisztességesen**, valamint az érintett számára **átlátható** módon kell végezni.

A KFT biztosítja az Érintett jogainak érvényesülését, és megteszi a szükséges intézkedéseket annak érdekében, hogy az adatkezelés annak minden szakaszában jogszerű legyen.

2.2. Célhoz kötöttség:

Személyes adat kizárólag **meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében** kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak.

Személyes adat akkor kezelhető, ha ahhoz az érintett – különleges adat esetén írásban - hozzájárul, vagy azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete elrendeli.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához **elengedhetetlen, a cél elérésére alkalmas**.

Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.

2.3. Adattakarékosság:

A személyes adatok az adatkezelés céljai szempontjából **megfelelőek** és **relevánsak** kell, hogy legyenek, és a **szükségesre** kell korlátozódniuk.

Az adatok körét a célhoz szükséges minimumra kell korlátozni.

2.4. Az adatok pontossága és teljessége:

Biztosítani kell az adatok pontosságát, teljességét és – ha szükséges – naprakészségét.

A KFT törekszik arra, hogy az általa kezelt adatok pontosak és naprakészek legyenek.

A személyes adatoknak pontosnak és szükség esetén **naprakésznek** kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

2.5. Korlátozott tárolhatóság:

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 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.

A személyes adat csak a cél megvalósulásához szükséges mértékben és **ideig** kezelhető.

Biztosítani kell azt, hogy az adatok tárolása **a lehető legrövidebb időtartamra korlátozódjon**. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg.

2.6. Integritás és bizalmi jelleg:

A személyes adatok kezelését oly módon kell végezni, hogy **megfelelő technikai vagy szervezési intézkedések alkalmazásával** biztosítva legyen a személyes adatok megfelelő **biztonsága**, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

A KFT a személyes adatokat bizalmasan kezeli, az adatok megőrzése érdekében az adattároláshoz, feldolgozáshoz kapcsolódó informatikai és egyéb biztonságos adatkezelést elősegítő minden intézkedést megtesz.

2.7. A Tájékoztató az alábbi hatályos jogszabályok alapján került kialakításra:

Magyarország Alaptörvénye

2011. évi CXII törvény az információs önrendelkezési jogról és az információszabadságról szóló tv.

2016/679/EU Rendelet (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (GDPR)

2013. évi V. tv. a Polgári Törvénykönyvről

2012. évi I. tv a Munka Törvénykönyvéről

2003. évi C. tv. az Elektronikus Hírközlésről

2013. évi CLXV. tv. a Panaszokról és a Közérdekű bejelentésekről

2003. évi XCII. tv. az adózás rendjéről

2008. évi XLVIII. tv. a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól

2000. évi tv. a számvitelről

2017. évi CLI törvény az adóigazgatási rendtartásról

1995. évi LXVI. törvény a köziratokról, közlevéltárakról és magánlevéltári anyag védelméről

2005. évi CLXIV. törvény a kereskedelemről

2012. évi LXXXVIII. törvény a termékek piacfelügyeletéről

2009. évi LXXVI. törvény a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól

Jogszabályok elérhetősége: net.jogtar.hu

3. Az adatkezelés jogalapjai

Figyelemmel arra, hogy KFT több célból is kezelhet személyes adatot, az adatkezelés jogalapja is többféle lehet. Annak érdekében, hogy a személyes adatok kezelése **jogszerű** legyen, annak

- az **érintett hozzájárulásán kell alapulnia**, vagy
- valamely **egyéb jogszerű, jogszabály által megállapított** – akár e rendeletben, akár más tagállami jogban foglalt – **alappal kell rendelkeznie**, ideértve az
- adatkezelőre vonatkozó **jogi kötelezettségeknek való megfelelés szükségességét**,
- az érintett által kötött esetleges **szerződés teljesítését**, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges;
- az adatkezelés **közérdekű** vagy az adatkezelőre ruházott **közhatalmi jogosítvány** gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- az adatkezelés az adatkezelő vagy egy harmadik fél **jogos érdekeinek érvényesítéséhez** szükséges.

3.1. Az érintett hozzájárulása (GDPR 6. cikk (1) bek. a) pont)

Az adatkezelés jogalapja elsősorban az Érintett hozzájárulása. Az Érintett a hozzájárulását azzal adja meg, hogy a KFT-vel kapcsolatba lép, és kezdeményezi a kapcsolatfelvételt.

Amennyiben az Érintett adatait a KFT felveszi, a hozzájárulást az Érintett az adatkezelési tájékoztató elfogadásával adja meg.

Online adatfelvétel esetén a hozzájárulás megadása jelölőnégyzet elfogadásával történik.

A hozzájárulás minden esetben önkéntes. A KFT szolgáltatásai és termékei máshol elérhető, helyettesíthető, az esetek jelentős részében nélkülözhető szolgáltatások és termékek, így az Érintett önkéntes elhatározásán alapul, hogy a KFT-vel kapcsolatba lép, és igénybe veszi a szolgáltatásokat/termékeket, vagy érdeklődik a szolgáltatások/termékek igénybe vétele felől. A KFT az Érintettet minden esetben tájékoztatja az adatkezelésről.

3.2. A KFT és az Érintett között létrejött szerződés (GDPR 6. cikk (1) bek. b) pont)

Amennyiben az Érintett a KFT-vel szerződést köt, a szerződésben és a kapcsolódó nyomtatványokon megadja azon adatait, amelyek szükségesek a szerződés teljesítéséhez.

A szerződés minden esetben tartalmazza az Érintett tájékoztatását az adatkezelésről.

Amennyiben az Érintett a szerződéskötést megelőzően megadja adatait a szerződés előkészítése, megkötése, az igények felmérése érdekében a KFT ezen lépések érdekében kezeli az Érintett adatait, az Érintett tájékoztatása mellett.

A szerződés megkötése minden esetben önkéntes. Az Érintett a szolgáltatásokról és az adatkezelésről szóló tájékoztató alapján hozhat döntést arról, hogy a szerződést megkötö-e, vagy sem.

A jelen pont szerinti esetben az adatkezelés a szerződés teljesítése és az Érintett által kezdeményezett lépések megtétele érdekében történik, a GDPR hivatkozott pontja alapján.

Amennyiben az Érintett valamely, a KFT által kért, vagy szerződésben megjelölt adat kezeléséhez nem járul hozzá, jogában áll az adat megadását megtagadni. Amennyiben az adat kezelése jogszabály alapján kötelező, vagy az adat hiányában a szerződés nem teljesíthető, az adat megadásának hiányában a szerződés nem jön létre. Erről az Érintett minden esetben tájékoztatást kap.

3.3. Jogszabályban foglalt kötelezettség teljesítése (GDPR 6. cikk (1) bek. c) pont)

Az adatkezelés jogalapja bizonyos esetekben jogszabály rendelkezése.

A főbb, adatkezelést is előíró jogszabályok az Tájékoztató 2.7. pontjában vannak meghatározva.

3.4. A KFT vagy egy harmadik fél jogos érdekeinek érvényesítése (GDPR 6. cikk (1) bek. f) pont)

Amennyiben az adatkezelés szükséges a KFT vagy harmadik fél jogos érdekének érvényesítéséhez, az adatot a KFT felhasználja ezen érdek érvényesítése céljából.

A jelen bekezdés szerinti adatkezelés kivételes, arra csak egyedi elbírálás (ún. érdekmérlegelési teszt) alapján kerül sor, a jelen Tájékoztatóban meghatározott esetekben.

A KFT az érdekmérlegelési teszt során minden esetben pontosan azonosítja azt az érdeket, amely indokolja az adatkezelést, és megvizsgálja, hogy más módon (jogalappal) az adatkezelés megvalósítható-e. Az érdekmérlegelési teszt során minden esetben vizsgálatra kerül az érintett jogainak esetleges sérelme, és azon intézkedések lehetősége, amelyek ezen jogok esetleges sérelmét csökkentik, illetve az érintettnek segítséget nyújtanak a jogaik érvényesítésében

4. Az egyes adatkezelések részletezése

4.1. A munkavállalók személyes adatainak nyilvántartása és kezelése

Az adatkezelés leírása:

A munkavállalók adatainak kezelése és nyilvántartása a munkaszerződés teljesítése, munkabérek és egyéb juttatások kifizetése, számviteli-, adózási-, társadalombiztosítási kötelezettségek teljesítése céljából.

Kezelt adatok köre:

Az aktuálisan hatályos munkaügyi-, számviteli-, adó- és társadalombiztosítási jogszabályok által kötelezően előírt személyes adatok.

Az adatkezelés célja:

Az adatkezelés célja a munkabérek és egyéb juttatások kifizetése (folyósítása), adó-, társadalombiztosítási és egyéb számviteli jogszabályokban foglaltak teljesítése. Munkaszerződésben vállaltak teljesítése.

Az adatkezelés jogalapja:

GDPR 6. cikk (1) (b) pontja szerinti jogalap (munkaszerződés szerződése teljesítése).
GDPR 6. cikk (1) (c) pontja szerinti jogalap (jogi kötelezettség teljesítése)

Az adatkezelés időtartama:

A vonatkozó hatályos jogszabályok szerinti kötelező iratmegőrzési szabályok szerint.

A munkahelyi adatkezelésre vonatkozó speciális szabályok, valamint a Hatósági ajánlások a Tájékoztató 5. fejezetében kerültek feltüntetésre. A KFT ezen ajánlásokat betartva végzi munkavállaló adatainak kezelését.

4.2. A megrendelők, valamint a beszállító partnerek magánszemély kapcsolattartóinak személyes adatai:

Az adatkezelés leírása:

Amennyiben a személyes adat a nem természetes személy (egy cég) szerződő partnerünk munkavállalójáé, akkor a személyes adatokat a szerződéses partnerük továbbítja felénk a kapcsolattartáshoz szükséges mértékben.

Ezen adatkezelési körben a személyes adatok kezelése kizárólag a szerződés teljesítése céljából, a szerződő partnerünk és saját üzleti érdekeink céljából történik, és ezen adatokat kizárólag ezzel kapcsolatban használjuk fel.

Kezelt adatok köre:

A céges megrendelőkkel, illetve a beszállítókkal kötött szerződések magánszemély kapcsolattartói.

Név, beosztás, telefonszám, e-mail cím.

Az adatkezelés célja:

Az adatkezelés célja a megrendelések, illetőleg a szállítások lebonyolítása során a kapcsolattartás biztosítása.

Az adatkezelés jogalapja:

GDPR 6. cikk (1) (b) pontja szerinti jogalap (szerződése teljesítése) természetes személy szerződéses partner személyes adatainak kezelésére.

Ilyenkor a szerződéses partnerünk a GDPR 6. cikk (1) (b) pontja alapján szerzi meg és kezeli a személyes adatokat, míg cégünk a GDPR 6. cikk (1) (b és f) pontja szerint a szerződés teljesítése, továbbá a szerződéses partnerünk jogos érdekében (továbbá cégünk jogos érdekében) vesszük át tőle és kezeljük a személyes adatokat a célhoz szükséges mértékben és ideig.

Az adatkezelés időtartama:

Az adatkezelés addig tart, amíg az üzleti kapcsolat az érintett céggel és annak kapcsolattartójával fennáll.

4.3. Munkaidő-nyilvántartó kártyás beléptető rendszer („Zeus”)**Az adatkezelés leírása:**

A munkavállalók munkaidő-nyilvántartását egy kártyás be- illetve kiléptető rendszer regisztrálja. A rendszer használatát a német anyavállalatunk vette meg az ISGUS GmbH-től, aki üzemelteti ezt a rendszert. Ennek egy modulja került hozzánk telepítésre és testreszabásra.

Kezelt adatok köre:

A rendszer egy szoftveren keresztül bérelszámolási adatokkal együtt tartja nyilván a munkavállalók személyes adatait. A közvetlen azonosítás a munkavállalók adószáma alapján történik.

Az adatkezelés célja:

Az adatkezelés célja a munkavállalók munkaidő-nyilvántartása, a munkahelyre való érkezésük és távozásuk dokumentálása.

Az adatkezelés jogalapja:

GDPR 6. cikk (1) (b) pontja szerinti jogalap (munkaszerződése teljesítése)

GDPR 6. cikk (1) (f) pontja (a munkaadó jogos érdeke)

A munkavállalók a munkaviszony létesítésekor aláírtak (aláírnak) egy ezzel kapcsolatos tájékoztatót a rendszerről, valamint a beléptető kártya átvétele is dokumentálásra kerül.

Az adatkezelés időtartama:

Amennyiben a munkavállaló munkaviszonya megszűnik, a rendszerből adatai törlésre kerülnek.

A nyilvántartott adatok a munkaidő-nyilvántartási iratok kötelező megőrzési idejére korlátozódnak. Rendszeres belépés esetén a belépésre való jogosultság megszűnésekor haladéktalanul.

4.4. A munkavállalók pályázatainak kezelése:

Az adatkezelés leírása:

A munkavállalók álláshirdetésre való jelentkezéskor elküldik a KFT részére pályázataikat (önéletrajzukat, motivációs leveleiket).

Kezelt adatok köre:

E-mail cím, név, telefonszám, önéletrajzokban szokásos adatok (lakcím, születési idő, iskolai végzettségek, családi állapot, szakmai tapasztalatok), motivációs levél, bizonyítvány másolatok.

Az adatkezelés célja:

Az önéletrajzok, pályázatok esetében az adatkezelés célja az, hogy a meghirdetett munkakört betöltsék, illetve ezen dokumentumok segítik és támogatják a munkaerő-kiválasztási folyamatot.

Az adatkezelés jogalapja:

A jelentkező a pályázatának (önéletrajz, motivációs levél) elküldésével ráutaló magatartással hozzájárul adatainak a felvételi eljárás keretében történő kezeléséhez.

GDPR 6. cikk (1) (a) pontja szerinti hozzájárulás (a pályázatok megőrzése esetén).

A pályázatok megőrzése esetén a hozzájárulást a KFT a felvételi eljárás lezárását követően kéri a jelentkezőktől.

Az adatkezelés időtartama:

Ha a KFT, mint munkáltató a jelentkezők közül kiválaszt egy személyt a meghirdetett állásra, akkor megszűnt az adatkezelés célja, és a ki nem választott jelentkezők személyes adatait törölni kell.

Ezzel egyidejűleg fennáll a KFT törlési kötelezettsége abban az esetben is, ha az érintett még a jelentkezés során meggondolja magát, visszavonja pályázatát.

A KFT csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrzi meg a pályázatokat. Ebben az esetben az adatkezelés időtartama a hozzájárulás megadását követő 3 év.

4.5. A KFT-vel szerződéses kapcsolatban álló adatfeldolgozók:

„**Adatfeldolgozó**” meghatározása: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében – szerződés alapján - személyes adatokat kezel, személyes adatok feldolgozását végzi.

„**Adatfeldolgozás**” meghatározása: 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 adaton végzik.

Az adatfeldolgozó a tudomására jutott személyes adatokat kizárólag a KFT rendelkezési szerint dolgozhatja fel, az adatkezelés érintően érdemi döntést nem hozhat, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat a KFT rendelkezései szerint köteles tárolni és megőrizni.

A KFT az adatfeldolgozásra vonatkozó szerződéseket írásba foglalja.

Kártyás beléptető-rendszer szervere:

ISGUS GmbH

Oberdorfstr. 18-2278054 Villingen-Schwenningen

info@isgus.de

<http://www.isgus.de>

Bérszámfejtés:

PARAMÉTER Bt.

6000 Kecskemét, Forrás utca 4/b.

Tel.: 76/505-818, Fax: 76/505-819

www.parameter.hu

Informatika, rendszergazda, IT-szolgáltatások

iFact HUNGARY KFT

6000 Kecskemét, Avar utca 13.

5. Az érintettek jogai és érvényesítésük:

A TRUPLAST KFT számára fontos a személyes adatok megfelelő kezelése és mindent megtesz azért, hogy a személyes adatok kezelése jogszerűen és a lehető legnagyobb biztonságban történjen.

Tájékoztatjuk hogy az adatkezeléssel kapcsolatos jogait, ideértve a hozzájárulása visszavonásához való jogát is, az azonosítását követően az alábbi elérhetőségeket keresztül gyakorolhatja:

A társaságunk székhelyén: 6078 Jakabszállás, Petőfi Sándor u. 44. szám alatt személyesen.

Adatvédelemért feleős munkatárs neve, elérhetősége: Tóthné Szlovák Marianna

Telefon: +36 30 438 - 2545

E-mail: szlovak.m@truplast.hu

5.1. Általános szabályok:

Ha az adatkezelés az érintett hozzájárulásán alapul, jogosult azt bármely időpontban visszavonni.

A hozzájárulás visszavonása nem érinti a visszavonást megelőző adatkezelés jogszerűségét.

A GDPR szerint az érintett kérelmezheti tőlünk az általunk kezelt személyes adataihoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint gyakorolhatja az adathordozhatósághoz való jogát. Társaságunk legkésőbb a kérelem beérkezésétől számított 25 napon belül tájékoztatja Önt a beadványa alapján hozott intézkedésekről.

Ha kérelmét elektronikus úton nyújtotta be, akkor a tájékoztatást elektronikus úton adjuk meg, kivéve, ha az érintett azt másként kéri.

Ha intézkedéseket nem indokol a beadvány, akkor legkésőbb 25 napon belül erről is tájékoztatást küldünk, valamint arról, hogy mely hatóságnál nyújthat be panaszt, és hogyan élhet bírósági jogorvoslati jogával.

A TRUPLAST KFT az érintett jogosultság gyakorlásával kapcsolatban hozott intézkedést díjmentesen biztosítja.

Ha kérelme egyértelműen megalapozatlan, vagy – különösen ismétlődő jellege miatt – túlzó, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre a TRUPLAST KFT ésszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.

Ha a TRUPLAST KFT-nek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett azonosításához szükséges információ nyújtását kérheti.

5.2. Előzetes tájékoztatáshoz való jog:

Az adatgyűjtés során a TRUPLAST KFT a jelen adatvédelmi tájékoztató ismertetése keretében a személyes adatok megszerzését megelőzően, de legkésőbb a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

- a) az adatkezelő – ha van ilyen – képviselőjének, adatfeldolgozónak a neve és elérhetősége;
- b) az adatvédelemért felelős munkatárs elérhetőségei;
- c) a személyes adatok tervezett kezelésének célja;
- d) az adatkezelés jogalapja;
- e) ha az adatkezelés jogalapja jogos érdek érvényesítése, az adatkezelő vagy harmadik fél jogos érdekei;
- f) a kezelt személyes adatok megőrzésének időtartama, az időtartam meghatározásának szempontjai;
- g) az érintettet az adatkezelés kapcsán megillető jogok, azaz hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról, azok érvényesítésének módja;
- h) ha az adatkezelés jogalapja a hozzájárulás, a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- i) a kezelt személyes adatok továbbítása esetén annak címzettjei, a címzettek kategóriái;
- j) adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat;
- k) a hatósághoz címzett panasz benyújtásának jogáról;
- l) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének alapfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása;
- m) az esetleges automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

5.3. Hozzáféréshez való jog:

Az érintett jogosult a TRUPLAST KFT-hez fordulni, hogy a rá vonatkozóan kezelt személyes adatok másolatát és az azok kezelésével összefüggő információkat a KFT rendelkezésére bocsássa.

A KFT köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 25 napon belül írásban, közérthető formában válaszolni.

Az érintett kérelmére a KFT tájékoztatást ad:

- a) az érintettre vonatkozóan a KFT által kezelt személyes adatokról;
- b) az adatkezelés céljáról;
- c) jogalapjáról;
- d) a kezelt adatok megőrzési időtartamáról;
- e) az esetlegesen igénybevett adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, valamint ez esetben a kezelt adatok forrásáról;
- f) az érintett személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről;
- g) az érintettet az adatkezelés kapcsán megillető jogokról;
- h) a hatósághoz címzett panasz benyújtásának jogáról,
- i) automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint ezekben az esetekben az alkalmazott logikára és az arra vonatkozó információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír;
- j) ha a személyes adatok nem az érintettől kerültek megszerzésre, a személyes adatok forrásáról.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

A tájékoztatás ingyenes, ha a tájékoztatást kérő az adott évben azonos adatkörre vonatkozóan tájékoztatási kérelmet a KFT-hez még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg.

A tájékoztatás megtagadása esetén a KFT írásban közli az érintettel, hogy a felvilágosítás megtagadására a hatályos jogszabályok mely rendelkezése alapján került sor. A felvilágosítás megtagadása esetén a KFT tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

5.4. A helyesbítéshez való jog:

Az érintett kérésére a KFT indokolatlan késedelem nélkül helyesbíti a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

A KFT a helyesbítés megtörténtéről az érintettet külön nem tájékoztatja.

A helyesbítésről a KFT tájékoztatja azt az adatkezelőt és az adatfeldolgozót, amely részére a helyesbítéssel érintett személyes adatot továbbította, közölte, kivéve, ha ez lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére a KFT a tájékoztatottak kilétéről információt ad.

5.5. Törléshez („elfeledtetéshez”) való jog:

A személyes adatot a KFT törli, ha kezelése jogellenes, az érintett kéri, az hiányos vagy téves – és ez az állapot jogszerűen nem korrigálható - feltéve, hogy a törlést törvény nem zárja ki, ha az adatkezelés célja megszűnt, az adatok tárolásának törvényben meghatározott határideje lejárt, vagy azt a bíróság vagy a Hatóság elrendelte.

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

- a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- d) a személyes adatokat jogellenesen kezelték;
- e) a személyes adatokat az adatkezelőre alkalmazandó jogi kötelezettség teljesítéséhez törölni kell.

5.6. Hozzájárulás visszavonása:

Az Érintett bármikor visszavonhatja az adatai kezeléséhez adott hozzájárulását, kérheti az adatai törlését. A KFT a törlést csak akkor tagadja meg, amennyiben az adatkezelés jogszabályon alapul, vagy az adatkezelés szükséges jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

A KFT a helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíti, akiknek korábban az adatot adatkezelés céljára továbbította. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti. A megadott személyes adatok valóságáért a felhasználó felel.

Törlésre irányuló kérelem esetén annak benyújtásától számított legfeljebb 15 nap alatt a KFT megvizsgálja a törlés lehetőségét, és írásban reagál. Amennyiben ezzel a kérelmező nem ért egyet, jogosult a közléstől számított 30 napon belül bírósághoz fordulni.

Amennyiben kárt az adatkezelés körén kívül eső elháríthatatlan ok idézett elő, vagy a károsult szándékos vagy súlyosan gondatlan magatartásából származott, a KFT nem köteles megtéríteni az okozott kárt.

5.7. Korlátozás:

Az érintett jogosult arra, hogy kérésére a KFT korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- d) (jogos érdek érvényesítése esetén) tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az Érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

5.8. Tiltakozás:

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

A fentebb említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

5.9. Adathordozhatóság:

Az Érintett jogosult arra, hogy a rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa, feltéve, hogy az adatkezelés automatizált módon történik. Az Érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok más adatkezelőhöz történő közvetlen továbbítását.

5.10. Jogorvoslat:

A megkeresés érkezhetszóban vagy írásban, e-mailben.

Az Érintett a jogainak sérelme esetén kérheti, hogy a KFT a jogellenes adatkezelést szüntesse meg, az adatkezelést, az Érintett kérelmének elutasítását vizsgálják meg.

Az Adatkezelők az Érintett ilyen irányú panaszát minden esetben kivizsgálják, és annak eredményéről az Érintettet tájékoztatják.

Az érintett a jogainak megsértése esetén az adatkezelő ellen bírósághoz vagy az adatvédelmi hatósághoz fordulhat.

Jogorvoslati lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál lehet élni:

Név: Nemzeti Adatvédelmi és Információszabadság Hatóság

Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Honlap: <http://www.naih.hu>

Telefon: +36 (1) 391-1400

Telefax: +36 (1) 391-1410

E-mail: ugyfelszolgalat@naih.hu

II. Munkahelyi adatkezelésre vonatkozó speciális szabályok

A munkahelyi adatkezelések több csoportba sorolhatóak.

Egyrészt különbség tehető abban a tekintetben, hogy létező munkaviszonyról beszélünk-e, vagy sem.

A munkaviszony létesítése előtt megvalósuló adatkezelés alapvetően az azt megelőző pályáztatási eljárással, valamint a munkakörre való alkalmasság vizsgálatával összefüggésben valósul meg.

A munkaviszony megszűnését követően szintén történik adatkezelés, amikor is például a munkáltató jogszabályi kötelezettség alapján nyilvántartja a volt munkavállalója személyes adatait.

A munkaviszony fennállása alatti adatkezelések között is differenciálhatunk.

- Egyrészt például **társadalombiztosítási, adózási okokból** szükséges személyes adatok kezelése, de ekkor is felmerülhet **az alkalmassággal kapcsolatban adatkezelés**. Szintén gyakori adatkezelésként jelenik meg az egyre jobban elterjedő visszaélés-bejelentési rendszerekkel összefüggő adatkezelés.
- További adatkezelés a **munkavégzéssel összefüggésben** keletkezik: minősítési, fegyelmi vétségekkel és büntetésekkel kapcsolatos eljárások során. Ezen túlmenően a **munkavállaló ellenőrzésével** kapcsolatban is felmerül személyes adatok kezelése. Ez utóbbi esettel kapcsolatban elmondható, hogy a technika fejlődésével **egyre gyakoribb a munkavállalók technikai eszközökkel történő ellenőrzése**. Ebbe a körbe tartozik többek között a munkavállalók kamerás megfigyelése, elektronikus levelezésük, valamint internethasználatuk ellenőrzése, a rendelkezésükre bocsátott úgynevezett „céges mobiltelefon” használatának ellenőrzése, a GPS navigációs rendszer alkalmazása során történő ellenőrzés, illetve a biometrikus rendszerek alkalmazásával megvalósuló ellenőrzés.

1. A munkahelyi adatkezelés során érvényesülő adatvédelmi alapelvek

1.1. A célhoz kötött adatkezelés elve

Az Infotv.1 és az Mt. egyaránt tartalmazza az adatvédelem alapelveit, amelyek kiemelten fontosak ahhoz, hogy bizonyos, a munkáltató rendelkezései szerint kialakított adatkezelések jogszerűek legyenek.

Infotv.: 4. § (1) bekezdés Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.

Mt.: 10. § (1) bekezdés A munkavállalótól csak olyan (...) adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

Ezen alapelvből fakadó gyakorlati követelmények:

- Az adatkezelés célját az adatok rögzítését megelőzően, világosan és egyértelműen meg kell határozni. A célnak kellően részletesnek kell lennie annak érdekében, hogy azonosíthatóak legyenek a szükséges adatkezelési műveletek és az alkalmazandó további garanciális szabályok. A cél meghatározásának részletezettsége alapvetően az adatkezelés körülményeitől és a kezelt személyes adatok fajtáitól függ. Általánosságban elmondható, hogy a túl tág, általános fogalmakkal körülírt cél nem felel meg a követelménynek.
- A munkáltatónak minden egyes adatkezelés esetében adatkezelési célonként külön-külön meg kell határozni azt a jogot, amelynek gyakorlásához szükséges valamely személyes adat kezelése, vagy azt a kötelezettséget, amelynek teljesítése szükségessé teszi az adatkezelést.
- A célhoz kötött adatkezelés elve a hivatkozott Mt. 10. § (1) bekezdésben is megjelenik. Ez azt jelenti, hogy a munkáltatónak minden adatkezeléséhez célt kell rendelnie. Azaz személyes adat csak akkor kezelhető, ha az lényeges, ha az adat kezelése nélkül a munkaviszony létesítése, fenntartása, megszűnése nem lenne lehetséges. A munkáltatónak az adatkezelései jogszerűségét elsősorban azzal kell alátámasztania, hogy minden adatkezelése vonatkozásában igazolni tudja az adatkezelés célját, és azt, hogy az adatkezelés a cél eléréséhez szükséges.
- Mindezek alapján a munkáltató köteles a munkavállalóktól kért adatok körét előre oly módon meghatározni, hogy az adatok csakis a munkaviszony létesítéséhez, fenntartásához, megszűnéséhez kapcsolódjanak. A munkavállalókat tájékoztatni kell arról, hogy a tőlük kért adatok, velük szemben alkalmazott vizsgálatok milyen információként szolgálhatnak a munkáltató számára. Minden olyan adat kérése, mely nem ad lényeges tájékoztatást a munkaviszony létesítése, fenntartása, megszüntetése szempontjából, indokolatlanul korlátozza a munkavállalók magánszféraját, személyes adataikkal való rendelkezés jogukat – különösen akkor, ha a munkáltató az adatszolgáltatás megtagadása esetén kilátásba helyezi például a munkaviszony létesítésének megtagadását.
- Amennyiben az adatokon eltérő célokból végeznek műveleteket, akkor a célokat egyenként definiálni kell. Továbbá az adatkezelésnek minden szakaszában meg kell felelnie az adott adatkezelési célnak, és tilos adatokat kezelni olyan újabb célból, amely összeegyeztethetetlen az eredetivel. Így például, ha a munkáltató a munkaszerződés alapján rendelkezésére álló adatokat fel akarja használni belső képzés szervezésére (így különösen a munkavállalók nevét, munkakörét, végzettségét), akkor ez a munkajogviszonyból fakadó, korábbi adatkezelésekhez képest új adatkezelési cél, amelyet külön definiálni kell.
- Bizonyos munkakörök esetén munkaviszonyra vonatkozó szabály alkalmassági vizsgálatot írhat elő. Ebben a körben különösen fontos szerepe van a tisztességes adatkezelés követelményének, ugyanis a munkáltató – például a munkahelyi felvételi eljárás során – kizárólag olyan kérdést intézhet a munkavállalók felé, amely a munkaviszony, alkalmassági vizsgálat szempontjából releváns, és az érintettek személyiségi jogait – így a személyes adatok védelméhez való jogukat – nem sérti. Az adatkezelés tisztességes volta az emberi méltóság védelmével áll szoros kapcsolatban, a tisztességtelen adatkezelési gyakorlat az érintetteket nem csak személyes adataikhoz fűződő jogában, de emberi méltóságukban is súlyosan sértheti.

5.11. A szükségesség-arányosság elve

Infotv.: 4. § (2) bekezdés Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

Mt.:

9. § (2) bekezdés A munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos.

11. § (1) bekezdés A munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető.

Ezen alapelvnek elsődlegesen a munkáltatói ellenőrzéseknél van jelentősége.

Az alapelvből fakadó gyakorlati követelmények:

- Az alkalmazott eszköznek alkalmasnak kell lennie a cél elérésére, vagyis csak akkor lehet ellenőrzést folytatni, ha egyértelmű, hogy az alkalmazni kívánt eszköz, módszer által az ellenőrzés útján a védeni kívánt munkáltatói érdekek, jogok sérelme megelőzhető.
- Az ellenőrzés csak a szükséges mértékű adatkezeléssel járhat. Ez egyszerre jelenti az adatkezelés időbeni korlátozottságát, és azt is, hogy a személyes adatokat csak a szükséges esetben, és csak az arra feljogosított személyek használhatják fel.
- Az ellenőrzés csak a munkával összefüggésben történhet, a munkavállalók magánélete nem ellenőrizhető. Ezzel kapcsolatban fontos kiemelni, hogy a munkavállalókat a munkahelyen is megilleti a magánélethez való jog, és ezt a munkáltatónak tiszteletben kell tartania. A „munkahelyi magánélet” tipikus színterei az ebédlő, az öltöző, a pihenőhelyiség, a mosdók. - Az ellenőrzésnek minden esetben a munkavállalók emberi méltóságának tiszteletben tartásával kell történnie. Az ellenőrzés nem irányulhat a munkavállalók megfélemlítésére, megalázására, zaklatására, zavarására, és ezeket nem is eredményezheti.

6. Az adatkezelés jogalapja

A magyar és az uniós jogszabályi rendelkezések alapján különböző jogalapok alkalmazhatóak annak érdekében, hogy az adatkezelés jogszerű legyen, amelyek közül a munkahelyi adatkezelés során alapvetően három jogalap jöhet szóba:

- az érintett hozzájárulása,
- törvényi felhatalmazás, illetve
- a munkáltató jogos érdekén alapuló adatkezelés.

2.1. Az érintett hozzájárulása

A hozzájárulás jogalapjának legfontosabb feltétele, hogy annak önkéntesnek, azaz mindenfajta külső befolyástól mentesnek kell lennie. A hozzájárulás jogalként csak akkor jöhet szóba, ha valódi választási lehetőség áll az érintett rendelkezésére, és nem áll fenn a megtévesztés, a megfélemlítés, a kényszerítés vagy más jelentős negatív következmény veszélye a hozzájárulás megtagadása esetén. Az önkéntesség hiányában az adatkezelő nem rendelkezik megfelelő jogalappal az adatkezeléshez.

A munkavégzésre irányuló jogviszonyokban azonban nem értelmezhető a hozzájárulás önkéntessége: a munkáltató és a munkavállaló közötti alá-fölérendeltségi viszonyban, ha az alkalmazott a hozzájárulását megtagadja, ez anyagi vagy nem anyagi természetű hátrányt okozhat neki.

Az érintett hozzájárulására, mint jogalapra, a munkahelyi adatkezelések esetében tehát csak kivételesen lehet hivatkozni, alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli „előnyöket” szerez a munkavállaló, és nem érheti őt semmilyen hátrány az adatkezelés megtagadása esetén. A hozzájárulás megfelelő jogalap lehet, ha az adatkezelésre nem a munkaviszonytal összefüggésben kerül sor, vagyis ha az adatkezelés a munkáltatói jogok gyakorlásával nem áll kapcsolatban. Például egy munkáltató egy futóversenyre csapatot szervez, amelyhez a munkáltatónak továbbítania kell a szervezők részére azon munkavállalóinak az adatait, akik részt vennének a versenyen, mivel a munkáltató állja a nevezés költségeit. Emellett a munkáltató pólókat is biztosít a versenyre, ezért a munkavállalók póló méretét továbbítania kell a pólót készítő vállalkozás részére. Ez két különböző adattovábbítást jelent, és mindkettőhöz egymástól függetlenül önkéntes hozzájárulást tud adni a munkavállaló anélkül, hogy ennek bármilyen következménye lenne a munkaviszonyára nézve.

A fent kifejtettek alapján elmondható tehát, hogy a munkáltatói adatkezelések esetében a hozzájárulás mint jogalap csak szűk körben jelenik meg, amikor is ténylegesen fennállhat az önkéntesség.

6.1. Törvényen alapuló adatkezelés

A munkahelyi adatkezelések egy jelentős része törvényi rendelkezésen alapul: vagy olyan törvényi előíráson, amely kötelezővé teszi az adatkezelést, vagy olyan jogszabályon, amely csupán lehetővé teszi az adatkezelést. Mindkét esetben előfordul, hogy az adott törvény az adatkezelés valamennyi körülményét szabályozza, de olyan jogszabály által nevesített adatkezelés is létezik, amelynél a törvény az adatkezelés részleteit, körülményeit nem határozza meg, azokat az adatkezelőre bízva.

Törvényen alapuló, kötelező adatkezelést széles körben rendelnek el az adókötelezettségre, társadalombiztosításra vonatkozó jogszabályok. Ezen jogszabályok rendelkezései a munkáltatók és a munkavállalók számára kötelezettségként jelennek meg, vagyis ezek ténylegesen kötelező adatkezelések.

Ezen túlmenően a munkaviszonyra is irányadóak lehetnek olyan törvények, amelyek az adatkezelést a munkáltató számára lehetővé teszik. Ebbe a körbe tartozik például a munkáltatói visszaélés-bejelentési rendszerrel, illetve a munkáltató ellenőrzési jogosultságával összefüggő adatkezelés a munkavégzés tekintetében. Azonban ezek nem tekinthetők klasszikusan törvényi felhatalmazáson alapuló adatkezeléseknek, hanem közelebb állnak a munkáltató jogos érdekén alapuló adatkezelések csoportjához, hiszen a munkáltatók több-kevesebb mozgástérrel rendelkeznek az adatkezelési körülmények meghatározásában.

6.2. A munkáltató jogos érdekén alapuló adatkezelés

A munka világában az érintett hozzájárulása helyett – a fenti szűk esetkört leszámítva – más jogalapok alkalmazása indokolt.

Személyes adat kezelhető abban az esetben is, ha a munkahelyi adatkezelés a munkáltató – kivételesen harmadik fél – jogos érdekének érvényesítéséhez szükséges, kivéve, ha ennél az érdekeknél magasabb rendűek a munkavállalók személyes adatai védelméhez és a magánéletük tiszteletben tartásához való joguk.

A jogalap egyik fő jellemzője az, hogy ez a munkavállalók hozzájárulásától függetlenül jogszerűvé teheti a munkáltató adatkezelését, feltéve, ha a munkáltató jogos érdeke arányosan korlátozza a munkavállalók személyes adatok védelméhez való jogát, magánszféráját.

A munkáltatóra hárul azon kötelezettség, hogy belső szabályzatban vagy más írásbeli dokumentumban kidolgozza ezen jogalap alkalmazásával végzett adatkezeléseit. Fontos garanciális szempont, hogy a munkáltató írásban rögzítse ezen az jogalap alkalmazásával együtt járó adatkezelési körülményeket, hiszen a munkavállalók így tudnak meggyőződni arról, hogy a szóban forgó munkahelyi adatkezelés valóban arányosan korlátozza a jogaikat. Emellett a Hatóság vagy a bíróság is így tudja ellenőrizni, vizsgálni azt, hogy a munkáltató adatkezelése megfelelt-e az adatvédelmi követelményeknek.

A jogalap alkalmazása során a munkáltatónak két követelményre kell figyelemmel lennie. Egyrészt ezen jogalap alkalmazásakor a magyar jogszabályi előírásokat, így különösen az Mt. és az Infotv. rendelkezéseit kell alapul vennie. Másrészt ezzel egyidejűleg el kell végeznie az érdekmérlegelési tesztet. Az érdekmérlegelési teszt elvégzése során a munkáltatónak számos szempontra figyelemmel kell lennie, ezért a Hatóság egy lehetséges forgatókönyvet javasol, amely mellett természetesen elfogad más módszereket is ennek a tesztnek az elvégzésére.

1. lépés:

A munkáltatónak a tervezett adatkezelés megkezdése előtt át kell tekintenie, 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:

A munkáltatói jogos érdek lehető legpontosabb meghatározása (így különösen az Mt. 10. § (1) bekezdésének figyelembe vételével).

3. lépés:

Annak meghatározása, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek.

4. lépés:

Annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket a munkavállalók felhozhatnak az adatkezeléssel szemben).

5. lépés:

Annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott munkavállalói jogokat, várákozásokat.

Az érdekmérlegelésen alapuló munkahelyi adatkezelések esetében többek között az alábbi garanciák biztosíthatják az adatkezelés szükségesség-arányosságát (természetesen más garanciális intézkedések is szóba jöhetnek):

- A fokozatosság elvének érvényesülése. Ennek a garanciának elsődlegesen a munkáltatói ellenőrzésekkel együtt járó adatkezelések esetén van jelentősége. A munkáltatónak a munkavállalók munkaviszonyal összefüggő magatartásának ellenőrzése körében lehetőleg olyan módszert kell választania, amely nem jár együtt személyes adat kezelésével. Ha nincs ilyen, akkor a magánszférát legkevésbé korlátozó módszert kell alkalmaznia, amelynek nyomán korlátozott körben ismer meg személyes adatokat.
- A munkavállaló jelenlétének biztosítása. Ugyancsak a munkáltatói ellenőrzések keretében van szerepe ezen garanciának. Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, akkor biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során (így például a felvételek visszanezésekor vagy az e-mail elolvasásakor).

6.3. Az Mt. és az Infotv. szabályai az adattovábbítás jogalapjával kapcsolatban

Infotv.: 5. § (1) bekezdés: Személyes adat akkor kezelhető, ha a) ahhoz az érintett hozzájárul, vagy b) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).

Mt.: 10. § (2) bekezdés: A munkáltató a munkavállalóra vonatkozó (...) adatot (...) harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet.

Az Infotv. 3. § 13. pontja értelmében adattovábbításnak minősül az, amikor személyes adatot meghatározott harmadik személy számára hozzáférhetővé tesznek. Az Infotv. 3. § 22. pontja alapján harmadik személy az adatkezelőn, az érintetten és az adatfeldolgozón kívül minden más személy és szervezet. A munkaviszonyban az érintett a munkavállaló, az adatkezelő a munkáltató, és minden, rajtuk kívüli személy harmadik személynek minősül, így például harmadik személynek minősülnek a munkáltatóval egy vállalatcsoportban lévő más vállalatok is. Ebből fakadóan adattovábbításnak tekinthető az is, amikor a munkáltató egy közös adatbázisba tölti fel a munkavállalók személyes adatait, amely adatbázishoz más adatkezelők (más leányvállalatok, az anyavállalat) is hozzáférhet.

Ugyanez a helyzet a munkáltató tulajdonosát tekintve is: főszabályként a tulajdonosi jogok gyakorlása nem teszi szükségessé, és nem engedi meg a munkavállalókra vonatkozó személyes adatok tulajdonos részére való továbbítását. Kivételt ez alól csupán a vezető állású munkavállalók jelenthetnek, egyéb esetben azonban a tulajdonos részére csak személyazonosításra alkalmatlan adatok továbbíthatóak.

Az Mt. rendelkezéséből következik az is, hogy egy álláspályázatra jelentkezéskor az állást meghirdető munkáltató nem jogosult a korábbi munkáltatótól információkat gyűjteni, és így módon „leinformálni” a pályázót. Ebben az esetben a korábbi munkáltató semmilyen személyes adatot nem közölhet az állást meghirdető munkáltatóval, hiszen – törvényi felhatalmazás hiányában – az Mt. 10. § (2) bekezdése csak a munkavállaló hozzájárulásával tehetné ezt meg.

7. Az előzetes tájékoztatás követelménye

Infotv.: 20. § (1)-(2) bekezdés: Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező. Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Mt.:

9. § (2) bekezdés: A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról a munkavállalót előzetesen tájékoztatni kell.

10. § (2) bekezdés: A munkáltató köteles a munkavállalót tájékoztatni személyes adatainak kezeléséről.

11. § (2) bekezdés: A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

Ezen rendelkezésekből fakadó gyakorlati követelmények:

- Az érintett az előzetes, megfelelő tájékoztatás alapján képes felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára.
- Az előzetes tájékoztatásra vonatkozó követelményeket a jogalkotó az Infotv. 20. §-ában fogalmazta meg. Az előzetes, megfelelő tájékoztatás kötelezettségének központi eleme az Infotv. 20. § (2) bekezdése, amely felsorolja azokat az alapvető adatkezelési körülményeket, amelyekről az adatkezelőnek tájékoztatást kell nyújtania. Az előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlás részletesen foglalkozik az előzetes tájékoztatási kötelezettséggel.
- Amennyiben a munkáltató technikai eszközzel kíván ellenőrzést végezni – tekintve, hogy az ellenőrzés személyes adatok kezelésével jár együtt – úgy az nem lehet titkos, arról a munkavállalókat előzetesen tájékoztatni kell, így például a munkavállalóknak tisztában kell lenniük az ellenőrzés módjával, céljával.
- A munkahelyi adatkezelésekkel összefüggésben kiemelten fontos arról tájékoztatást nyújtani, hogy a munkáltató szervezetrendszerén belül ki férhet hozzá a személyes adatokhoz. Azt a személyi kört, akik hozzáférhetnek a személyes adatokhoz, adatkezelési célonként külön-külön kell meghatározni.

Egyes speciális munkahelyi adatkezelések

1. Az álláspályázatra jelentkezés és a magán-munkaközvetítés

1.1. „Anonim álláshirdetések”

Anonim álláshirdetések alatt azok az álláshirdetések értendők, amelyekben a munkáltató nem tünteti fel a cégnevet, ezért az álláspályázat elküldésének időpontjában a jelentkezők nem lehetnek tisztában azzal, hogy mely munkáltatónak az állására jelentkeznek.

A Hatóság gyakorlata szerint az álláshirdetésre jelentkezők információs önrendelkezési jogának szerves része az, hogy az érintettek az adatkezelő kilétére kiterjedő megfelelő tájékoztatást kapjanak már az adatkezeléshez való hozzájárulás megadása előtt, valamint hogy tudomással rendelkezzenek arról, hogy kikkel szemben tudnak élni az Infotv.-ben szereplő jogaikkal. Bizonyos esetekben ezzel szemben állnak a munkáltató gazdasági vagy egyéb érdekei, hogy kiléte rejtve maradjon a pályázat során mindaddig, amíg ez indokolt (például egy cég nem szeretné, ha idő előtt kiderülne, hogy „belép a piacra”, ezt szeretné a konkurencia előtt titokban tartani). Ebben a gyakorlatban rendkívül egyenlőtlen helyzetben vannak a felek, hiszen míg az érintettek jelentkezésük elküldésével azonnal „kiadják magukat”, minden személyes adatukat megismeri az álláshirdetést feladó munkáltató, addig a munkáltató egyáltalán nem ad semmilyen tájékoztatást a személyéről, ezáltal is fokozva a munkavállalók kiszolgáltatottságát, és a munkáltató információs fölényét.

Alapvetően nem fogadható el a munkáltatók részéről az anonim álláshirdetések feladása, mivel az esetek túlnyomó többségében ezzel aránytalanul sérül a jelentkezők információs önrendelkezési joga, így különösen az a joga, hogy a jelentkezők az adatkezelés megkezdése előtt (a pályázati anyag elküldése előtt) valamennyi lényeges adatkezelési körülményéről tájékoztatást kapjanak.

A munkáltatók érdekei csak különösen indokolt, rendkívüli esetben, és akkor is legfeljebb korlátozott mértékben (például egy rövid, átmeneti időtartamig) írhatják felül a jelentkezők információs önrendelkezési jogát.

1.2. Az álláspályázatra jelentkező munkavállaló valamely közösségi oldalon létrehozott profiljának megtekintése

Egy munkáltató igyekszik a lehető legtöbbet megtudni az álláshirdetésre jelentkezőkről, minden lehetséges forrásból szeretne információt gyűjteni róluk, hogy azok alapján közülük a legmegfelelőbb személyt válassza ki. Ennek egyik kézenfekvő megoldása az, ha a munkáltató megnézi a jelentkezőnek a közösségi oldalon található profiloldalát.

A közösségi oldalakon mindenki maga állítja be, hogy az általa megosztott tartalmat ki láthatja, ki férhet hozzá. Az érintett kontroll alatt tudja tartani azt, hogy milyen, mindenki számára nyilvános információk érhetőek el róla a közösségi oldalon keresztül.

A Hatóság álláspontja szerint továbbá életszerűtlen elvárni a munkáltató oldaláról, hogy ne tekinthesse meg azokat a bárki számára elérhető, nyilvános információkat, amelyeket az álláshirdetésre jelentkező személy osztott meg magáról.

A közösségi oldalak megtekintésével összefüggésben azonban a munkáltatónak az alábbi adatvédelmi követelményekre kell tekintettel lennie:

- Előzetes tájékoztatást kell biztosítani a jelentkezők számára. Így például ismertetni kell a jelentkezőkkel, hogy a felvételi eljárás folyamata kiterjed arra is, hogy a munkáltató is megtekinti a jelentkező közösségi oldalon létrehozott, bárki számára nyilvános információit. Azaz a munkáltató nem „rejtheti el” ezen gyakorlatát a jelentkezők elől, fel kell fednie a kiválasztási folyamat minden lényeges részét. - Nem fogadható el az, ha a munkáltató a korlátozottan nyilvános adatokat ismeri meg. Ilyen például az az eset, amikor az álláshirdetésre jelentkező személy tagja valamely zárt csoportnak egy közösségi oldalon belül, és ennek ismeretében a munkáltató megkér valakit, aki szintén tagja ennek a zárt csoportnak, hogy nézze meg, mit is csinál a jelentkező ezen személy a zárt csoporton belül. Ezen információk már nem teljesen nyilvánosak, ezért ezek megismerése már korlátozza a jelentkező magánéletéhez való jogát.
- Fontos továbbá az is, hogy – az Mt. 10. § (1) bekezdésében foglaltakkal összhangban – csak azok az információk ismerhetők meg, amelyek lényegesek az álláspályázattal vagy a munkakörrel kapcsolatban. A munkaviszony létesítése szempontjából így például nem lényeges adat a magánéletre, párkapcsolatra, családi életre, vallásra vonatkozó adat.
- Az érintett közösségi oldalon végzett, nyilvános tevékenysége megismerhető, következtetést vonható le arról, de a további adatkezelési műveletek már jogellenesnek minősülnek. Vagyis arra nincs lehetőség, hogy a jelentkező profiloldalát a munkáltató lementse, tárolja vagy más számára továbbítsa.

1.3. A pályázatok, önéletrajzok megőrzése

Az Infotv. 4. § (1)-(2) bekezdése alapján az önéletrajzok, pályázatok esetében az adatkezelés célja az, hogy a meghirdetett munkakört betöltsék. Ennek megfelelően, ha a munkáltató a jelentkezők közül kiválasztott egy személyt a meghirdetett állásra, akkor megszűnt az adatkezelés célja, és – az Infotv. 17. § (2) bekezdés d) pontja alapján – a ki nem választott jelentkezők személyes adatait törölni kell. Ezzel egyidejűleg fennáll a törlési kötelezettség abban az esetben is, ha az érintett még a jelentkezés során meggondolja magát, visszavonja pályázatát.

Emellett a pályázati anyagok kezelésével kapcsolatban figyelembe kell venni a speciális jogszabályi rendelkezéseket is.

A munkáltató alapvetően csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a pályázatokat, feltéve, ha azok megőrzésére az Infotv. 4. § (1)-(2) bekezdésével összhangban álló adatkezelési célja elérése érdekében szükség van. A Hatóság ezzel kapcsolatban kiemeli, hogy ha az érintett elküldi a pályázati anyagát a munkáltató számára, akkor ez nem jelenti azt, hogy hozzá is járul ahhoz, hogy a pályázati anyagát a munkáltató megőrizze, mivel ebben az esetben megkérdőjelezhető a munkavállaló hozzájárulásának önkéntessége.

Erre tekintettel a Hatóság álláspontja szerint az a jó gyakorlat a munkáltató részéről, ha a hozzájárulást a felvételi eljárás lezárását követően kéri a jelentkezőktől. Emellett a munkáltatónak a pályázati anyagok megőrzése esetében is egy konkrét, az adatkezelés céljához és az adatkezelés pontosságának, naprakészségének elvéhez igazodó időtartamot kell meghatározni.

1.4. A pályázati anyagok kezelésével kapcsolatos egyéb adatvédelmi követelmények

A jelentkezők információs önrendelkezési jogát az biztosítja a legmagasabb szinten, ha tájékoztatást kapnak arról is, ha a munkáltató nem őt választotta az adott állásra. Ennek megfelelően a munkáltató részéről nem fogadható el az a gyakorlat, ha például az álláshirdetésben kiköti, hogy amennyiben az adott jelentkező nem kap külön értesítést, akkor a munkáltató nem vette fel a jelentkezőt az adott állásra.

Az Infotv. szabályozása alapján személyes adatnak minősül az adatból levont, az érintettre vonatkozó következtetés is. Ennek megfelelően, ha a munkáltató bármilyen feljegyzést készít a pályázóról, akkor az is a pályázó személyes adatának minősül.

Ezzel kapcsolatban két adatvédelmi követelményt szükséges tisztázni:

- Egyrészt erre is kiterjed az érintettet tájékoztatáshoz való joga, vagyis, hogy megismerje, a munkáltató milyen következtetéseket vont le a pályázati anyagával összefüggésben.
- Másrészt a munkáltatónak törölnie kell az ilyen természetű, az érintettre levont következtetéseket tartalmazó feljegyzéseket is.

1.5. A magán-munkaközvetítő által kezelhető adatok

A 118/2001. (VI. 30.) Korm. rendelet 10. § (1) bekezdés e) pontja meghatározza, hogy milyen adatokat nem lehet kezelni magán-munkaközvetítés során. A jogszabály értelmében tilos olyan személyes adatokat kezelni, amelyekre a munkát keresők alkalmasságának a megítéléséhez nincs szükség, illetve amelyek a keresett munkával nincsenek közvetlen összefüggésben. Erre tekintettel a magán-munkaközvetítő a képesítésre, szakmai tapasztalatra vonatkozó adatokat és az alkalmasság megítéléséhez szükséges adatokat kezelheti.

Ha a munkát kereső munkavállaló azt tapasztalja, hogy a magán-munkaközvetítő mégis olyan adatot kér tőle, amely adat kezelésének célja nem egyértelmű, akkor az érintett magyarázatot, tájékoztatást kérhet a magán-munkaközvetítőtől.

2. Alkalmassági vizsgálatok

2.1. Általános adatvédelmi követelmények

Az Mt. 10. § (1) bekezdése alapján a munkavállalókkal szemben kizárólag két típusú alkalmassági vizsgálat alkalmazható:

- Egyrészt vannak olyan alkalmassági vizsgálatok, amelyeket munkaviszonyra vonatkozó szabály ír elő.
- Másrészt vannak olyanok is, amelyeket nem ír ugyan elő munkaviszonyra vonatkozó szabály, de amelyre a munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükség van.

Az alábbi adatvédelmi követelmények az alkalmassági vizsgált mindkét esetkörére egyaránt vonatkoznak:

- Részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is.
- A vizsgált munkavállalók, illetve a vizsgálatot végző szakember ismerhetik meg az eredményeket. Ezt azért is fontos hangsúlyozni, mert a tesztből akár olyan következtetés is levonható, amely maga az érintettek, a munkavállalók számára sem volt ismert. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban nem ismerheti meg.

2.2. A munkáltató által előírt alkalmassági vizsgálatok követelményei

Ebben az esetben a munkáltatónak el kell végeznie a már korábban ismertetett érdekmérlegelési tesztet, hiszen az alkalmassági vizsgálatok elvégzésével együtt járó adatkezelés esetében is az adatkezelés jogalapja a munkáltató jogos érdeke lehet. Az érdekmérlegelési teszt során a munkáltatónak számos szempontra kell figyelemmel lennie.

Így például a munkáltató által választott módszernek alkalmasnak kell lennie a cél elérésére, a munkaviszonnyal kapcsolatos, releváns adatot kell a teszteredményből kapni.

Másfelől az alkalmassági vizsgálat szükségességét a munkáltatónak meg kell indokolnia.

Az adatkezelésnek természetesen célhoz kötöttnek kell lennie, azaz csak akkor lehet jogszerű, ha annak a vizsgálatnak az elvégzése szükséges a munkaviszony létesítése, fenntartása szempontjából.

Ezen túlmenően az alkalmassági vizsgálatokkal kapcsolatban a munkáltatónak további sajátosságokra kell figyelemmel lennie. Így példaként említhető a munkáltatók által gyakran alkalmazott, a különböző kompetenciák, személyiségjegyek felmérésére alkalmas tesztek kitöltetése. A tesztek eredménye azonban túlmutathat az alkalmasság megítélésén, és a munkavállalók személyes – és bizonyos esetekben különleges – adataira világít rá.

A tesztek két fő típusát lehet elhatárolni:

- léteznek munkaalkalmasságra, felkészültségre irányuló tesztlapok, illetve
- pszichológiai vagy személyiségjegyeket kutató tesztlapok.

Az előbbieket a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitöltetheti a munkavállalókkal.

Más megítélés alá esnek a pszichológiai vagy személyiségjegyeket kutató tesztlapok. Az egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében kitöltethető a munkavállalók nagyobb csoportjával a személyiségjegyek kutatására alkalmas tesztlap, de csak akkor, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása.

2.3. A munkaviszony fennállta alatt végzett munkahelyi tréningek adatvédelmi követelményei

Általában a tréningek, különböző alkalmassági vizsgálatok keretén belül elvégzett tesztek komoly személyiségjellemzést adnak a munkavállalókról, amelyek megismerése, tárolása, nyilvántartása nem fogadható el a munkáltatók részéről. A tesztek kitöltése a trénernek (szakembernek) ad iránymutatást a tréningen résztvevő munkavállalókról: kinek milyen képességét szükséges fejleszteni, milyen módszerrel lehet eredményesebb munkavégzést elérni. Azaz a teszteredményeket a szakértő kezeli a tréning során, és ennek átadása a munkáltató részére nem elfogadható. Továbbá a tréninget követően a tréner vagy a trénercég arra alapvetően nem jogosult, hogy egy tréningen résztvevő személy eredményeit névhez köthetően a jövőben is kezelje, ehelyett javasolt a kitöltött tesztlapok, dokumentumok kitöltő részére való átadása.

3. A munkavállalók feddhetetlen előéletének igazolása

A hatósági erkölcsi bizonyítvány mint jogintézmény célja többek között az, hogy a munkavállaló a munkáltató előtt erkölcsi alkalmasságát az adott munkakörrel kapcsolatosan igazolja. Erre az érintettet a munkaviszony létesítése előtt, a felvételi eljárás során, illetőleg a munkaviszony fennállása alatt is felszólíthatja a munkáltató, amennyiben az erkölcsi alkalmasság igazolása valamely ágazati jogszabályban meghatározottak szerint, az adott munkakör betöltéséhez valóban elengedhetetlen. Ilyen, jogszabály által előírt adatkezelés található például az Mt. 44/A. §-ában, amelynek alapján nem létesíthető munkajogviszony azzal a személlyel, akivel szemben az Mt. 44/A. §-ában szereplő kizáró feltételek fennállnak.

A Bnyt., illetve a vonatkozó törvények rendelkezései értelmében a hatósági erkölcsi bizonyítvány közokirat, melynek tartalmát mindenki – a munkáltató is – köteles a kiállításától számított kilencven napig valósan elfogadni. A munkavállalók egyes munkaviszonyokra való erkölcsi alkalmasságát tehát ezen okirat megkérésével lehet igazolni.

Számos esetben a munkáltatók arra kérik a munkavállalókat, hogy a hatósági erkölcsi bizonyítvány helyett a bünyügyi nyilvántartó szervtől igényeljék a bünyügyi nyilvántartási rendszerben kezelt adataikra vonatkozó tájékoztatást. Jóllehet, a Bnyt. lehetővé teszi azt, hogy az érintett személy a bünyügyi nyilvántartásban szereplő személyes adatairól tájékoztatást kérjen, ennek célja azonban az, hogy az érintett átláthassa személyes adatainak kezelését és nem az, hogy az érintett személyt – a bünyezett előélet alóli mentesüléstől függetlenül – ilyen formán beszerzett adatokkal a munkáltató átvilágítsa.

Azon munkáltatói szándék, miszerint a munkavállaló erkölcsi alkalmasságát az érintett kérelmére a bünyügyi nyilvántartási rendszerben kezelt adatairól kiállított tájékoztatással kívánja megállapítani, súlyosan sérti az érintett személyes adatai védelméhez való jogát, jogellenesen diszkriminálhatja és ellentétes a hátrányos jogkövetkezmények alóli mentesüléshez fűződő közérdekkel.

A munkáltatók azon gyakorlatát, hogy a hatósági erkölcsi bizonyítvány helyett a munkavállalótól a bünyügyi nyilvántartási rendszerben kezelt adataira vonatkozó tájékoztatást – annak díj- és illetékmentes kiállítása miatt – is elfogadják az illetékekről szóló 1990. évi XCIII. törvény 2016. január 1-jét követő módosítása sem indokolja, hiszen a hatályos jogi szabályozás szerint a hatósági erkölcsi bizonyítvány kiállítása iránti eljárás évente négy alkalommal illetékmentes.

8. Munkahelyi kamerás megfigyelés

Külön jogszabály nem rendelkezik a munkahelyen alkalmazott elektronikus megfigyelőrendszerek alkalmazásáról.

- Az Mt. rendelkezései önmagukban nem adnak felhatalmazást a munkáltatónak elektronikus megfigyelőrendszerek alkalmazására, ahhoz a munkáltatónak minden esetben el kell végeznie a jelen tájékoztató jogalapjainál részletesen ismertetett érdekmérlegelési tesztet.
- Kamerákat a munkavállalók és az általuk végzett tevékenység elsődleges, kifejezett megfigyelése céljából működtetni nem lehet. Jogellenesnek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása, amelynek – akár nem deklaratív – célja a munkavállalók munkahelyi viselkedésének a befolyásolása.

Az Mt. mellett az Szvtv. mint mögöttes jogszabály rendelkezéseit is figyelembe kell venni. Az Szvtv. négy esetben teszi lehetővé az elektronikus megfigyelőrendszer alkalmazását:

- az emberi élet, testi épség, személyi szabadság védelme,
- a veszélyes anyagok őrzése,
- az üzleti, fizetési, bank- és értékpapírtitok védelme,
- vagyonvédelem.

A célhoz kötött adatkezelés elvéből fakadóan tehát munkahelyen elektronikus megfigyelőrendszert alkalmazni elsődlegesen az Szvtv.-ben elismert ezen célokból lehet, illetve a rögzített felvételek is ezen célokból használhatóak fel. Amennyiben a munkáltatók más célból szeretnék alkalmazni a kamerás megfigyelést, akkor ott igazolniuk kell azt a jogos érdeket, amely szükségessé teszi a kamera alkalmazását.

Az elektronikus megfigyelőrendszerek alkalmazhatóságának fontos feltétele, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzóknak, az illemhelyiségekben vagy például orvosi szobában, váróban.

Emellett alapvetően szintén nem lehet elektronikus megfigyelőrendszert alkalmazni az olyan helyiségben sem, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve, mint például a munkavállalók számára biztosított ebédlő. Ez alól kivételt jelenthet az az esetkör, ha ebben a helyiségben valamilyen védendő vagyontárgy található (így például étel-ital automata), amellyel összefüggésben igazolható valamilyen munkáltatói érdek (például a munkavállalók többször megrongálták a berendezést és a károkat a munkáltatónak kellett állnia). Ebben az esetben e konkrét cél érdekében kamera helyezhető el a helyiségben, azonban ekkor a munkáltatónak különös figyelemmel kell lennie arra, hogy a kamera látószöge kizárólag a védendő vagyontárgyra irányulhat.

A kamerák látószögével kapcsolatban fontos megjegyezni, hogy a munkáltató elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmazhat, közterület megfigyelésére azonban nem.

Az elektronikus megfigyelőrendszer által rögzített felvételek tárolásának időtartamára – más törvényi rendelkezés hiányában – alkalmazni kell az Szvtv. 31. § (2)-(4) bekezdésében szereplő szabályokat.

Ennek megfelelően a munkáltató a rögzített felvételeket főszabályként 3 munkanapig tárolhatja, kivéve, ha a megfigyelt helyiséggel kapcsolatban fennállnak az Szvtv. 31. § (3)-(4) bekezdésének feltételei. Ezen túlmenően – a célhoz kötött adatkezelés elvével és az érdekmérlegelés tesztjével összhangban – a munkáltatónak kell igazolni azt, hogyha valamely kamera által rögzített felvételeket három munkanapnál hosszabb időtartamig szükséges megőrizni.

A munkáltatónak az elektronikus megfigyelőrendszer alkalmazására vonatkozó tájékoztatójában ki kell térnie többek között

- az adatkezelés jogalapjára, illetve annak sajátosságára (munkáltatói jogos érdeken alapuló adatkezelés),
- a felvétel tárolásának helyére és időtartamára,
- a felvételek tárolásával kapcsolatos adatbiztonsági intézkedésekre,
- az adatok megismerésére jogosult személyek körére, illetőleg arra, hogy a felvételeket mely személyek, szervek részére, milyen esetben továbbíthatja,
- a felvételek visszanezésére vonatkozó szabályokra, illetőleg arra, hogy a felvételeket milyen célból használhatja fel a munkáltató,
- arra, hogy a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel összefüggésben és milyen módon tudják gyakorolni a jogaikat, illetve jogaik megsértése esetén a munkavállalók milyen jogérvényesítési eszközöket vehetnek igénybe.

A tájékoztatási kötelezettséggel kapcsolatban szükséges kiemelni, hogy a munkáltatónak minden egyes kamera vonatkozásában pontosan meg kell jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. A munkáltató ezzel igazolni tudja a munkavállalók számára azt, hogy miért tekinthető szükségesnek az adott terület megfigyelése.

Nem fogadható el az a gyakorlat, amikor a munkáltató általánosságban tájékoztatja a munkavállalókat arról, hogy elektronikus megfigyelőrendszert alkalmaz a munkahely területén. Tilos továbbá a rejtett kamera használata.

5. A munkáltató által a munkavállaló rendelkezésére bocsátott e-mail fiók használatának ellenőrzése

Előzetes intézkedések

Napjainkban a legtöbb munkahelyen a munkáltató „céges e-mail fiókot” bocsát a munkavállalók rendelkezésére (leggyakrabban név@cégnév.hu felépítésű e-mail címetek) annak érdekében, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviselőjében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel. A „céges e-mail fiók” használatával kapcsolatban gyakori probléma, hogy a levelezőrendszert a munkavállalók saját, személyes céljaikra is használják. Ez visszas helyzetet teremthet abban az esetben, ha a munkáltató – az Mt. 11. §-ában foglalt jogával élve – ellenőrizni kívánja a „céges email fiók” tartalmát és a munkavállalók által folytatott levelezést.

E probléma megelőzéseként a munkáltatónak mindenekelőtt egy belső szabályzatot kell megalkotnia a „céges e-mail fiók” használatának, ellenőrzésének szabályairól. Ezzel ugyanis hatékonyan meg lehet előzni azt, hogy a munkavállalók (és adott esetben más, a magánjellegű levelezésben szereplő érintettek) személyes adatait is kezelje a munkáltató.

A belső szabályzatban többek között az alábbiakra szükséges kitérni:

- használható-e magáncélokra a „céges e-mail fiók”,
- az e-mail fiókról biztonsági másolat készítésének és megőrzésének a szabályozására, illetve arra, hogy mikor kerül sor az e-mailek végleges törlésére,
- az e-mail fiók használata ellenőrzésének részletes szabályaira.

Jó gyakorlat lehet a munkáltató részéről továbbá az is, ha bizonyos időközönként emlékezteti a munkavállalókat arra, hogy milyen előírások vonatkoznak a „céges e-mail fiók” használatára (például félévente a levelezőrendszerben megjelenik egy olyan tájékoztatás, hogy a munkavállaló az e-mail fiók használata során magáncélból ne küldjön levelet). Ezzel ugyanis biztosítható az, hogy a munkavállalók kiemelt figyelmet fordítsanak arra, hogy a „céges e-mail fiókot” a munkáltató rendelkezései szerint használják. A munkáltató megelőző intézkedései ellenére is (például a munkáltató a szabályzatban megtiltja a „céges levelezőrendszer” személyes célú használatát) a munkavállalók sokszor magáncélra is használják az e-mail fiókot. Ebben az esetben – függetlenül attól, hogy a munkáltató egyébként belső szabályzatában megtiltotta az e-mail fiók magáncélú használatát –, a munkáltató a levelezőrendszerben személyes adatokat is kezel, és a munkáltatónak a további intézkedései (például a „céges e-mail fiók” használatának ellenőrzése) során be kell tartania az adatvédelmi követelményeket.

Adatvédelmi követelmények

A „céges e-mail fiók” ellenőrzése esetében a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ezért a munkáltatónak az adatkezelés megkezdése előtt el kell végeznie az érdekmérlegelés tesztjét. Ezen ellenőrzés esetében kiemelt figyelmet kell fordítani az célhoz kötött adatkezelés elvén és a szükségesség-arányosság követelményén túl az érintettek magánszférájára is, hiszen adott esetben különféle, a munkaviszonyhoz nem kapcsolódó személyes adat is a munkáltató tudomására juthat, illetve vele munkaviszonyban nem álló személyek (az e-mailek küldői vagy címzettjei) adatait is megismerheti.

Ennek megfelelően a munkáltatónak már előzetesen, a szabályzat megalkotása során meg kell határoznia azt, hogy milyen céljai, érdekei miatt kerülhet sor az e-mail fiók ellenőrzésére. Ezen érdekeknek ténylegesnek és valósnak, a munkáltató tevékenységéhez, piaci helyzetéhez és a munkavállalók munkaköréhez igazodóknak kell lenniük.

Ezen túlmenően a munkáltatónak az email fiók használatának ellenőrzése előtt közölnie kell a munkavállalókkal, hogy milyen érdeke miatt kerül sor a munkáltatói intézkedésre. Másrészt a munkáltatónak a fokozatosság elvére figyelemmel lépcsőzetes ellenőrzési rendszert kell kidolgoznia, amelyben megfelelően érvényesülhet a személyes adatok védelme, illetve hogy az ellenőrzés minél kisebb mértékben érintse a munkavállalók magánszféráját.

Így például az ellenőrzés első lépéseként az e-mail cím és a levél tárgyának az ellenőrzése is elegendő lehet, hiszen bizonyos esetekben már pusztán az e-mail cím felépítéséből és az e-mail tárgyából is lehet látni azt, hogy az magáncélú e-mail cím lesz, és ezért nem szükséges megismerni az e-mail tartalmát. Különösen fontos ez abban az esetben, ha a munkáltató a belső szabályzatban engedélyezi, hogy a munkavállalók a „céges e-mail fiókot” személyes célból is használják, hiszen ekkor a munkavállalók a szabályzattal összhangban magánjellegű leveleket küldhetnek mások számára, vagy fogadhatnak másoktól. Emellett, ha például a munkáltató nem engedélyezi az e-mail fiók magáncélú használatát, és az ellenőrzés pusztán arra terjed ki, hogy megállapítsa azt, hogy a munkavállalók betartották-e ezt a munkáltatói rendelkezést, akkor szintén elegendő az e-mail címének és tárgyának megtekintése, és nem szükséges a levél tartalmának megismerése, hiszen munkajogi jogkövetkezményeket már ezen tény megállapítása alapján is alkalmazhat a munkavállalókkal szemben.

A magánjellegű levelekkel kapcsolatban szükséges kiemelni azt is, hogy az ilyen e-mailek tartalmát a munkáltató nem jogosult megismerni. A kialakult adatvédelmi gyakorlat szerint a munkáltató nem jogosult az e-mail fiókban tárolt magánjellegű e-mailek tartalmát ellenőrizni még akkor sem, ha az ellenőrzés tényéről előzetesen a munkavállalókat tájékoztatta.

Az ellenőrzést ekkor a munkavállalók személyes adataik védelméhez való joga, illetve azoknak a nem munkavállaló harmadik személyeknek a személyes adataik védelméhez való joga – továbbá más személyiségi joga, így elsősorban a magántitokhoz és a levéltitokhoz való joga – korlátozza, akik az e-mailt a munkavállalóknak küldték vagy tőlük azt kapták.

Ezt követően kerülhet sor az e-mail fiók használatának magasabb szintű, részletekbe menő ellenőrzésére, azonban itt is ügyelni kell a fokozatosságra, illetve arra, hogy milyen információk állnak a munkáltató rendelkezésére a konkrét jogsértéssel kapcsolatban. Ugyanis ezek az információk befolyásolhatják az ellenőrzés fókuszát, menetét. Így például a munkáltató rendelkezésére állhat az az információ, hogy az e-mailhez csatolt nagy méretű mellékletben továbbítottak egy, az üzleti érdeke szempontjából fontos dokumentumot, és ekkor a forgalmi adatok elemzése útján megállapítható, hogy a levelezőrendszeren keresztül történt-e nagy méretű mellékletet tartalmazó e-mail kiküldése. Ha pedig meghatározott időintervallumban történt jogsértő e-mail kiküldése, akkor nyilvánvalóan elegendő ezen e-mailek áttekintése is.

Az e-mailek tartalmának ellenőrzésére is ebben az esetben van lehetősége a munkáltatónak, hiszen ezekkel kapcsolatban már nagy valószínűség szerint kizárható, hogy munkavállaló magánszféráját érintő e-mail tartalmát ismerhetné meg. Az e-mail fiók használatánál főszabályként biztosítani kell a munkavállaló jelenlétét. A munkáltatói ellenőrzés e formájánál ugyanis a munkavállaló és harmadik személyek különböző személyes adatai lehetnek benne a levelezőrendszerben, amelyek megismerésére a munkáltató nem jogosult. Ha ez ellenőrzésnél a munkavállaló jelen van, és jelezheti valamely email tartalmának megtekintése előtt, hogy azok személyes adatokat tartalmaznak, akkor ezzel biztosítható, hogy a munkáltató ne sértse meg ezt a tilalmat. Ahhoz, hogy az e-mail fiók ellenőrzése jogszerű legyen, a munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára.

A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy: - milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az e-mail fiók ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdekek miatt kerül sor az ellenőrzésre), - a munkáltató részéről ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

6. A munkáltató által a munkavállaló rendelkezésére bocsátott laptop ellenőrzése

Előzetes intézkedések

A munkáltató bizonyos munkakörben dolgozó munkavállalók számára „céges laptopot” biztosíthat a munkájuk elvégzéséhez. Ezzel összefüggésben is felmerülhet az a probléma, hogy a laptopot a munkavállalók saját, személyes céljaira is használhatják, amely visszas helyzetet teremthet abban az esetben, ha a munkáltató a laptop tartalmáról biztonsági mentést kíván készíteni vagy – az Mt. 11. §-ában foglalt jogával élve – ellenőrizni kívánja a laptopon tárolt adatokat. A munkáltatónak ezért mindenekelőtt egy belső szabályzatot kell megalkotnia a „céges laptop” használatának, ellenőrzésének szabályairól. Ezzel ugyanis hatékonyan meg lehet előzni azt, hogy a munkavállalók (és adott esetben más érintettek) személyes adatait is kezelje a munkáltató. A belső szabályzatban többek között az alábbiakra szükséges kitérni:

- használható-e magáncélokra a „céges laptop”,
- a laptopról biztonsági mentés készítésének és megőrzésének a szabályozására, illetve arra, hogy mikor kerül sor az e-mailek végleges törlésére,
- a laptopon tárolt adatok ellenőrzésének részletes szabályaira.

Amennyiben a munkáltató engedélyezi a laptop magáncélú használatát, akkor erre vonatkozóan plusz intézkedéseket szükséges meghoznia, így például a laptop merevlemezén több partíciót létrehozni, amellyel biztosítható, hogy a merevlemez egyik részén található a munkavégzéssel összefüggő adatok, míg a másik részén pedig a munkavállaló személyes adatai. Ugyanis mind a laptopról készített biztonsági mentés során, mind a laptop ellenőrzése során a munkáltatónak kiemelt figyelmet kell fordítania arra, hogy a munkavállalók magánélettel kapcsolatos személyes adatait nem kezelheti. Ennek megfelelően úgy kell kialakítani a biztonsági mentés szabályait, hogy az ne terjedjen ki a laptopon tárolt személyes adatokra. Ezen túlmenően a munkáltatói ellenőrzést is úgy kell a munkáltatónak végrehajtania, hogy az ellenőrzés ne érintse a laptopon található személyes adatokat, azokat az ellenőrzéssel összefüggésben nem tárolhatja.

Adatvédelmi követelmények

A „céges laptop” tartalmának ellenőrzése esetében a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ezért a munkáltatónak az adatkezelés megkezdése előtt el kell végeznie az érdekmérlegelés tesztjét.

Ezen ellenőrzés esetében kiemelt figyelmet kell fordítani az célhoz kötött adatkezelés elvén és a szükségesség-arányosság követelményén túl az érintettek magánszférájára is, hiszen adott esetben különféle, a munkaviszonyhoz nem kapcsolódó személyes adat is a munkáltató tudomására juthat, illetve vele munkaviszonyban nem álló személyek adatait is megismerheti. Ennek megfelelően a munkáltatónak már előzetesen, a szabályzat megalkotása során meg kell határozni azt, hogy milyen céljai, érdekei miatt kerülhet sor a „céges laptop” tartalmának ellenőrzésére. Ezen érdekeknek ténylegesnek és valósnak, a munkáltató tevékenységéhez, piaci helyzetéhez és a munkavállaló munkaköréhez igazodóknak kell lenniük.

Ezen túlmenően a munkáltatónak a laptop tartalmának ellenőrzése előtt közölnie kell a munkavállalóval, hogy pontosan milyen érdeke miatt kerül sor a munkáltatói intézkedésre.

Másrészt a munkáltatónak a fokozatosság elvére figyelemmel lépcsőzetes ellenőrzési rendszert kell kidolgoznia, amelyben megfelelően érvényesülhet a személyes adatok védelme, illetve hogy az ellenőrzés minél kisebb mértékben érintse a munkavállalók magánszféráját. A laptop tartalmának az ellenőrzése során ezért főszabályként biztosítani kell a munkavállalók jelenlétét.

A munkáltatói ellenőrzés e formájánál ugyanis a munkavállalók és harmadik személyek különböző személyes adatai lehetnek a laptopon, amelyek megismerésére a munkáltató nem jogosult. Ha az ellenőrzésnél a munkavállaló jelen van, és jelezheti valamely email tartalmának megtekintése előtt, hogy azok személyes adatokat tartalmaznak, akkor ezzel biztosítható, hogy a munkáltató ne sértse meg ezt a tilalmat.

Speciális követelmények, ha a laptop magáncélú használatát nem engedélyezi a munkáltató

Amennyiben a szabályzatban a munkáltató nem engedélyezi a „céges laptop” magáncélú használatát, akkor ebben a munkáltató kifejezetten hívja fel a munkavállalók figyelmét arra, hogy a laptop csak munkavégzéssel összefüggő célokra használható, és a munkáltató valamennyi, a laptopon tárolt adatait ellenőrizheti. Ebben az esetben a munkavállalók tisztában vannak azzal, hogy személyes adatokat nem tárolhatnak a laptopon, vagy ha ezt mégis megteszik, a munkáltató velük szemben munkajogi jogkövetkezményeket alkalmazhat.

Mint már korábban szó volt róla, a munkáltató ebben az esetben is pusztán azt a tényt rögzítheti, hogy a munkavállalók a laptopon – a belső szabályzat előírásai ellenére – személyes adatokat tároltak, azonban ezen túlmenően a munkáltató nem kezelhet személyes adatokat, tehát azt már nem rögzítheti, hogy a munkavállalók pontosan milyen adatokat is tároltak a gépen (például milyen fényképeket, videókat, dokumentumokat).

Egyéb adatvédelmi követelmények

Ahhoz, hogy a laptop tartalmának az ellenőrzése jogszerű legyen, a munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára.

A tájékoztatásban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az laptop ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak a „céges laptop” ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

7. Az internethasználat ellenőrizhetősége

Az ellenőrzés e formájával összefüggésben előzetesen érdemes kiemelni, hogy a munkavállaló által meglátogatott weboldal vagy az internethasználatával kapcsolatban a számítógépen rögzített, lementett információk (például az elmentett felhasználónév, jelszó) a munkavállaló személyes adatainak tekinthetők. Ebből fakadóan a munkáltatónak a munkavállalók internethasználatával összefüggésben is tekintettel kell lenniük az adatvédelmi követelményekre.

Az ellenőrzést megelőzően a munkáltatónak célszerű egy belső szabályzatot készítenie, amelyben ki kell térnie többek között:

- arra, hogy mely honlapok megtekintését tiltja (blokkolja) a munkahelyi számítógépeken,
- az ellenőrzés lefolytatására vonatkozó részletes szabályokra.

Amennyiben a munkáltató szabályzata előre meghatározza, hogy mely honlapok megtekintését blokkolja a munkáltató informatikai rendszere, akkor ezzel jelentősen csökkenteni lehet annak esélyét, hogy az internethasználat esetleges ellenőrzésére egyáltalán sor kerüljön.

Ezzel egyidejűleg ugyanakkor a munkáltatói ellenőrzés lehetőségének is meg kell maradnia, hiszen a munkavállalók adott esetben a tiltást „kijátszhatják” vagy más, a tiltásban nem szereplő, de ahhoz hasonló honlapot tekinthetnek meg a munkahelyükön, amely miatt a munkáltató – az Mt. 11. §- ában foglalt jogával élve – ellenőrizheti, hogy munkavállalók megtartották-e a belső szabályzat előírásait, és adott esetben munkajogi jogkövetkezményt alkalmazhat velük szemben.

Az internethasználat ellenőrzése esetén – mint más munkáltatói ellenőrzéseknél is – szintén a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ennek megfelelően a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét a rendszer bevezetése előtt.

Az érdekmérlegelési teszt elvégzése során a munkáltatónak többek között az alábbi követelményeket kell betartania:

A munkáltatónak előzetesen meg kell határoznia azt, hogy milyen céljai, érdekei miatt kerülhet sor az internethasználat ellenőrzésére. Ezen érdekeknek ténylegesnek és valósnak, a munkáltató tevékenységéhez, piaci helyzetéhez, a munkavállaló munkaköréhez igazodóknak kell lenniük. Ezen túlmenően a munkáltatónak az internethasználat ellenőrzése előtt közölnie kell a munkavállalókkal, hogy pontosan milyen érdekei miatt kerül sor a munkáltatói intézkedésre.

Az ellenőrzés csak az ahhoz szükséges személyes adatok megismerésére terjedhet ki. Ha például a munkáltató bizonyos honlapok látogatását blokkolja, és az ellenőrzése pusztán arra terjed ki, hogy megállapítsa azt, hogy munkavállaló betartotta-e ezt a munkáltatói rendelkezést, akkor elegendő a honlap címének a megismerése és feljegyzése, és nem szükséges a munkavállaló tevékenységének részletes feltérképezése (mit is csinált a honlapon, milyen felhasználó nevet és jelszavat mentett el, esetleg milyen fájlokat mentett le a honlapról).

Ahhoz, hogy az internethasználat ellenőrzése jogszerű legyen, a munkáltatónak előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára.

A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az internethasználat ellenőrzésére (illetve természetesen a konkrét ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre),
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségeik vannak a munkavállalóknak az internet használatának ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

8. A „céges mobiltelefon” használatának ellenőrizhetősége

Előzetes intézkedések

Egyre több munkáltatónál elterjedt gyakorlat, hogy „céges mobiltelefont” biztosítanak a munkavállalók számára, amelynek magáncélú használata sok esetben nem tisztázott. Ezért ebben az esetben szükséges, hogy a munkáltató belső szabályzatban rendelkezzen többek között arról, hogy használható-e magáncélokra a „céges mobiltelefon”, és ha igen, akkor a magáncélú hívások költségeit a munkavállalóknak kell-e viselniük, valamint arra is, hogy milyen esetben kerülhet sor a „céges telefon” használatának ellenőrzésére.

A nem engedélyezett magáncélú telefonhasználat ellenőrzése

Amennyiben a munkáltató nem engedélyezi a „céges mobiltelefon” magáncélú használatát, akkor a munkáltató kifejezetten hívja fel a munkavállalók figyelmét arra, hogy a mobiltelefon csak munkavégzéssel összefüggő célokra használható, és a munkáltató valamennyi kimenő hívás hívószámát és adatait ellenőrizheti. Ebben az esetben a munkavállalók tisztában vannak azzal, hogy magáncélú hívást nem kezdeményezhetnek, vagy ha ezt mégis megteszik, a munkáltató – élve az Mt. 11. §-ában szereplő ellenőrzési jogával – megismerheti a hívásokat annak érdekében, hogy a magáncélú és a munkavégzési célú telefonhasználatot elkülönítse, illetve a magáncélú hívások tényét deklarálja, bizonyítsa.

Azonban ezen túlmenően a munkáltató nem kezelhet személyes adatokat, tehát azt már nem ismerheti meg, hogy a munkavállaló magáncélból kit és mikor hívtak fel, minthogy ennek megismerése már nem elengedhetetlenül szükséges az ellenőrzés céljához, illetve az Mt. 11. § (1) bekezdése is kimondja azt, hogy a munkavállaló magánélete nem ellenőrizhető.

Az engedélyezett magáncélú telefonhasználat ellenőrzése

Ha a „céges mobiltelefon” magáncélra is használható, akkor a Hatóság jó gyakorlatnak tekinti azt, ha a kimenő hívások két előhívóval vehetőek igénybe: az egyik előhívó a hivatalos, a másik előhívó a magáncélú hívások során használható. A hivatalos hívások adatait a munkáltató megismerheti, a magáncélú hívások adatait nem. A munkáltató ezzel kapcsolatban előírhatja, hogy a magáncélú hívások költségeit a munkavállaló viselje. A Hatóság emellett a magáncélú telefonhasználat engedélyezése során elfogadhatónak tartja azt is, hogy a munkáltató hívásrészletezőt kér a telefonszolgáltatótól és felhívja a munkavállalót arra, hogy a dokumentumon a magáncélú hívások esetében a hívott számokat tegye felismerhetetlenné.

A fennmaradó telefonszámokat a munkáltató megismerheti, hiszen azokat a munkáltató képviselőjében hívta fel a munkavállaló. A munkáltató természetesen ekkor is előírhatja, hogy a magáncélú hívások költségeit a munkavállaló viselje.

A fenti ellenőrzések esetén is érvényes, hogy a munkáltató nem kezelhet személyes adatokat, tehát azt már nem ismerheti meg, hogy a munkavállaló magáncélból kit és mikor hívott fel.

További adatvédelmi követelmények

A „céges mobiltelefon” használatának ellenőrzése esetén ugyancsak a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ennek megfelelően a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét a rendszer bevezetése előtt. Az érdekmérlegelési teszt elvégzése során a munkáltatónak a fent már kifejtett követelményeket kell betartania. Ennek megfelelően a munkáltatónak meg kell határoznia, hogy milyen módon használhatják a munkavállalók a „céges mobiltelefont”, illetve az ellenőrzés is ehhez az előíráshoz kapcsolódhat. Az ellenőrzés nem terjedhet ki arra, hogy a munkavállaló magáncélból kit és mikor hívtak fel.

Mint már korábban, a többi munkáltatói ellenőrzésnél is szó volt róla, az adatkezelés jogszerűségéhez elengedhetetlen, hogy a munkáltató előzetesen részletes tájékoztatást biztosítson a munkavállaló számára.

A tájékoztatóban a munkáltatónak ki kell térnie többek között arra, hogy:

- hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor a „céges mobiltelefon” használatának ellenőrzésére,
- a munkáltató részéről ki végezheti az ellenőrzést,
- milyen szabályok szerint kerülhet sor ellenőrzésre és mi az eljárás menete,
- milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak „céges mobiltelefon” ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

9. GPS navigációs rendszer alkalmazhatósága

A GPS navigációs rendszer által tárolt adat a gépjárművet vezető személyes adatának is minősül, minthogy annak alapján következtetéseket lehet levonni a munkavállalóra (például mikor, milyen útvonalon haladt a munkavállaló, mennyi idő alatt milyen távolságot tett meg).

A GPS alkalmazását a Hatóság logisztikai célból javasolja alkalmazni, a jármű helyzetének a meghatározására kell szolgálnia, nem pedig a munkavállaló követésére.

A munkafolyamatok, és ezáltal közvetve a munkavállaló ellenőrzése kizárólag munkával, munkaszervezéssel összefüggő célokat szolgálhat.

A GPS rendszer alkalmazása esetén – mint más munkáltatói ellenőrzéseknél is – szintén a munkáltatói jogos érdek lesz az adatkezelés jogalapja, ennek megfelelően a munkáltatónak el kell végeznie az érdekmérlegelés tesztjét a rendszer bevezetése előtt. A GPS navigációs rendszer alkalmazása esetében az érdekmérlegelési teszt egyik központi kérdése, hogy milyen cél érdekében kívánja alkalmazni a munkáltató a rendszert, és miért is jelenti e rendszer alkalmazása a munkavállalók személyes adatainak védelméhez fűződő jogának arányos korlátozását. Elfogadható a munkáltató részéről az, ha a rendszer alkalmazásának célja az, hogy a munkáltató egyes munkakörök esetében hatékonyabban szervezze meg a munkafolyamatokat, így például ha a munkáltatónak munkaszervezési szempontból szükséges tudnia azt, hogy egy futár vagy egy fuvarozó az adott időpontban hol jár. Ezen kívül abban az esetben is jogszerű a GPS alkalmazása, ha a gépjármű szállítmánya, rakománya (így például jelentős összegű készpénz, nagy értékű vagyontárgy, veszélyes áru szállítása), vagy maga a gépjármű, illetve annak értéke ezt kifejezetten indokolja.

Jogszerűen alkalmazható GPS továbbá akkor is, ha a munkavállalók életének, testi épségének a megóvása a GPS rendszer alkalmazásának célja (például konfliktus zónán keresztül történő szállítás): amennyiben valamilyen incidens történik, akkor a GPS rendszeren keresztül meg lehet ismerni, hogy merre is járhatott gépjármű a kérdéses időpontban. Emellett az adatokat az Mt. 11. §-án alapuló munkáltatói ellenőrzés során is fel lehet használni, ha a munkáltató azt tapasztalja, hogy munkavállaló nem teljesítette a munkaviszonyából fakadó kötelezettséget (például a munkavállaló indokolatlanul eltért a munkáltatói utasításba adott útvonaltól).

Ezen túlmenően a GPS navigációs rendszer jogszerű alkalmazásához is szükséges, hogy a munkáltató megfelelő tájékoztatást biztosítson a munkavállalók részére, így a tájékoztatónak többek között ki kell térnie arra, hogy - hogy milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az GPS navigációs rendszer adatainak felhasználására, - a munkáltató részéről ki férhet hozzá ezen adatokhoz, - milyen szabályok szerint kerülhet sor az adatok megismerésére, és mi az eljárás menete - amennyiben a munkáltató az Mt. 11. §-ával összhangban végez ellenőrzést, akkor szabályaira (a fokozatosság elvének betartása) és mi az eljárás menete, ki végezheti az ellenőrzést a munkáltató részéről, - milyen jogai és jogorvoslati lehetőségei vannak a munkavállalónak a GPS rendszer alkalmazásával együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés csak munkaidőben történhet és nem ellenőrizhető a munkavállalók földrajzi helyzete munkaidőn kívül.

Egy olyan gépjármű esetében, amellyel jelentős értékű anyagot nem szállítanak, vagy az adott munkavállaló a munkáját otthonában, „home office”-ban látja el, a GPS alkalmazása nem indokolt. Ez azt jelenti, hogy a munkavállalónak lehetőséget kell adni arra, hogy a GPS-t kikapcsolja akkor is, ha az nála marad (például ha a járművet munkaidőn kívül is magánál tarthatja).

10. Biometrikus rendszerek alkalmazhatósága

A biometrikus rendszer

- Egyrészt vannak fizikai és fiziológiai alapú technikák, amelyek a személyek fizikai és fiziológiai jellemzőit vizsgálják (például az ujjlenyomat-ellenőrzés).
- Másrészt vannak a viselkedésen alapuló technikák, amelyek a személyek viselkedését mérik, ide tartozik például a gépirás elemzése, a valamilyen tudatalatti gondolatra, például hazugságra utaló mintázatok.

A biometrikus rendszerek olyan biometrikus adatokat használó alkalmazások, amelyek lehetővé teszik a személyek automatikus azonosítását, illetve hitelesítését, ellenőrzését.

A biometrikus rendszereken keresztül végzett adatkezelés különböző folyamatokat foglal magában, így a felvételt, a tárolást és a megfeleltetést.

Biometrikus felvétel: a biometrikus adatok valamely biometrikus forrásból való kinyerése és azoknak egy egyénhez való kapcsolása. A felvételi szakasz tipikusan az első alkalom, amikor egy egyén kapcsolatba kerül egy adott biometrikus rendszerrel. A felvételhez a legtöbb esetben az egyén személyes közreműködése szükséges (például ujjlenyomattvételezés esetén), ami megfelelő alkalmat adhat a tájékoztatásra és a tisztességes adatfeldolgozásról szóló tájékoztatásra.

Biometrikus tárolás: a felvétel során megszerzett adatok későbbi felhasználás céljából tárolhatók helyben, abban a műveleti központban, ahol a felvételre sor került (például egy olvasóban), vagy az egyén által hordozott valamely eszközön (például egy intelligens kártyán), illetve elküldhető tárolásra egy központosított adatbázisba, amely hozzáférhető egy vagy több biometrikus rendszer számára.

Biometrikus megfeleltetés: ez az a folyamat, amelynek során a (felvételnél rögzített) biometrikus adatokat (sablon) összevetik egy új mintából gyűjtött biometrikus adatokkal (sablonnal) azonosítás, ellenőrzés (hitelesítés) vagy kategorizálás céljából.

Előzetes adatvédelmi követelmények

Egy biometrikus rendszer megfelelőségének értékelése és az arányosság elemzése során előzetesen az alábbiakat kell mérlegelni:

- A rendszer szükséges-e a meghatározott igény kielégítéséhez, azaz használata elengedhetetlen-e ehhez, vagy inkább annak legkényelmesebb vagy legköltséghatékonyabb módja.
- A rendszer valószínűleg elég hatékony lesz-e az adott igény kielégítésében, tekintettel a használni tervezett biometrikus technológia sajátos jellemzőire.
- Arányos-e az elvárt előnyökkel, ha a rendszer miatt sérül a magánélet védelme. Ha az előnyök viszonylag kisebbek, például kényelmesebb az eljárás vagy kismértékű költségmegtakarítás érhető el, akkor nem helyénvaló, ha sérül a magánélet védelme.
- Annak megfontolása, hogy a magánéletbe kisebb mértékben beavatkozó módszerek elérhetnék-e a kívánt célt. Az arányosság elvének egyik központi kérdése, hogy van-e alternatívája a biometrikus rendszer alkalmazásának.

Az adatkezelő minden esetben köteles ellenőrizni, hogy egyes alternatív intézkedések lehetnének-e a kitűzött célra tekintettel ugyanolyan hatékonyak, de kisebb beavatkozással járók, és köteles ezeket az alternatívákat választani.

Természetesen vannak esetek, amikor a biometrikus rendszerek használata az adatkezelő jogszerű érdekét szolgálja. Az ilyen érdek azonban csak akkor jogszerű, ha az adatkezelő bizonyítani tudja, hogy az érdeke objektív módon magasabb rendű az érintett azon jogánál, hogy ne vegyék fel egy biometrikus rendszerbe.

A fentiek alapján megállapítható, hogy általánosságban a biometrikus rendszerek alkalmazása nem elengedhetetlen és nem a legkíméletesebb eszköz a munkavállalók ellenőrzésénél. Így például az ujjlenyomatos munkaidő-nyilvántartással kapcsolatban megállapítható, hogy a munkavállalók ellenőrzését mint célt más, a magánszférát kímélőbb módszerekkel is el lehet érni, ezért ebből a célból nem lehet biometrikus rendszert bevezetni.

11. A belső visszaélés-bejelentési rendszer (whistleblowing) adatvédelmi követelményei

A visszaélés-bejelentési rendszer

Ez egy olyan belső jelentéstételi rendszer, amelyen keresztül jelezni lehet a jogszabálysértő vagy a munkáltató magatartási szabályait sértő cselekményeket, és ezen bejelentéseket aztán vagy a munkáltató vagy egy külső szervezet kivizsgálja. Bejelentést bárki tehet, akinek a bejelentés megtételéhez vagy a bejelentés tárgyát képező magatartás orvoslásához méltányolható jogos érdeke fűződik (így például a munkavállalók, a munkáltatóval szerződéses viszonyban álló személyek).

Követelmények:

- A munkáltatónak a visszaélés-bejelentési rendszer működésére, valamint a bejelentéssel kapcsolatos eljárásra vonatkozóan részletes, magyar nyelvű tájékoztatót kell készítenie, illetve azt a honlapján közzé kell tennie. Emellett, ha a munkáltató rendelkezik magatartási szabályokkal, akkor ezt is nyilvánosságra kell hoznia a honlapon (a Pktv. nem kötelezi a munkáltatókat arra, hogy a belső visszaélés-bejelentési rendszer létrehozása érdekében magatartási szabályokat alkossanak meg).
- A Hatóság álláspontja szerint az a tájékoztatás elfogadható, amely megfelelő részletességgel és pontossággal összefoglalja az eljárási szabályokat és a bejelentési rendszer működését, fenntartva a munkáltató számára annak lehetőségét, hogy a számára lényeges – akár az üzleti titok fogalmába tartozó – információkat ne hozza nyilvánosságra, feltéve, hogy az információk elhagyása nem lehetetleníti el a visszaélés-bejelentési rendszer lényeges körülményeiről való tájékozódást.
- Nem megfelelő, ha a tájékoztatást csupán a cég belső-intranetén teszik elérhetővé. Ez következik a Pktv. rendelkezéseiből is, melyek azt a kötelezettséget róják a munkáltatóra, hogy a visszaélés-bejelentési rendszerrel összefüggő tájékoztatókat (magatartási szabályokat, eljárásra vonatkozó szabályokat) a munkáltató a saját, nyilvános, bárki számára elérhető honlapján hozza nyilvánosságra. Ennek az is az indoka, hogy a Pktv. szabályozása alapján a bejelentési rendszerbe nem csak a munkavállalók, hanem a munkáltatóval munkaviszonyon kívüli más, szerződéses viszonyban álló, vagy olyan személyek is tehetnek bejelentést, akiknek a bejelentés megtételéhez vagy a bejelentés tárgyát képező magatartás orvoslásához méltányolható jogos érdekük fűződik. Ennek megfelelően tehát a foglalkoztatói szervezeteknek sokkal szélesebb személyi kör számára kell tájékoztatást nyújtaniuk, hiszen olyan személyek is tehetnek bejelentést (például beszállítók, alvállalkozók), akik a belső hálózathoz (intranethez) adott esetben nem férhetnek hozzá. A Pktv. rendelkezéseinek sérelmét jelentené az a gyakorlat, ha ezen tájékoztatókat a munkáltató kizárólag az intraneten keresztül tenné közzé.

A kezelhető személyes adatok köre és ideje

- A bejelentés megtételekor a bejelentő a nevét és lakcímét, jogi személy bejelentő esetén annak székhelyét és a bejelentést benyújtó törvényes képviselőjének nevét köteles megadni. Emellett a bejelentőnek nyilatkoznia kell arról, hogy a bejelentést jóhiszeműen teszi olyan körülményekről, amelyekről tudomása van, vagy kellő alappal feltételezi, hogy azok valóságosak. A Pktv. egyébként felhatalmazást biztosít a bejelentőnek, valamint a bejelentésben érintett személynek a bejelentésben megadott személyes adatainak a bejelentés kivizsgálása céljából történő kezelésére.
- A Pktv. rendelkezései szerint a bejelentési rendszerben különleges adatok kezelése tilos. A Pktv. 14. § (3) bekezdése egyértelmű jogalkotói rendelkezés, amely felülírja az Infotv. rendelkezéseinek alkalmazását, mind a kezelhető adatok, mind pedig az alkalmazható jogalapok tekintetében. Ennek megfelelően, mivel a jogalkotó kategorikusan kizárta annak lehetőségét, hogy a visszaélés-bejelentési rendszeren keresztül különleges adatokat kezeljenek, ezért a visszaélés-bejelentési rendszert úgy kell kialakítani, hogy annak keretében a munkáltató különleges adatokat ne kezelhessen.
- A bejelentési rendszerből haladéktalanul törölni kell a bejelentésben nem érintett harmadik személyre vonatkozó, a bejelentés kivizsgálásához nem szükséges, valamint a Pktv. szerint nem kezelhető adatokat.
- A Pktv. meghatározza a személyes adatok kezelésének lehetséges időtartamát. Eszerint a bejelentés kivizsgálására alapvetően 30 nap áll rendelkezésre, de a vizsgálat legfeljebb 3 hónapig tarthat. Ezt követően dönteni kell, hogy a munkáltató alkalmaz-e intézkedést a bejelentés alapján. Amennyiben igen, akkor a vizsgálat alapján megismert személyes adatokat a bejelentés alapján indított eljárások jogerős lezárásáig lehet kezelni. Azonban ha a vizsgálat alapján a bejelentés nem megalapozott vagy további intézkedés megtétele nem szükséges, akkor a személyes adatokat 60 napon belül törölni kell.

Adatvédelmi követelmények:

- A visszaélés-bejelentési rendszer esetében nem csak a bejelentő számára kell tájékoztatást nyújtani az adatkezelésről, hanem a Pktv. kifejezett tájékoztatási kötelezettséget ír elő a bejelentésben érintett személy esetében is, akit a vizsgálat megkezdésekor részletesen tájékoztatni kell a rá vonatkozó bejelentésről, az Infotv. alapján megillető jogairól, valamint az adatai kezelésére vonatkozó szabályokról.
- A bejelentési rendszert úgy kell kialakítani, hogy a nem névtelen bejelentő személyét a bejelentést kivizsgálókon kívül más ne ismerhesse meg. A bejelentést kivizsgálók a vizsgálat lezárásáig vagy a kivizsgálás eredményeképpen történő formális felelősségre vonás kezdeményezéséig a bejelentés tartalmára és a bejelentésben érintett személyekre vonatkozó információkat kötelesek titokban tartani, és azokat – a bejelentésben érintett személy tájékoztatása kivételével – nem oszthatják meg a foglalkoztatói szervezet egyetlen más szervezeti egységével vagy munkatársával sem.

III. GDPR (kivonat a rendeletről)

A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Mindenkinek **joga van** a rá vonatkozó személyes adatok **védelméhez** állampolgárságától és lakóhelyétől függetlenül.

Ez hozzájárul a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség, valamint a gazdasági unió megteremtéséhez.

A személyes adatok védelméhez való jog **nem abszolút jog, azt az arányosság elvével összhangban**, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal.

A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását.

E fejlemények egy olyan szilárd és az eddiginél következetesebb uniós adatvédelmi keretet igényelnek, amelyet erős kikényszeríthetőség támogat. A belső piac működéséből eredő gazdasági és társadalmi integráció lényegesen megnövelte a személyes adatok határokon átnyúló áramlását. Megnövekedett az állami és a magánszereplők, köztük a természetes személyek, egyesületek és a vállalkozások között Unió-szerte zajló személyes adatok cseréje.

E fejlemények egy olyan szilárd és az eddiginél következetesebb uniós adatvédelmi keretet igényelnek, amelyet erős kikényszeríthetőség támogat.

A természetes személyek számára biztosítani kell, hogy saját személyes adataik felett maguk rendelkezzenek.

A személyes adatok Unión belüli áramlása előtti akadályok elhárítása érdekében a természetes személyeknek az ilyen adatok kezelésével összefüggésben fennálló jogait és szabadságait **minden tagállamban azonos szintű védelemben kell részesíteni**, a szabályok következetes és egységes alkalmazását az Unió egész területén biztosítani kell.

A tagállamok számára lehetővé kell tenni, hogy az e rendeletben foglalt szabályok alkalmazását pontosító nemzeti rendelkezéseket tartsanak fenn vagy vezessenek be.

Ez a rendelet nem zárja ki olyan tagállami jog elfogadását, amely meghatározza a különleges adatkezelési helyzetek körülményeit, ezen belül pontosabban megállapítja, hogy milyen feltételek mellett jogszerű a személyes adatok kezelése.

Ahhoz, hogy a személyes adatok az Unió egész területén hatékony védelemben részesüljenek, az érintettek jogait, valamint a személyes adatokat kezelő, illetve az adatkezelést meghatározó személyek kötelezettségeit megerősíteni és részletesen meghatározni szükséges, ugyanakkor pedig az egyes tagállamokban a személyes adatok védelmére vonatkozó szabályok betartásának ellenőrzéséhez és biztosításához egyenértékű hatáskört is biztosítani szükséges, és a jogsértőkre azonos szankciókat kell alkalmazni.

A mikro-, kis- és középvállalkozások sajátos helyzetének figyelembevétele érdekében a 250 főnél kevesebb személyt foglalkoztató szervezetek esetében e rendelet a nyilvántartás vezetése tekintetében eltérést tartalmaz. Emellett, e rendelet alkalmazása során az uniós intézményeket és szerveket, és a tagállamokat és azok felügyeleti hatóságait ösztönözni kell, **hogy vegyék figyelembe a mikro-, kis- és középvállalkozások sajátos szükségleteit.**

A természetes személyeket a személyes adataik kezelésével kapcsolatban e rendelet alapján nyújtott védelem állampolgárságuktól és lakóhelyüktől függetlenül megilleti.

A természetes személyek védelmének **technológiailag semlegesnek kell lennie** és nem függhet a felhasznált technikai megoldásoktól. **A természetes személyek védelme a személyes adatok automatizált eszközök útján végzett kezelése mellett a manuális kezelésre is vonatkozik, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni.** Olyan iratok, illetve iratok csoportjai, és azok borítóoldalai, amelyek nem rendszerezettek meghatározott szempontok szerint, nem tartoznak e rendelet hatálya alá.

E rendelet nem vonatkozik

- a nemzetbiztonsággal kapcsolatos tevékenységek.
- Unió közös kül- és biztonságpolitikájával összefüggésben végzett adatkezelésre.

Ez a rendelet nem alkalmazandó a személyes adatoknak a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelésére, amely így semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe. Személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történt kapcsolattartás és online tevékenységek. E rendeletet kell alkalmazni azonban azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják.

Az adatkezelő vagy adatfeldolgozó a tevékenységi helyén folytatott működése során, az Unió területén végzett bármely személyesadat-kezelést e rendelettel összhangban kell végezni, tekintet nélkül arra, hogy maga az adatkezelés az Unió területén történik-e. A tevékenységi hely valamely tevékenység tényleges és valós, tartós jelleget biztosító keretek közötti gyakorlását feltételezi. E keretek jogi formája – legyen szó akár fióktelepről vagy jogi személyiséggel rendelkező leányvállalatról – e tekintetben nem meghatározó tényező.

Az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó általi kezelése abban az esetben is e rendelet hatálya alá tartozik, amennyiben az érintettek Unión belüli magatartásának a megfigyeléséhez kapcsolódnak. Annak meghatározása, hogy az adatkezelés az érintettek magatartásának megfigyelésének minősül-e, meg kell vizsgálni, hogy a természetes személyeket nyomon követik-e az interneten, illetve ezt követően a természetes személy profiljának megalkotását is magában foglaló adatkezelési technikákat alkalmaznak-e, annak érdekében, hogy elsősorban a természetes személyre vonatkozó döntéseket hozzanak, valamint, hogy elemezzék vagy előre jelezzék a természetes személy személyes preferenciáit, magatartását vagy beállítottságát.

Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

Valamely természetes személy azonosíthatóságának meghatározásakor **minden olyan módszert figyelembe kell venni** – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy **a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja.**

Az adatvédelem elveit ennek megfelelően az **anonim információkra nem kell alkalmazni**, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelyek következtében az érintett nem vagy többé nem azonosítható. Ez a rendelet ezért nem vonatkozik az ilyen anonim információk kezelésére, a statisztikai vagy kutatási célú adatkezelést is ideértve.

A természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel. Ezáltal olyan nyomok keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a természetes személyes profiljának létrehozására és az adott személy azonosítására.

Az adatkezelésre csak akkor kerülhet sor, ha **az érintett egyértelmű megerősítő cselekedettel**, például **írásbeli** – ideértve az elektronikus úton tett –, **vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez.** Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során **bejelöl egy erre vonatkozó négyzetet**, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó **technikai beállításokat hajt végre**, valamint bármely egyéb **olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi.** A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak. A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed. **Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni.** Ha az érintett hozzájárulását elektronikus felkérést követően adja meg, a felkérésnek egyértelműnek és tömörnek kell lennie, és az nem gátolhatja szükségtelenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kéri.

A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal.

A személyes adatok kezelésének **jogszerűnek** és **tisztességesnek** kell lennie. A természetes személyek számára **átláthatónak** kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció **könnyen hozzáférhető és közérthető legyen**, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.

A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.

A személyes adatoknak a kezelésük céljára **alkalmasaknak** és **relevánsaknak** kell lenniük, az adatok körét pedig a **célhoz szükséges minimumra kell korlátozni**. Ehhez pedig biztosítani kell különösen azt, hogy a személyes adatok **tárolása a lehető legrövidebb időtartamra korlátozódjon**. Személyes adatok csak abban az esetben kezelhetők, ha **az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni**. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, **az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg**. A pontatlan személyes adatok **helyesbítése** vagy **törlése** érdekében minden észszerű lépést meg kell tenni. A személyes adatokat olyan módon kell kezelni, amely **biztosítja azok megfelelő szintű biztonságát** és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

Annak érdekében, hogy a személyes adatok kezelése jogszerű legyen, annak **az érintett hozzájárulásán kell alapulnia**, vagy valamely egyéb jogszerű, **jogszabály által megállapított – alappal kell rendelkeznie**, ideértve az adatkezelőre vonatkozó **jogi kötelezettségeknek való megfelelés** szükségességét, az érintett által kötött esetleges **szerződés teljesítését**, illetve az érintett által kért, a szerződéskötést megelőzően megteendő lépéseket.

Ha az adatkezelés az érintett hozzájárulásán alapul, az adatkezelő számára lehetővé kell tenni, hogy **bizonyítani tudja, hogy az adatkezelési művelethez az érintett hozzájárult** (az érintett tisztában legyen azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy ezt milyen mértékben tette).

Az adatkezelő **előre megfogalmazott hozzájárulási nyilatkozatról gondoskodik**, amelyet **érthető és könnyen hozzáférhető formában** bocsát rendelkezésre, nyelvezetének pedig **világosnak és egyszerűnek kell lennie**, és **nem tartalmazhat tisztességtelen feltételeket**. Ahhoz, hogy a hozzájárulás tájékoztatáson alapuljon minősüljön, az érintettnek legalább tisztában kell lennie az adatkezelő kilétével és a személyes adatok kezelésének céljával. A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás nélküli megtagadása vagy visszavonása, hogy ez kárára válna.

Annak biztosítása érdekében, hogy hozzájárulást önkéntesen adták, a hozzájárulás olyan egyedi esetekben nem szolgálhat érvényes jogalapként a személyes adatok kezeléséhez, amelyekben az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn, különösen ha az adatkezelő közhatalmi szerv, és az adott helyzet valamennyi körülményét figyelembe véve ezért valószínűtlen, hogy a szóban forgó hozzájárulás megadása önkéntesen történt.

Az adatkezelés jogszerűnek minősül, ha arra valamely **szerződés** vagy szerződéskötési szándék keretében van szükség.

Az adatkezelést szintén jogszerűnek kell tekinteni akkor, amikor az az érintett **életének vagy más természetes személy érdekeinek védelmében történik.**

Az adatkezelő vagy valamely harmadik fél **jogos érdeke jogalapot teremthet az adatkezelésre**, feltéve hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait.

Személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelése szintén az érintett adatkezelő jogos érdekének minősül. **Személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.**

A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték.

Az **átláthatóság** elve megköveteli, hogy a nyilvánosságnak vagy az érintettnek nyújtott **tájékoztatás tömör, könnyen hozzáférhető és könnyen érthető legyen, valamint hogy azt világos és közérthető nyelven fogalmazzák meg**, illetve – ezen túlmenően – szükség esetén vizuálisan is megjelenítsék. Az ilyen tájékoztatás **nyújtható elektronikus formátumban is**, így például a nyilvánosságnak szánt tájékoztatás **közölhető valamely honlapon keresztül**. Ez különösen olyan helyzetekben lehet fontos, amikor a szereplők nagy száma és a gyakorlat technológiai összetettsége megnehezíti az érintett számára annak megismerését és megértését, hogy gyűjtenek-e róla személyes adatokat, és ha igen, ki és milyen célból, ilyen például az online reklámozás esete.

Az érintettnek lehetősége van díjmentesen kérelmezni, illetve adott esetben megkapni különösen a személyes adatokhoz való **hozzáférést**, azok **helyesbítését és törlését**, valamint **gyakorolja a tiltakozáshoz való jogát**. Az adatkezelő ennek megfelelően biztosítja a kérelmek elektronikus benyújtását lehetővé tevő eszközöket is különösen, ha a személyes adatok kezelése elektronikus úton történik. **Az adatkezelőt kötelezni kell arra, hogy az érintett kérelmére indokolatlan késedelem nélkül, de legkésőbb egy hónapon belül válaszoljon, és ha az adatkezelő az érintett bármely kérelmének nem tesz eleget, indokolnia kell azt.**

A tisztességes és átlátható adatkezelés elve megköveteli, hogy az **érintett tájékoztatást kapjon** az adatkezelés tényéről és céljairól.

Az érintettet továbbá a **profilalkotás** tényéről és annak következményeiről tájékoztatni kell. Ha a személyes adatokat az érintettől gyűjtik, az érintettet arról is tájékoztatni kell, hogy köteles-e a személyes adatokat közölni, valamint hogy az adatszolgáltatás elmaradása milyen következményekkel jár.

Az érintettre vonatkozó személyes adatok kezelésével **összefüggő tájékoztatást az adatgyűjtés időpontjában kell az érintett részére megadni**. Ha az adatkezelő a személyes adatokat a gyűjtésük eredeti céljától eltérő célból kívánja kezelni, a további adatkezelést megelőzően az érintettet erről az eltérő célról és minden egyéb szükséges tudnivalóról tájékoztatnia kell.

Az érintett jogosult, hogy **hozzáférjen** a rá vonatkozóan gyűjtött adatokhoz, valamint arra, hogy egyszerűen és észszerű időközönként, az adatkezelés jogszerűségének megállapítása és ellenőrzése érdekében gyakorolja e jogát. Ezért minden érintett számára biztosítani kell a jogot arra, hogy **megismerje különösen a személyes adatok kezelésének céljait**, továbbá ha lehetséges, azt, hogy a személyes adatok **kezelése milyen időtartamra vonatkozik**, a személyes adatok **címzettjeit**, azt, hogy a személyes adatok **automatizált kezelése milyen logika alapján történt**, valamint azt, hogy az adatkezelés – legalább abban az esetben, amikor az profilalkotásra épül – **milyen következményekkel járhat**, továbbá hogy minderről tájékoztatást kapjon.

Az adatkezelő minden észszerű intézkedést megtesz a hozzáférést kérő érintett személyazonosságának megállapítására, különösen az online szolgáltatásokkal és az online azonosítókkal összefüggésben. Az adatkezelő nem őrizheti meg a személyes adatokat kizárólag abból a célból, hogy a lehetséges kérelmeket meg tudja válaszolni.

Az érintett jogosult arra, hogy kérhesse a rá vonatkozó személyes adatok **helyesbítését** és **megilleti őt az „elfeledtetéshez való jog”**, ha a szóban forgó adatok megőrzése sérti e rendeletet vagy az olyan uniós vagy tagállami jogot, amelynek hatálya az adatkezelőre kiterjed. **Az érintett jogosult különösen arra, hogy személyes adatait töröljék és a továbbiakban ne kezeljék**, ha a személyes adatok gyűjtése vagy más módon való kezelése **az adatkezelés eredeti céljaival összefüggésben már nincs szükség, vagy ha az érintettek visszavonták az adatok kezeléshez adott hozzájárulásukat, vagy ha személyes adataik kezelése egyéb szempontból nem felel meg e rendeletnek**.

Ugyanakkor a személyes adatok további megőrzése jogszerűnek tekinthető, ha az a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, valamely jogi kötelezettségnek való megfelelés, illetőleg közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy a népegészségügy területét érintő közérdekből, közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

A személyes adatok kezelésének **korlátozására** alkalmazott módszerek közé tartozhat többek között a szóban forgó személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezése vagy **a felhasználók számára való hozzáférhetőségük megszüntetése, vagy egy honlapról az ott közzétett adatok ideiglenes eltávolítása**. Az adatkezelés korlátozását az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani, oly módon, hogy **a személyes adatokon további adatkezelési műveleteket ne végezzenek el és azokat ne lehessen megváltoztatni**. Azt a tényt, hogy a személyes adatok kezelése korlátozott, egyértelműen jelezni kell a rendszerben.

Ha a személyes adatok kezelése automatizált módon történik, az érintettek számára – a saját adataik feletti rendelkezés további erősítése érdekében – lehetővé kell tenni azt is, hogy az általuk az adatkezelő rendelkezésére bocsátott, rájuk vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban megkapják, és azokat egy másik adatkezelő részére továbbítsák.

Ez a jog abban az esetben gyakorolható, ha az érintett a személyes adatokat a hozzájárulása alapján bocsátotta rendelkezésre, illetve ha az adatkezelés szerződés teljesítéséhez szükséges.

Az érintett azon joga, hogy továbbítsa, illetve megkapja a rá vonatkozóan kezelt személyes adatokat, nem teremthet olyan kötelezettséget az adatkezelők számára, hogy egymással műszakilag kompatibilis adatkezelő rendszereket vezessenek be vagy tartsanak fenn.

Az érintett jogosult arra, hogy az adatokat az adatkezelők egymás között közvetlenül továbbítsák, ha ez technikailag megvalósítható.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett számára biztosítani kell a jogot arra, hogy bármikor díjmentesen tiltakozzon a rá vonatkozó személyes adatok e célból történő – eredeti vagy további – kezelése ellen, amelybe beletartozik a profilalkotás is, ha az a közvetlen üzletszerzéshez kapcsolódik. Az érintett figyelmét e jogra kifejezetten fel kell hívni, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Az érintett jogosult arra, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen alapuló – akár intézkedést is magában foglaló – döntés hatálya, amely a rá vonatkozó egyes személyes jellemzők kiértékelésén alapul, és amely rá nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti, mint például egy online hitelkérelem automatikus elutasítása vagy emberi beavatkozás nélkül folytatott online munkaerő-toborzás. Ilyen adatkezelésnek minősül a „profilalkotás” is, vagyis a természetes személyekre vonatkozó személyes jellemzők bármilyen automatizált személyes adatok kezelése keretében történő kiértékelése, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők elemzésére és előrejelzésére, ha az az érintettre nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti.

Az adatkezelő hatáskörét és felelősségét szabályozni kell. Az adatkezelőt kötelezni kell különösen arra, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek e rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is az e rendelet által előírt szintű.

Ahhoz, hogy az adatkezelő igazolni tudja az e rendeletnek való megfelelést, olyan **belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania**, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit.

Az olyan alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek, a termékek, szolgáltatások és alkalmazások előállítóit arra kell ösztönözni, hogy e termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védeleméhez való jogot.

Annak biztosítása érdekében, hogy az e rendeletben az adatfeldolgozó által az adatkezelő nevében elvégzendő adatkezelésre vonatkozóan előírt követelmények teljesüljenek, ha az adatkezelő adatfeldolgozót bíz meg az adatkezelési tevékenységek elvégzésével, **csakis olyan adatfeldolgozókat vehet igénybe, amelyek megfelelő garanciákat nyújtanak – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy az e rendelet követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtják, ideértve az adatkezelés biztonságát is.** Az adatkezelő kötelezettségei teljesítésének bizonyítására felhasználható, ha az adatfeldolgozó csatlakozik valamelyik jóváhagyott magatartási kódexhez vagy jóváhagyott tanúsítási mechanizmushoz. Az adatkezelés adatfeldolgozó általi elvégzését uniós vagy tagállami jog alapján létrejött szerződés vagy egyéb jogi aktus szabályozza, amely köti adatfeldolgozót az adatkezelővel szemben, meghatározza az adatkezelés tárgyát és időtartamát, az adatkezelés jellegét és céljait, a személyes adatok típusát és az érintettek kategóriáit.

Az adatkezelő és az adatfeldolgozó dönthet egyedi szerződés vagy általános szerződési feltételek alkalmazása mellett.

Az adatkezelő vagy az adatfeldolgozó az e 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.

Az e rendeletnek való megfelelés olyan esetek érdekében történő előmozdítása érdekében, amikor valószínűsíthető, hogy az adatkezelési műveletek magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, az e kockázat forrását, jellegét, egyediségét és súlyosságát felmérő adatvédelmi hatásvizsgálat elvégzéséért az adatkezelő felel. Ha az adatvédelmi hatásvizsgálat szerint az adatkezelési műveletek olyan magas kockázattal járnak, amelyet az adatkezelő nem képes a rendelkezésre álló technológia és a végrehajtási költségek szempontjából is megfelelő intézkedésekkel mérsékelni, az adatkezelést megelőzően a felügyeleti hatósággal konzultálni kell.

Az **adattvédelmi incidens** megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, így amint az adatkezelő tudomására jut az adattvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adattvédelmi incidens a tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adattvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az érintettet az adatkezelő indokolatlan késedelem nélkül tájékoztatja, ha az adattvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket.

A nemzetközi kereskedelem és a nemzetközi együttműködés bővítéséhez szükség van a személyes adatoknak az Unió kívüli országok és a nemzetközi szervezetek viszonylatában megvalósuló forgalmára. Az ilyen forgalom növekedése új kihívásokat és problémákat támaszt a személyes adatok védelme tekintetében. Mindazonáltal **a személyes adatoknak az Unióból harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezetek részére történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban e rendelettel biztosított védelem szintje.**

Tárgy:

Ez a rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg. (2) Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

Tárgyi hatály:

E rendeletet kell alkalmazni **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.**

Területi hatály:

E rendeletet kell alkalmazni a személyes adatoknak **az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók** tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.

E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:

- a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
- b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.

A személyes adatok kezelésére vonatkozó elvek

A személyes adatok:

- 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; 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 („**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**”).

Az adatkezelő felelős az alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („**elszámoltathatóság**”).

Az adatkezelés jogszerűsége

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

- 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 gyermek.

A hozzájárulás feltételei:

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

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 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.

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 – feltételül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

A gyermek hozzájárulására vonatkozó feltételek:

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 személyes adatok különleges kategóriáinak kezelése:

A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.

Az előző bekezdés **nem alkalmazandó** abban az esetben, ha:

- a) az érintett kifejezett hozzájárulását adta,
- b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges,
- c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni,
- d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára
- e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott,
- f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el,
- g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján,
- h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása érdekében szükséges,
- i) az adatkezelés a népegészségügy területét érintő közérdekből szükséges,
- j) az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges.

Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

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

Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni.

Az adatkezelő az érintett jogai gyakorlására irányuló kérelmének a teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az érintettet nem áll módjában azonosítani.

Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Az információkat és a tájékoztatást és intézkedést díjmentesen kell biztosítani.

Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

- a) észszerű összegű díjat számíthat fel, vagy
- b) megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adatkezelőt terheli.

Tájékoztatás és a személyes adatokhoz való hozzáférés:

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

- a) az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
- b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
- c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- d) az adatkezelő vagy harmadik fél jogos érdekei (ha az adatkezelés ezen a jogcímen kívánja végezni);
- e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- f) adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

Az adatkezelő a személyes adatok megszerzésének időpontjában, annak érdekében, hogy a tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

- a) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
- b) az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
- c) a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása;
- f) az esetleges automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Ha a személyes adatokat **nem az érintettől szerezték meg**, az adatkezelő az érintett rendelkezésére bocsátja a következő információkat:

- a) az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
- b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
- c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- d) az érintett személyes adatok kategóriái;
- e) a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- f) adott esetben annak ténye, hogy az adatkezelő valamely harmadik országbeli címzett vagy valamely nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

Az érintett hozzáférési joga:

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- a) az adatkezelés céljai;
- b) az érintett személyes adatok kategóriái;
- c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- h) az esetleges automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

A helyesbítéshez való jog:

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

A törléshez való jog („az elfeledtetéshez való jog”):

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

- IV. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- V. az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- VI. az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- VII. a személyes adatokat jogellenesen kezelték;
- VIII. a személyes adatokat az adatkezelőre alkalmazandó jogi kötelezettség teljesítéséhez törölni kell;

Az adatkezelés korlátozásához való jog:

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

- a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- d) (jogos érdek érvényesítése esetén) tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség:

Az adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

Az adathordozhatósághoz való jog:

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

- a) az adatkezelés hozzájáruláson, vagy szerződésen alapul; és
- b) az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

A tiltakozáshoz való jog:

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a 6. cikk (1) bekezdésének e) (közhatalmi jogosítvány) vagy f) (jogos érdekek érvényesítése) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

A fentebb említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást:

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Az előző bekezdés nem alkalmazandó abban az esetben, ha a döntés:

- a) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- b) meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
- c) az érintett kifejezett hozzájárulásán alapul.

Az adatkezelő köteles megfelelő intézkedéseket tenni, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

Az adatkezelő feladatai:

Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

Ha az az **adatkezelési tevékenység vonatkozásában arányos**, az előző bekezdésben említett intézkedések részeként **az adatkezelő megfelelő belső adatvédelmi szabályokat** is alkalmaz.

Beépített és alapértelmezett adatvédelem:

Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Az adatfeldolgozó:

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.

Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

Az adatfeldolgozó által végzett adatkezelést szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben:

- a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli;
- biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- 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;
- az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges.

Ha egy adatfeldolgozó e rendeletet sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni.

Az adatkezelő vagy az adatfeldolgozó irányítása alatt végzett adatkezelés:

Az adatfeldolgozó és bármely, az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi.

Az adatkezelési tevékenységek nyilvántartása:

Minden adatkezelő és – ha van ilyen – az adatkezelő képviselője a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet.

E nyilvántartás a következő információkat tartalmazza:

- a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- b) az adatkezelés céljai;
- c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk,
- f) ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidők;
- g) ha lehetséges, a technikai és szervezési intézkedések általános leírása.

Az adatkezelés biztonsága:

Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a) a személyes adatok álnevesítését és titkosítását;
- b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak:

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A bejelentésben legalább:

- a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

Az érintett tájékoztatása az adatvédelmi incidensről:

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről; világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét.

Adatvédelmi hatásvizsgálat:

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, **valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve**, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

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 adatkezelő konzultál a felügyeleti hatósággal.

Az adatvédelmi tisztviselő kijelölése:

Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:

- a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
- b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;
- c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak és a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait.

Az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a felügyeleti hatósággal közli.

Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

- a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- b) ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- d) együttműködik a felügyeleti hatósággal; és
- e) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.