



Tartalomjegyzék - Mellékletek jegyzéke

GDPR megfelelési csomag

1. Tartalomjegyzék, mellékletek jegyzéke, leírása - Adobe Acrobat Document (.pdf)

Jelen melléklet arra szolgál, hogy számba vehessük a csomag tartalmát, illetve a mellékletek számát, terjedelmét.

2. GDPR kézikönyv – Adobe Acrobat Document (.pdf)

A GDPR kézikönyv egy olyan hasznos dokumentum, mely lépésről lépésre veszi át a GDPR megfelelést, így tisztázva az alapvető feladatokat és célokat a cégek számára. Ez az adatvédelmi jogban és informatikai biztonságban egyaránt jártas szakembereink által készített segédlet konkrét GDPR megfelelési projektek tapasztalatai alapján készült, így gyakorlati útmutatóként szolgál a GDPR megfelelés lépéseihez.

3. GDPR cselekvési terv - Adobe Acrobat Document (.pdf)

Ez a melléklet tartalmaz egy 12 lépéses cselekvési tervet a GDPR megfeleléshez, illetve a különböző lépésekhez kapcsolódóan az általunk csatolt, adott pontnál alkalmazandó mellékletek megjelölését. Ennél a dokumentumnál a NAIH GDPR megfelelési lépésekre tett ajánlását vettük alapul, és minden egyes lépésnél megjelöltük, mely általunk csatolt anyagok használhatók fel az adott pont teljesítéséhez.

4. Adatvédelmi szabályzat minta - Microsoft Word-dokumentum (.docx)

A GDPR által lefektetett elszámoltathatóság elvének és a jogszerű adatkezelés, illetve adatfeldolgozás követelményének való megfelelés mindenkit kötelez, aki a GDPR hatálya alá tartozik. A GDPR 24. cikk (2) bekezdése kimondja, hogy az adatkezelőnek a személyes adatok védelmének biztosítása céljából megvalósított technikai és szervezési intézkedések részeként belső adatvédelmi szabályokat alkalmaznia, ha ez az adatkezelési tevékenység vonatkozásában arányos. Bár nem jelenthető ki ez alapján minden adatkezelőre kiterjedő kötelezettség, szervezeti működés esetén az adatkezeléssel kapcsolatos kérdésekre is kiterjedő belső szabályzat hiányában az adatkezelő nehezen tud megfelelni az adatvédelemmel kapcsolatos jogszabályi követelményeknek, valamint enélkül a megfelelés igazolása - az elszámoltathatóság elve szerint - szintén akadályozott.

A GDPR e követelményének való megfelelést tesszük könnyebbé jogi szakértelemmel rendelkező kollégáink által megalkotott, mind a GDPR rendelkezéseit, mind egyéb jogszabályokat figyelembe vevő adatvédelmi szabályzat mintánk segítségével.

5. Adatkezelési tájékoztató minta - Microsoft Word-dokumentum (.docx)

Az adatkezelésről minden esetben szükséges az érintetteket tájékoztatni a GDPR 12-14. cikkeiben előírt kötelezettségnek megfelelően. Az említett cikkekben foglalt követelményeknek való megfeleléshez az adatkezelési tájékoztató kötelező tartalmát a GDPR 13-14. cikkei meghatározzák. Legalább az itt felsorolt információkat tartalmaznia kell az adatkezelési tájékoztatónak, vagyis a tájékoztatóban az adatkezelő az érintetteket (pl. kamerák alkalmazás esetén a megfigyelt területre belépőket) tájékoztatja az általa végzett adatkezelés részleteiről, valamint az érintettet megillető jogokról, jogorvoslati lehetőségekről és azok érvényesítésének módjáról.

Adatkezelési tájékoztató mintánk tartalmazza mindezen feltételeket az átlátható tájékoztatásra vonatkozó követelmények teljesítése érdekében.

6. Munkavállalói titoktartási nyilatkozat - Microsoft Word-dokumentum (.docx)

A GDPR által követelményként megfogalmazott elszámoltathatóság elvéből következik, hogy az adatkezelőnek és adatfeldolgozónak kell bizonyítania adatkezelésének jogszerűségét, így azt is, hogy munkavállalóik megfelelő tájékoztatást kaptak a személyes adatok kezeléséről, annak elveiről, és hogy ezek tudatában titoktartási kötelezettséget vállaltak azon személyes adatokra vonatkozóan, melyekkel munkájuk során kapcsolatba kerülhetnek.

A titoktartási nyilatkozatot az újonnan belépő munkavállalókkal munkába lépésük idején, illetve a már alkalmazásban lévő munkavállalókkal szükséges aláíratni.

Csomagunkban egy olyan titoktartási nyilatkozat sablon található, amely általánosan alkalmazható a munkáltatók által, hogy biztosítsák és bizonyítsák, személyes adatokkal kapcsolatba kerülő munkavállalóik megfelelő titoktartási kötelezettséget vállaltak.

7. Ábra annak eldöntésére, hogy mely esetekben szükséges adatvédelmi tisztviselő kijelölése - Adobe Acrobat Document (.pdf)

A GDPR 37. cikke szerint meghatározott bizonyos esetekben az adatkezelőnek és adatfeldolgozónak adatvédelmi tisztviselőt kell kijelölnie.

Annak ellenére, hogy a GDPR meghatározza, hogy mely esetekben szükséges adatvédelmi tisztviselő kijelölése, ennek eldöntése, így sem egyértelmű feladat. E döntés megkönnyítésére hoztunk létre egy ábrát, mely kicsit vizualizálva, érthetőbb módszerrel segít eligazodni ebben a kérdésben.

8. Adatregiszter sablon - Microsoft Excel-munkalap (.xlsx)

A GDPR 30. cikke szerint - néhány kivétellel - minden adatkezelőnek kötelessége adatkezelési tevékenységeiről nyilvántartást vezetni. Ahhoz, hogy ez a nyilvántartás jogilag megfelelő legyen, tartalmaznia kell a rendeletben meghatározott kötelező elemeket. Éppen ezért létrehoztunk egy olyan adatregiszter sablont ügyfeleink részére, melynek helyes kitöltésével megfelelhetnek a GDPR által támasztott nyilvántartási kötelezettségüknek.

9. Magas kockázatú folyamatokat megállapító módszertan - Microsoft Excel-munkalap (.xlsx)

Sok szempontból fontos lehet, hogy tisztában legyünk vele, mely adatkezelési folyamataink számítanak magas kockázatúnak. Először is tisztáznunk kell egy fontos kérdést, amely felett sok esetben hajlamosak vagyunk átsiklani: az, hogy egy folyamat magas kockázatú, az nem a vállalkozásra jelentett kockázat mértékét jelöli, hanem azt a kockázatot, amely a természetes személyek jogaira és szabadságait érinti. Ennek a ténynek a figyelembe vételével kell tehát megvizsgálnunk a kérdést.

Miért is fontos tehát tudnunk, hogy mely adatkezelési folyamataink számítanak magas kockázatúnak?

Egyrészt ez egy fontos szempont lehet a prioritási sorrend megállapításában, hiszen a magas kockázatú folyamatok mindenképp előtérbe helyezendők az alacsonyabb kockázatúakkal szemben, amikor akár GDPR megfelelésről van szó, akár az adatvédelmi

tisztviselő tevékenységének, feladatainak meghatározásáról. Természetesen ez nem azt jelenti, hogy az alacsonyabb kockázatú folyamatokkal nem kell GDPR szempontból foglalkoznunk, hanem azt, hogy a magas kockázatúakat célszerű sorrendben előrébb venni az intézkedések kapcsán, hiszen ezek a folyamatok magasabb veszélyt jelenthetnek a természetes személyek jogaira és szabadságaira nézve.

Másrészt, ha megválaszoljuk azt a kérdést, melyek a magas kockázatú adatkezelési folyamataink, megválaszoltuk azt is, mely esetekben szükséges az adatvédelmi hatásvizsgálat elvégzése. Hiszen a GDPR 35. cikke szerint olyan adatkezelés esetén, mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek az adatkezelés megkezdése előtt hatásvizsgálatot kell végeznie annak megállapítására, hogy a tervezett adatkezelés hogyan érintik a személyes adatok védelmét.

Annak megállapítására, hogy mely adatkezelési folyamatok számítanak magas kockázatúnak, létrehoztunk egy módszertant, mely a GDPR rendelkezései, illetve a W29-es munkacsoport ajánlásai alapján készült.

10. Hatásvizsgálat módszertan, sablon - Makróbarát Microsoft Excel-munkalap (.xlsm)

A GDPR 35. cikke szerint olyan adatkezelés esetén, mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek az adatkezelés megkezdése előtt hatásvizsgálatot kell végeznie annak megállapítására, hogy a tervezett adatkezelés hogyan érintik a személyes adatok védelmét.

A hatásvizsgálat lényege, hogy a magas kockázatúnak minősített tervezett adatkezeléseket egyenként megvizsgáljuk olyan szempontból, hogy megfelelnek e a GDPR követelményrendszerének, illetve, hogy a tervezett biztonsági intézkedések és az érintettekre jelentett kockázatok összevetésével megfelelően alacsony mértékű maradványkockázattal számolhatunk e, így az adatkezelés elvégezhető, vagy a felügyeleti hatóságok általi előzetes konzultációra szükséges bocsátani.

Az adatvédelmi hatásvizsgálat fontos eszköze az elszámoltathatóságnak, hiszen ennek elvégzésével, megőrzésével és szükség esetén eredményeinek rendelkezésre bocsátásával tudják az adatkezelők bizonyítani a felügyeleti hatóságok felé, hogy adatkezelésük megfelel a törvényi követelményeknek, és hogy megfelelő biztonsági intézkedésekkel hatékonyan csökkentik az adatkezeléssel járó kockázatokat.

A GDPR meghatározza ugyan, hogy bizonyos esetekben hatásvizsgálatot kell végezni, azonban annak módszertanára nem kapunk egyértelmű iránymutatást, ennek kidolgozását a hatásvizsgálat elvégzéséért felelős cégekre bízta. Ennek köszönhetően nincs egy konkrét általános módszertan, amely mindenki által alkalmazandó, viszont többféle megközelítés létezik.

Cégünk kialakított egy módszertant, és erre építve egy sablont, amely megfelel a GDPR követelményrendszerének, illetve a kitöltendő részek mindegyike olyan magyarázatokkal van ellátva, amely lehetővé teszi annak megfelelő kitöltését.

Annak megállapítása sem minden esetben egyértelmű, hogy mely adatkezelések esetén szükséges az adatvédelmi hatásvizsgálat elvégzése, így a hatásvizsgálat részeként mellékelünk egy magas kockázatú folyamatok megállapításában segítséget nyújtó módszertant is.

11. A NAIH iránymutatása az adatvédelmi hatásvizsgálatról - Adobe Acrobat Document (.pdf)

Ez a dokumentum a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) iránymutatásait tartalmazza az adatvédelmi hatásvizsgálat elvégzéséről.

12. Érdelmérlegelési teszt módszertan, sablon – Microsoft Excel-munkalap (.xlsx)

A GDPR szerint csak meghatározott jogalapok szerinti adatkezelés számít jogszerűnek. Az adatkezelés jogalapját a legtöbb helyen fel kell tüntetni, így az adatkezelési nyilvántartásokban, hatásvizsgálatokban, az érintettek tájékoztatásakor. Azokban az esetekben, amikor az adatkezelés jogalapjaként kizárólag az adatkezelő, vagy egy harmadik fél jogos érdekét tudjuk megjelölni, szükséges egy érdelmérlegelési teszt lefuttatása annak bizonyítására, hogy ezen érdekekkel szemben nem élveznek elsőbbséget az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek a személyes adatok védelmét teszik szükségessé. A GDPR azonban arra nem tartalmaz egyértelmű utasítást, hogy ezt milyen módszerrel tudjuk eldönteni.

Ennek következtében az érdelmérlegelési teszt egy kényes területe a GDPR-nak, nem létezik még rá egy mindenki által elfogadott, hozzáférhető, általános módszertan. Ennek a követelménynek való megfelelésre is van azonban kidolgozott megoldásunk. Jogi szakértelemmel rendelkező kollégáink kidolgoztak egy érdek-mérlegelés módszertant és sablont, hogy még ezt a nehezen megfogható területet is átláthassuk a rendeletnek, és megfelelhessünk neki.

13. A NAIH iránymutatása az adatvédelmi incidenskezelésről - Adobe Acrobat Document (.pdf)

Ez a dokumentum a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) iránymutatásait tartalmazza az adatvédelmi incidensek kezelésével, nyilvántartásával és kötelező bejelentésével kapcsolatban.

14. Adatvédelmi incidensek nyilvántartása – Microsoft Excel-munkalap (.xlsx)

A GDPR 33. cikke kimondja, hogy az adatkezelőt az adatvédelmi incidensről való tudomásszerzést követően alapvetően bejelentési kötelezettség terheli az illetékes hatósághoz, mely kötelezettségnek igen rövid határidőn belül eleget kell tennie. Az adatfeldolgozót ugyanez a bejelentési kötelezettség az adatkezelővel szemben terheli. Az említett bejelentésnek meg kell felelnie a GDPR által támasztott tartalmi követelményeknek. A rendelet kimondja továbbá azt is, hogy az adatkezelő köteles nyilvántartani az adatvédelmi incidenseket szintén bizonyos tartalmi követelményeknek megfelelően, mely lehetővé teszi a felügyeleti hatóság számára, hogy ellenőrizze e cikknek való megfelelést.

A GDPR szerint tehát törvényi kötelezettség terheli az adatkezelőt az adatvédelmi incidensek nyilvántartására vonatkozóan. Ennek a követelménynek való megfelelést segítjük azzal, hogy biztosítunk egy sablont az incidensek nyilvántartásához, mely a GDPR követelményrendszerének figyelembe vételével készült közérthető módon, így kitöltése nem jelent majd komoly terhet az adott vállalkozás számára. Az adott sablon továbbá segítséget nyújt az adatvédelmi incidensekkel kapcsolatos bejelentési kötelezettség teljesítéséhez is, hiszen tartalmazza a hatóságnak történő bejelentés GDPR szerinti kötelező elemeit is.

15. Érdekeltek felek – indikatív ábra, amely segítséget nyújt annak eldöntéséhez, hogy ki adatkezelő, közös adatkezelő, adatfeldolgozó, al-adatfeldolgozó - Adobe Acrobat Document (.pdf)

Az adatkezelésben az adatkezelőn kívül más érdekelt felek is részt vesznek, akik tevékenységükkel maguk is közreműködnek az adatkezelésben. Annak eldöntése, hogy mely felek pontosan mely érdekelt feleknek számítanak olyan szempontból nagyon fontos, hogy tisztában lehessünk felelősségük megoszlásával. Ennek meghatározása, átláthatósága egyszerűnek tűnik ugyan egy olyan vállalkozásnál, ahol maximum egy adatkezelő és egy adatfeldolgozó állnak egymással kapcsolatban, bonyolódhat azonban a kérdés bonyolultabb, nagyobb adatkezelői adatfeldolgozói hálózattal rendelkező vállalkozásoknál, ahol azonban ezeknek a feleknek a felelősségét a GDPR követelményeinek megfelelően rendezni kell.

Ebben a kérdésben nyújthat segítséget ez az általunk alkotott egyszerű ábra.

16. Adatfeldolgozói szerződés minta - Microsoft Word-dokumentum (.docx)

Amennyiben az adatkezelő nevében az adatkezelést más végzi, az adatkezelő felelőssége, hogy csak olyan adatfeldolgozót vehet igénybe, amely megfelelő garanciákat nyújt a GDPR követelményeinek való megfelelésre. Ez azért fontos, mert a természetes személyek jogainak védelme indokolja, hogy önmagában azért, mert az adatkezelő továbbít bizonyos személyes adatokat egy adatfeldolgozónak, ettől még az ő felelőssége nem szűnik meg az említett adatok védelmével kapcsolatban.

A GDPR kimondja, hogy az adatfeldolgozó által végzett adatkezelést az alkalmazandó jog alapján létrejött olyan, a kötelező tartalmi elemeknek megfelelő szerződésnek, vagy más jogi aktusnak kell szabályoznia, mely köti az adatfeldolgozót az adatkezelővel szemben. Abban az esetben pedig, amikor az EGT-n kívülre is történik adattovábbítás, még inkább felértékelődik az adatfeldolgozók és adatkezelők felelősségét szabályozó szerződések.

Jogi szakértelemmel rendelkező kollégáink megalkottak ezért egy olyan adatfeldolgozói szerződés mintát, mely tartalmazza a jogszabályi követelményeket, és segítségére lehet a vállalkozásoknak abban, hogy rendezze az adatkezelők és adatfeldolgozók közötti felelősség megoszlást.

17. Adatkezelői szerződés minta - Microsoft Word-dokumentum (.docx)

Amikor az adatkezelő adatfeldolgozókat vesz igénybe, kicsit egyszerűbb a felelősségek megállapítása, hiszen ezt a GDPR sok helyen rendezi. Abban az esetben azonban, amikor több adatkezelő működik együtt (közös, illetve együttes adatkezelés esetén), már nem ilyen egyértelmű a felelősség megoszlás, hiszen alapvetően azonos felelősségi szinten lévő érdekelt felekről beszélünk.

A GDPR követelményként fogalmazza meg, hogy közös adatkezelés esetén az adatkezelők megállapodásban kötelesek rendezni feladataikkal összefüggő felelősségük megoszlását.

E követelménynek való megfelelés segítésére létrehoztunk egy adatkezelői szerződés mintát, mely megfelel a GDPR követelményeinek.