A PARMA PRODUKT Gyógyszergyártó Korlátolt Felelősségű Társaság Adatvédelmi Irányelve

A PHOENIX csoport Adatvédelmi Irányelve alapján

GGL_Group Data Protection_20171219

Hatálybalépés: 2018. 05. 25.

Felváltott irányelv: nincs

Terjedelem:	Csoport	X	
Jóváhagyva:	Csoportbeli vállalat	**PARMA PRODUKT Gyógyszergyártó Korlátolt Felelősségű Társaság** székhely: 1145 Budapest, Uzsoki u. 36/a. cégjegyzékszám: 01-09-469287, adószám: 12147296-2-42, nyilvántartást vezető cégbíróság: Fővárosi Törvényszék Cégbírósága	2017. 12. 19.
	PHOENIX		

1. Általános rendelkezések 4

1.1 Bevezetés 4

1.2 Célkitűzés 4

1.3 Tárgyi hatály 4

1.4 Területi hatály 5

1.5 Jogszabályok 5

1.6 Az Irányelv megváltoztatása 5

1.7 Fogalommeghatározások 5

2. Elvek 7

2.1 A személyes adatok kezelésére vonatkozó elvek 7

2.2 A hozzájárulás feltételei 9

2.3 A személyes adatok különleges kategóriáinak kezelése 9

3. Az érintett jogai 10

3.1 Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések 10

3.2 Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik, illetve ha a személyes adatokat nem az érintettől szerezték meg 11

3.3 Az érintett hozzáférési joga 11

3.4 A helyesbítéshez való jog 11

3.5 A törléshez való jog („az elfeledtetéshez való jog”) 12

3.6 Az adatkezelés korlátozásához való jog 12

3.7 Az adathordozhatósághoz való jog 12

3.8 A tiltakozáshoz való jog 13

4. Az adatkezelő és az adatfeldolgozó 13

4.1 Az adatkezelés biztonsága 13

4.2 Közös adatkezelők 14

4.3 Az adatfeldolgozó 14

4.4 Együttműködés a felügyeleti hatósággal 14

4.5 Adatvédelmi incidens 15

4.6 Adatvédelmi hatásvizsgálat 16

4.7 Az adatvédelmi tisztviselő kijelölése 16

4.8 Az adatvédelmi tisztviselő jogállása 17

4.9 Az adatvédelmi tisztviselő feladatai 18

5. A személyes adatok továbbítása 19

6. Jogorvoslat, felelősség és szankciók 20

7. Adatkezelés a foglalkoztatással összefüggően 21

8. Záró rendelkezések 21

9. A PHOENIX csoport igazgatóságának felhatalmazása 22

1. Általános rendelkezések

1.1 Bevezetés

A PHOENIX csoport kiváló hírnévnek örvend, ami munkavállalóink kemény munkájának és pozitív magatartásának az eredménye. A PHOENIX csoport fontos kérdésnek tekinti az ügyfelek, betegek, beszállítók, üzleti partnerek és munkavállalók személyes adatainak védelmét. Az adatvédelmi jogszabályok megsértése súlyos következményekkel járhat – ilyenek például a bírságok és a hivatalos vizsgálatok –, a legsúlyosabb következmény azonban a jó hírnevünk sérelme lenne. Ez az Irányelv azt ismerteti, hogy a PHOENIX munkavállalóinak milyen intézkedéseket kell követniük a szervezet szintjén kezelt személyes adatok integritásának és biztonságának megőrzése érdekében, amit a PHOENIX csoport Igazgatósága is teljes mértékben támogat.

1.2 Célkitűzés

Ez az Irányelv a PHOENIX csoportban a személyes adatok kezelése tekintetében az érintettek védelmére vonatkozó szabályokat állapítja meg. Ennek az Irányelvnek az a célja, hogy az adatvédelmi jogszabályokkal (így egyebek mellett adott esetben az Európai Unió Általános Adatvédelmi Rendeletével, a GDPR-rel) összhangban védje az érintettek alapvető jogait és szabadságjogait.

1.3 Tárgyi hatály[1]

Ez az Irányelv azon személyes adatok és különleges személyes adatok kezelésére vonatkozik, amelyek azonosított vagy azonosítható természetes személyekre vonatkoznak. Vonatkozik úgy az elektronikus úton kezelt, mint a papíralapú és megfelelő nyilvántartási rendszerben tárolt adatokra. Ez az Irányelv egyformán vonatkozik a jogi személyek adataira azokban az országokban, ahol a jogi személyek (pl. korlátolt felelősségű társaságok) adatai az egyének személyes adataival azonos mértékű védelemben részesülnek.

Ezt az Irányelvet a PHOENIX csoport hatályos irányelveivel együtt kell alkalmazni.

---

1 GDPR 2. cikk

1.4 Területi hatály[2]

Ez az Irányelv a PHOENIX csoport minden szervezetére és üzletágára vonatkozik. Eltérő meghatározás hiányában az Európai Unió (EU) minden tagállamára és az Unióban kereskedelmi tevékenységet folytató valamennyi Unión kívüli szervezetre, továbbá minden más országra vonatkozik.

1.5 Jogszabályok

Ez az Irányelv az európai adatvédelmi jogszabály (konkrétan a GDPR) rendelkezéseit veszi alapul, amely szigorú, az Unió minden tagállamában alkalmazandó adatvédelmi előírásokat állapít meg.

Bizonyos jogi területeken a tagállamok nemzeti jogszabályai és rendelkezései az uniós jognál szigorúbbak is lehetnek. Általában ugyanez vonatkozhat az Unión kívüli országokra is. A PHOENIX csoport valamennyi szervezete és azok munkavállalói kötelesek betartani a vonatkozó helyi jogszabályokat.

1.6 Az Irányelv megváltoztatása

A PHOENIX csoport Igazgatósága fenntartja a jogot, hogy a Csoport Adatvédelmi Vezetőjével konzultálva megváltoztassa vagy módosítsa ezt az Irányelvet. A PHOENIX csoport munkavállalóinak be kell tartaniuk az Irányelvben foglalt rendelkezéseket.

1.7 Fogalommeghatározások[3]

Az Irányelv értelmében (továbbá a GDPR-rel összhangban):

a. az érintett *„hozzájárulása"*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
b. *„adatkezelő"*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó

---

2 GDPR 3. cikk

3 GDPR 4. cikk

különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

c. *„egészségügyi adat"*: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

d. *„munkavállaló"*: a PHOENIX csoport valamely szervezete által alkalmazott személy;

e. *„nyilvántartási rendszer"*: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

f. *„személyes adat"*: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

g. *„adatvédelmi incidens"*: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

h. *„különleges személyes adatok"*: 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;

i. *„PHOENIX csoport"*: része minden társaság, amelyben a részvények/részesedés többsége a PHOENIX csoport valamely szervezetének tulajdonában van;

j. *„adatkezelés"*: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

k. *„adatfeldolgozó"*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében (számára) személyes adatokat kezel;

l. *„felelős adatvédelmi tisztviselő"*: az adott szervezet adatvédelmi tisztviselője, az adott ország Helyi Adatvédelmi Tisztviselője (LDPO), az adott ország Helyi Adatvédelmi Koordinátora (LDPC) vagy a Csoport Adatvédelmi Vezetője;

m. *„az adatkezelés korlátozása"*: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

2. Elvek

2.1 A személyes adatok kezelésére vonatkozó elvek[4]

Jogszerűség, tisztességes eljárás és átláthatóság[5]

Az adatkezelést jogszerűen, tisztességesen és az érintett számára átlátható módon kell végezni. Az adatkezelés kizárólag akkor jogszerű, ha:

a. ahhoz az érintett hozzájárulását adta (lásd az Irányelv 2.2 bekezdését);
b. az adatkezelés valamely – érintetthez kapcsolódó – szerződés teljesítéséhez 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 feladat végrehajtásához szükséges és/vagy
f. az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

Célhoz kötöttség[6]

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Forduljon előtte a felelős adatvédelmi tisztségviselőhöz (még a terv megvalósítása előtt), ha az adatkezelés célján változtatni szeretne.

Adattakarékosság

A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, az adatok körét pedig a célhoz szükséges minimumra kell korlátozni, és törölni kell őket, ha már nincs rájuk szükség. A helyi igazgatóság gondoskodik róla, hogy teljesüljenek az adatmegőrzésre és -selejtezésre vonatkozó helyi követelmények.

A munkavállalók rendszeresen (legalább évente egyszer) felülvizsgálják a nyilvántartásokat, és a helyi követelményekkel való összhang érdekében adott esetben leselejtezik őket. Az osztályvezetők

4 GDPR 5. cikk
5 GDPR 6. cikk
6 GDPR 5. cikk

felelősek a felülvizsgálatért.

A munkavállalóknak tájékoztatniuk kell a felelős adatvédelmi tisztviselőt, ha a selejtezési intézkedéseknél szabálytalanságokat vagy az adateszközöknél nem egyértelmű, akár hibás selejtezési szabályokat is tapasztalnak.

A részleteket lásd: „Adatmegőrzésre vonatkozó iránymutatás" (I. függelék).

Pontosság

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

Korlátozott tárolhatóság[7]

A tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

Integritás és bizalmas jelleg[8]

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.

Elszámoltathatóság

Adatkezelőként a PHOENIX csoport szervezetei felelősséggel tartoznak annak igazolásáért, hogy képesek megfelelni az előzőekben felsorolt GDPR-elveknek. Minden munkavállalónak részt kell vennie a PHOENIX csoport adatvédelmi képzésén.

Az adatkezelőnek teljes körű nyilvántartást kell vezetnie az adatkezelési tevékenységekről. [9] Minden munkavállaló (különösen az osztályvezetők) kötelesek előzetesen (még a terv megvalósítása előtt) tájékoztatni a felelős adatvédelmi tisztviselőt, ha a személyes adatok kezelésében újítás vagy változtatás történik, hogy aktualizálhassa a nyilvántartásokat és ellenőrizhesse az adatkezelésre

7 GDPR 5. cikk
8 GDPR 5. cikk
9 GDPR 30. cikk

vonatkozó követelményeket.

2.2 A hozzájárulás feltételei[10]

Ha az adatkezelés hozzájáruláson alapul, a hozzájárulás csak akkor tekinthető jogszerűnek, ha az érintett egyértelmű megerősítő cselekedettel önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja az őt érintő személyes adatok kezeléséhez.[11] Ezenkívül teljesülniük kell a következő feltételeknek:

a. a hozzájárulásnak olyan formában kell történnie, amellyel igazolható, hogy az érintett a személyes adatainak kezeléséhez hozzájárult;
b. a más ügyekre is vonatkozó írásbeli nyilatkozat keretében történő hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel;
c. az érintett jogosult arra, hogy hozzájárulását bármikor egyszerűen visszavonja. A hozzájárulás megadása előtt az érintettet tájékoztatni kell arról, hogy a hozzájárulást hogyan lehet visszavonni;
d. 16 év alatti gyermek hozzájárulása (az életkor tekintetében lásd a helyi jogszabályokat) az információs társadalommal összefüggő szolgáltatások[12] (pl. online szolgáltatások) vonatkozásában csak akkor tekinthető jogszerűnek, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.[13]

A hozzájárulási nyomtatványmintákért forduljon a felelős adatvédelmi tisztviselőhöz.

2.3 A személyes adatok különleges kategóriáinak kezelése[14]

Tilos a különleges személyes adatok kezelése, kivéve, ha:

a. az érintett kifejezett hozzájárulását adta (DE jogszabály ilyetén előírása esetén a kifejezett hozzájárulás sem feltétlenül elégséges önmagában);
b. az adatkezelő vagy az érintett számára a foglalkoztatás, valamint a szociális biztonság és szociális védelem területén fennálló jogi előírások teljesítése és jogok gyakorlása miatt szükséges

---

10 GDPR 7. cikk

11 32. preambulumbekezdés

12 Információs társadalommal összefüggő szolgáltatás minden, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás.

13 GDPR 8. cikk

14 GDPR 9. cikk

az adatkezelés;

c. az adatkezelés az érintett létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
d. az adatkezelés a jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
e. az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
f. az adatkezelés orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása érdekében szükséges;
g. az adatkezelés a népegészségügy területét érintő közérdek miatt szükséges. Ebben az esetben az adatkezelést titoktartási kötelezettség hatálya alatt álló szakembernek vagy az ő felügyelete alatt valaki másnak vagy egy olyan személynek kell végeznie, aki ugyancsak titoktartási kötelezettség hatálya alatt áll.

A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatoknak a kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést a nemzeti jog lehetővé teszi.[15]

Különleges személyes adatok kezelése előtt mindenképpen javasolt konzultálni a felelős adatvédelmi tisztviselőjével. Ha kétségei vannak a jogalap tekintetében, az előzetes konzultáció kifejezetten kötelező!

3. Az érintett jogai

3.1 Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

Minden érintett rendelkezik a következő jogokkal:

- a hozzáférés joga;
- a helyesbítéshez való jog;
- a törléshez való jog;
- az adatkezelés korlátozásához való jog;
- az adathordozhatósághoz való jog;
- a tiltakozáshoz való jog.

15 GDPR 10. cikk

Adatkezelőként a PHOENIX csoportnak az előzőekben felsorolt jogok biztosítása előtt meg kell tennie az érintett személyazonosságának ellenőrzéséhez szükséges intézkedéseket. Az adatkezeléssel kapcsolatos tájékoztatás és kommunikáció formájának az érintett számára tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek, nyelvezetének pedig világosan és egyszerűen megfogalmazottnak kell lennie. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül ad tájékoztatást.

3.2 Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik, illetve ha a személyes adatokat nem az érintettől szerezték meg[16]

A PHOENIX csoport köteles a szükséges információkat az érintett rendelkezésére bocsátani függetlenül attól, hogy a személyes adatokat közvetlenül az érintettől vagy máshonnan szerezte meg. Ezt a gyűjtés időpontjában, illetve ha valaki mástól szerezték, egy ésszerű határidőn belül, legkésőbb azonban egy hónapon belül kell megtenni. A tájékoztatási nyomtatványmintákért forduljon osztályvezetőjéhez és/vagy a felelős adatvédelmi tisztviselőhöz.

3.3 Az érintett hozzáférési joga[17]

Az érintett jogosult arra, hogy a PHOENIX csoporttól, mint adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e (úgynevezett Érintetti Hozzáférési Kérelem, röviden ÉHK vagy angol rövidítés szerint SAR). Ha igen, az érintett kérésére biztosítani kell számára a hozzáférést a személyes adatokhoz és további információkhoz, így különösen az adatkezelés céljához vagy céljaihoz, a személyes adatok érintett kategóriáihoz stb. Forduljon osztályvezetőjéhez és/vagy a felelős adatvédelmi tisztviselőhöz azzal kapcsolatban, hogy kell-e válaszolni az adott ÉHK-ra (SAR-ra), és ha igen, hogyan.

3.4 A helyesbítéshez való jog[18]

Az érintettek jogosultak arra, hogy kérjék személyes adataik helyesbítését – ha pontatlanok –, illetve

---

16 GDPR 13. és 14. cikk

17 GDPR 15. cikk

18 GDPR 16. cikk

hiányos személyes adataik kiegészítését (ideértve a kiegészítő nyilatkozatot is). A kérelmeket indokolatlan késedelem nélkül kell elintézni.

3.5 A törléshez való jog („az elfeledtetéshez való jog")[19]

Az érintettek jogosultak azt kérni, hogy töröljék a személyes adataikat, például olyankor, ha az adatok nem szükségesek már a PHOENIX csoport által eredetileg gyűjtött célra, vagy az érintett visszavonja a hozzájárulását. Ha a PHOENIX csoport adatkezelőként nyilvánosságra hozta az információt, megteszi a szükséges lépéseket a személyes adatokat kezelő adatkezelők tájékoztatása érdekében, miszerint az érintett kérte adatainak törlését („az elfeledtetéshez való jog"). A PHOENIX csoport szervezeteinek nem minden esetben kell az információt törölniük, ilyen például az, ha valamilyen jogi kötelezettségnek kell eleget tenniük. Ilyen esetben forduljon osztályvezetőjéhez és/vagy a felelős adatvédelmi tisztviselőhöz.

3.6 Az adatkezelés korlátozásához való jog[20]

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, például ha adatkezelőként a PHOENIX csoportnak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez. Ilyen esetben forduljon osztályvezetőjéhez és/vagy a felelős adatvédelmi tisztviselőhöz.

Adatkezelőként a PHOENIX csoport ésszerű intézkedéseket tesz annak érdekében, hogy a korlátozás kéréséről tájékoztassa mindazokat, akikkel az adatokat megosztotta.

3.7 Az adathordozhatósághoz való jog[21]

Az érintett jogosult arra, hogy a rá vonatkozó, általa a PHOENIX csoport, mint adatkezelő rendelkezésére bocsátott személyes adatokról tagolt, széles körben használt, géppel olvasható formátumban másolatot kapjon. Az érintett jogosult arra, hogy kérésére az adatkezelő adja át az

---

19 GDPR 17. cikk

20 GDPR 18. cikk

21 GDPR 20. cikk

adatokat egy másik adatkezelőnek. Ez vonatkozik arra az esetre, ha az adatkezelés hozzájárulás, szerződés alapján történik, illetve az adatokat automatizált eszközök útján dolgozzák fel. Ilyen esetben forduljon osztályvezetőjéhez és/vagy a felelős adatvédelmi tisztviselőhöz.

3.8 A tiltakozáshoz való jog[22]

Az érintett jogosult arra, hogy bármikor tiltakozzon személyes adatainak kezelése ellen, különösen ha az közvetlen üzletszerzés, profilalkotás vagy kutatás céljából történik. Adatkezelőként a PHOENIX csoport a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést kényszerítő erejű jogos okok indokolják. Ilyen esetben forduljon osztályvezetőjéhez és/vagy a felelős adatvédelmi tisztviselőhöz.

4. Az adatkezelő és az adatfeldolgozó

4.1 Az adatkezelés biztonsága

Adatkezelőként a PHOENIX csoport megfelelő technikai és szervezési/szervezeti intézkedéseket hajt végre annak érdekében, hogy garantálja a kockázat mértékének megfelelő szintű adatbiztonságot (pl. a személyes adatok álnevesítése és titkosítása).[23] Ennek célja, hogy a PHOENIX csoport Információbiztonsági Irányelvében foglaltak szerint biztosítsa a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegét, integritását, rendelkezésre állását és ellenálló képességét. Az adatkezelő gondoskodik továbbá a beépített és alapértelmezett adatvédelemről oly módon, hogy az adatvédelmi elvek megvalósításához szükséges garanciákat beépíti a folyamatokba. Ezzel biztosítható, hogy kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek.[24] Az Információbiztonsági Irányítási Rendszer folyamatos javításának biztosítása, valamint az új technikai követelmények alkalmazásának garantálása érdekében időszakos felülvizsgálati és audit eljárásokat állapítottunk meg.[25] Üzletmenet-folytonossági és katasztrófa-helyreállítási tervet állapítottunk meg annak biztosítása érdekében, hogy fizikai vagy műszaki incidens esetén képesek legyünk a

22 GDPR 21. cikk
23 GDPR 24. cikk
24 GDPR 25. cikk
25 GDPR 32. cikk

személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben visszaállítani.

4.2 Közös adatkezelők

Közös adatkezelőkről van szó, és írásbeli szerződésre van szükség, ha két vagy több adatkezelő (pl. a PHOENIX valamely szervezete és egy másik külső szolgáltató) közösen határozza meg a személyes adatok kezelésének eszközeit és céljait. További információkért forduljon a felelős adatvédelmi tisztviselőhöz.[26]

4.3 Az adatfeldolgozó[27]

Az adatkezelő nevében/számára más (pl. egy informatikai vagy humánerőforrás-szolgáltató) által végzett adatkezelés csak akkor megengedett, ha az adatfeldolgozó az érintett jogainak védelmét biztosító megfelelő garanciákat nyújt, és arról szerződést is aláírtak. Az adatfeldolgozót körültekintően kell kiválasztani, és rendszeresen auditálni kell. A szerződést és az auditnyomtatványt kérje el a felelős adatvédelmi tisztviselőtől.

Ugyanez érvényes akkor, ha a PHOENIX csoport valamely szervezete egy másik szervezet (pl. informatikai szolgáltatások esetén a PHOENIX csoport informatikai GmbH-ja) nevében/számára kezel személyes adatokat.

Ezenkívül annak biztosítása érdekében is intézkedéseket kell tenni, hogy az adatkezelő teljesítse a PHOENIX csoport Információbiztonsági Irányelvében meghatározott előírásokat, és az adatokat csakis az utasításoknak megfelelően kezelje.[28] Szigorúan tilos az uniós polgárok személyes adatainak kezelése, ha az adatkezelés az Unión kívül történik, kivéve, ha teljesülnek az adatok továbbítására vonatkozó különös feltételek (lásd az Irányelv 5. fejezetét).

4.4 Együttműködés a felügyeleti hatósággal

A PHOENIX csoport és munkavállalói kötelesek együttműködni a helyi adatvédelmi felügyeleti

---

26 GDPR 26. cikk

27 GDPR 28. cikk

28 GDPR 29. cikk

hatóságokkal. Ha munkavállalóként Önt megkeresi valamelyik helyi felügyeleti hatóság, azonnal forduljon a felelős adatvédelmi tisztviselőhöz.[29]

4.5 Adatvédelmi incidens

Az adatvédelmi incidenseket a munkavállalónak vagy az osztályvezetőnek a PHOENIX csoport portálján (a https://phoenixgroup-databreach.integrityplatform.org) keresztül azonnal jelentenie kell a felelős adatvédelmi tisztviselőnek. Ha az incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell arról az érintettet.[30]

Ha az incidens valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül tájékoztatni kell a helyi felügyeleti hatóságot (amit a felelős adatvédelmi tisztviselő intéz). Ennek az incidensről értesülést követően legkésőbb 72 órán belül meg kell történnie.[31]

Nem kell tájékoztatni a felügyeleti hatóságot és/vagy az érintettet, ha a GDPR nem alkalmazandó (különösen az Unión kívüli országokban), és a helyi jogban nincs a GDPR-ben szereplővel azonos kötelezettség.

Csoport vonatkozású incidens esetén a Helyi Adatvédelmi Tisztviselő vagy a Helyi Adatvédelmi Koordinátor a Csoport Adatvédelmi Vezetőjét is értesíti.

Az okozott kockázat mérséklése, valamint a felügyeleti hatóságok, illetve a szóban forgó érintettek felé történő jelentés folyamatának felgyorsítása érdekében minden adatvédelmi incidens esetén az adott adatvédelmi incidensre vonatkozó eljárást kell követni, ami garantálja az adatvédelmi jogszabályok követelményeinek betartását. A részleteket lásd: „Adatvédelmi incidensekre vonatkozó iránymutatás” (2. függelék).

Ha az adatvédelemmel kapcsolatban kérdése van, vagy attól tart, hogy sérültek a személyes adatok,

---

29 GDPR 31. cikk

30 GDPR 34. cikk

31 GDPR 33. cikk

a probléma megbeszélése érdekében a felelős adatvédelmi tisztviselőhöz fordulhat.

4.6 Adatvédelmi hatásvizsgálat

Adatvédelmi hatásvizsgálat (DPIA)[32] szükséges az adatkezelés előtt, ha az adatkezelés – különösen új technológiák alkalmazása esetén – valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

DPIA szükséges a következő esetekben:

a. új technológiák bevezetése,
b. automatizált adatkezelés – a profilalkotást is ideértve – olyan döntést vagy döntéseket eredményez, amelyek joghatással járnak a természetes személyekre nézve,
c. különleges kategóriába tartozó adatok nagy számban történő kezelése folyik,
d. bűncselekményekre vonatkozó adatok kezelése,
e. nyilvános helyek nagymértékű, módszeres megfigyelése.
f. A további eseteket lásd a helyi felügyeleti hatóságok listájában.

Annak biztosítása érdekében, hogy a DPIA-t a személyes adatok kezelésében bevezetett újítás vagy változtatás előtt elvégezzék, az adott munkavállalónak előzetesen (még a terv megvalósítása előtt) tájékoztatnia kell a felelős adatvédelmi tisztviselőt. Forduljon a felelős adatvédelmi tisztviselőhöz, aki DPIA-nyomtatványokat, iránymutatást és folyamatos tájékoztatást tud biztosítani.

A (Helyi) Adatvédelmi Tisztviselőnek konzultálnia kell a helyi felügyeleti hatósággal abban az esetben, ha a DPIA azt jelzi, hogy az adatkezelő által a kockázat mérséklése érdekében tett intézkedések hiányában az adatkezelés magas kockázattal járna az érintettek jogaira és szabadságaira nézve.

4.7 Az adatvédelmi tisztviselő kijelölése[33]

A PHOENIX csoport minden szervezetének el kell döntenie, hogy szükséges-e kijelölni egy adatvédelmi tisztviselőt. Ennek megállapításánál meg kell vizsgálni és figyelembe kell venni a helyi jog és a GDPR rendelkezéseit. A GDPR kimondja, hogy ha a fő tevékenység olyan adatkezelési műveleteket foglal magában, amelyek az érintettek nagymértékű, rendszeres és szisztematikus

---

[32] GDPR 35. cikk
[33] GDPR 38. cikk

nyomon követését teszik szükségessé, vagy ha a fő tevékenység a személyes adatok különleges kategóriáinak nagy számban történő kezeléséből áll, akkor az adatvédelmi tisztviselő kijelölése kötelező (azokban az országokban, ahol kiskereskedelmi tevékenység folyik, mindenképpen ajánlott akkor is, ha egyébként a GDPR/helyi jogszabály alapján nem kötelező).

Ha egy országban egynél több adatvédelmi tisztviselő is van, közülük az egyiket ki kell nevezni Helyi Adatvédelmi Tisztviselőnek (LDPO). Ha egy adatvédelmi tisztviselő sincs, ki kell nevezni egy személyt Helyi Adatvédelmi Koordinátornak (LDPC). Az LDPO és/vagy az LDPC a helyi igazgatóságnak tartozik felelősséggel. A szervezetek adatvédelmi tisztviselői, az LDPO-k és az LDPC-k felelősek a saját szervezetükön/országukon belül az érintettek jogainak védelméért, illetve azért, hogy szorosan együttműködjenek egymással és a Csoport Adatvédelmi Vezetőjével.

A PHOENIX csoport kinevezte a Csoport Adatvédelmi Vezetőjét, aki az országok LDPO-ival és LDPC-ivel, illetve a Csoport Információbiztonsági Igazgatójával közösen összehangolja a PHOENIX csoport jelentős adatvédelmi kérdéseit érintő együttműködést. A Csoport Adatvédelmi Vezetője a PHOENIX Csoport igazgatóságának tartozik felelősséggel. A Csoport Adatvédelmi Vezetője szorosan együttműködik a PHOENIX csoport országaival. A feladata, hogy nyomon kövesse a csoport szintű irányelveket (ezt az Irányelvet, továbbá a részletes irányelveket), kidolgozza és aktualizálja őket.

A feladatra kijelölt személy az adatvédelmi jog és gyakorlat területén rendelkezik a szükséges szakmai képesítéssel és tudással.

A PHOENIX Csoport kinevezte a Csoport Információbiztonsági Igazgatóját, aki minden vonatkozó biztonsági területen tanácsokat ad a PHOENIX csoportnak. A Csoport Információbiztonsági Igazgatójának feladata a PHOENIX csoport információbiztonsági előírásainak kidolgozása, fejlesztése és nyomon követése.

4.8 Az adatvédelmi tisztviselő jogállása[34]

Az adatvédelmi tisztviselők, az LDPO-k, az LDPC-k és a Csoport Adatvédelmi Vezetője megfelelő módon és időben bekapcsolódik a személyes adatok védelmének szabályozásával kapcsolatos minden ügybe, projektbe, változtatásba vagy műveletbe.

[34] GDPR 38. cikk

A Csoport Igazgatósága, a helyi igazgatóság és minden munkavállaló támogatja az adatvédelmi tisztviselőt, az LDPO-kat, az LDPC-ket és a Csoport Adatvédelmi Vezetőjét a feladatok ellátásában.

Az adatvédelmi tisztviselők, az LDPO-k, az LDPC-k és a Csoport Adatvédelmi Vezetője rendelkeznek a szervezetnél az üzleti modell jellegének és összetettségének megfelelő forrásokkal, ideértve azokat, amelyek a csoport szintű adatvédelmi ügyek és projektek esetén a kölcsönös segítségnyújtással, együttműködéssel és részvétellel összefüggésben szükségesek.

A szervezeten belül független és védett a jogállásuk, és a PHOENIX csoport megfelelő szervezetének legmagasabb szintű vezetésének tartoznak felelősséggel.

A személyes adatok kezelésével kapcsolatban természetes kapcsolattartási pontok az érintettek felé, illetve kapcsolattartási pontok a felügyeleti hatóságok felé.

A feladataik teljesítésével kapcsolatban titoktartási kötelezettség és/vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti őket.

A felelős adatvédelmi tisztviselők, az LDPO-k, az LDPC-k és a Csoport Adatvédelmi Vezetőjének kapcsolattartási adatait közzé kell tenni a szervezetek/országok intranetein (COIN) vagy hasonló helyeken.

4.9 Az adatvédelmi tisztviselő feladatai[35]

Az adatvédelmi tisztviselők, az LDPO-k, az LDPC-k és a Csoport Adatvédelmi Vezetője felelős a PHOENIX csoport, mint adatkezelő és adatfeldolgozó szervezeteinek/országainak, valamint a szervezetek/országok munkavállalóinak tájékoztatásáért és értesítéséért.

Adatkezelőként a PHOENIX csoport helyi igazgatóságai felelősek azért, hogy biztosítsák a jogszabályokban, rendelkezésekben és a csoport szintű irányelvekben az adatvédelemre vonatkozóan megfogalmazott követelmények betartását. Az igazgatóságok mindenekelőtt felelősek az érintettek jogainak védelméért.

Az érintetteknek a személyes adatok kezelését érintő alapvető jogainak és szabadságjogainak védelme érdekében az adatvédelmi tisztviselők, az LDPO-k, az LDPC-k és a Csoport Adatvédelmi

35 GDPR 39. cikk

Vezetője felelős azért, hogy nyomon kövessék az adatvédelemre vonatkozóan (adott esetben) a GDPR, a helyi jogszabályok és rendelkezések, ezen Irányelv és a PHOENIX csoport további részletes irányelveinek betartását.

A Csoport Adatvédelmi Vezetője az LDPO-kkal és/vagy az LDCP-kkel szorosan együttműködve (pl. rendszeres telefonkonferenciákon, értekezleteken stb. keresztül) meghatározza az általános keretrendszert, amely az adatvédelmi rendelkezésekkel kapcsolatos tájékoztatás és tanácsadás vonatkozásában (adatkezelőként vagy -feldolgozóként) a PHOENIX csoport helyi szervezeteinek támogatási fórumaként szolgál.

Az LDPO-k és az LDCP-k nyomon követik és a Csoport Adatvédelmi Vezetőjének jelentik a szervezetüknél/országukban tapasztalt szabálytalanságokat és esetleges kockázatokat. Tájékoztatják őket a felügyeleti hatóságok ellenőrzéseiről. Az LDPO-k és az LDCP-k biztosítják országukban az adatkezelőknek, -feldolgozóknak és munkavállalóknak szóló kellő képzést és felvilágosító tevékenységet. A Csoport Adatvédelmi Vezetője biztosítja a csoport szintű e-oktatást.

A feladatkörök részletesebb áttekintését tekintse meg a 3. függelékként csatolt RACI-mátrixban.

5. A személyes adatok továbbítása

Általában megengedett a személyes adatok továbbítása abban az országban, ahol az adatokat gyűjtik, az Európai Unióban (EU) és az Európai Gazdasági Térségben (EGT) (ideértve az átadást követően egy harmadik országban végzett adatkezelést), ha az adatkezelés a GDPR (különösen annak II. fejezete) szerint is megengedett.

A személyes adatok továbbítása valamely uniós/EGT-országból egy harmadik (Unión/EGT-n kívüli) országba csak akkor megengedett, ha további követelmények is teljesülnek. Ilyen esetben kérdezze a felelős adatvédelmi tisztviselőt. Megengedett a továbbítás:

- ha az Európai Bizottság úgy határozott, hogy a harmadik ország megfelelő szintű védelmet biztosít („megfelelőségi határozat", ilyen pl. Svájc)[36]; vagy
- ha az átvevő fél megfelelő garanciákat nyújtott (pl. kötelező erejű vállalati szabályok, a

[36] GDPR 45. cikk

Bizottság által elfogadott általános adatvédelmi kikötések, jóváhagyott magatartási kódex)[37]; vagy

- bármely bíróság ítélete vagy közigazgatási hatóság döntése szerint, ha nemzetközi megállapodáson alapul[38]; vagy
- ha a továbbítás meghatározott, speciális helyzetben történik (pl. az érintett kifejezetten hozzájárult, szerződés teljesítéséhez szükséges, jogi igények előterjesztése, érvényesítése és védelme miatt szükséges, az érintett létfontosságú érdekeinek védelme miatt szükséges)[39]; vagy
- ha a továbbítás az adatkezelő kényszerítő erejű jogos érdekében szükséges, és az adatkezelő tájékoztatja a felügyeleti hatóságot.[40]

6. Jogorvoslat, felelősség és szankciók

A jogorvoslati lehetőségek a következők:

- Az érintett panaszt jogosult benyújtani a felügyeleti hatósághoz.[41]
- A természetes vagy jogi személy a felügyeleti hatósággal szemben hatékony bírósági jogorvoslatra jogosult.[42]
- Az érintett az adatkezelővel vagy az adatfeldolgozóval szemben hatékonybírósági jogorvoslatra jogosult[43] és
- Az érintett nonprofit jellegű szervet, szervezetet vagy egyesületet jogosult megbízni.[44]

Az adatvédelmi incidensek az érintettek vagyoni vagy nem vagyoni kártérítési igényét eredményezhetik.[45] A hatóságok akár 10 vagy 20 millió EUR összegű vagy vállalatok, például a PHOENIX csoport esetén az előző pénzügyi év teljes éves világpiaci forgalmának 2 vagy 4%-át kitevő

---

[37] GDPR 46. cikk

[38] GDPR 48. cikk

39 GDPR 49. cikk

[40] GDPR 49. cikk (1) bekezdés vége.

41 GDPR 77. cikk

[42] GDPR 78. cikk

[43] GDPR 79. cikk

[44] GDPR 80. cikk

[45] GDPR 82. cikk

közigazgatási bírságot is megállapíthatnak.[46] A helyi jogszabályok szerint a jogsértés büntetőeljáráshoz is vezethet.[47] A jogsértésekért felelősségre vonható munkavállalók a helyi foglalkoztatási joggal összhangban helyben lefolytatott fegyelmi eljárásban megállapított szankciókkal sújthatók.

7. Adatkezelés a foglalkoztatással összefüggően

A helyi jog alapján a személyes adatok foglalkoztatással összefüggő kezelése tekintetében a jog vagy kollektív szerződések konkrétabb szabályokat is meghatározhatnak.[48]

8. Záró rendelkezések

Ezt az Irányelvet 2018. május 25-től kell alkalmazni.

[46] GDPR 83. cikk

[47] GDPR 84. cikk

[48] GDPR 88. cikk

9. A PHOENIX csoport igazgatóságának felhatalmazása

Oliver Windholz	Helmut Fischer
Vezérigazgató	Gazdasági igazgató

Frank Große-Natrop	Stefan Herfeld
Üzemeltetési és logisztikai igazgató	Kiskereskedelmi igazgató

A PHOENIX Csoport Adatvédelmi Irányelve alapján elfogadta Budapesten, 2018. év május hó 23 napján a PARMA PRODUKT Gyógyszergyártó Korlátolt Felelősségű Társaságra vonatkozóan 2018. év május hó 25-i hatállyal:

PARMA PRODUKT Kft.

.....	.....	.....
Dr. Csongrádi Balázs ügyvezető	Dr. Nyeste Rudolf ügyvezető	Valtinyi Zsuzsanna ügyvezető

Mellékletek:

1. Adatmegőrzésre vonatkozó iránymutatás
2. Adatincidensekre vonatkozó iránymutatás
3. RACI-mátrix

A PHOENIX csoport Adatvédelmi Irányelvének 1. melléklete:

Adatmegőrzésre vonatkozó iránymutatás

Bevezetés

Ez az iránymutatás azt ismerteti, hogy a PHOENIX csoport iratainak megfelelő (vagyis a törvényes adatmegőrzési követelmények szerinti) védelmét és nyilvántartását hogyan lehet biztosítani. Biztosítja továbbá azt, hogy megfelelő időben leselejtezzék az iratokat, amelyek már nem szükségesek vagy értéküket vesztették.

A PHOENIX csoport minden üzleti nyilvántartására vonatkozik (akár van bennük személyes adat, akár nincs, papíralapúak vagy elektronikusok, a Csoport informatikai részlege, a helyi informatika vagy a szolgáltatók által üzemeltetett alkalmazások).

1. Fogalommeghatározások

Adathordozó: bármely hordozó, amely képes adatokat rögzíteni, például papírdokumentumok, merevlemezek (pl. egy személyi számítógépben, notebook számítógépben, táblagépben, kiszolgálóban, telefaxban vagy fénymásolóban), CD-k, DVD-k, lemezek, mágnesszalag-kazetták, intelligens kártyák (pl. SD-kártyák), USB-memóriák, mikrofilmek.

Törlés: olyan eljárás, amikor a személyes adatokat visszafordíthatatlan módon megváltoztatják úgy, hogy utána már nem léteznek vagy felismerhetetlenek, és nem lehet őket használni vagy helyreállítani. Az adatok törlése helyett az adathordozókat is meg lehet semmisíteni. Egy másik lehetőség az adatok anonimizálása, vagyis az az eljárás, amikor a személyes adatokat visszafordíthatatlan módon megváltoztatják úgy, hogy az érintettet közvetlenül vagy közvetve sem lehet már beazonosítani. Egyes adatvédelmi szabályok szerint az adatokat az adatmegőrzési idő alatt zárolni kell.

Nyilvántartás: minden dokumentált információ függetlenül a jellemzőktől, hordozóktól, fizikai megjelenési formáktól (pl. elektronikus vagy papíralapú), illetve az a mód, ahogyan rögzítik és tárolják őket. A nyilvántartásba beletartoznak a számlák, szerződések, könyvek, rajzok, levelek, mágnes-/optikai lemezek, feljegyzések, e-mailek, szöveges állományok, kép- és hangfájlok, PDF-dokumentumok, minden Microsoft Office vagy egyéb formátumú fájl – eredetiek vagy másolatok.

Adatmegőrzési kötelezettségek: megtalálhatók a helyi és európai adatvédelmi jogszabályokban, különrendeletekben, szerződésekben stb. A szükségesség és adattakarékosság általános elvét kell követni (vagyis a személyes adatok kezelését a kezelés céljához szükséges minimumra kell korlátozni), ha az adatokra nincs már szükség.

Adatmegőrzési időszak: az az idő, amíg a helyi jogi kötelezettségek (pl. jogszabály, szerződés, adattakarékosság) szerint a nyilvántartásnak rendelkezésre kell állnia.

2. **Folyamat**

Lásd az 1. mellékletben szereplő folyamatábrát és folyamatleírást.

3. **Adatmegőrzés és -törlés**

Az adatmegőrzési kötelezettségek jobb áttekinthetősége érdekében az általános minta szerint minden ország elkészíti magának a selejtezési kategóriák táblázatát (lásd 2. melléklet).

Az általános folyamat alól vannak kivételek a személyes adatok jogellenes gyűjtésére; az érintett törvényes kérését követő személyes adatokra; a rendszereken elvégzett javítás, szétszerelés és törlés után; egy vállalkozás átadása esetén, incidensek esetén, valamint peres ügyek vagy követelések esetén.

Külön selejtezési időszakok vonatkoznak az archívumokra, a (helyreállítási célú) tartalék másolatokra és a naplózási protokollokra.

4. **Az adathordozók selejtezése**

Ha az adathordozó nem szükséges már, feladatát vesztette vagy a szervezeten belül vagy kívül valaki máshoz kerül, a felhasználónak ellenőriznie kell, hogy tárolnak-e rajta személyes vagy bizalmas adatokat. Ilyen esetben törölni kell az adatokat.

Minden adathordozót (a papírdokumentumok kivételével) megsemmisítés céljából át kell adni az informatikai osztálynak. Az informatikai osztály megsemmisíti (pl. kalapáccsal, mágnessel, a szalagok feldarabolásával), vagy megsemmisítés céljából átadja őket egy szolgáltatónak (akivel adatfeldolgozói szerződése van). Az adatok megsemmisítéséhez biztonságos hulladéktárolókat lehet biztosítani.

Ugyanez érvényes akkor is, ha az adattárolókat a PHOENIX csoporton kívül adják át valakinek. Az adathordozókat fizikailag kell törölni, ha visszaküldik a gyártónak. Ha ez nem lehetséges,

adatfeldolgozói szerződést kell aláírni.

Ha az adathordozót a PHOENIX csoporton belül adják át egy felhasználónak, kivételesen a tároló eszköz formázása és az alkalmazások újratelepítése is elegendő, ha nem tárolnak rajtuk fontos (pl. a helyi igazgatóságra vonatkozó) adatokat.

A papírdokumentumokat a munkavállalónak biztonságos hulladéktárolókba kell leraknia (amelyeket az a szolgáltató biztosít, aki megsemmisíti őket, és akivel adatfeldolgozói szerződést kötöttek), vagy (megfelelő biztonsági szintű) iratmegsemmisítőben meg kell semmisítenie.

A részletekről a helyi vezetőség helyi szabályzatban rendelkezik.

5. **Dokumentálás**

Az országok dokumentálják a helyi végrehajtási követelményeket, nevezetesen arra vonatkozóan, hogy milyen rendszereket és egyéb adateszközöket, illetve milyen adattípusokat használnak; milyen adattípusokra milyen törlési szabályok vonatkoznak; milyen a selejtezési mechanizmus; mi jellemzi a selejtezési mechanizmust; ki a felelős a mechanizmus elindításáért és nyomon követéséért, a selejtezés dokumentálásáért. Ezt az ellenőrzőlistát lehet használni az audittervre is.

Az országok elkészítik a RACI-mátrixot (lásd a 3. mellékletben az általános mintát), és a mátrix szerint összeállítják és megvalósítják a követelményeket.

6. **A folyamattal kapcsolatos felelősség**

A helyi vezetés gondoskodik arról, hogy a folyamatot végrehajtsák, különösen pedig arról, hogy az adateszközökre legyenek selejtezési szabályok.

Az országban lennie kell a rendszerekről és az adateszközökről összeállított listának (helyben, később pedig egy központi adattárban).

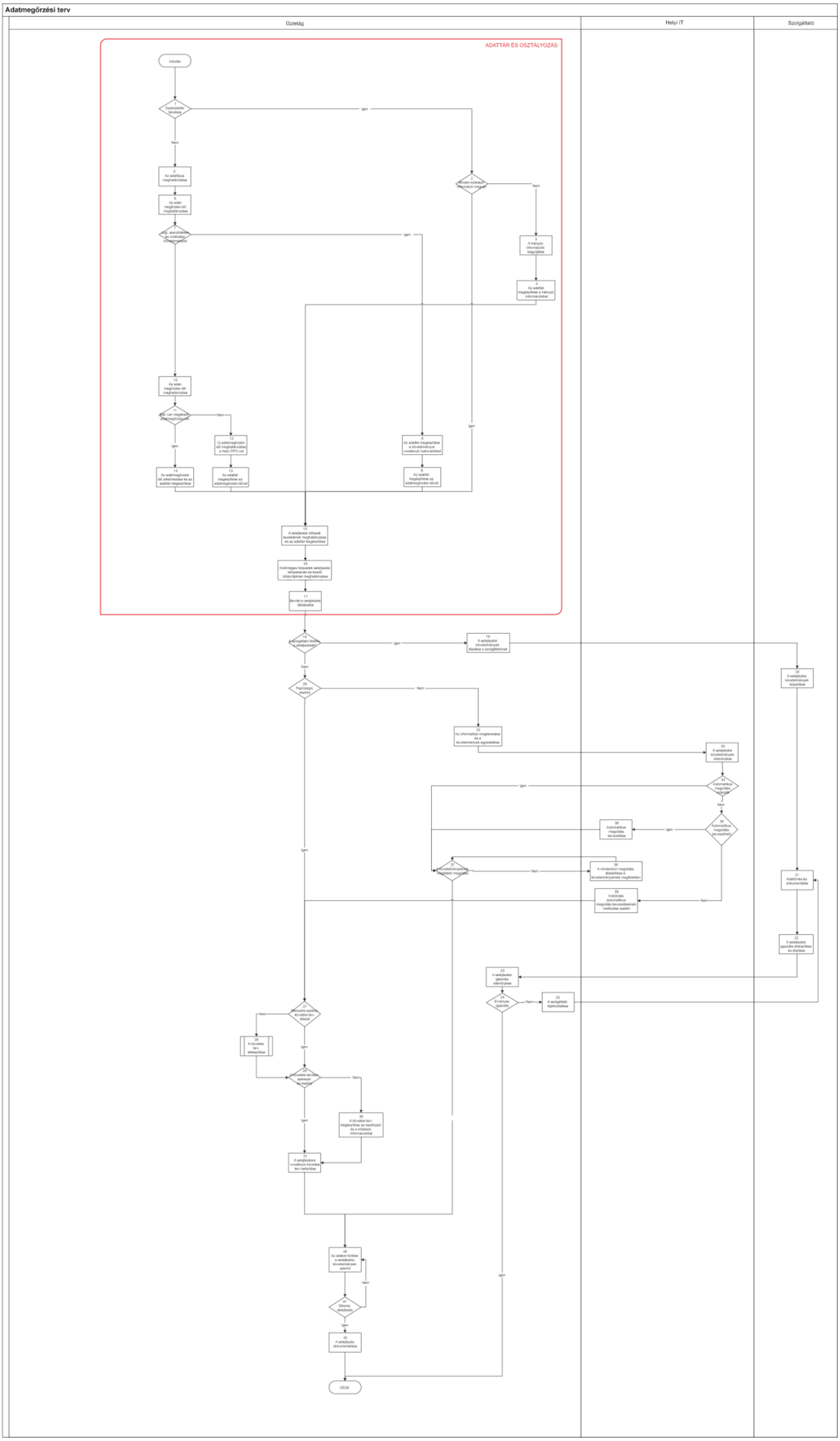
Az ország egyezteti a szolgáltatókkal a selejtezésre vonatkozó kötelezettségeket (lásd az adatfeldolgozók szerződéses nyomtatványát).

A selejtezésre vonatkozó kérést az osztályvezetők adják ki az informatikának.

1. melléklet: Folyamatábra és -leírás

2. melléklet: Selejtezési kategóriák táblázata

3. melléklet: RACI-mátrix


Adatmegőrzési terv
Üzletág
Helyi IT
Szolgáltató
ADATTÁR ÉS OSZTÁLYOZÁS
Indulás
Igen
Nem
5 Az adattípus meghatározása
6 Az adat-megőrzési idő meghatározása
3 A hiányzó információk begyűjtése
4 Az adattár kiegészítése a hiányzó információkkal
10 Az adat-megőrzési idő meghatározása
12 Új adatmegőrzési idő meghatározása a helyi DPO-val
14 Az adatmegőrzési idő alkalmazása és az adattár kiegészítése
13 Az adattár kiegészítése az adatmegőrzési idővel
8 Az adattár kiegészítése a követelményre vonatkozó tudnivalókkal
9 Az adattár kiegészítése az adatmegőrzési idővel
15 A selejtezési időszak kezdetének meghatározása és az adattár kiegészítése
16 Különleges helyzetek selejtezési időszakának és kezdő időpontjának meghatározása
17 Bevitel a selejtezési táblázatba
19 A selejtezési követelmények átadása a szolgáltatónak
20 A selejtezési követelmények teljesítése
26 Papíralapú eszköz
32 Az informatikai megkeresése és a követelmények egyeztetése
33 A selejtezési követelmények ellenőrzése
36 Automatikus megoldás bevezetése
35 Automatikus megoldás bevezethető
38 A mindenkori megoldás átalakítása a követelményeknek megfelelően
39 Indoklás automatikus megoldás bevezetésének mellőzése esetén
21 Adattörlés és dokumentálás
22 A selejtezési igazolás elkészítése és átadása
23 A selejtezési igazolás ellenőrzése
24 Érvényes igazolás
25 A szolgáltató tájékoztatása
28 A követési terv elkészítése
30 A követési terv kiegészítése az eszközzel és a kötelező információkkal
31 A selejtezésre vonatkozó követési terv betartása
40 Az adatok törlése a selejtezési követelmények szerint
41 Sikeres selejtezés
42 A selejtezés dokumentálása
VÉGE

1. melléklet: Folyamatleírás

Az „Adatmegőrzésre vonatkozó iránymutatás” című 1. melléklethez

ADATTÁR ÉS OSZTÁLYOZÁS

1) Eszközleltár felvétele
   Az adateszközöket leltárba kell venni, a folyamat e lépése során az illetékes osztálynak/részlegnek tisztáznia kell, hogy az elemzés tárgyát képező adateszköz szerepel-e már a leltárban.

2) Az összes kötelező információ rendelkezésre állása
   Abban az esetben, ha az eszköz szerepel már a leltárban, ellenőrizni kell azt, hogy az adatkezelő tevékenységekről vezetett nyilvántartásban (lásd jelenleg az Információs Eszközjegyzék kérdőívet és az informatikai kérdőívet) meghatározott kötelező információk rendelkezésre állnak-e.

3) A hiányzó információk begyűjtése
   Ha kiderül, hogy a kötelező információk hiányoznak, az illetékes osztály/részleg felelős az összes hiányzó információ begyűjtéséért. Abban az esetben, ha a felügyeleti információk hiányoznak, tájékoztatást kell kérni a felelős DPO-tól.

4) Az adattár kiegészítése a hiányzó információkkal
   Az összes hiányzó információ begyűjtése után gondoskodni kell az adattár frissítéséről és kiegészítéséről.

5) Az adattípus meghatározása
   Abban az esetben, ha az eszközt még nem leltározták fel, az első lépés az eszköz adattípusának meghatározása. Adattípus az adateszközök minden része, amelyet a rendes működéshez felhasználnak, például kapcsolattartási adatok, fizetési adatok, tranzakciós adatok.

6) Az adatmegőrzési idő meghatározása
   Az adattípus besorolását követően meg kell határozni az adatmegőrzési időszakot, vagyis azt az időt, amíg a jogszabályi iratmegőrzési kötelezettségek céljából az adatokat meg kell őrizni az adattárban.

7) Jogi, szerződéses és működési követelmények
   Ellenőrizni kell, hogy a szóban forgó eszközre vonatkozik-e olyan jogi, szerződéses vagy működési rendelkezés, amely esetlegesen a megőrzésre vonatkozó követelményeket állapít meg. Bizonytalanság esetén tájékoztatást kell kérni a felelős DPO-tól.

8) Az adattár kiegészítése a követelményre vonatkozó tudnivalókkal
Az átláthatóság és nyomon követhetőség érdekében az adattárat ki kell egészíteni az adatmegőrzési követelményre vonatkozó tudnivalókkal. Ez különösen fontos például ahhoz, hogy alkalmazkodni tudjunk a jogszabályi változásokhoz.

9) Az adattár kiegészítése az adatmegőrzési idővel
Az adatmegőrzést befolyásoló megfelelő követelmények megállapítása után az adattárat ki kell egészíteni a vonatkozó adatmegőrzési idővel.

10) Az adatmegőrzési idő meghatározása
Ha a szóban forgó eszközre nem vonatkoznak jogi, szerződéses vagy működési rendelkezések, az illetékes osztálynak/részlegnek meg kell határoznia a megfelelő adatmegőrzési időt (a legrövidebbet, ami szükséges).

11) Már van megfelelő adatmegőrzési idő
Új adatmegőrzési idő meghatározása előtt meg kell győződni arról, hogy az adott kategóriába tartozó eszközökhöz van-e már hozzárendelve olyan adatmegőrzési idő, amelyet a szóban forgó eszközhöz is hozzá lehet rendelni.

12) Új adatmegőrzési idő meghatározása a DPO-val
Abban az esetben, ha megfelelő adatmegőrzési idő nem létezik még, a felelős DPO-hoz kell fordulni az új adatmegőrzési idő meghatározásáért.

13) Az adattár kiegészítése az adatmegőrzési idővel
A felelős DPO megkérdezése, illetve az új adatmegőrzési idő egyeztetése után a megfelelő eszközhöz rendelve ki kell egészíteni az adattárat.

14) Az adatmegőrzési idő alkalmazása és az adattár kiegészítése
Abban az esetben, ha már létezik megfelelő adatmegőrzési idő, a szóban forgó eszközhöz kell rendelni, és ki kell egészíteni az adattárat.

15) A selejtezési időszak kezdetének meghatározása és az adattár kiegészítése
Miután valamennyi kötelező információ összegyűlt, az adattárat ki kell egészíteni a selejtezési időszakkal és a kezdő időponttal.
A selejtezési időpont azt jelenti, hogy a tartási időszak után az adatvédelmi jogszabály szerint egy elfogadható időn belül törölni kell az érintett adatokat (ha az adatmegőrzési idő pl. 8 év, a selejtezési időszak kezdete pedig az év vége, akkor a selejtezési idő 9 év mindig az év végén).

16) Különleges helyzetek selejtezési időszakának és kezdő időpontjának meghatározása
Minden illetékes osztály/részleg kerülhet különleges helyzetbe (pl. rendszerjavítás vagy peres ügyek esetén), amikor selejtezési tervet kell alkalmazni. Ezzel is ki kell egészíteni az adattárat.

17) Bevitel a selejtezési táblázatba

Az adattár és osztályozás szakaszának utolsó lépése az, hogy az összegyűjtött információkat bevisszük a selejtezési táblázatba, hogy egyszerű áttekintést kapjunk az adott illetékes osztály/részleg felelősségi körébe tartozó eszközökről, illetve a vonatkozó selejtezési időszakokról, kiegészítve a kezdő időponttal – azaz hogy mennyi idő után kell az intézkedést végrehajtani –, illetve az ehhez tervezett munkaráfordítással.

SELEJTEZÉS ÉS ELLENŐRZÉS

18) A szolgáltató felelős a selejtezésért

Ellenőrizni kell, hogy az eszközök selejtezésének felelőssége átkerült-e szerződéssel a szolgáltatóhoz.

Amennyiben a selejtezést nem külső szolgáltató végzi, a selejtezésért az illetékes osztály/részleg felel.

19) A selejtezési követelmények átadása a szolgáltatónak

Ha az információk selejtezéséért valamelyik szolgáltató felelős, gondoskodni kell a meghatározott selejtezési időszakok közléséről – a kezdő időpontokkal együtt – és ezek betartásáról. Ennek érdekében a szolgáltató rendelkezésére kell bocsátani a selejtezési időpontokat.

20) A selejtezési követelmények teljesítése

A kezdő időpontokat is tartalmazó selejtezési időszakok kézhezvétele után a szolgáltatónak minden szükséges követelményt teljesítenie kell annak érdekében, hogy az adatokat a követelményekben meghatározottak szerint törölhesse.

21) Adattörlés és dokumentálás

Miután az eszközök selejtezési időszaka elkövetkezett, a szolgáltató törli az adatokat, és megfelelően dokumentálja a törlést.

22) A selejtezési igazolás elkészítése és átadása

Sikeres selejtezést követően a szolgáltatónak el kell készítenie és az illetékes osztálynak/részlegnek át kell adnia a selejtezési igazolást.

23) A selejtezési igazolás ellenőrzése

Tekintettel arra, hogy végső soron az illetékes osztály/részleg felelős az adatok törléséért – függetlenül attól, hogy a feladatot egy szolgáltató hajtja-e végre –, a selejtezési igazolást felül kell vizsgálni. Ellenőrizni kell, hogy a selejtezési igazolás minden szükséges információt tartalmaz-e annak biztosítása érdekében, hogy az adatokat a szerződés szerint törölték.

24) Érvényes igazolás

A selejtezési igazolásban szereplő információk ellenőrzése után az illetékes osztálynak/részlegnek a selejtezési igazolást el kell fogadnia vagy el kell utasítania.

25) A szolgáltató tájékoztatása

A szolgáltatót tájékoztatni kell abban az esetben, ha az igazolás érvénytelen vagy helytelen, például hiányzik vagy hibás valamilyen információ, a gazdálkodó részlegnek kétségei merültek fel azzal kapcsolatban, hogy a szóban forgó adatokat törölték stb. Ekkor a 21. lépéstől újrakezdve folytatódik a folyamat.

26) Papíralapú eszköz

Az illetékes osztálynak/részlegnek először azt kell ellenőriznie, hogy a selejtezendő eszköz papíralapú vagy elektronikus úton tárolt.

27) Manuális eszközkövetési terv létezik

Minden részlegnél léteznie kell valamilyen követési tervnek az összes olyan eszközre vonatkozóan, amelyeket manuálisan kell leselejtezni. Ellenőrizni kell, hogy létezik-e ilyen.

28) A követési terv elkészítése

Amennyiben nincs követési terv, el kell készíteni, aminek tartalmaznia kell egyebek mellett a szóban forgó papíralapú és elektronikus eszközöket is. Ilyen információk például a vonatkozó selejtezési időpontok, az utóbbiak kezdő időpontja, a nem automatikus törlés indokolása (digitális eszközök esetén), illetve a selejtezés ellenőrzése.

29) Az eszköz szerepel a követési tervben

Ellenőrizni kell, hogy a szóban forgó eszköz szerepel-e már a követési tervben.

30) A követési terv kiegészítése az eszközzel

Abban az esetben, ha az eszköz nem szerepel benne, a követési tervet ki kell egészíteni vele és az összes szükséges információval.

31) A selejtezésre vonatkozó követési terv betartása

Amikor már az összes eszköz szerepel a követési tervben, gondoskodni kell arról, hogy minden felelős munkavállaló betartsa a dokumentumban meghatározott selejtezési időpontokat.

32) A felelős informatikai szolgáltató megkeresése és a követelmények egyeztetése

Ha az eszközt elektronikus úton tárolják, a selejtezési követelmények egyeztetése érdekében a felelős informatikai szolgáltatóhoz (helyi, csoportinformatika, harmadik fél) kell fordulni. Ennek célja egy automatikus megoldás bevezetése (legjobb erőfeszítés – best effort).

33) A selejtezési követelmények ellenőrzése

A felelős informatikai szolgáltató az illetékes osztállyal/részleggel közösen ellenőrzi a követelményeket.

34) Automatikus megoldás működik

A felelős informatikai szolgáltató ellenőrzi, hogy a szóban forgó eszközre vonatkozóan van-e már bevezetve valamilyen automatikus törlési megoldás.

35) Automatikus megoldás bevezethető

Ellenőrizni kell, hogy a legjobb erőfeszítés (best effort) szerint be lehet-e vezetni valamilyen automatikus, a korábban meghatározott követelményeknek megfelelő megoldást.

36) Automatikus megoldás bevezetése

Miután minden követelmény teljesült, ki kell dolgozni és be kell vezetni az automatikus megoldást.

37) A megoldás megfelel a követelményeknek

Megvalósítást követően az illetékes osztálynak/részlegnek ellenőriznie kell, hogy a kapott megoldás megfelel-e az elemzés folyamatában meghatározott követelményeknek.

38) A jelenlegi megoldás átalakítása a követelményeknek megfelelően

Abban az esetben, ha a követelmények nem teljesülnek, jelenteni kell az informatikai szolgáltatónak, majd annak megfelelően módosítani kell.

39) Indokolás automatikus megoldás bevezetésének mellőzése esetén

Olyankor, amikor az automatikus megoldás bevezetése nem lehetséges vagy nem megvalósítható, az illetékes osztállyal/részleggel közölni kell a vonatkozó indokokat. Ezt követően az eszközt a 27. és azt követő lépésekben foglaltak szerint fel kell venni a manuális követési tervbe.

40) Az adatok törlése a selejtezési követelmények szerint

Az illetékes osztálynak/részlegnek gondoskodnia kell arról, hogy az adatokat a követelményrendszer szerint töröljék.

41) Sikeres selejtezés

A megfelelőség biztosítása érdekében ellenőrizni kell, hogy a selejtezést sikeresen végrehajtották.

42) A selejtezés dokumentálása

Ha a szóban forgó eszközök selejtezése sikeresen megtörtént, megfelelően dokumentálni kell a selejtezéskövetési tervekben.

2. melléklet: Selejtezési kategóriák táblázata az „Adatmegőrzésre vonatkozó iránymutatás” című 1. melléklethez

Kezdő időpont		Általános selejtezési időszak						
		azonnal	42 nap	1 év	3 év	5 év	8 év	100 év
	a begyűjtéstől			kapcsolódási adatok				
	a folyamat végétől	webnaplók	műveleti naplók		általános munkajogi adatok	reklamációk. kötelmi jogi jellegű adatok	levelek. könyvelési adatok, tételes számla, számviteli bizonylat alátámasztásául szolgáló adatok	
	a kapcsolat végétől			egyéb törzsadatok			szerződések, törzsadatok	a TB ellátásra való jogosultság szempontjából releváns munkaügyi iratok

Sötétszürke = jogszabályból következő időszak

Világosszürke = szabadon megválasztott időszak

A konkrét selejtezéssel és selejtezési időszakokkal kapcsolatban mindig egyeztessen a számviteli vezetővel, illetőleg a DPO-val, mert egyes iratokra, adatokra jogszabály alapján külön megőrzési időszakok vonatkozhatnak.

Különleges selejtezési időszakok

Helyzet

Jogellenesen gyűjtött személyes adatok

Az érintett törvényes kérését követő személyes adatok
A rendszereken elvégzett javítás, szétszerelés és törlés után
Egy vállalkozás átadása esetén
Incidensek esetén
Peres ügyek vagy követelések esetén
Archívumok
Tartalék másolatok (helyreállítás céljából)
Naplózási protokollok (alkalmazások)
Naplózási protokollok (infrastruktúra)
Átviteli rendszerek (alkalmazások)
Adateszközök speciális felhasználási célú másolatai

Az informatikai rendszer maradványai, például költöztetés során nem törölt adateszközök

3. melléklet: RACI-mátrix az „Adatmegőrzésre vonatkozó iránymutatás” című 1. melléklethez

ID	Adatmegőrzési/selejtezési terv elkészítése és végrehajtása	Végtermék	Csoport igazgatóság	Helyi igazgatóság	HGDP	LDPO/LDPC	Üzletág	Csoport IT	Helyi IT	Szolgáltató
	PHOENIX csoport szintű adatmegőrzési terv (egyszeri intézkedés)									
1.1	A PHOENIX csoport adatmegőrzési tervének / selejtezési szabályainak meghatározása	Data Deletion rules (.doc)	A		R	I		C		
1.2	A PHOENIX csoport adatmegőrzési irányelv mintájának elkészítése	Data Retention policy template (.doc)	A		R	I		C		
1.3	A PHOENIX csoport adatselejtezési mintatáblázatának elkészítése	Data Deletion matrix (.xls)	A		R	I		C		
	PHOENIX helyi adatmegőrzési terv (egyszeri intézkedés)									
2.1	A csoport mintáján alapuló helyi irányelv megvalósítása	Local Data Deletion policy (.doc)		A	C	R			I	
2.2	A helyi feladatokra vonatkozó helyi RACI elkészítése	Local Data retention RACI (.xls)		A	C	R			I	
2.3	A személyes adatokat tartalmazó adathordozók leltárának elkészítése és nyilvántartása	Local system inventory (.xls)		A		C	R		I	
2.4	A helyi selejtezési kategóriák táblázatának kitöltése	Local Data retention matrix (.xls)		A	C		R		I	
2.5	A helyi adatmegőrzési terv kidolgozása és dokumentálása	Local Data deletion concept (.doc)		A	C	R			I	
2.6	Az adatmegőrzési tervet támogató IT-megoldások elkészítése (adott esetben)	Template for retention concept (.xls)		A	I			C	R	
2.7	A helyi adatmegőrzési terv végrehajtása	Implementation plan (.xls)		A	C	R		I		
2.8	A szükséges SOP-dokumentumok megírása	SOP (.doc)		A		C	R		I	
2.9	Az adatvédelmi audit lebonyolítása szükség szerint	Data Retention Audit report (.doc)		A	C	R			I	
	ADATTÁR ÉS OSZTÁLYOZÁS (állandó folyamat)									
3.1.	Eszközleltár felvétele	Információs eszközjegyzék		A		I	R		C	
3.2.	Minden kötelező információ megvan	Információs eszközjegyzék		A		I	R		C	
3.3	A hiányszó információk begyűjtése	Információs eszközjegyzék		A		I	R		C	
3.4	A leltár kiegészítése a hiányzó információkkal	Információs eszközjegyzék		A		I	R		C	
3.5	Az adattípus meghatározása	Információs eszközjegyzék		A		I	R		C	
3.6	Az adatmegőrzési idő meghatározása	Információs eszközjegyzék		A		I	R		C	
3.7	Jogi, szerződéses és működési követelmények meghatározása	Információs eszközjegyzék		A		I	R		C	
3.8	A leltár kiegészítése a követelményre vonatkozó tudnivalókkal	Információs eszközjegyzék		A		I	R		C	
3.9	A leltár kiegészítése az adatmegőrzési idővel	Információs eszközjegyzék		A		I	R		C	
3.10	Az adatmegőrzési idő meghatározása	Információs eszközjegyzék		A		I	R		C	
3.11	Már van megfelelő adatmegőrzési idő	Információs eszközjegyzék		A		I	R		C	
3.12	Új adatmegőrzési idő meghatározása a helyi DPO-val	Információs eszközjegyzék		A		C	R		I	
3.13	A leltár kiegészítése az adatmegőrzési idővel	Információs eszközjegyzék		A		C	R		I	
3.14	Az adatmegőrzési idő alkalmazása és a leltár kiegészítése	Információs eszközjegyzék		A		I	R		C	
3.15	A selejtezési időszak kezdetének meghatározása és a leltár kiegészítése	Információs eszközjegyzék		A		I	R		C	
3.16	Különleges helyzetek selejtezési időszakának és kezdő időpontjának meghatározása	Információs eszközjegyzék		A		I	R		C	
3.17	Bevitel a selejtezési táblázatba	Update to Data Deletion matrix (.xls)		A		I	R		C	
	SELEJTEZÉS ÉS ELLENŐRZÉS (állandó folyamat)									
3.18	Annak ellenőrzése, hogy a szolgáltató felel-e a selejtezésért	Data Processing Agreement (.doc)		A		I	R		C	
3.19	A selejtezési táblázat átadása a szolgáltatónak	Updated Data retention matrix (.xls)		A		I	R		C	
3.20	A selejtezési követelmények teljesítése	Proof of deletion (.doc)		A		I	C			R
3.21	Az adatok törlése és a selejtezés dokumentálása	Proof of deletion (.doc)		A		I	C			R
3.22	A selejtezési igazolás elkészítése és átadása	Proof of deletion (.doc)		A		I	C			R
3.23	A szolgáltató selejtezési igazolásának ellenőrzése	Proof of deletion (.doc)		A		I	R		C	
3.24	A selejtezési igazolás elfogadása vagy elutasítása	Proof of deletion (.doc)		A		I	R		C	
3.25	A szolgáltató tájékoztatása	Data Processing Agreement (.doc)		A		I	R		C	I
3.26	Annak ellenőrzése, hogy az eszköz papíralapú-e	Template for retention concept (.xls)		A		C,I	R			
3.27	Manuális eszközkövetési terv létezik	Template for retention concept (.xls)		A		C,I	R			
3.28	A követési terv elkészítése	Template for retention concept (.xls)		A		C,I	R			
3.29	A követési tervben szerepel az eszköz	Template for retention concept (.xls)		A		C,I	R			
3.30	A követési terv kiegészítése az eszközzel	Template for retention concept (.xls)		A		C,I	R			
3.31	A selejtezésre vonatkozó követési terv betartása	Template for retention concept (.xls)		A		C,I	R			
3.32	A felelős informatikai szolgáltató megkeresése és a követelmények egyeztetése	Local Data retention matrix (.xls)		A		C	R		I	
3.33	A selejtezési követelmények ellenőrzése	Local Data retention matrix (.xls)		A		I	C		R	
3.34	Automatikus megoldás működik	Template for retention concept (.xls)		A		I	C		R	
3.35	Automatikus megoldás bevezethető	Template for retention concept (.xls)		A		I	C		R	
3.36	Automatikus megoldás bevezetése	Updated design document (.doc)		A		I	C		R	
3.37	A megoldás megfelel a követelményeknek	Updated design document (.doc)		A		I	R		C	
3.38	A jelenlegi megoldás átalakítása a követelményeknek megfelelően	Updated design document (.doc)		A		I	C		R	
3.39	Indokolás automatikus megoldás bevezetésének mellőzése esetén	Template for retention concept (.xls)		A		I	C		R	
3.40	Az adatok törlése a selejtezési követelmények szerint	Proof of deletion (.doc)		A		I	R		C	
3.41	Sikeres selejtezés	Proof of deletion (.doc)		A		I	R		C	
3.42	A selejtezés dokumentálása	Proof of deletion (.doc)		A		I	R		C	

R = responsible (felelős)
A = accountable (elszámoltatható)
C = consulting (tanácsadó)
I = informing (tájékoztat)

HGDP = a Csoport Adatvédelmi Vezetője
LDPO = Helyi Adatvédelmi Tisztviselő
LDPC = Helyi Adatvédelmi Koordinátor

Fogalommeghatározás: Az alkalmazás üzletági felelőse, például az osztályvezető, részlegvezető, az alkalmazás kulcsfelhasználója, az alkalmazás üzletági

A PHOENIX csoport Adatvédelmi Irányelvének 2. melléklete:

Adatvédelmi incidensekre vonatkozó iránymutatás

1. Bevezetés

Ez az iránymutatás ismerteti azokat a kötelező eljárásokat, amelyeket abban az esetben kell a munkavállalóknak alkalmazniuk, ha a PHOENIX csoportban valamilyen adatvédelmi incidenst tapasztalnak, vagy arra gyanakszanak, hogy adatvédelmi incidens történt.

Adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Fontos, hogy legyen egy olyan eljárás, amely lehetővé teszi az időben történő megfékezést, értékelést és válaszadást abban az esetben, ha a PHOENIX csoportnál valamilyen adatvédelmi incidenst tapasztalnak. Így csökkenteni lehet a természetes személyeket és a szervezetet is érő esetleges károkat.

2. Az adatvédelmi incidensek típusai

A GDPR szerint adatvédelmi incidens például az olyan esemény, amikor a személyes adatokat – véletlenül vagy szándékosan – feltörik, nyilvánosságra hozzák, lemásolják, továbbítják, megszerzik, eltávolítják, megsemmisítik, ellopják vagy jogosulatlan személyek felhasználják.

Idetartoznak egyebek mellett a következő események:

- Bizalmas vagy érzékeny adatok, különleges adatok vagy olyan berendezések elvesztése vagy ellopása, amelyeken ilyen adatokat tárolnak (pl. notebook számítógép, okostelefon, USB-memória, iPad/táblagép vagy papírirat elvesztése)
- Eszköz ellopása vagy meghibásodása
- Adatok vagy információs rendszerek jogosulatlan felhasználása, hozzáférése vagy módosítása
- Információkhoz vagy informatikai rendszer(ek)hez jogosulatlan hozzáférés megszerzésére irányuló (meghiúsult vagy sikeres) kísérlet
- Érzékeny / bizalmas adatok jogosulatlan nyilvánosságra hozatala
- Weboldalak lecserélése
- Informatikai támadás
- Előre nem látható körülmények, úgymint tűz vagy árvíz

- Emberi hiba
- „Álneves" jogsértések („csalások"), amikor a tulajdonos szervezettől megtévesztéssel szereznek meg információkat

3. Eljárás

3.1 Incidensek bejelentése

A PHOENIX csoport minden munkavállalója köteles a felelős adatvédelmi tisztviselőnek azonnal jelenteni a PHOENIX csoport portálján (a https://phoenixgroup-databreach.integrityplatform.org) keresztül az adatvédelmi incidenseket és információbiztonsági incidenseket. Ha a portál nem működik vagy elérhetetlen, a felelős adatvédelmi tisztviselőnek kell e-mailt küldeni.

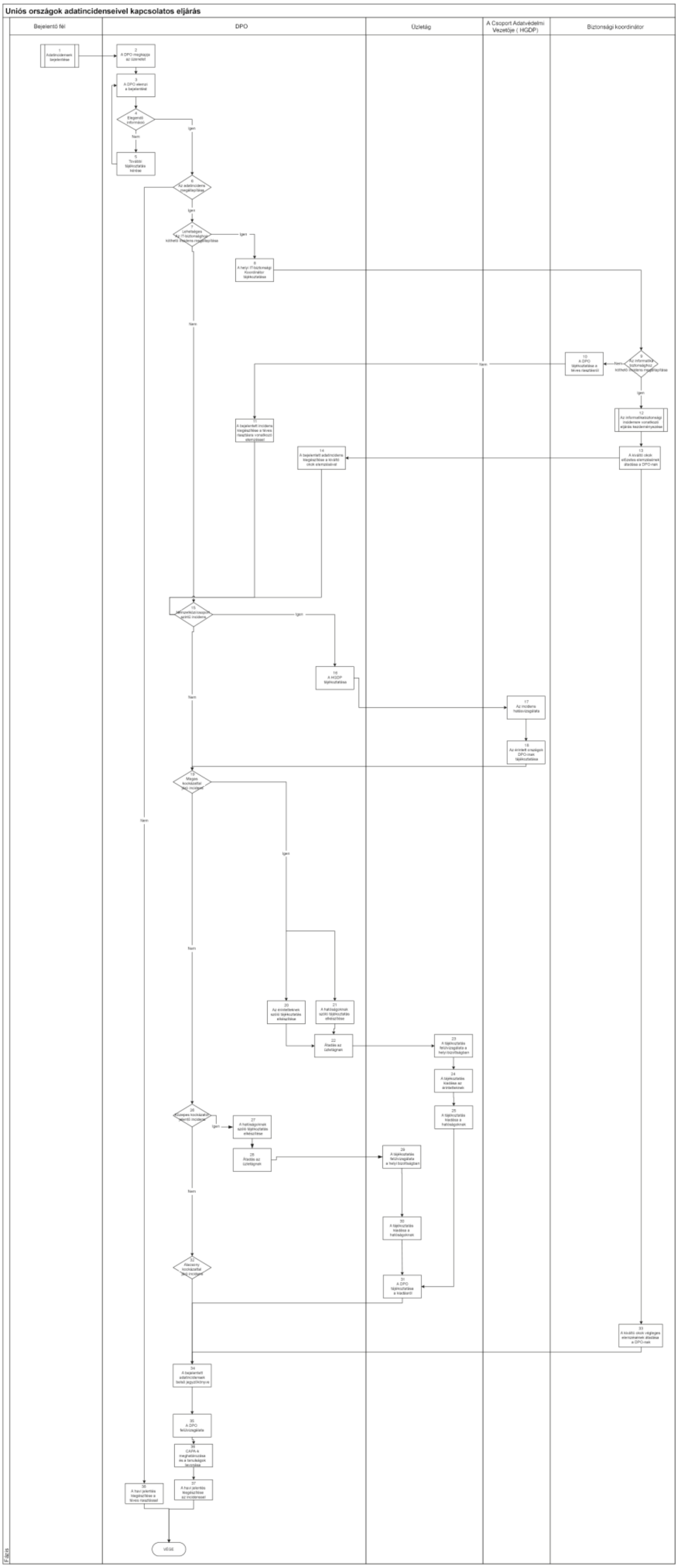
Ha az incidens rendes munkaidőn kívül történik vagy derül ki, az első adandó alkalommal jelenteni kell, amint lehet.

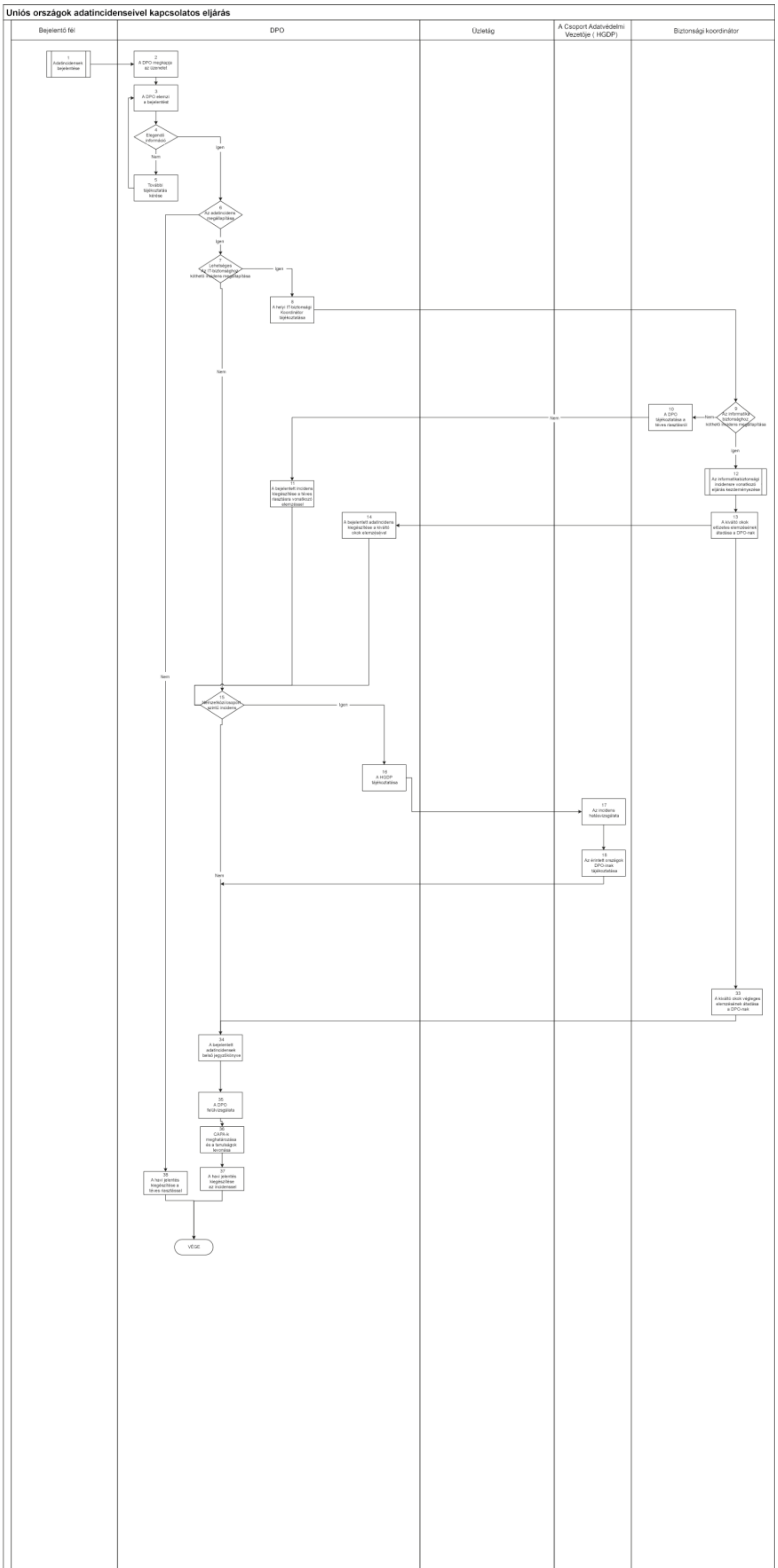
3.2 Folyamatleírás

A PHOENIX csoport minden munkavállalójától elvárjuk, hogy az adatvédelmi incidensekre vonatkozó eljárást kövesse (lásd 1. melléklet).

Nem kell tájékoztatni a felügyeleti hatóságot és/vagy az érintettet, ha a GDPR nem alkalmazandó (különösen az Unión kívüli országokban), és a helyi jogban nincs a GDPR-ben szereplővel azonos kötelezettség.

1. melléklet: Folyamatábra és -leírás


Uniós országok adatincidenseivel kapcsolatos eljárás
Bejelentő fél
DPO
Üzletág
A Csoport Adatvédelmi Vezetője (HGDP)
Biztonsági koordinátor
1 Adatincidensek bejelentése
2 A DPO megkapja az üzenetet
3 A DPO elemzi a bejelentést
4 Elegendő információ
Igen
Nem
5 További tájékoztatás kérése
6 Az adatincidens megállapítása
7 Lehetséges az IT-biztonsághoz köthető incidens megállapítása
8 A helyi IT-biztonsági Koordinátor tájékoztatása
9 Az informatikai biztonsághoz köthető incidens megállapítása
10 A DPO tájékoztatása a téves riasztásról
11 A bejelentett incidens kiegészítése a téves riasztásra vonatkozó elemzéssel
12 Az informatikaibiztonsági incidensre vonatkozó eljárás kezdeményezése
13 A kiváltó okok előzetes elemzésének átadása a DPO-nak
14 A bejelentett adatincidens kiegészítése a kiváltó okok elemzésével
15 Nemzetközi/csoport szintű incidens
16 A HGDP tájékoztatása
17 Az incidens hatásvizsgálata
18 Az érintett országok DPO-inak tájékoztatása
19 Magas kockázattal járó incidens
20 Az érintetteknek szóló tájékoztatás elkészítése
21 A hatóságoknak szóló tájékoztatás elkészítése
22 Átadás az üzletágnak
23 A tájékoztatás felülvizsgálata a helyi bizottságban
24 A tájékoztatás kiadása az érintetteknek
25 A tájékoztatás kiadása a hatóságoknak
26 Közepes kockázatot jelentő incidens
27 A hatóságoknak szóló tájékoztatás elkészítése
28 Átadás az üzletágnak
29 A tájékoztatás felülvizsgálata a helyi bizottságban
30 A tájékoztatás kiadása a hatóságoknak
31 A DPO tájékoztatása a kiadásról
32 Alacsony kockázattal járó incidens
33 A kiváltó okok végleges elemzésének átadása a DPO-nak
34 A bejelentett adatincidensek belső jegyzőkönyve
35 A DPO felülvizsgálata
36 CAPA-k meghatározása és a tanulságok levonása
37 A havi jelentés kiegészítése az incidenssel
38 A havi jelentés kiegészítése a téves riasztással
VÉGE
Fázis


Uniós országok adatincidenseivel kapcsolatos eljárás
Bejelentő fél
DPO
Üzletág
A Csoport Adatvédelmi Vezetője (HGDP)
Biztonsági koordinátor
1 Adatincidensek bejelentése
2 A DPO megkapja az üzenetet
3 A DPO elemzi a bejelentést
4 Elegendő információ
Igen
Nem
5 További tájékoztatás kérése
6 Az adatincidens megállapítása
Igen
7 Lehetséges az IT-biztonsághoz köthető incidens megállapítása
Igen
8 A helyi IT-biztonsági Koordinátor tájékoztatása
Nem
9 Az informatikai biztonsághoz köthető incidens megállapítása
Nem
10 A DPO tájékoztatása a téves riasztásról
Nem
Igen
11 A bejelentett incidens kiegészítése a téves riasztásra vonatkozó elemzéssel
12 Az informatikaibiztonsági incidensre vonatkozó eljárás kezdeményezése
13 A kiváltó okok előzetes elemzésének átadása a DPO-nak
14 A bejelentett adatincidens kiegészítése a kiváltó okok elemzésével
Nem
15 Nemzetközi/csoport szintű incidens
Igen
16 A HGDP tájékoztatása
17 Az incidens hatásvizsgálata
18 Az érintett országok DPO-inak tájékoztatása
Nem
33 A kiváltó okok végleges elemzésének átadása a DPO-nak
34 A bejelentett adatincidensek belső jegyzőkönyve
35 A DPO felülvizsgálata
36 CAPA-k meghatározása és a tanulságok levonása
37 A havi jelentés kiegészítése az incidenssel
38 A havi jelentés kiegészítése a téves riasztással
VÉGE
F 8215

1. melléklet: Folyamatleírás

AZ „ADATVÉDELMI INCIDENSEKRE VONATKOZÓ IRÁNYMUTATÁS” című 2. melléklethez

1. Adatvédelmi incidensek bejelentése
   A bejelentő fél az adatvédelmi incidens bejelentését a PHOENIX csoport által biztosított eszközben/portálon található (a https://phoenixgroup-databreach.integrityplatform.org) megfelelő nyomtatvány kitöltésével hozza létre. A nyomtatványon kért kötelező információkat minél részletesebben kell megadni.

2. A DPO megkapja az üzenetet
   Az adatvédelmi incidens bejelentésében megadott információk alapján a DPO-t automatikusan értesíti a jelentéskészítő eszköz. A PHOENIX csoport ezzel értesül az incidensről, és meg kell állapítania, hogy történt-e adatvédelmi incidens.

3. A DPO elemzi a bejelentést
   Az incidens besorolása érdekében a DPO elemzi a bejelentést, majd ellenőrzi, hogy minden szükséges információt megadtak-e.

4. Elegendő információ
   A bejelentés elemzése alapján a DPO eldönti, hogy a bejelentő féltől kell-e további tájékoztatást kérni.

5. További tájékoztatás kérése
   Ha a bejelentés részletessége nem éri el a kívánt szintet, a DPO bekéri a bejelentő személytől a hiányzó információkat, amennyiben teljesülnek a követelmények.

6. Az adatvédelmi incidens megállapítása
   Ha a bejelentést kitöltötték és a megadott információk megalapozzák, a DPO-nak el kell döntenie, hogy adatvédelmi incidens történt, vagy csak téves riasztásról van szó (téves eredmény, mert adatvédelmi incidensnek tűnt, de nem volt az). Legkésőbb ilyenkor a PHOENIX csoport már „tud” az adatvédelmi incidensről, és fel kell mérnie, hogy mekkora a veszély a magánszemélyekre nézve. Ha a bejelentés téves riasztás volt, az eljárás a 37. lépéstől folytatódik tovább.

7. Informatikai biztonsághoz köthető incidens lehetősége
   Miután az adatvédelmi incidenst megállapította, a DPO ellenőrzi, hogy informatikai biztonsági incidenshez köthető-e, ami olyan eseményt jelent, amely a PHOENIX csoport valamely információs forrásának vagy eszközének bizalmas jellegét, integritását vagy rendelkezésre állását befolyásolja. Ezek közé tartoznak egyebek mellett a következők: olyan (meghiúsult vagy sikeres) kísérletek, amelyek a rendszerhez vagy annak adataihoz való jogosulatlan hozzáférés

megszerzésére; váratlan fennakadás vagy szolgáltatás-megtagadás okozására; a rendszer jogosulatlan adatkezelésre vagy -tárolására történő felhasználására; a tulajdonos tudta, utasítása vagy hozzájárulása nélkül a rendszer hardver-, firmware- vagy szoftverjellemzőiben történő változtatásra irányulnak. Ha a DPO nem biztos benne, a helyi IT-biztonsági Felelőstől kell tanácsot kérnie.

8. A helyi IT-biztonsági Koordinátor tájékoztatása
   Ha az adatvédelmi incidens informatikai biztonsági incidenshez köthető, vagy ha a DPO nem biztos benne, a DPO-nak a helyi IT-biztonsági Koordinátorhoz kell fordulnia, akinek az incidensre vonatkozó összes szükséges információt át kell adnia. A DPO és a helyi IT-biztonsági Koordinátor között szoros együttműködésre van szükség, amíg az adatvédelmi incidenssel kapcsolatos eljárást le nem zárják.

9. Az informatikai biztonsághoz köthető incidens megállapítása
   A bejelentés kézhezvétele és elemzése után a Helyi Biztonsági Koordinátornak meg kell állapítania, hogy az incidens informatikai biztonsági incidenshez köthető-e vagy sem.

10. A DPO tájékoztatása a téves riasztásról
    Ha a Helyi Biztonsági Koordinátor arra a következtetésre jut, hogy nincs bizonyíték az informatikai biztonsági incidens fennállására, a téves riasztásról tájékoztatni kell a felelős DPO-t.

11. A bejelentett incidens kiegészítése a téves riasztásra vonatkozó elemzéssel
    A bejelentések hatékonyságának javítása érdekében a bejelentett incidenst ki kell egészíteni a téves riasztással, ha pedig lehet, a jelentés kiadását követően CAPA-kat (korrekciós és megelőző intézkedéseket) kell meghatározni.

12. Az informatikai biztonsági incidensre vonatkozó eljárás kezdeményezése
    Ha a helyi Biztonsági Koordinátor igazolja, hogy az incidenst valamilyen informatikai biztonsági incidens okozta, meg kell indítani a megfelelő eljárást.

13. A kiváltó okok előzetes elemzésének átadása a DPO-nak
    Tekintettel arra, hogy a kiváltó okok elemzésének (RCA) véglegesítése hosszabb időt vehet igénybe, el kell készíteni, és a felelős DPO-nak át kell adni az előzetes RCA-t. Ennek igen nagy jelentősége van, mivel az adatvédelmi incidens okának szerepelnie kell a hatóságoknak és az érintetteknek szóló előzetes jelentésekben. Ha lehetséges, a CAPA-knak szerepelniük kell a DPO-nak szóló jelentésben.

14. A bejelentett adatvédelmi incidens kiegészítése a kiváltó okok elemzésével
    Ha az előzetes RCA-t kézhez kapta, a DPO kiegészíti vele a bejelentett adatvédelmi incidenst.

15. Nemzetközi/csoport szintű incidens
    A DPO-nak meg kell állapítania, hogy az incidens csak a saját országára vonatkozik, vagy a PHOENIX csoport országai közül mások is érintettek benne. A Csoport Adatvédelmi Vezetőjét (HGDP) kell tájékoztatni, ha más országokat is érint az incidens.
16. A HGDP tájékoztatása
    A felelős DPO-nak az incidensre vonatkozóan rendelkezésre álló összes szükséges információt át kell adnia annak érdekében, hogy a Csoport Adatvédelmi Vezetője foglalkozni tudjon az adatvédelmi incidenssel.

17. Az incidens hatásvizsgálata
    A kapott információk alapján a HGDP-nek fel kell mérnie az incidens hatását, először az érintett országokat, utána pedig azt, hogy mennyire súlyos az adatincidens.

18. Az érintett országok DPO-inak tájékoztatása
    Nemzetközi/csoport szintű incidens esetén a HGDP átveszi a koordinátor szerepét, és az érintett országokban az összes felelős DPO tájékoztatásával gondoskodik arról, hogy az incidens kezelésének legyen egy nyílt kommunikációs csatornája, és minden illetékes felügyeleti hatóság megfelelő tájékoztatást kapjon.

19. Magas kockázattal járó incidens
    A DPO-nak fel kell mérnie, hogy az incidens valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve (lásd GDPR 34. cikk (1) bekezdés). Ebben az esetben az incidenst magas kockázatba kell sorolni, és az illetékes felügyeleti hatóságoknak szóló bejelentést és az érintetteknek szóló tájékoztatást is el kell készíteni (az Unión kívüli országokban csak akkor van bejelentés/tájékoztatás, ha a helyi jogszabályok előírják). Indokolatlan késedelem nélkül, de legkésőbb 72 órán belül bejelentést kell tenni az illetékes felügyeleti hatóságok felé. Ha a bejelentés hosszabb időt vesz igénybe, a bejelentéshez mellékelni kell a késedelem megfelelő indokolását. Indokolatlan késedelem nélkül tájékoztatni kell a szóban forgó érintetteket. Ezzel egyidejűleg a PHOENIX csoportnak intézkednie kell az incidens megfékezése és a helyreállítás érdekében.

20. Az érintetteknek szóló tájékoztatás elkészítése
    Ha a helyi rendelkezések mást nem állapítanak meg, a csoport szintű minta alapján a felelős DPO-nak el kell készítenie, illetve felülvizsgálatra elő kell készítenie az érintetteknek szóló tájékoztatást (az Unión kívüli országokban csak akkor van tájékoztatás, ha a helyi jogszabályok előírják).

21. A felügyeleti hatóságoknak szóló bejelentések elkészítése

Ha a helyi hatóságok nem biztosítanak bejelentési mechanizmust (pl. webportál), a bejelentést a csoport szintű minta alapján kell elkészíteni és felülvizsgálatra előkészíteni (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják).

22. Átadás az üzletágnak/vezetőségnek

Megfogalmazás után a bejelentéseket/tájékoztatásokat a (CAPA-kat is tartalmazó) jelentéssel együtt át kell adni a helyi bizottságnak, amely felelős a bejelentés megtételének/tájékoztatás kiadásának jóváhagyásáért (az Unión kívüli országokban csak akkor van tájékoztatás, ha a helyi jogszabályok előírják).

23. A tájékoztatások felülvizsgálata a helyi bizottságban

A helyi bizottság ellenőrzi, hogy magas kockázattal járó-e az incidens (minden érintettet/stakeholder-t be kell vonni, aki szükséges). Ezután a helyi bizottságnak át kell tekintenie és jóvá kell hagynia mind a hatóságnak szóló bejelentést, mind az érintetteknek szóló tájékoztatást, majd el kell döntenie, hogy ki felelős a megtételükért/kiadásukért (pl. az üzletág/vezetőség vagy a felelős DPO), mielőtt elküldik őket a megfelelő címzetteknek (az Unión kívüli országokban csak akkor van tájékoztatás, ha a helyi jogszabályok előírják).

24. A tájékoztatás kiadása az érintetteknek

Ha a helyi bizottság áttekintette és jóváhagyta, a kijelölt személy (az üzletág/vezetőség vagy a felelős DPO) kiadja a tájékoztatásokat az incidensben érintetteknek (az Unión kívüli országokban csak akkor van tájékoztatás, ha a helyi jogszabályok előírják).

25. Bejelentés megtétele az illetékes felügyeleti hatóságok felé

Ha a helyi bizottság áttekintette és jóváhagyta, a kijelölt személy (az üzletág/vezetőség vagy a felelős DPO) megteszi a bejelentést a helyi illetékes felügyeleti hatóságok felé a rendelkezésre bocsátott megoldás vagy a csoport szintű bejelentési nyomtatvány felhasználásával (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják).

26. Közepes kockázattal járó incidens

A DPO-nak fel kell mérnie, hogy az incidens valószínűsíthetően kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve (viszont nem valószínű, hogy magas kockázattal jár, lásd GDPR 33. cikk (1) bekezdés). Ebben az esetben az incidenst közepes kockázatba kell sorolni, és csak a felügyeleti hatóságoknak szóló bejelentést kell elkészíteni (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják). Indokolatlan késedelem nélkül, de legkésőbb 72 órán belül meg kell tenni a bejelentést az illetékes felügyeleti hatóság felé. Ha a bejelentés hosszabb időt vesz igénybe, a bejelentéshez mellékelni

kell a késedelem megfelelő indokolását. Ezzel egyidejűleg a PHOENIX csoportnak intézkednie kell az incidens megfékezése és a helyreállítás érdekében.

27. Az illetékes felügyeleti hatóságoknak szóló bejelentés elkészítése
Ha a helyi hatóságok nem biztosítanak bejelentési mechanizmust (pl. webportál), a bejelentést a csoport szintű minta alapján kell elkészíteni és felülvizsgálatra előkészíteni (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják).

28. Átadás az üzletágnak/vezetőségnek
Megfogalmazás után a bejelentést a (CAPA-kat is tartalmazó) jelentéssel együtt át kell adni a helyi bizottságnak, amely felelős a bejelentés megtételének jóváhagyásáért (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják).

29. A bejelentés felülvizsgálata a helyi bizottságban
A helyi bizottság ellenőrzi, hogy közepes kockázattal járó-e az incidens (minden érintettet/stakeholder-t be kell vonni, akikre szükség van). A helyi bizottságnak át kell tekintenie és jóvá kell hagynia a bejelentést, majd el kell döntenie, hogy ki felelős a bejelentés megtételéért (pl. az üzletág/vezetőség vagy a felelős DPO), mielőtt elküldik a megfelelő címzetteknek (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják).

30. Bejelentés megtétele az illetékes felügyeleti hatóságok felé
Ha a helyi bizottság áttekintette és jóváhagyta, a kijelölt személy (az üzletág/vezetőség vagy a felelős DPO) megteszi a bejelentést a helyi felügyeleti hatóságok felé a rendelkezésre bocsátott megoldás vagy a csoport szintű bejelentési nyomtatvány felhasználásával (az Unión kívüli országokban csak akkor van bejelentés, ha a helyi jogszabályok előírják).

31. A DPO tájékoztatása a kiadásról/megtételről
Ha a bejelentéseket megtették/tájékoztatásokat kiadták (az Unión kívüli országokban csak akkor van bejelentés/tájékoztatás, ha a helyi jogszabályok előírják), tájékoztatni kell a DPO-t (feltéve, hogy nem a DPO a kijelölt személy).

32. Alacsony kockázattal járó incidens
Ha a DPO arra a következtetésre jut, hogy az incidens valószínűsíthetően (sem a GDPR 33. cikk (1), sem pedig a 34. cikk (1) bekezdése szerint) nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, sem az érintetteket, sem pedig a hatóságokat nem kell tájékoztatni, csak egy belső jelentést kell készíteni.

33. A kiváltó okok végleges elemzésének átadása a DPO-nak

Ha az informatikai biztonsági incidens felügyeleti eljárása lezárult, a kiváltó okok végleges elemzését át kell adni a felelős DPO-nak, majd ki kell egészíteni vele az adatvédelmi incidensekre vonatkozó belső nyilvántartást. A végleges RCA-ban szerepelnie kell egy részletes elemzésnek, amely tartalmazza a hasonló incidensek mérséklését és megelőzését célzó CAPA-kat is.

34. A bejelentett adatvédelmi incidensek belső jegyzőkönyve

Az incidens kockázati besorolásától függetlenül belső jegyzőkönyvet kell felvenni, amelynek tartalmaznia kell az incidens hatását és okait. A jegyzőkönyvet és a kapcsolódó dokumentációt a felelős DPO-nak meg kell őriznie és a GDPR szerint nyilván kell tartania.

35. A DPO felülvizsgálata

A felelős DPO elvégzi az incidens okának vagy okainak, a válaszadás hatékonyságának és annak teljes körű felülvizsgálatát, hogy kell-e változtatást végrehajtani a rendszereken, irányelveken és eljárásokon.

36. CAPA-k meghatározása és a tanulságok levonása

Hasonló incidensek jövőbeli ismételt előfordulásának megelőzése érdekében az incidens megtörténése után a helyi bizottságnak meg kell határoznia a CAPA-kat és a levonható tanulságokat. (Megjegyzés: ekkor megkezdődik a PDCA-ciklus (= Plan – tervezés, Do – végrehajtás, Check – ellenőrzés, Act – válasz ciklusa.)

37. A havi jelentés kiegészítése az incidenssel

Az adatvédelmi incidensek csoport szintű átláthatóságának megteremtése érdekében a havi jelentéseket a PHOENIX csoport által biztosított eszközben ki kell egészíteni minden egyes incidenssel, majd át kell adni a Csoport Adatvédelmi Vezetőjének, szükség szerint pedig át is kell vele tekinteni.

38. A havi jelentés kiegészítése a téves riasztással

Ha a felelős DPO arra a következtetésre jut, hogy a bejelentett adatvédelmi incidens téves riasztás volt, annak meg kell jelennie a havi jelentésekben. Ha lehet, az indokokat is meg kell adni, illetve meg kell határozni a megfelelő CAPA-kat.

Kifejezések és fogalommeghatározások:

Téves riasztás (lásd 6. sz.)

Informatikai biztonsági incidens (lásd 7. sz.)

Nemzetközi/csoport szintű incidens (lásd 15. sz.)

Magas kockázattal járó incidens (lásd 19. sz.)

Közepes kockázattal járó incidens (lásd 26. sz.)

Alacsony kockázattal járó incidens (lásd 32. sz.)

A PHOENIX csoport Adatvédelmi Irányelvének 3. melléklete

„RACI-mátrix"

Szerep Tevékenység	Csoport igazgatóság	Helyi igazgatóság	Érintett	Munkavállaló	Tanácsadó	Adatkezelő	Adatfeldolgozó	HGDP	LDPO	LDPC	LSC
Adatvédelem (lásd Irányelv 1.1)	R	R	I	R	(R, C)	A	R	R	R	R	(R)
Személyes adatok kezelése (lásd 1.1 és 2.)			I	R	R	A	R				
A helyi iránymutatások alkalmazása (lásd 1.5)		A				C,I	I	A	R	R	
A GDPR-irányelv jóváhagyása (lásd 1.6)	A		(I)	I				C			
A GDPR-irányelv felülvizsgálata (lásd 1.6)	A		(I)	I		C,I	I	R	C	C	
Felvilágosítás és képzés biztosítása (lásd 4.9)		A		I	(R, C)				R	(R)	
Tudatosság és képzés elvégzése (lásd 2.1)	A	A		R		R	R	R	R	R	
Új/megváltoztatott eljárás bevezetése (lásd 2.1)	A	A		R		R	R	I	I	I	I
Adatmegőrzés és -selejtezés (lásd 2.1)	A	A	(I)	R		R	R	C	C	C	(C)
Iratfelülvizsgálat (lásd 2.1)	A	A		R		R		C	C	C	C
Tájékoztatás selejtezési intézkedésekkel kapcsolatos szabálytalanság	A	A		R		R		C	C	C	C
Adathordozók selejtezése (lásd 2.1)	A	A		R	(R)	R	R	C	C	C	C
Megfelelőség igazolása (lásd 2.1)	A	A				R	R	C, I	C, I	C, I	
Kezeléssel kapcsolatos iratok megőrzése (lásd 2.1)	A	A		R		A, R	A, R	C, I	C, I	C, I	
Az érintett személyazonosságának ellenőrzése a jogok gyakorlása cél	A	A		R		A		C	C	C	
A SAR (Érintett Adathozzáférési Kérelme) megválaszolása 1 hónapon b	A	A		R		R		R, C	R, C	R, C	
Tájékoztatásadás az érintettnek (lásd 3.2)	A	A		R		R		C	C	C	
Gondoskodás az adatkezelés biztonságáról (lásd 4.1)	A	A		R		R	R	C	C	C	C
Közös adatkezelésre vonatkozó megállapodás (lásd 4.2)	A	A	(I)	I, (C)		R	I	C	C	C	
Adatkezelői megbízási szerződés (lásd 4.3)	A	A				R	(R), I, C	C	C	C	C
Megbízott adatkezelő kiválasztása és auditálása (lásd 4.3)	A	A				R	I	C	R, C	R, C	C
Együttműködés a felügyeleti hatósággal (lásd 4.4)	A	A		R		R	R	R	R	R	R
Incidensek/adatincidensek bejelentése (lásd 4.5)	A	A		R	R	A, R	R		(R)	(R)	(R)
Incidensek bonyolítása (lásd 4.5) ideértve a belső jelentést						A, R	R	R	R	R	R
Adatincidens jelentése az érintettnek (lásd 4.5)	I	A, (R)	I			A, R		R	R	R	(C)
Adatincidens jelentése a csoporton belül (lásd 4.5)	A	(R)						I	R	(R)	(R)
Adatincidens jelentése a hatóságoknak (lásd 4.5)		A, (R)				I	(I)	R	R	R	(C)
Egyéb szabálytalanságok jelentése (lásd 4.5)	A	A	(R)	R	(R)	(R)	(R)	R	R	R	(R)
Adatvédelmi hatásvizsgálat (lásd 4.6)	A	A	(C)	(I), C	(C)	R	I	C	C	C	C
DPO kijelölése (lásd 4.7)		A				R	R		I		
Helyi DPO és/vagy Helyi DPC kijelölése (lásd 4.7)		R						I	I	I	I
A Csoport Helyi Adatvédelmi Vezetőjének kinevezése (lásd 4.7)	R	I						I	I	I	I
A Csoport Információbiztonsági Tisztviselőjének kinevezése (lásd 4.7)	R*							I	I	I	I
Az HGDP, LDPO, LDPC, LSC támogatása az adatvédelemben (lásd 4.8)	R	R		R		R	R				
Kapcsolattartási pont (lásd 4.8)	A	(R), A						R	R	(R)	
Tanácsadás és tájékoztatásadás a PHOENIX adatkezelőnek (lásd 4.9)								A	R	R	
Tanácsadás és tájékoztatásadás a PHOENIX adatfeldolgozónak (lásd 4.9)								A	R	R	
Megfelelőség nyomon követése (lásd 4.9)	I	I				I	I	R	R	R	R
Adattovábbítás az Unión kívüli országokban garanciák mellett (lásd 5.	A	A	I	R		R	R	R	C	C	C

R = responsible (felelős)
A = accountable (elszámoltatható)
C = consulting (tanácsadó)
I = informing (tájékoztató)

HGDP = Csoport Adatvédelmi Vezetője
LDPO = Helyi Adatvédelmi Tisztségviselő
LDPC = Helyi Adatvédelmi Koordinátor
LSC = Helyi Biztonsági Koordinátor

Megjegyzés: új rendszerek bevezetése – lásd Információbiztonsági Irányelv

* = átadva a PHOENIX Group IT GmbH-nak