A PHOENIX Pharma Gyógyszerkereskedelmi Zártkörűen Működő Részvénytársaság Adatvédelmi Irányelve

A PHOENIX csoport csoportszintű adatvédelmi szabályzata alapján
GGL_Corporate Data Protection_20210201

Hatálybalépés napja: 2021.02.01.

Felváltott irányelv: GGL_Group Data Protection_20171219

Alkalmazás szintje:

Csoport	X
Magyarországi alcsoport	
PHOENIX Pharma Zrt.	

Jóváhagyás dátuma: 2021. 01. 28.

A vállalati adatvédelmi szabályzatban használt fogalmak

Adatvédelmi szabályzat	A PHOENIX csoport csoportszintű adatvédelmi szabályzata
CDP útmutató	Vállalati adatvédelmi útmutató
CIO	Informatikai igazgató
CISO	Információbiztonsági igazgató
DPA	Adatfeldolgozási szerződés
DPIA	Adatvédelmi hatásvizsgálat
DPO	Adatvédelmi tisztviselő
EU/EGT	Európai Unió / Európai Gazdasági Térség
FH	Felügyeleti hatóság
GDPR	Az (EU) 2016/679 általános adatvédelmi rendelet
HCDP	Vállalati adatvédelmi vezető
Helyi koncepció	Helyi adatvédelmi koncepció
LSC	Helyi biztonsági koordinátor
Munkavállaló	A PHOENIX csoport alkalmazásában álló természetes személy
PHOENIX csoport	Az összes olyan vállalat, amelyben a PHOENIX Pharma SE vagy valamely leányvállalata birtokolja a részvények többségét, vagy amely a holdingtársaság vagy annak leányvállalatai közvetlen vagy közvetett irányítása alatt áll.
PHOENIX társaság	A PHOENIX csoporthoz tartozó leányvállalat
PIA	Privacy-hatásvizsgálat
SOP-k	Szabványműveleti eljárások
TSZI-k	Technikai és szervezési intézkedések
Vállalati koncepció	Vállalati adatvédelmi koncepció

1. Bevezetés

(1) Mai világunkban meghatározó szerep jut az adatoknak. Vásárlóink, munkavállalóink és üzleti partnereink szinte minden tranzakció és interakció során megosztják velünk az adataikat. A személyes adat olyan információ, amely lehetővé teszi egy élő személy közvetlen vagy közvetett azonosítását, ami történhet olyan rendelkezésre álló adatok alapján, mint a személy neve, helymeghatározási adatai, egészségügyi adatai, de akár olyan kevésbé nyilvánvaló módon, mint pl. IP-címből.

(2) A személyes adatok élő személyhez kapcsolódnak (az érintett). Az adatvédelmi szabályok biztosítják, hogy megfelelően és jogszerűen használjuk az egyének személyes adatait. Az adatvédelmi jogszabályok rögzítik a személyes adatok kezelésének alapvető elveit és szabályait.

(3) A PHOENIX csoport komolyan veszi a munkavállalói, üzleti partnerei és vásárlói személyes adatainak és magánszférájának a védelmét. Ez az Adatvédelmi szabályzat azt hivatott biztosítani, hogy a személyes adatok kezelése megfeleljen az adatvédelmi jogszabályoknak, és ennek megfelelően tükrözi a GDPR-ben foglalt kötelezettségeket és elveket.

2. Tárgyi hatály

(1) Ez a szabályzat az adatokból azonosítható élő személyek személyes adatainak és személyes adatok különleges kategóriáiba tartozó adatainak a kezelésére vonatkozik. A szabályzat hatálya mind az elektronikusan, mind pedig a nyomtatott formában kezelt, és a megfelelő irattári rendszerben tárolt adatokra kiterjed. Azokban az országokban, ahol a jogi személyek (pl. kft-k) adatait a magánszemélyek adataival azonos védelem illeti meg, ez a szabályzat a jogi személyek adataira is ugyanúgy alkalmazandó.

(2) A szabályzat kiterjed:

a) a PHOENIX csoport minden munkavállalójára;

b) minden PHOENIX társaságra;

c) azon szervezetekre, amelyekkel olyan szerződést kötöttünk, amely szerint a csoport információs javaihoz való hozzáférés a jelen szabályzat érvényre juttatása mellett lehetséges (partnerek közös vállalkozásban, franchise-partnerek stb.);

d) valamennyi, a PHOENIX csoport tulajdonában vagy közvetlen ellenőrzése alatt álló információs javakhoz közvetlenül hozzáférő harmadik fél (pl. külső tanácsadók);

e) valamennyi, a PHOENIX csoport tulajdonában vagy közvetlen ellenőrzése alatt álló információs javakhoz közvetlenül hozzáférő szolgáltató. A fentieknek bizonyítaniuk kell, hogy megfelelő szinten betartják a jelen szabályzatot.

(3) Valamennyi, a PHOENIX csoport tulajdonában vagy közvetlen ellenőrzése alatt álló információs javakhoz közvetlenül hozzáférő szolgáltatót és szerződő felet szerződésben kell kötelezni a jelen szabályzat betartására és a titoktartás vállalására. Az adatfeldolgozónak minősülő szolgáltatókkal adatfeldolgozási szerződést kell aláíratni (lásd a 6. fejezetet).

(4) A PHOENIX társaság a munkavállalói feletti jogkörét gyakorolva a jelen szabályzatot beépíti a munkavállalókra helyben kötelező szabályokba, a helyben alkalmazandó munkajogi szabályoknak megfelelően.

(5) A PHOENIX társaság gondoskodik arról, hogy minden munkavállalója megfelelően elérhesse és megismerhesse ezt a szabályzatot, szükség esetén a helyi nyelven, különösen az intraneten való közzététel útján. Az eredeti angol nyelvű változat tekintendő irányadónak.

(6) A jelen szabályzat bevezetése az egyik olyan tevékenység, amely szükséges a GDPR-nek való megfelelés eléréséhez. A további e körbe tartozó feladatok a 10. fejezetben találhatók.

(7) Elképzelhető, hogy a nemzeti jogszabályok és egyéb előírások szigorúbbak a GDPR-nél és/vagy ennél a szabályzatnál. Minden PHOENIX társaság és munkavállalói kötelesek megfelelni a vonatkozó helyi jogszabályoknak.

(8) Helyi adaptációra lehetőség van, de ez nem eredményezhet a jelen szabályzatban foglaltaknál alacsonyabb szintű adatvédelmet. A jelen szabályzattól vagy a vállalati adatvédelmi sztenderdektől csak kivételes esetben, a PHOENIX csoport (HCDP, PHOENIX csoport Igazgatósága) engedélyével lehet eltérni. Az erre irányuló kérést és a kivétel megadását dokumentálni kell. A kéréshez szükséges mintadokumentumot a vállalati adatvédelmi vezető (HCDP) tudja rendelkezésre bocsátani.

3. Szervezet: Szerepek és feladatkörök az adatvédelem területén

3.1 Igazgatóság (csoportszinten)

(1) A vállalati adatvédelmi vezető (HCDP) támogatja a PHOENIX csoport Igazgatóságát a vállalati adatvédelem megszervezésében, megvalósításában, fenntartásában, felülvizsgálatában és fejlesztésében. Az Igazgatóság meghatározott jelentéseket kér a HCDP-től.

(2) A HCDP feladatainak teljesítését segítendő, az Igazgatóság automatikusan megfelelő módon és időben tájékoztatja a HCDP-t valamennyi, a személyes adatok kezelését érintő nemzetközi ügyről, projektről, változásról vagy műveletről, és adott esetben be is vonja őt a folyamatokba (az információkhoz való passzív hozzáférés joga). Az Igazgatóság támogatja a HCDP-t a feladatai végrehajtásában.

(3) A HCDP-nek olyan erőforrásokkal kell rendelkeznie, hogy az tükrözze az üzleti modell jellegét és komplexitását a csoportban. A HCDP független pozíciót tölt be a szervezetben, és az Igazgatóság tagjának/tagjainak tartozik elszámolással.

3.2 Igazgatótanács (céges szinten)

(1) A PHOENIX Társaság ellenőrzi, hogy a helyi jog szerint kötelező-e adatvédelmi tisztviselőt (DPO-t) kinevezni, és teljesíti a további vonatkozó jogi előírásokat is (pl. tájékoztatja az adatvédelmi hatóságot, közzéteszi a helyi adatvédelmi tisztviselő (DPO) elérhetőségi adatait stb.).

(2) Ha a GDPR vagy a helyi adatvédelmi jogszabályok szerint nem kötelező adatvédelmi tisztviselőt (DPO-t) kinevezni, a PHOENIX társaság kapcsolattartó személyt jelöl ki az adatvédelmet érintő feladatokra és a vállalati szintű adatvédelmi osztállyal való kommunikációra. Belső kommunikációs célokra cégen belül ezt a személyt is adatvédelmi tisztviselőnek (DPO-nak) hívjuk. Az elnevezés (rövidítés) használata ebben az esetben nem jelenti azt, hogy az adott személy a GDPR-nek megfelelően, hivatalosan kinevezett adatvédelmi tisztviselő (DPO) lenne.

(3) A PHOENIX társaság adatvédelmi tisztviselőjeként (DPO-jaként) eljáró harmadik személyt szerződésben kell kötelezni a jelen szabályzat betartására.

(4) Egy adott ország PHOENIX társaságai dönthetnek úgy, hogy ugyanaz a személy képviselje őket a vállalati szintű adatvédelmi osztállyal való kommunikáció során.

(5) A hivatalosan vagy cégen belül kinevezett adatvédelmi tisztviselőnek (DPO-nak) rendelkeznie kell a szükséges szakképesítéssel, és ismernie kell az adatvédelmi jog-szabályokat és gyakorlatokat.

(6) Az adatvédelmi tisztviselő (DPO) feladatainak teljesítését segítendő, a helyi Igazgatótanács automatikusan megfelelő módon és időben tájékoztatja az adatvédelmi tisztviselőt (DPO-t) valamennyi, a személyes adatok védelmére vonatkozó szabályozást érintő ügyről, projektről, változásról vagy műveletről, és adott esetben be is vonja őt a folyamatokba. A helyi Igazgatótanács támogatja az adatvédelmi tisztviselőt (DPO-t) a feladatai ellátásában.

(7) Az adatvédelmi tisztviselőnek (DPO-nak) olyan erőforrásokkal kell rendelkeznie, hogy az tükrözze az üzleti modell jellegét és komplexitását a PHOENIX társaságnál. Az adatvédelmi tisztviselő (DPO) független pozíciót tölt be a PHOENIX társaságnál, és legmagasabb szintű vezetőknek tartozik elszámolással.

(8) Az adatvédelem tekintetében az Igazgatótanács az elszámoltatható szerv, függetlenül attól, hogy maga látja-e el ezt a szerepet a folyamatban. Az Igazgatótanács gondoskodik az adatvédelmi jogszabályok és a jelen szabályzat betartásáról, pl. a megfelelő szervezet-rendszer és eljárások kiépítésével, aminek következtében az ügyvezetésnek rendelkeznie kell a Folyamatgazda szerepének ellátásához szükséges eszközökkel és jogkörrel, és gondoskodik a sikeres megfelelésről.

(9) Minden munkavállaló számára megfelelően biztosítani kell a hatályos adatvédelmi szabály-zatok és folyamatok megismerhetőségét, a munkaköréhez igazodóan. Az adatvédelemmel kapcsolatos szabályzatokat és eljárásokat, valamint feladat- és szerepköröket rendszeresen (kétévente) át kell tekinteni és felül kell vizsgálni; a helyi felülvizsgálatért felelős személy az adatvédelmi tisztviselő (DPO).

3.3 Munkavállalók

(1) Minden munkavállaló titoktartásra köteles a PHOENIX társaság által kezelt személyes adatok tekintetében. Ezt a kötelezettséget bele kell foglalni a munkaszerződésbe és/vagy a felvételkor átadott dokumentációba.

(2) A PHOENIX csoport minden munkavállalójának kötelező (online és/vagy személyes) adatvédelmi képzést végezni, a munkaköréhez és felelősségi köréhez igazodóan. A képzési terv a bevezetendő tevékenységek körébe tartozik (lásd a 10. fejezetben).

(3) Minden munkavállaló támogatja a DPO-t és a HCDP-t a feladatai ellátásában, például azzal, hogy kérésre hozzáférést biztosít számukra a személyes adatokhoz (érintetti megkeresés esetén) és az adatkezelési műveletekhez, információkat szolgáltat vagy dokumentumokat ad át.

(4) Minden munkavállaló az ügy korai szakaszában bevonja a DPO-t/HCDP-t minden olyan ügybe, amely érinti a személyes adatok védelmét.

(5) Minden munkavállaló követi és betartja az adatvédelmi elveket az adatkezelés során (lásd a 4. fejezet).

(6) Minden munkavállaló jelenti az adatvédelmi incidenseket cégen belül (lásd a 9. fejezetben).

3.4 Folyamatgazda

(1) Folyamatgazdának a PHOENIX társaság azon munkavállalója tekintendő, aki konceptuálisan felel egy személyes adatok kezelésével járó üzleti folyamatért vagy belső folyamatért.

(2) A folyamatgazda felel az úgynevezett adatkezelési tevékenységért. Az adatkezelési tevékenység olyan műveletsor, mint például egy konkrét üzleti folyamat, vagy egy informatikai eszköz.

(3) A folyamatgazda nevesítve vagy pozíciója szerint szerepel az adatkezelési tevékenységekről felvett nyilvántartásban (lásd az 5. fejezetben).

(4) A folyamatgazda az adatkezelési tevékenység megtervezésekor, bevezetésekor és későbbi módosításakor a következő szabályok szerint jár el:

a) bevonja a DPO-t a privacy-hatásvizsgálatba (előzetes hatásvizsgálatba);
b) adatvédelmi hatásvizsgálatot végez, ha az kötelező (lásd az 5. fejezetben);
c) elkészíti és karbantartja az adatkezelési tevékenységről szóló nyilvántartást (lásd az 5. fejezetben);
d) biztosítja az érintettek adatkezelésre vonatkozó tájékoztatását;
e) az adatkezelés során gondoskodik az adatvédelmi elvek betartásáról (a megfelelő osztályok bevonása útján);
f) felülvizsgálja a külső szolgáltatót; ha a szolgáltatók adatokat kezelnek a PHOENIX társaság részére a társaság nevében és utasításainak megfelelően, gondoskodik az adatfeldolgozási szerződések megkötéséről;
g) gondoskodik az érintettek jogainak érvényesüléséről;
h) gondoskodik a hozzáférési jogok és adatmegőrzési idők meghatározásáról és alkalmazásáról.
i) EU-n/EGT-n kívüli országba történő adattovábbítás esetén bevonja az adatvédelmi tisztviselőt (DPO-t), és betartja az EU-n/EGT-n kívüli országba történő adattovábbításra vonatkozó speciális rendelkezéseket;
j) minden dokumentációt úgy készít el, hogy igazolható legyen az adatvédelmi szabályok betartása.

(5) Az adatkezelési tevékenység technikai támogatása átadható külső szolgáltatónak (lásd a 6. fejezetben) vagy az IT-osztálynak, de a fenti szabályok betartásáért való felelősség ebben az esetben is a folyamatgazdánál marad. Az adatvédelmi tisztviselő (DPO) segíti és tanácsokkal látja el a folyamatgazdát.

(6) A PHOENIX társaság saját megfelelő adatvédelmi rendszert alakíthat ki, a hozzá tartozó terminusokkal, szerepekkel és feladatkörökkel. A folyamatgazda szerepét az így meghatározott szervezet látja el.

3.5 Adatvédelmi tisztviselő (DPO)

(1) A DPO fő feladata az érintettek magánszférájának védelme a társaság szintjén/országosan végzett személyesadat-kezelési műveletek során (vásárlók, betegek, munkavállalók stb. adatai). A DPO a hivatalos kapcsolattartó az érintettek és a felügyeleti hatóság felé.

(2) A DPO felel a szervezet és a munkavállalók számára biztosított adatvédelmi tanácsadásért. A DPO felel az adatvédelmi jog betartásának ellenőrzéséért. A DPO határozza meg a helyi koncepció tartalmát (részletesen lásd a 10. fejezetben).

(3) A DPO fő feladatkörei:
- tájékoztatás: kampányok és képzési programok;
- a helyi adatvédelmi szabályzat, valamint a kapcsolódó szabályzatok és utasítások karbantartása;
- az országban használt mintadokumentumok (adatfeldolgozási szerződés, adatvédelmi tájékoztató, beleegyező nyilatkozat stb.) karbantartása;
- támogatás nyújtása az adatfeldolgozási szerződés megkötésére irányuló tárgyalások során: az alapvető adatfeldolgozási szerződések és uniós modellként szolgáló szerződéses klauzulák áttekintése; a DPO mint a jogi és/vagy a beszerzési osztály támogatója,
- új helyi projektek előzetes értékelése: az adatvédelmi előírások és ajánlások meghatározása;
- segítségnyújtás az adatvédelmi hatásvizsgálatok elvégzéséhez;
- segítségnyújtás az adatvédelmi tevékenységek nyilvántartásának létrehozásához és karbantartásához;
- koordináció az érintettek jogainak gyakorlása terén: belső folyamatok fenntartása az érintettek jogainak gyakorlása terén;
- támogatás az adatvédelmi incidensek és jogsértések kezeléséhez: koordináció és segítségnyújtás a felügyeleti hatóságnak/érintetteknek szóló tájékoztatáshoz
- Irányítás és konzultáció: az adatvédelmi szabályozásnak való megfelelés folyamatos monitorozása

(4) A DPO tájékoztatja a HCDP-t a PHOENIX társaságnál felmerülő adatvédelmi ügyekről és nagyobb kapcsolódó projektekről. A DPO évente vagy kérésre soron kívül is jelentést tesz a HCDP-nek az ún. országjelentések felhasználásával.

3.6 Vállalati szintű adatvédelem

(1) A vállalati szintű adatvédelmi osztály fő feladata a PHOENIX csoport és az adatvédelmi tisztviselők (DPO-k) támogatása az adatvédelmi feladataikban.

(2) A vállalati adatvédelmi vezető (HCDP) a DPO-éhoz hasonló feladatokat lát el, csak nemzetközi kontextusban. A HCDP tanácsokkal segíti és monitorozza az adatvédelmi jognak való megfelelést a csoportban; a HCDP koordinálja és támogatja az adatvédelem terén megvalósuló nemzetközi koordinációt.

(3) A HCDP határozza meg a vállalati koncepció tartalmát (részletesen lásd a 10. fejezetben).

(4) A HCDP fő feladatai:
- tájékoztatás: kampányok és képzési programok (ideértve a PHOENIX csoportban tartott online képzéseket is);
- a csoportszintű adatvédelmi szabályzat fenntartása;
- a vállalati szintű adatvédelmi sztenderdek létrehozása;
- támogatás nyújtása a fő nemzetközi adatfeldolgozási szerződések megkötésére irányuló tárgyalások során;
- új helyi/nemzetközi projektek előzetes értékelése: az adatvédelmi előírások és ajánlások meghatározása;
- segítségnyújtás az adatvédelmi hatásvizsgálatok elvégzéséhez a csoport szintjén (vállalati mintadokumentumok a helyi DPO-k számára);

- csoportszintű rendszer fenntartása az adatvédelmi incidensek jelentésére: ő a jelentéstételi platform adminja.
- Az adatvédelmi incidensek kezelésének irányítása: koordináció és segítségnyújtás a felügyeleti hatóságnak/érintetteknek szóló tájékoztatáshoz; nemzetközi szempontok felmerülése esetén;
- konzultáció és folyamatos monitorozás az adatvédelmi szabályozásnak való megfelelés terén.

(5) A vállalati adatvédelmi csapat tagja(i) konkrét területeken támogatja/támogatják a HCDP-t a tevékenységei ellátásában a helyi vagy nemzetközi színtéren. A vállalati adatvédelmi csapat tagja a HCDP utasításai szerint jár el, és közvetlenül a HCDP alá van rendelve.

3.7 Információbiztonság

(1) Az információbiztonsági igazgató (CISO) felel az információbiztonsági sztenderdek biztosításáért és alkalmazásáért a PHOENIX csoportban. Ennek érdekében a CISO megfelelő biztonsági szabályzatokat, irányelveket, sztenderdeket hoz létre, és meghatározza a PHOENIX csoport biztonsági koncepciójának tartalmát.

(2) A CISO és a helyi biztonsági koordinátor (LSC) felel a személyes adatok védelmét szolgáló technikai és szervezési intézkedések (TSZI-k) bevezetéséért és dokumentálásáért. A TSZI-k dokumentációja segítségével dokumentálható a GDPR biztonsági elvének való megfelelés (lásd a 4. fejezetben).

(3) A CISO és a HCDP, illetve helyi szinten az LSC és a DPO szorosan együttműködik és kommunikál egymással a TSZI-k tárgyában. A HCDP/DPO listát készít a TSZI-kre vonatkozó főbb előírásokról.

(4) Az LSC támogatja a DPO-t a szolgáltatók felülvizsgálatában. Az LSC ellenőrzi az adatfeldolgozónak minősülő szolgáltatóknál bevezetett TSZI-ket (lásd a 6. fejezetben).

4. A személyes adatok kezelésének jogszabályi keretei

(1) Az alábbi listában a GDPR 5. cikkében található modell alapján összegeztük az általánosan elfogadott adatvédelmi elveket.

(2) Minden munkavállaló köteles követni és betartani az adatvédelmi elveket az adatkezelés során. Minden munkavállaló köteles a PHOENIX csoportban és/vagy a PHOENIX társaságban betöltött szerepének és feladatkörének megfelelően követni az adatvédelmi előírásokat.

1. elv: Jogszerűség, tisztességes eljárás és átláthatóság

(1) Az adatkezelésnek tisztességesnek kell lennie, vagyis nem kerülhet sor kiszámíthatatlan vagy félrevezető adatkezelésre. Az érintettet tájékoztatni kell a személyes adatai kezelésével kapcsolatos fontos részletekről.

(2) Személyes adatok csak akkor kezelhetők, ha az adatkezelésnek megvan a jogalapja. Az adatkezelés hatféle jogalapra alapozható:

(a) **Hozzájárulás:** az egyén egyértelműen hozzájárult a személyes adatok konkrét céllal való kezeléséhez.

(b) **Szerződés:** az adatkezelés a PHOENIX társaság és az egyén között létrejött szerződés miatt, vagy a szerződés megkötését megelőző konkrét lépések megtételéhez szükséges.

(c) **Jogi kötelezettség**: az adatkezelés a jogszabályoknak való megfeleléshez szükséges (a szerződéses kötelezettségek nem ide tartoznak).
(d) **Létfontosságú érdekek**: az adatkezelés valaki életének a védelme érdekében szükséges.
(e) **Közfeladat**: az adatkezelés közérdekű feladat ellátásához vagy közhatalmi jogosítvány gyakorlásához szükséges, és a feladat vagy jogosítvány jogalapja egyértelmű.
(f) **Jogos érdekek**: az adatkezelés a PHOENIX társaság jogos érdekei vagy egy harmadik fél jogos érdekei miatt szükséges, kivéve, ha olyan alapos ok van az érintett személyes adatainak védelmére, amely ok elsőbbséget élvez a fenti jogos érdekekkel szemben.

(3) Nem áll fenn a jogalap, ha ugyanaz a cél a személyes adatok kezelése nélkül is elérhető. A jogalapot az adatkezelés megkezdése előtt meg kell határozni, és dokumentálni is kell az adatvédelmi tevékenységekről felvett nyilvántartásban (lásd az 5. fejezetben).

(4) Egyik jogalap sem fontosabb a másiknál – hogy melyik jogalap a legmegfelelőbb, az a cél(ok)tól és az érintettel fennálló kapcsolattól függ.

A hozzájárulásra vonatkozó speciális szabályok

(1) A hozzájárulás nem eredendően jobb vagy fontosabb a fenti alternatíváknál. A hozzájárulás az egyénnek biztosított tényleges választási lehetőségen és az ellenőrzés lehetőségén alapul.

(2) A hozzájárulásnak önkéntesnek kell lennie. A hozzájárulásnak egyértelműnek kell lennie, és pozitív választásban kell kifejeződnie. A hozzájárulás megadására határidő nincs, és a megadott hozzájárulás érvényességi ideje az adatkezelés körülményeitől függ.

Speciális szabályok az adatvédelmi jogszabályok (GDPR) szerint különleges kategóriába tartozó adatokra vonatkozóan

(1) A GDPR a következőképpen definiálja a különleges kategóriába tartozó adatokat:
- faji vagy etnikai származásra utaló személyes adatok;
- politikai véleményre utaló adatok;
- vallási vagy világnézeti meggyőződésre utaló adatok;
- szakszervezeti tagságra utaló adatok;
- genetikai adatok;
- biometrikus adatok (ha egyedi azonosításra használják őket);
- egészségügyi adatok;
- egy személy szexuális életére vonatkozó adatok;
- egy személy szexuális irányultságára vonatkozó adatok.

(2) A személyes adatok különleges kategóriáinak kezelésére szigorúbb szabályok vonatkoznak. A jogalap igazolásán túl a GDPR 9. cikkében foglalt külön feltételek egyikének is teljesülnie kell:
(a) kifejezett hozzájárulás;
(b) munkajogi, társadalombiztonsági és szociális védelem (ha jogilag megengedett);
(c) létfontosságú érdekek;
(d) nonprofit szervezetek;
(e) az érintett által nyilvánosságra hozott adatok;
(f) jogi igények vagy igazságszolgáltatási jogkörben eljáró bíróságok;

(g) jelentős közérdek (jogszabály alapján);
(h) egészségügyi vagy szociális ellátás (jogszabály alapján);
(i) közegészségügy (jogszabály alapján);
(j) archiválás, kutatás, statisztika (jogszabály alapján).

(3) Az adatvédelmi tisztviselőt (DPO-t) minden különlegesadat-kategóriát érintő tervezési folyamatba vagy projektbe be kell vonni.

A jogszerűséghez, tisztességességhez és átláthatósághoz kapcsolódó adatvédelmi követelmények
– Az adatkezelési tevékenység megkezdése előtt világosan határozza meg a jogalapot. – Gondoskodjon arról, hogy az adatkezelési tevékenység ne léphesse túl a fentiek szerint meghatározott jogalap által biztosított kereteket. – Egyeztessen a jogalapról a DPO-val, és a helyi szabályoknak megfelelően dokumentálja a jogalapot. – Vonja be a DPO-t, ha különleges kategóriába eső adatok is kezelendők. – Gondoskodjon a folyamatok, a célok és a jogalap teljeskörű dokumentálásáról. – Tájékoztassa az érintetteket az adatkezelésről, pl. annak céljáról és az adatkezelő kilétéről az adatkezelési tájékoztatóban; világosan kommunikálja az érintettek felé, hogy hogyan, milyen mértékben és milyen célokból kezeljük a személyes adataikat. – Tartsa tiszteletben az érintettek hozzáféréshez és helyesbítéshez való jogát. – Olyan eljárásokat és utasításokat kell kidolgozni, amelyek világosan meghatározzák, hogy az érintettek miként gyakorolhatják az adataikhoz való hozzáférésre és az adataik helyesbítésére vonatkozó jogaikat az adatkezelés egyes szakaszaiban. – Olyan funkciókat kell beépíteni a rendszerbe, amelyek lehetővé teszik a hozzáférési, helyesbítési és tiltó megkeresések, valamint az adatkezeléssel szembeni tiltakozások kezelését. – Belső szabályokat kell kialakítani, amelyek szerint változások, például a hozzájárulás visszavonása esetén felülvizsgálható a jogalap érvényessége.

A hozzájárulással kapcsolatos követelmények

- A hozzájárulásnak konkrétan tartalmaznia kell az adatkezelő nevét (PHOENIX társaság), az adatkezelés céljait és az adatkezelési tevékenységek típusait.
- Kifejezett hozzájárulást kell adni, szóban megerősítve – önmagában semmilyen pozitív cselekvés nem elegendő. Az általános vagy meghatározatlan tartalmú hozzájárulás nem elegendő.
- A hozzájárulásnak pozitív választásban kell kifejeződnie. Ne használjon előre bepipált jelölőnégyzeteket vagy más olyan módszert, amely alapbeállításként kezeli a hozzájárulás megadását.
- A hozzájárulás-kéréseket különítse el az egyéb szerződéses feltételektől (a hozzájárulás kérését kiemelten, az egyéb feltételektől elkülönítve kell elhelyezni, tömören és könnyen érthetően kell megfogalmazni, és felhasználóbarát módon kell megjeleníteni).
- Ne tegye egy szolgáltatás előfeltételévé az adatkezelési hozzájárulás megadását.
- Biztosítsa, hogy a hozzájárulás egyszerűen visszavonható legyen, és kommunikálja a visszavonás módját.
- Tartsa meg a megadott hozzájárulást bizonyítási célra, annak rögzítésével, hogy ki, mikor, hogyan és mit mondott el az érintetteknek.

2. elv: Célhoz kötöttség

(1) A személyes adatokat csak meghatározott, egyértelmű és jogszerű célból lehet gyűjteni, és nem szabad az eredeti célokkal összeegyeztethetetlen módon tovább kezelni őket.

(2) Ha az új cél összeegyeztethető, a további adatkezeléshez új jogalap nem szükséges.

(3) Ha az új cél nagyon eltér az eredeti céltól, váratlan lenne, vagy az egyénre nézve indokolatlan hatással járna, akkor az valószínűleg összeegyeztethetetlen az eredeti céllal.

A célhoz kötöttséghez kapcsolódó adatvédelmi követelmények

- Csak meghatározott, egyértelmű, jogszerű és korlátozott céllal kezeljen személyes adatokat.
- Az informatikai rendszerben történő adatkezelést korlátozza az eredetileg meghatározott célra.
- Különböző típusú adatok gyűjtése és különböző céllal való adatkezelés esetében gondoskodjon a célhoz kötöttség érvényesítéséről.
- Vezessen be belső szabályokat az összeegyeztethetőségi igények eseti értékelésére, hogy lehetővé váljon a cél módosítása.
- A GDPR 30. cikke szerinti adatkezelési nyilvántartási (dokumentációs) kötelezettség részeként vezetendő dokumentációban rögzítse a személyes adatok kezelésének célját vagy céljait.
- Világosan kommunikálja az érintettek felé, ha az adatkezelés eredetileg meghatározott célja megváltozott.

3. elv: Adattakarékosság

(1) A személyes adatoknak az adatkezelés céljai szempontjából megfelelőeknek és relevánsaknak kell lenniük, és a szükségesre kell korlátozódniuk.

(2) A személyes adatokat törölni kell, ha már nincs szükség rájuk.

Az adattakarékossághoz kapcsolódó adatvédelmi követelmények
– Határozza meg, hogy mennyi az a minimálisan szükséges személyes adat, amelyre a cél megvalósulása érdekében szükség van, és csak ennyi adatot tároljon. – Rendszeresen tekintse át, hogy a személyes adatok továbbra is relevánsak és a céloknak megfelelőek-e, és törölje azt, amire már nincs szükség. – Fontolja meg fokozott adatvédelmet biztosító speciális technológiák használatát, amelyek segítségével elkerülhető a személyes adatok túlzott használata vagy lehetővé válik az adatok anonimizált használata, és ha lehetséges, használjon ilyen technológiákat. – Gondoskodjon arról, hogy a személyes adatok megfelelőek, relevánsak legyenek, és mennyiségük ne legyen túlzott a célhoz viszonyítva.

4. elv: Pontosság

(1) A személyes adatoknak pontosaknak kell lenniük, és szükség esetén frissíteni kell őket.

(2) Minden észszerű intézkedést meg kell tenni annak érdekében, hogy a pontatlanként azonosított személyes adatok – tekintettel az adatkezelés céljára – haladéktalanul törlésre vagy helyesbítésre kerüljenek.

A pontossághoz kapcsolódó adatvédelmi követelmények
– Gondoskodjon arról, hogy a személyes adatok pontosak és naprakészek legyenek. – Vezessen be olyan folyamatokat, amelyekkel biztosítható és fenntartható a kezelt adatok pontossága, pl. a rendszerbe táplált adatok minőségének automatikus ellenőrzése az adatkezelést megelőzően. – Gondoskodjon arról, hogy az érintett helyesbíthesse az aktualitásukat vesztő adatokat.

5. elv: Korlátozott tárolhatóság

(1) A személyes adatokat olyan formában kell tárolni, hogy az érintettek legfeljebb addig legyenek azonosíthatók, amíg erre az adatgyűjtés célja szerint szükség van.

(2) A Folyamatgazda meghatározza az adatmegőrzési/törlési időt, amelyet rögzít a PHOENIX társaság adatmegőrzési szabályzatában.

(3) Minden PHOENIX társaságnak legyen adatmegőrzési/törlési szabályzata.

A korlátozott tárolhatósághoz kapcsolódó adatvédelmi követelmények
– A személyes adatokat legfeljebb addig tartsa meg, amíg erre az eredetileg meghatározott cél szerint szükség van. – Az érintettek személyének azonosítását lehetővé tevő formában tárolt személyes adatok esetében előre határozza meg az adatmegőrzési időt. – Gondoskodjon arról, hogy az előírt adatmegőrzési idők arányban álljanak az adatgyűjtés céljával, és korlátozottak legyenek. – A különböző célokra gyűjtött adatokhoz elkülönítve rendelje hozzá és kezelje az adatmegőrzési időt. – Külön figyelmet kell fordítani a papíralapon tárolt személyes adatokra, mert ezek megléte nehezen követhető nyomon. – Alakítson ki rendszerfunkciókat a megőrzési idő kezelésére és a további szükséges lépések, vagyis a törlés vagy anonimizálás elvégzésére.

6. elv: Biztonság (integritás és bizalmas jelleg)

(1) A PHOENIX társaság megfelelő technikai és szervezési intézkedéseket (TSZI-ket) tesz annak érdekében, hogy a személyes adatokat a felmerülő adatvédelmi kockázatoknak megfelelő módon tudja védeni.

Az érintettel kapcsolatos adatvédelmi kockázat különösen az alábbiak miatt merülhet fel:
- személyes adatok véletlen megsemmisítése és/vagy
- személyes adatok elvesztése és/vagy
- személyes adatok véletlen megváltoztatása és/vagy
- személyes adatok jogosulatlan közlése és/vagy
- személyes adatokhoz való jogosulatlan hozzáférés.

(2) A megfelelő TSZI-k értékelése során az alábbiakat kell figyelembe venni:
- a tudomány és technológia állását; és
- a megvalósítás költségeit; és
- az adatkezelés jellegét, hatókörét, körülményeit és céljait; és
- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatot (azaz pl. a vásárlók vagy munkavállalók magánszféráját érintő kockázatot).

(3) A TSZI-knek biztosítaniuk kell a PHOENIX rendszereinek és szolgáltatásainak, valamint a használatuk során kezelt személyes adatoknak a „bizalmas jellegét, integritását és hozzáférhetőségét.

A biztonsághoz kapcsolódó adatvédelmi követelmények (integritás és bizalmas jelleg)

- Követni kell az információbiztonsági szabályzatokban, irányelvekben, sztenderdekben és tájékoztató anyagokban foglaltalkat.
- Amennyiben a csoportszintű vagy a helyi szabályzat kötelezővé teszi ezt, be kell vonni az adatkezelési tevékenységbe a helyi biztonsági koordinátorokat (LSC-ket) vagy az információbiztonsági igazgatót (CISO).
- Az adatkezelési tevékenység tervezésekor figyelembe kell venni pl. a kockázat-értékelést, a szervezeti szabályzatokat vagy a technikai intézkedéseket.
- A kockázatértékelés alapján olyan szervezési és technikai intézkedéseket kell kialakítani és bevezetni, amelyek segítségével a kockázatok az elfogadható szintre csökkenthetők.
- Az olyan adatkezelési tevékenységeket, amelyeknél a kockázat enyhítése nem eredményes, mellőzni kell.
- Biztosítsa, hogy a felelős vezetők világos döntést hozzanak arról, hogy mely kockázatokat fogadják el, és miért.
- Ahol van rá mód, álnevesítést és titkosítást kell használni.

Az információbiztonsághoz kapcsolódó adatvédelmi követelmények

Bizalmas jelleg:
A személyes adatokat védeni kell a jogosulatlan vagy véletlen közléssel szemben. Mind a belső, mind a külső támadókkal (pl. hackerek, frusztrált vagy kíváncsi munkavállalók), mind pedig a gondatlanságból adódó vagy strukturális fenyegetésekkel (pl. képzelten munkavállalók, szerepkörtől függő jogosultságok rendszere) számolni kell.

Integritás:
A személyes adatokat hiánytalanul és helyesen kell megadni. Az adatok jogosulatlan megváltoztatását azonosítani kell (pl. naplózás/naplófájlok segítségével), és biztosítani kell az adatok javítására szolgáló eljárásokat.

Hozzáférhetőség:
A személyes adatoknak szükség esetén hozzáférhetőknek kell lenniük. Ez azt is jelenti, hogy elvesztés vagy megsemmisítés esetére biztosítani kell a helyreállíthatóságot (pl. biztonsági mentések révén).

Be kell vezetni egy eljárást a TSZI-k eredményességének rendszeres felülvizsgálatára, felmérésére és értékelésére (pl. behatolástesztelés, külső és belső értékelések).

7. elv: Elszámoltathatóság

(1) A PHOENIX társaság felelőssége, hogy képes legyen bizonyítani a GDPR fent felsorolt elveinek való megfelelését.

(2) A bizonyítás minden érintett munkavállaló számára alapvető feladat. Az elszámoltathatósági mechanizmusok fenntartását dokumentálni kell. Ez a dokumentáció felhasználható az elszámoltathatóság, a felelősségvállalás és a GDPR-nek való megfelelés bizonyítására.

(3) A PHOENIX társaság köteles hiánytalan nyilvántartást vezetni az adatkezelési tevékenységekről. Minden munkavállaló, főleg a folyamatgazdák előzetesen (a tervek megvalósítása előtt) tájékoztassák az adatvédelmi tisztviselőt (DPO-t) az új vagy módosított adatkezelési tevékenységekről (lásd az 5. fejezetet).

Az elszámoltathatósághoz kapcsolódó adatvédelmi követelmények
– Gondoskodjon arról, hogy a fenti elveknek való megfelelés a megfelelő dokumentáció révén bizonyítható legyen. – Előzetesen tájékoztassa a DPO-t az új vagy módosított adatkezelési tevékenységről, elegendő időt hagyva neki az adatkezelési tevékenység értékelésére.

5. Új vagy módosított adatkezelési tevékenység

5.1 Sztenderd megközelítés

(1) Minden új adatkezelési tevékenység esetén előzetesen be kell vonni a DPO-t. A folyamatgazda vagy projektmenedzser felel azért, hogy megfelelő módon megtörténjen az egyeztetés a DPO-val.

(2) A DPO ellenőrzi az adatkezelés jogalapját. A DPO felsorolja a főbb adatvédelmi követelményeket a privacy-hatáselemzésben (PIA). A PIA tartalma az adott adatkezelési tevékenységtől függ. A DPO tájékoztat arról, hogy kötelező-e adatvédelmi hatásvizsgálatot (DPIA-t) végezni (lásd az 5.2. pontban).

(3) Ha az adatvédelmi tevékenység vagy a projekt nemzetközi, a vállalati adatvédelmi vezetőt (HCDP-t) is be kell vonni. A HCDP elvégzi a vállalati PIA-t/DPIA-t, ami a helyi PIA/DPIA mintája lesz; a helyi DPO helyi szinten áttekinti a helyi adatvédelmi követelményeket. A HCDP a szolgáltatókat is felülvizsgálja, és/vagy más dokumentációt/mintadokumentumokat (pl. adatvédelmi tájékoztatót) is készít. A HCDP minden nemzetközi adatkezelési tevékenységről előzetesen tájékoztatja a DPO-kat.

(4) A PIA eredménye megfelelő adatokat tartalmaz az adatvédelmi tevékenységek nyilvántartásához. A nyilvántartás kötelező elemeit a GDPR 30. cikke tartalmazza. A nyilvántartás vezetéséért a folyamatgazda felel. Az adatkezelési tevékenységek nyilvántartási folyamatáért az adatvédelmi tisztviselő (DPO) felel.

5.2 Adatvédelmi hatásvizsgálat (DPIA)

(1) Az adatvédelmi hatásvizsgálat (DPIA) elvégzéséért a folyamatgazda felel. Az adatvédelmi hatásvizsgálatba (DPIA-ba) be kell vonni az adatvédelmi tisztviselőt (DPO-t) és a helyi biztonsági koordinátort (LSC-t) (és/vagy nemzetközi projekteknél a vállalati adatvédelmi vezetőt (HCDP-t)/vállalati információbiztonsági igazgatót (CISO)), valamint a további érdekelt feleket (pl. üzemi tanács, informatikai rendszertervező(k), jogi osztály stb.).

(2) Az adatvédelmi hatásvizsgálat (DPIA) folyamatának célja az adatkezelési tevékenység (pl. egy projekt) adatvédelmi kockázatainak azonosítása és minimalizálása. Az adatvédelmi hatásvizsgálat (DPIA) a GDPR szerint azon adatkezelési műveletek esetében kötelező, amelyek valószínűsíthetően magas kockázatot jelentenek természetes személyekre nézve. Ide tartozik néhány konkrét adatkezelési típus, de más nagyobb, személyesadat-kezeléssel járó projektek esetén is helyes gyakorlat a DPIA elvégzése. DPIA-ra van szükség a következő helyzetekben:

- új technológiák bevezetése;
- automatizált adatkezelés, ideértve a profilalkotást, amely magánszemélyekre nézve jogi hatást keletkeztető döntésekkel zárul;
- különleges kategóriába tartozó adatok nagy számban történő kezelése;
- bűncselekményekkel kapcsolatos adatok kezelése;
- nyilvánosan hozzáférhető adatok szisztematikus, nagy számban történő monitorozása stb.

(3) A DPIA-ban kötelező:

- jellemezni az adatkezelés jellegét, hatókörét, körülményeit és céljait; és
- értékelni a szükségességet, arányosságot és a jogszabályi megfelelést biztosító intézkedéseket; és
- azonosítani és felmérni a magánszemélyekre vonatkozóan fennálló kockázatokat; és
- azonosítani a fenti kockázatok enyhítését célzó további intézkedéseket.

A kockázat szintjének megítélésekor a PHOENIX társaságnak mind a valószínűség, mind pedig a súlyosság szempontjából mérlegelnie kell a magánszemélyekre gyakorolt hatásokat. A kockázat magas lehet akkor is, ha bármilyen sérelem nagy valószínűséggel fordulhat elő, és akkor is, ha – ugyan kisebb valószínűséggel – de súlyos sérelemre lehet számítani.

(4) Amennyiben adott körülmények között a DPIA arra utal, hogy az adatkezelés nagy kockázatot jelent az érintettek jogaira és szabadságaira, ha az adatkezelő nem vezet be a kockázat enyhítését célzó intézkedéseket, a DPO egyeztet a helyi felügyeleti hatósággal.

6. Szolgáltatókkal fennálló szerződések

6.1 Az adatfeldolgozó bevonására vonatkozó szabályok

(1) A szolgáltató akkor minősül adatfeldolgozónak, ha a PHOENIX társaság nevében, és kizárólag annak utasításai szerint jár el.

(2) Ha a PHOENIX társaság úgy határoz, hogy igénybe veszi egy adatfeldolgozó adatkezeléssel kapcsolatos szolgáltatásait, adatfeldolgozási szerződést kell kötnie vele. Cégcsoporton belüli adatfeldolgozás esetén külön DPA mintadokumentum és eljárás alkalmazandó.

(3) Ha az adatfeldolgozó DPA-ja eltér a helyi vagy vállalati szintű DPA mintadokumentumtól, a végleges verziót jóvá kell hagyatni az adatvédelmi tisztviselővel (DPA-val) vagy a jogi osztállyal. A felülvizsgálatot a folyamatgazdának kell elindítania.

(4) A DPA-tárgyalások szerves részét képezi a szolgáltató/adatfeldolgozó TSZI-inek felülvizsgálata. A felülvizsgálat során ellenőrizni kell a szolgáltató TSZI-it, hogy meggyőződhessünk azok GDPR-nek való megfeleléséről, különösen az adatbiztonság terén

(GDPR 32. cikk). Ezt az ellenőrzés az adatvédelmi tisztviselő (DPO) koordinálja, a helyi biztonsági koordinátor (LSC) támogatásával.

(5) A DPA-t írásban kell lebonyolítani, és dokumentálni kell.

(6) Az adatfeldolgozónak minősülő szolgáltatóknál rendszeres auditot kell végezni. A szolgáltató adatvédelmi auditálásának tervezésekor (így az auditálandó időszak meghatározásakor is) mérlegelni kell az adatkezelési tevékenységhez kapcsolódó adatvédelmi kockázatokat. Az auditálandó időszak legalább 24 hónap legyen. Az adatvédelmi tisztviselő (DPO) és a helyi biztonsági koordinátor (LSC) az audit elvégzése során támogatja a folyamatgazdát. Az adatvédelmi audit tervezése a bevezetési tevékenységek körébe tartozik (lásd a 10. fejezetben).

6.2 Az EU-n kívülre történő adattovábbítás szabályai

(1) A GDPR korlátozza a személyes adatok EU-n/EGT-n kívülre történő továbbítását, kivéve, ha az érintettek jogainak védelme más módon biztosítva van, vagy ha a GDPR-ben meghatározott, korlátozott számú kivételek valamelyike merül fel.

(2) A PHOENIX társaságnak mindig a teljes beszállítói láncot ismernie kell (mely társaság / mely ország / mely szolgáltatás /mely adatkategória). A PHOENIX társaságnak a teljes adatfeldolgozói láncban garantálnia kell az adatvédelem GDPR-nek megfelelő szintjét.

(3) A nem EU/EGT országban/szolgáltatónál a védelem megfelelő szintjét bizonyos, a GDPR-ben előre meghatározott garanciákkal lehet biztosítani (pl.):
- bizottsági megfelelőségi nyilatkozat;
- kötelező erejű vállalati szabályok;
- az EU általános adatvédelmi kikötései stb.

(4) A garancia típusát a szolgáltatók kiválasztási kritériumai közé kell sorolni. A bizottsági megfelelőségi nyilatkozat megbízható garanciának számít, de megjegyzendő, hogy az egyes megfelelőségi nyilatkozatok tárgyi hatálya országonként eltérő lehet. A kötelező erejű vállalati szabályok szintén erős garanciának tekinthetők.

(5) Minden EU-n/EGT-n kívülre történő adattovábbítás/adatfeldolgozás esetén előzetesen be kell vonni az adatvédelmi tisztviselőt (DPO-t).

(6) A PHOENIX társaság minden EU-n/EGT-n kívülre történő adattovábbításról nyilvántartást vezet.

6.3 Egyéb szolgáltatókra vonatkozó szabályok

Valamennyi, a PHOENIX csoport tulajdonában vagy közvetlen ellenőrzése alatt álló, személyes adatot tartalmazó információs javakhoz közvetlenül hozzáférő szolgáltatót és szerződő felet szerződésben kell kötelezni a jelen szabályzat betartására és a titoktartás vállalására.

7. Az érintettek jogainak érvényesítése

(1) A GDPR az alábbi jogokat biztosítja a természetes személyeknek:

a) **tájékoztatáshoz való jog**
Az érintettet az adatfelvétel időpontjában vagy az első lehetséges időpontban el kell látni a vonatkozó információkkal.

b) **hozzáféréshez való jog**
Az érintett jogosult megerősítést kérni arra vonatkozóan., hogy kezelünk-e rá vonatkozó adatokat, és ha igen, ezekre az adatokra vonatkozóan is tájékoztatást kérhet a GDPR 15. cikke szerint.

c) **helyesbítéshez való jog**
Az érintett kérheti a rá vonatkozó pontatlan adatok kiegészítését vagy kijavítását.

d) **törléshez való jog**
Az érintett kérheti a személyes adatai törlését, ha nincs olyan jogi kötelezettség, amely szerint meg kellene őrizni azokat.

e) **adatkezelés korlátozásához való jog**
Az érintett kérheti az adatkezelés korlátozását a GDPR 18. cikke szerint.

f) **adathordozhatósághoz való jog**
Az érintett jogosult arra, hogy másolatot kérjen a PHOENIX társaság által róla tárolt személyes adatokról, ahogy kérheti azok más adatkezelő számára történő továbbítását is.

d) **tiltakozáshoz való jog**
Az érintettnek bármikor joga van tiltakozni a személyes adatai kezelésével szemben, különösen, ha direktmarketing, profilalkotás vagy kutatás céljára használjuk azokat.

(2) A PHOENIX társaság köteles megfelelő technikai és/vagy szervezési intézkedésekkel biztosítani, hogy a vállalat lehetővé tegye az érintettek jogainak érvényesítését. Az intézkedéseket dokumentálni kell.

Példa: Az informatikai rendszereket úgy kell kiválasztani és kialakítani, hogy az egy érintetthez kapcsolódó adatokat ki lehessen nyomtatni, így érvényesíthető legyen a hozzáféréshez való jog, vagy olyan eljárást kell alkalmazni, amelynek segítségével manuálisan kiszedhetők a rendszerből az egy személyre vonatkozó adatok.

(3) Ha egy érintett a PHOENIX társasághoz fordulva érvényesíteni kívánja valamely érintetti jogát, az adott munkavállaló haladéktalanul továbbítja a kérését az adatvédelmi tisztviselőnek (DPO), és a további helyi szabályok szerint jár el.

8. Beépített adatvédelem

Amennyiben egy rendszerben adatvédelmi alapbeállítások alkalmazására van lehetőség, ezeket a beállításokat úgy kell elvégezni, hogy a használat céljára tekintettel csak a szükséges mennyiségű adatot, csak a szükséges ideig, és csak a szükséges mélységben kezeljünk, és a harmadik személyek általi hozzáférést a lehető legteljesebb mértékig korlátozzuk.

9. Adatvédelmi incidensek jelentése

9.1 Belső jelentéstétel

(1) Minden adatvédelmi incidenst azonnal jelenteni kell az adatvédelmi tisztviselőnek (DPO-nak):

a) a PHOENIX csoport oldalán keresztül:
https://phoenixgroup-databreach.integrityplatform.org/
VAGY

b) a helyi eszközben/eljárás szerint.

Példák:

- *Céges mobiltelefon/laptop vagy adathordozó elvesztése*
- *Téves címzettnek küldött üzenet*
- *Jogosulatlan hozzáférés a vásárlói portálhoz vagy a Speakuphoz*
- *A rendszer rosszindulatú szoftverrel való fertőződése, ha ez személyes adatokat érint*

(2) Az adatvédelmi tisztviselő (DPO) és a helyi biztonsági koordinátor (LSC) közös eljárást hoz létre a jelentéstétel céljára. A DPO és az LSC közösen felel azért, hogy a PHOENIX társaságnál ismert legyen az adatvédelmi jelentések rendje.

(3) A vállalati adatvédelmi vezető (HCDP) bevonására akkor van szükség, ha az adatvédelmi incidens nemzetközi vagy jelentős súlyú (az érintettekre nézve nagy adatvédelmi kockázattal vagy a PHOENIX csoportra nézve jogi kockázattal jár).

9.2 Az adatvédelmi incidensek kezelése

(1) A DPO a belső jelentés alapján meghatározza a felelős személyt/osztály(oka)t. A felelős alkalmazottak/vezetők eseti munkacsoportot alakítanak a DPO részvételével. Kritikus esetben a kommunikációs osztály és az Igazgatótanács is képviselteti magát a munkacsoportban.

(2) A munkacsoport megvizsgálja a tényállást, és felméri az érintettekre (vásárlókra, munkavállalókra stb.), illetve a PHOENIX társaságra vonatkozó kockázatot.

(3) A munkacsoport határoz a lehetséges kockázatenyhítő intézkedésekről, valamint a felügyeleti hatóság és/vagy az érintett(ek) tájékoztatásáról. Ezt a döntést 72 órán belül meg kell hozni (az adatvédelmi incidensről való tudomásszerzés időpontjától számítva), és követni kell az alábbi protokollt:

A PHOENIX társaság hivatalos tájékoztatásra köteles / nem köteles		
NEM ÁLL FENN KOCKÁZAT az érintettekre nézve - Tájékoztatási kötelezettség nincs	Az érintettek JOGAIRA nézve fennáll KOCKÁZAT - 72 órán belül tájékoztatni kell a felügyeleti hatóságot	Az érintettek JOGAIRA nézve MAGAS KOCKÁZAT áll fenn - 72 órán belül tájékoztatni kell a felügyeleti hatóságot - 72 órán belül vagy indokolatlan késedelem nélkül tájékoztatni kell az érintettet.
A munkacsoport minden esetben dokumentálja az adatvédelmi incidenst.		

(4) A DPO tájékoztatja az igazgatótanácsot a meghozott döntésről. A DPO betartja a helyi felügyeleti hatóság tájékoztatásra vonatkozó szabályait.

(5) Az adatvédelmi tisztviselő (DPO) és a helyi biztonsági koordinátor (LSC) közös, részletes eljárás létrehozásával gondoskodik az adatvédelmi incidensek helyi szintű kezeléséről.

10. Bevezetési tevékenységek

10.1 Bevezetési tevékenységek vállalati szinten

(1) A csoportszintű szabályzatok, vállalati adatvédelmi sztenderdek és vállalati minta-dokumentumok testesítik meg a vállalati adatvédelem fő bevezetési tevékenységeit.

(2) A vállalati szintű adatvédelem által létrehozott szabályzat egy, a teljesítendő konkrét követelményeket vagy szabályokat felvázoló, és az Igazgatóság által jóváhagyott dokumentum.

(3) A vállalati adatvédelmi útmutató nem szabályzat, hanem a vállalati adatvédelem által minimálisan megkövetelt sztenderd cselekvéseket, folyamatot vagy eszközt tartalmazza, amelyek segítségével biztosítható az adatvédelmi szabályzatnak (sztenderdnek) való megfelelés. Igazgatósági jóváhagyásra nincs szükség. A sztenderd nem érinti a szabályzatot, ugyanakkor a szabályzat végrehajtásának eszköze.

(4) A vállalati adatvédelmi sztenderdek gyűjteménye alkotja a vállalati adatvédelmi útmutatót (CPD útmutató).

(5) A vállalati adatvédelmi vezető (HCDP) az érintett vállalati érdekeltekkel és/vagy adatvédelmi képviselőkkel (DPO-kkal) egyeztetve elkészíti a végleges sztenderdet. A vállalati adatvédelmi vezető (HCDP) kiadja a sztenderdet az adatvédelmi tisztviselőknek (DPO-knak) és a bevont vállalati érdekelteknek. Az adatvédelmi tisztviselők (DPO-k) és a bevont érdekeltek felelnek a sztenderd további kiadásáért vagy érintett címzettekhez való eljuttatásáért.

(6) Az alábbi érdekeltek meghatározása csoportszinten történik a csoportszintű szabályzat vagy a vállalati adatvédelmi sztenderd esetében (témától függően):

- Információbiztonsági igazgató
- Vállalati rendszertervező (Enterprise Architect)
- CIO Iroda
- Vállalati jogi osztály
- Vállalati audit osztály
- Általános beszerzés
- Vállalati HR osztály

(7) A PHOENIX társaság megfelelő módon bevezeti a sztenderdet (pl. helyi szabályzatban, utasításként, technikai módosítás formájában), figyelembe véve a helyi jogi és szervezeti sajátosságokat. Helyi adaptációra lehetőség van, de ez nem eredményezhet a sztenderdben foglaltaknál alacsonyabb szintű adatvédelmet. A helyi adatvédelmi szabályoknak és műszaki megoldásoknak mindig a lehető legjobb adatvédelmet kell tükrözniük, és megfelelően védeniük kell az érintettek magánszféráját. A DPO évente vagy kérésre soron kívül is jelentést tesz a HCDP-nek a helyi megvalósításról az országjelentések felhasználásával.

(8) A vállalati mintadokumentum a PHOENIX csoport legjobb adatvédelmi gyakorlatát tükrözi.

10.2 A vállalati adatvédelmi koncepció

A főbb vállalati bevezetési tevékenységek alkotják az alábbi vállalati adatvédelmi koncepciót (Vállalati koncepció). Az adatvédelmi tisztviselő (DPO) a saját intézkedéseihez és a helyi bevezetési tevékenységekhez használja ezt a vállalati koncepciót:

Dokumentum típusa	Dokumentum/eszköz megnevezése
Szabályzat *(teljesítendő szabályok)*	• A PHOENIX csoport csoportszintű adatvédelmi szabályzata • További csoportszintű szabályzatok az adatvédelem területén, ha szükségesek • Információbiztonsági szabályzatok (biztosítják a személyes adatok integritását és bizalmas jellegét). *Igazgatóság által jóváhagyva* *A Helyi koncepciónak is része*
Csoportszintű adatfeldolgozási szerződések és csoportszintű közös adatkezelésről szóló szerződések	• Csoportközi tárgyalások eredménye *Igazgatóság és helyi Igazgatótanács által jóváhagyva* *A Helyi koncepciónak is része*
Vállalati adatvédelmi sztenderdek *(cselekvésre, folyamatra vagy eszközre vonatkozó minimumsztenderdek a PHOENIX csoportban)*	Példák • Nemzetközi adattovábbításról szóló sztenderd • Életciklusról szóló sztenderd az adatvédelmi koncepcióhoz • Adatvédelmi hatásvizsgálatról (DPIA-ról) szóló sztenderd • Adatmegőrzési koncepcióról szóló sztenderd • Adatvédelmi incidensek jelentéstételi rendszere • A Csoport online képzési platformja
Tájékoztató tevékenység	Csoportszintű tájékoztató kampány

10.3 A helyi adatvédelmi koncepció

(1) A helyi adatvédelmi tevékenységekből épül fel a helyi adatvédelmi koncepció (helyi koncepció). A DPO támogatja az Igazgatótanácsot a helyi koncepció tartalmának meghatározásában. A helyi koncepció keretei a következőképpen néznek ki:

Dokumentum típusa	Dokumentum/eszköz megnevezése
Helyi szabályzatok / SOP-k / Utasítás	Helyi adatvédelmi szabályzat (ha szükséges) A CDP útmutató vagy a helyi jogi előírások alapján készült helyi szabályozás: • A PIA/DPIA szabályozása • Az adatmegőrzési koncepció szabályozása • Az adatvédelmi incidensek kezelésének/jelentésének szabályozása • Az adatkezelési tevékenységek nyilvántartásának szabályozása • Az érintettek jogainak érvényesítésére vonatkozó szabályozás
Helyi mintadokumentumok	A vállalati mintadokumentumok alapján • Adatfeldolgozási szerződés • Ellenőrző listák az adatvédelmi tájékoztatóhoz • Szórólapok
TSZI-k	• Csoportszintű vagy helyi információbiztonsági szabályzatok • Formális és informális dokumentáció (pl. biztonsági mentések koncepciója, naplófájlok stb.)
Tájékoztató tevékenység	Helyi képzések és tájékoztató kampányok