Szab-17/2010-10 - Adatvédelmi szabályzat (bankcsoport szintű utasítás)

Folyamatgazda szakterület	adatvédelmi tisztviselő
Szakértők:	Dr. Dósa Imre – adatvédelmi tisztviselő
Kapcsolódó hatósági szabályozások	

Tartalomjegyzék

A VÁLTOZÁSOK ÖSSZEFOGLALÁSA: **2**

1 BEVEZETŐ RENDELKEZÉSEK **2**

1.1 A SZABÁLYZAT CÉLJA: 3

2 ÁLTALÁNOS RÉSZ **3**

2.1 A SZABÁLYZAT HATÁLYA: 3

3 KÜLÖNÖS RÉSZ **4**

3.1 AZ ADATKEZELÉSSEL KAPCSOLATOS ALAPVETŐ SZABÁLYOK 4

3.1.1 Az adatkezelés célhoz kötöttsége szükségessége és arányossága *4*

3.1.2 Az adatkezelés jogalapja *4*

3.1.3 Személyes adatok különleges kategóriájának kezelése *5*

3.2 BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM BIZTOSÍTÁSA 5

3.3 ADATVÉDELMI HATÁSVIZSGÁLAT 8

3.4 ADATTOVÁBBÍTÁS, ADATFELDOLGOZÁS 9

3.5 A KÖZVETLEN ÜZLETSZERZÉSI (DIREKT MARKETING) ÉS PIACKUTATÁSI CÉLÚ ADATKEZELÉSEK 9

3.6 A MUNKAVÁLLALÓK SZEMÉLYES ADATAINAK KEZELÉSE 10

3.7 A TÁRSASÁG NEM HITELEZÉSI ÜZLETI PARTNEREINEK ADATAI, AZOK KEZELÉSE 11

3.8 INFORMÁCIÓBIZTONSÁG, ADATBIZTONSÁG 11
3.9 AZ ADATVÉDELMI TISZTVISELŐ ÉS AZ ADATVÉDELMI NYILVÁNTARTÁS 11
3.9.1 Az Adatvédelmi tisztviselő 11
3.9.2 Konzultáció az adatvédelmi tisztviselővel 12
3.10 BELSŐ ADATVÉDELMI NYILVÁNTARTÁS 13
3.11 AZ ADATVÉDELMI INCIDENSEK 13
3.11.1 Eljárás adatvédelmi incidens gyanú esetén 14
3.11.2 Intézkedések a bejelentés alapján 14
3.11.3 Érintett tájékoztatása az adatvédelmi incidensről 15
3.11.4 Az incidens nyilvántartása 16
3.12 AZ ADATVÉDELMI OKTATÁS RENDJE 16
3.13 AZ ADATVÉDELMI KONTROLLOK 16
3.13.1 Az adatkezelések támogatása 16
3.13.2 Belső, más kontroll alá nem eső adatátadás workflow 17
3.13.3 Adatvédelmi riportok ellenőrzése 17
3.14 KÖZPONTI HITELINFORMÁCIÓS RENDSZERRE VONATKOZÓ SZABÁLYOK 17

4 MELLÉKLETEK: 17

A változások összefoglalása:

GDPR *alkalmazási tapasztalatok, belső ellenőrzési javaslatok beépítése, fogalomtár integráció.*

Kikerültek az alábbi szabályok:

- Tiszta asztal – Clean Desk policy
- Fejlesztés adatvédelmi követelményeinek kontrollja
- Dolgozatírás a Bankcsoportban

1 BEVEZETŐ RENDELKEZÉSEK

A **Budapest Hitel és Fejlesztési Bank Zrt.** (székhelye: 1138 Budapest, Váci út 193.; cégjegyzékszáma: Fővárosi Bíróság, mint Cégbíróság 01-10-041037), a **Budapest Lízing Zrt.** (székhelye: 1138 Budapest, Váci út 193.; cégjegyzékszáma: Fővárosi Bíróság, mint Cégbíróság 01-10-041997), a **Budapest Alapkezelő Zrt.** (székhelye: 1138 Budapest, váci út 193., cégjegyzékszáma: Fővárosi Bíróság Cégbírósága 01-10-041964), a **Budapest Eszközfinanszírozó Zrt.** (1138 Budapest,

Váci út 193., cégjegyzékszáma: Fővárosi Bíróság Cégbírósága Cg. 01-09-266772), (a továbbiakban együtt is, mint: **Társaság**) a jelen utasításban felsorolt jogszabályokban foglalt követelmények alapján, a jogszabályi előírások végrehajtása érdekében, az alábbi adatvédelmi-szabályzatot készítette.

1.1 A Szabályzat célja:

Jelen Szabályzat célja a Társaság leendő, meglévő vagy jogviszonyuk alapján már megszűntnek vagy elutasítottnak minősített ügyfelei, valamint a Társaság munkavállalói vagy egyéb, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyek, illetőleg a Társasággal szerződéses kapcsolatban álló partnerek vagy más harmadik természetes személyek (a továbbiakban együtt, mint: **Adatalany vagy Érintett**) által, meghatározott adatkezelési célból, a Társaság részére átadott személyes adataik kezelése, továbbítása, feldolgozása, tárolása során biztosítva legyen az adatalanyok információs önrendelkezési jogának maradéktalan érvényesülése, törvényes érdekeik és jogaik védelme, az adatok kezelésének jogszerű célhoz rendelése és a felhasználás alatt mindvégig e jogszerű célhoz kötöttsége. A Szabályzat célja továbbá az adatok kezelésének és továbbításának, jogszerűsége, fenntartható legyen azok minősége, és biztosítva legyen az adatok jogosulatlan személyek általi hozzáférhetetlensége. Az adatalanyi minőség - és ezáltal az adatvédelmi szabályoknak történő megfelelés követelménye - a személyes adat jogszerű módon történő megszerzésétől kezdődően, az adott jogviszony létrehozásán keresztül annak fennállása alatt és azt követően is fennáll mindaddig, amíg az adott adatalannyal összefüggésben a személyes adatok végleges és visszafordíthatatlan módon történő törlése, deperszonalizálása - vagy ahol az lehetséges, illetve szükséges, a megsemmisítése - végrehajtásra nem kerül.

E szabályzat célja továbbá, hogy meghatározza a Bankcsoportban vezetett adatvédelmi nyilvántartások működésének törvényes rendjét, biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak az érvényesülését, valamint hogy a személyes adatok kezelése a jogszabályokban előírtaknak megfelelően történjen.

Jelen Szabályzat a Bankcsoport tevékenységével összefüggően az adatvédelem alapvető elveit, alkalmazandó legfontosabb szabályait határozza meg. Adott és a jelen Szabályzatban is hivatkozott, kapcsolódó belső utasítások tartalmazhatnak részletes szabályokat egy meghatározott adatkezeléssel kapcsolatos követendő eljárásról, feladatokról és felelősségi körökről, az adattovábbítás módjáról és feltételeiről, az adatok törléséről.

2 ÁLTALÁNOS RÉSZ

2.1 A Szabályzat hatálya:

Jelen Szabályzat a Társaság valamennyi munkavállalójára, munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott munkatársára, ezen felül valamennyi szerződő partnerére, egyéb adatkezelőkre vagy adatfeldolgozóra kiterjed, akik/amelyek feladatuk ellátása során az Adatalany személyes adatnak minősülő adataival bármilyen jellegű műveletet végeznek (ahhoz hozzáférnek, azt kezelik, feldolgozzák, továbbítják, törlik, stb.)

A Szabályzat hatálya kiterjed a Társaságban - annak székhelyén, telephelyén és fióktelepén – folytatott valamennyi, természetes személy személyes adatait tartalmazó adatkezelésre illetve adatfeldolgozásra, függetlenül attól, hogy az adatkezelés illetve adatfeldolgozás teljesen vagy részben számítógépes eszközzel (elektronikus úton), illetve manuális módon történik.

A Szabályzat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete (a továbbiakban GDPR) követelményeinek történő megfelelés céljából, annak végrehajtására született, figyelemmel a jogszabályok ágazati adatvédelmi rendelkezéseire is.

3 KÜLÖNÖS RÉSZ

3.1 Az adatkezeléssel kapcsolatos alapvető szabályok

3.1.1 Az adatkezelés célhoz kötöttsége szükségessége és arányossága

Személyes adat csak meghatározott törvényes célból, jog gyakorlása, kötelezettség teljesítése érdekében kezelhető. Az adatkezelés célhoz kötöttségét, szükségességét és arányosságát az GDPR szabályozza. A célhoz kötöttséget az érintett hozzájárulása nem pótolja. Az adatkezelés céljának meghatározásakor az összes Bankcsoportban releváns adatkezelési célt számba kell venni. Az adatkezelési cél meghatározásáért az adatkezelést megalapozó termék, folyamat üzleti felelőse tartozik felelősséggel.

A statisztikai célra felvett, átvett vagy feldolgozott személyes adatok csak statisztikai célra használhatóak fel.

3.1.2 Az adatkezelés jogalapja

Személyes adat a Társaságnál akkor kezelhető, ha
a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés a Társasággal kötött olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az Társaságot terhelő jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy valamely adatkezelőre – különösen hatóságra – ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés a Társaság vagy egy harmadik személy jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé

Az a) pont szerinti esetben, a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

A meglévő szerződések esetén a jogalap változása külön jogcselekmény nélkül, a GDPR erejénél fogva áll be.

Példák:

- Az ügyfelekkel kötött pénzügyi szolgáltatási szerződés teljesítése körében kezelt adatok kezelésének jogalapja b) pont szerinti szerződés.
- A megfelelési kötelezettség alapján kezelt adatok – például pénzmosás megelőzés – jogalapja a c) pont szerinti jogi kötelezettség.
- Az üzleti érdekek védelmében folytatott – például csalás megelőzési célú – adatkezelés jogalapja az f) pont szerinti jogos érdek.

3.1.3 Személyes adatok különleges kategóriájának kezelése

A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos. Amennyiben ilyen személyes adat kezelése elengedhetetlen, a GDPR 9. cikke szerinti jogalap – különösen az érintett kifejezett hozzájárulását – biztosítani kell, például munkaügyi célú adatkezelés során.

A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet. Erkölcsi bizonyítvány bemutatása kérhető, ha a büntetlen előélet megállapítása jogszabályi követelmény, vagy ilyen adat kezelése érdekmérlegelési teszttel, adatvédelmi hatásvizsgálattal alátámasztott.

3.2 Beépített és alapértelmezett adatvédelem biztosítása

Az Új Termék, Csatorna Bevezetése (NPI)folyamatban, a projektek és Üzleti Fejlesztési Igény (mini projektek) üzleti követelmény specifikációjának összeállításakor a projektvezető a leszállítandók között felügyeli, az üzleti felelős pedig biztosítja:

1. Az adatvédelmi hatásvizsgálat elvégzését;
2. Az új adatkezelés adatvédelmi nyilvántartásban rögzítését

Minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát. A Bank az általános – minden adatkezelésre értelmezhető – tájékoztatást Üzletszabályzata útján nyújtja. Az adatkezelések specifikus tájékoztatása részletes adatkezelési tájékoztatásban található. A munkaügyi, belső adatkezelések tájékoztatását elsősorban az adatkezelésre vonatkozó szabályzat, utasítás tartalmazza.

A tájékoztatás kötelező tartalmi elemei:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
- az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
- a személyes adatok tervezett kezelésének célja, valamint
- az adatkezelés jogalapja;
- az adatkezelő vagy harmadik fél jogos érdekei,
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái,
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról történő tájékoztatás

Az érintett adatvédelmi jogai:

- Személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:
  a) az adatkezelés céljai;
  b) az érintett személyes adatok kategóriái;
  c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;

d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga; g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

- Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.
- Adattörléshez való jog érvényesítésekor a Bank a marketing célú adatkezelést megszünteti, az érintett azonosító adatát Robinson listára veszi. Egyedi hatósági határozattal elrendelt adattörlést informatikai hibajegy rögzítésével kell kezdeményezni.
- Az adatkezelő minden olyan címzettet tájékoztat a GDPR. 16. cikk, a 17. cikk (1) bekezdése, illetve a 18. cikk szerinti valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.
- Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta. A Bank az adathordozhatóság jogát lehetőleg pdf, ennek hiányában xls, csv, txt, rtf formátumokban teljesíti.
- Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.
- Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. A Bank az automatizált adatkezelésen alapuló döntésről részletes adatkezelési tájékoztatóban ad tájékoztatást.
- Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:
  a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
  b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
  c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez,

érvényesítéséhez vagy védelméhez; vagy
d) az érintett a 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Adatkezelő kötelezettségei:

- Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése GDPR-al összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. A Bank ezen kötelezettségét adatvédelmi keretrendszer működtetésével biztosítja. A keretrendszer tartalmazza az adatkezelésinyilvántartást, az adatvédelmi incidens nyilvántartást, az adatvédelmi hatásvizsgálatokat. A keretrendszer az IMRE és NORA rendszerekre figyelemmel, a Bank kockázatkezelési rendszereivel összhangba, azok tartalmára tekintettel működik.
- Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen. Az adatfeldolgozók felügyeletét a Bank a beszerzési rendszer útján látja el.
- Az adatfeldolgozó és bármely, az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi.

3.3 Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálatot a NAIH PIA rendszerében meghatározott kérdésekre, Selfie[1]-n található tartalommal, az adatvédelmi hatásvizsgálati útmutató figyelembe vételével kell elvégezni, az adatkezelési nyilvántartásban található adatkezelések közül a GDPR szerinti magas kockázatú adatkezelésekre. Új informatikai rendszer bevezetése vagy meglévő informatikai rendszer jelentős módosítása során a hatásvizsgálatot felül kell vizsgálni, és erről az adatvédelmi nyilvántartásban bejegyzést kell tenni. Mini projekteknél azok indításakor az Adatvédelmi tisztviselő tájékoztatást kap az igényről, ami után döntést hoz, hogy az igény tartalmaz-e adatvédelmi érintettséget és szükséges-e adatvédelmi hatásvizsgálatot készíteni. A hatásvizsgálat informatikai vonatkozású elemeinek kidolgozása szállítói feladat.

[1] Szabályzat módosításakor fejlesztés alatt

Projekt vagy mini projekt felelősének feladata, hogy az adatvédelmi tisztviselővel egyeztetve meghatározza, a fejlesztés érint-e személyes adatkezelést. Ha igen, akkor mely adatkezelési nyilvántartási elem(ek) hatásvizsgálatának felülvizsgálata szükséges.
Az adatvédelmi hatásvizsgálat során a Bankra kötelező adatbiztonsági intézkedéseket nem szükséges részletezni, hanem az adott adatkezelés speciális adatbiztonsági elemeit szükséges számbavenni.

Az adatvédelmi hatásvizsgálat informatikai biztonsági követelményei az U-07/2010-6 - Alkalmazásfejlesztés Biztonsági Követelményei - Bankcsoport szintű utasítás szabályzat szerint történik. Az adatbiztonság szintjének növelésére álnevesítést, titkosítást kell biztosítani minden olyan esetben, ahol ez a kockázatokra, a Bank teljesítő képességére tekintettel alkalmazható.

3.4 Adattovábbítás, adatfeldolgozás

Az adatfeldolgozókkal szemben támasztott adatvédelmi követelményeket a beszerzési szerződésminta adatvédelmi melléklete tartalmazza.

A Társaság az Adattovábbítási Hirdetményben, illetőleg ha az adattovábbítás kiszervezési tevékenység keretén belül történik, a Kiszervezési Hirdetményben teszi közzé azon belföldi és külföldi cégeket, amelyek részére adatokat továbbíthat. Az adattovábbítást tervező banki alkalmazott – aki különösen lehet az IT rendszergazda, a termékgazda, az operáció dolgozója, a behajtás dolgozója, a projektvezető illetve bármely adattovábbítást végző szervezeti egység dolgozója-, amennyiben a cég vagy a továbbítani kívánt adat nem szerepel az Adattovábbítási- vagy Kiszervezési Hirdetményben, a tervezett adattovábbítást legalább 30 nappal megelőzően az adatvédelmi tisztviselőt írásban értesíti a következővel: ki, mikor, hova, kinek a részére, milyen célból, milyen jogszabály vagy ügyfél felhatalmazás alapján kíván adatot továbbítani, és a továbbítani kívánt adatok pontos felsorolását. Az értesítés alapján az adatvédelmi tisztviselő megvizsgálja a tervezett adattovábbítás jogi feltételeit, és az adattovábbítást engedélyezi vagy megtiltja. Az adattovábbítás kizárólag az adatvédelmi tisztviselő engedélye után kezdhető meg, illetve folytatható. A Hirdetmények vezetéséről és a mindenkor hatályos verziók publikálásáról a Jogi Igazgatóság gondoskodik.

Európai Unió tagállamaiba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

A tulajdonos részére bármely személyes adatot érintő információ az adatvédelmi tisztviselő útmutatása alapján és a Vezérigazgató előzetes jóváhagyását követően továbbítható. Ismételt küldés esetén új engedélyt csak az adattovábbítás feltételeinek megváltozásakor kell kérni.

3.5 A Közvetlen üzletszerzési (direkt marketing) és piackutatási célú adatkezelések

A közvetlen üzletszerzési (direkt marketing) és piackutatási célú adatkezelések alapvető és elvi szabályai vonatkozásában a Budapest Bankcsoport információmenedzsment politikájában meghatározottakat kell alkalmazni.

A DM célú megkeresések részletes szabályait és a DM célú megkeresést kizáró ügyfelekkel kapcsolatos eljárási rendet a mindenkor hatályos, lakossági ügyfelekre irányadó „CRM" Utasítás szabályozza.

3.6 A munkavállalók személyes adatainak kezelése

A Társaság a munkavállalók személyes adatait a munkajogi szabályok szerint, bizalmasan kezeli. A munkavállaló személyi adatlapján, önéletrajzában, teljesítményértékelésben és a munkaviszonnyal összefüggő, a munkaviszony létesítése és fenntartása szempontjából lényeges nyilatkozatokban szereplő adatokat a Társaság bér- és társadalombiztosítási elszámolás, juttatás, a munkavállaló előmenetelének tervezése, érdekellentétek kezelése, valamint a Bankcsoport tagjai szolgáltatásainak és termékeinek ajánlása céljából nyilvántartja, kezeli. Ezeket, az adatokat a Társaság a részére bér- és tb-elszámolást végző társaság részére, a Bankcsoport tagjai részére az adatvédelmi előírásokat betartva külföldre is továbbíthatja.

A Társaság külföldre adatot kizárólag abban az esetben továbbít, ha a külföldi adatkezelőnél a magyar jogszabályok által támasztott követelményeket kielégítő adatkezelés feltételei minden egyes adatra nézve teljesülnek.

A Társaság, mint munkáltató általi adatkezelés a munkavállaló által aláírt munkaszerződésben, munkáltatói utasításban szabályozott. A Társaság új belépő munkavállalói a jelen pontban meghatározott adatkezeléshez történő hozzájárulást alapvetően írásban adják meg, de lehetőség van az illetékes szakterületek (Emberi Erőforrás, IT, JOG) bevonását követően kialakított elektronikus úton beszerzett hozzájárulásokat is beszerezni pl. már meglévő, e-mail címmel rendelkező munkavállaló vonatkozásában. Az elektronikus úton beszerzett hozzájárulások adatbiztonsági szabályoknak történő megfelelését (biztonságos tárolás, visszakereshetőség, egyénhez rendelhetőség, illetéktelenek hozzáférésének megakadályozása) biztosítani kell.

A munkavállaló a munkáltató által vezetett nyilvántartások rá vonatkozó adataiba bármikor betekinthet, vagy arról tájékoztatást kérhet. Ezen adatokhoz az Emberi Erőforrás kijelölt munkatársai, illetve azok férhetnek hozzá, akiket a Társaság belső utasításai erre feljogosítanak.

Adatszivárgás gyanúja/megtörténte esetén a munkavállaló köteles értesíteni az adatvédelmi tisztviselőt. A Társaság által a munkavállalók, munkavégzésre irányuló egyéb jogviszonyban foglalkoztatottak vagy szerződéses partnerek részére hivatali célú felhasználásra biztosított e-mail cím, internet elérhetőség, hivatali célú telefonhívások munkáltató általi ellenőrzésének, az ellenőrzéssel kapcsolatos jogok és kötelezettségek részletes szabályairól külön utasításban kell rendelkezni.

3.7 A Társaság nem hitelezési üzleti partnereinek adatai, azok kezelése

A Társaság természetes személyekkel meglevő szerződéseiben szereplő személyes adatok kezelésére vonatkozóan is az GDPR szabályait kell betartani.

A jogi személyekre, illetve jogi személyiséggel nem rendelkező gazdasági társaságokra a Társaság által az adott céggel meglevő szerződésekben kell rendelkezni az esetleg átadásra kerülő személyes adatok köréről, annak céljáról, időtartamáról, stb. és a szerződés keretei között, a jelen utasítás előírásait figyelembe véve kell az annak megfelelő kezelést biztosítani, melynek részletszabályait a mindenkor hatályos Beszerzési utasítás (Szab-18/2018 - A beszerzésről - bankcsoport szintű utasítás **)** tartalmazza.

3.8 Információbiztonság, adatbiztonság

Az információbiztonsági rendszabályok megalkotása a Bank illetékes területeinek – IT Biztonság, Kockázatkezelés és Törvényi Megfelelés - feladatkörébe tartozik. Az információbiztonsági rendszabályokat a külön utasítások tartalmazzák. Ilyen különösen az alkalmazás fejlesztés biztonsági követelményeiről, a jogosultság menedzsmentről, a naplózásról, az informatikai konfiguráció menedzsmentről, adatmentésről, archiválásról, üzletmenet folytonosságról, harmadik felek információbiztonsági követelményeiről szóló szabályozás.

Ha az információbiztonsági szabályok nem felelnek meg az adatbiztonság törvényben meghatározott követelményeinek vagy a jogalkalmazás alapján született hatósági állásfoglalásoknak, az adatvédelmi tisztviselő az adatbiztonsági kockázatot a vezérigazgatónak jelenti és az IMRE rendszerben rögzíti.

3.9 Az adatvédelmi tisztviselő és az adatvédelmi nyilvántartás

Ahol jogszabály, szabályzat, utasítás, hirdetmény belső adatvédelmi felelőst említ, azon adatvédelmi tisztviselőt kell érteni.

3.9.1 Az Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő jelen szabályzatban szabályozott tevékenysége körében a vezérigazgató felügyelete alá tartozik. Éves munkatervét készít, melyet a vezérigazgató jóváhagy. A munkaterv végrehajtásáról negyedévente írásban beszámol a vezérigazgatónak.

Az Adatvédelmi tisztviselő GDPR által meghatározott feladatait az alábbiak szerint látja el:

- közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában. (Konzultáció az adatvédelmi tisztviselővel) E-mail megkeresésekre 15 napon belül választ ad vagy közli a válaszadás akadályát. A Belső Ellenőrzéssel

együttműködve kapcsolatot tart a NAIH-al, Bankszövetség adatvédelmi munkacsoportjával, a tulajdonos cégcsoport adatvédelmi tisztviselőivel, szervezeteivel.

- ellenőrzi aGDPR és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását. A részletes adatvédelmi kontrollokat a Az adatvédelmi kontrollok tartalmazza;
- kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót. Az adatvédelmi tárgyú panaszok kivizsgálásában, intézésében a Panaszkezelési Szabályzatnak megfelelően vesz részt;
- elkészíti a belső adatvédelmi szabályzatot, felügyeli a kiszervezési, adattovábbítási hirdetményt;
- felügyeli a belső adatvédelmi nyilvántartás vezetését;
- gondoskodik az adatvédelmi ismeretek oktatásának szakmai tartalmáról a 3.12 szerint.
- Konzultációs kérdéssel a NAIH-hoz fordulhat.
- Képviseli a Bankot a Bankszövetség Adatvédelmi Munkacsoportjában.
- Közérdekű adatigénylés esetén az adatok kiadhatósága kérdésében segítséget nyújt”A külső és a belső kommunikáció szabályai bankcsoport szintű utasításban szabályozott eljárásban.
- A panaszkezelés adatszolgáltatása alapján a nem teljesített adatigénylésekről évente, a tárgyévet követő év január 15. napjáig jelentést állít össze a NAIH részére.

3.9.2 Konzultáció az adatvédelmi tisztviselővel

A feladatkörében felmerülő adatvédelmi, adatkezelési kérdésekben minden társasági alkalmazott köteles az adatvédelmi tisztviselővel előzetesen konzultálni, és a jelen utasításban meghatározott és szükséges jóváhagyásokat előzetesen kellő időben beszerezni.

Az Adatvédelmi tisztviselő olyan állásfoglalását, melynek tartalma más hasonló ügyekben is alkalmazható, adatbázisban rögzíti. A Bankcsoport szempontjából kiemelkedő állásfoglalásokról az adatvédelmi tisztviselő a vezérigazgatónak tájékoztatást ad.

Az adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon. Az adatkezelő és az adatfeldolgozó támogatja az adatvédelmi tisztviselőt feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek. Az adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének, a vezérigazgatónak tartozik felelősséggel. Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi

tisztviselőhöz fordulhatnak. Ezért az adatvédelmi tisztviselő a NAIH nyilvántartásába bejelentkezik. Minden szervezeti egység kötelessége az ilyen kérdések változatlan formában az adatvédelmi tisztviselőhöz történő haladéktalan eljuttatása. Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban munkajogi titoktartási kötelezettség köti. Az adatvédelmi tisztviselő kamarai jogtanácsosi feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

3.10 Belső adatvédelmi nyilvántartás

A GDPR alapján az adatkezelőnek az adatkezelésekről nyilvántartást kell vezetnie. A Bankcsoport belső adatvédelmi nyilvántartása:
https://selfie/sites/jog/GDPR/GYUJTLIST/GDPR_REGULA_BASE_keres.aspx
A nyilvántartásnak – az adatkezelő üzleti tevékenysége körében – a részletes adatkezelési tájékoztatásban meghatározott adatkezelésekhez kell igazodnia. Az egyéb – különösen munkaügyi, foglalkoztatási célú adatkezelések A nyilvántarás részét képezi, az adatkezelés címzettjei tekintetében:

- Adattovábbítási- és Kiszervezési Hirdetmények;
- Harmadik felek bankcsoporti adatokhoz hozzáférése

A nyilvántartást az adatkezelésért felelős üzleti adatgazda (termékfelelős, szervezeti egység vezető) vezeti, az adatvédelmi tisztviselő szakmai támogatásával. Az adatvédelmi nyilvántartást 2 évente felül kell vizsgálni. A felülvizsgálatot az adatvédelmi tisztviselő ellenőrzi. Az ellenőrzés megállapítása a tisztviselői beszámoló kötelező tartalmi eleme. A nyilvántartás az adatvédelmi tisztviselő felügyelete alatt működik.

3.11 Az adatvédelmi incidensek

Az adatvédelmi incidens fogalmát a GDPR határozza meg.

Adatvédelmi incidensnek minősül és a jelen szabályzatban foglaltakat kell alkalmazni abban az esetben is, ha a Bankkal adatfeldolgozói szerződéses viszonyban álló cég/vállalkozás érdekkörében, a Bank adatai vonatkozásában történt incidens, amit az adatfeldolgozási szerződésben előírtak szerint a Bank számára bejelentett.

Nem minősül adatvédelmi incidensnek az olyan működésbiztonsági esemény, amely személyes adatot nem érint. Az adatvédelmi incidens nem érinti az informatikai incidenskezelési utasításban szabályozott, meghatározott eljárást. Adott esetben ezek párhuzamosan indulnak. Az informatikai incidenskezelési eljárás alapján, amennyiben az adott esemény csak és kizárólag informatikai jellegű, adatvédelmi bejelentésre nincs szükség. Az adatvédelmi és informatikai incidenskezelési eljárás felelősei, tehát az informatikai incidens menedzser és az adatvédelmi tisztviselő egymást tájékoztatják az adatvédelmi incidensekről,

ha ennek technikai útja nem biztosított. Az incidens akkor minősül adatvédelmi incidensnek, ha az incidenssel érintett informatikai, távközlési, szoftver eszköz, dokumentum felügyeletéért felelős terület az incidens adatvédelmi jellegét visszaigazolja.

3.11.1 Eljárás adatvédelmi incidens gyanú esetén

Az IT incidens menedzsment, valamint a panaszkezelés az adatvédelmi incidens gyanúját informatikai eszközzel jelenti az adatvédelmi tisztviselőnek.

Az IT incidens menedzsment a Szab-09/2016 utasításban foglalt incidens jelentést követően az adatvédelmi incidens gyanúját informatikai eszközzel jelenti az adatvédelmi tisztviselőnek a rögzítésre kerülő CASD incidens rekord alapján.
Az átadott értékek a megállapodottak szerint:
- nem tudom értékkel, ha nem eldönthető a rendelkezésre álló információk alapján az adatvédelmi érintettség
- igen értékkel, ha megállapítható a rendelkezésre álló információk alapján az adatvédelmi érintettség
- nem értékkel ha kizárható a rendelkezésre álló információk alapján az adatvédelmi érintettség

Az adatvédelmi incidens gyanúját az azt észlelő munkavállaló haladéktalanul jelenti közvetlen vezetőjének. (A gyanú akkor megalapozott, ha személyes adat elveszett, elérhetetlen, illetéktelen személy birtokába került, hozzáférhetetlenné vált stb.). Az adatvédelmi incidens kockázati besorolásánál a jelen szabályzat rendelkezéseit kell figyelembe venni.

Az észlelő munkavállaló vagy közvetlen vezetője az incidens bejelentésére szolgáló Selfie felületen bejelentést tesz.

Ha a közvetlen vezetőnek kétsége van arról, hogy a rendkívüli esemény adatvédelmi incidens-e (például személyes adat érintett-e a rendkívüli esemény kapcsán), akkor rövid úton konzultál az adatvédelmi tisztviselővel. Az adatvédelmi tisztviselő minden esetben az ügy kivizsgálása érdekében egyezetés céljából megkeresi az információbiztonsági terület kijelölt munkavállalóját. A két terület együttes állásfoglalása minősítheti az incidenst adatvédelmi jellegűnek.

A bejelentést az adatvédelmi tisztviselő legkésőbb a következő munkanap végéig megvizsgálja és intézkedést tesz.

3.11.2 Intézkedések a bejelentés alapján

- Az incidens lezárása, ha a bejelentés adataiból megállapítható, hogy nem történt adatvédelmi incidens;

- Az adatvédelmi incidens kivizsgálásának előírása. A kivizsgálandó tények alapján a vizsgálatra a Panaszkezelést az adatvédelmi tisztviselő kéri fel vizsgálatra a határidő megjelölésével. A vizsgálat során az adatvédelmi tisztviselő/adatvédelemmel foglalkozó munkatárs feladata az adatvédelmi incidensek kockázati besorolásának elvégzése a melléklet alapján.
- Az incidens ismert részleteinek 72 órán belül történő bejelentése a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) részére, a mellékletbe foglalt adattartalommal minősített elektronikus aláírással ellátott e-mail útján.
- Válság stáb összehívása, ha az adatvédelmi incidens az érintettek tájékoztatásával jár, mert az érintettek aktív közreműködését igényli az adatvédelmi incidens okozta károk elhárítása, enyhítése. A válság stáb tagjai: Adatvédelmi tisztviselő, Szabályozói Megfelelési vezető, Üzletbiztonsági vezető, Informatikai Igazgató kijelölt munkavállalói, Kommunikációs vezető.
- Vezérigazgató értesítése az adatvédelmi incidensről. A vezérigazgató az adatvédelmi incidens bejelentésére nyitva álló 72 órás határidőn belül írásban az incidens nyilvánosságra hozatalát a Bank méltányolható gazdasági, reputációs érdekeire tekintettel megtilthatja, felfüggesztheti, feltételekhez kötheti.
- Amennyiben a Vezérigazgató a nyilvánosságra hozatallal egyetért és a válságstáb döntése szükségessé teszi, az adatvédelmi tisztviselő tájékoztatja a Kommunikációs vezetőt, aki a válságstáb döntése szerinti módon és tartalommal jár el.
- Az illetékes területek vezetői által jóváhagyott Intézkedési terv ismertetése a NAIH bejelentés kiegészítése keretében.
- Az adatvédelmi incidens lezáró jelentés elkészítése, Jogi Igazgató, Szabályozói Megfelelési vezető részére történő megküldése.

3.11.3 Érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. A tájékoztatást a válságstáb döntése szerinti terjedelemben, formában kell közzétenni. A tájékoztatás nem kell megtenni, ha a GDPR 34. cikk (3) bekezdésében meghatározottak szerint az incidens következményeinek kezelése/elhárítása megtörtént.
Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatóság gal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.
Az érintettek tájékoztatásának módját az adatvédelmi incidens jellege, kockázati besorolása és a válságstáb döntése határozza meg az egyedi eset elemzése és kivizsgálása alapján.
Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és a következő adatoknak kell kötelezően szerepelnie:

- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;
- ismertetni kell az érintett számára javasolt intézkedéseket, amelyeket az érintett saját érdekkörében megtehet az adatvédelmi incidens kockázatainak megelőzése vagy az okozott kár elhárítása érdekében.

3.11.4 Az incidens nyilvántartása

Az adatvédelmi tisztviselő az adatvédelmi vonatkozású panaszkezelési és informatikai riportok ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az adatvédelmi incidens gyanú időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat. A NAIH számára nyújtott adatvédelmi incidens bejelentést a nyilvántartás adataiból kell összeállítani.

3.12 Az adatvédelmi oktatás rendje

Valamennyi Társasághoz belépő új dolgozó, a belépést követően az E-Iránytű program keretében kap adatvédelmi oktatást. A Társaságnál az aktív állományban lévő alkalmazott részére szükség szerint adatvédelmi oktatást kell tartani. Az adatvédelmi oktatás tananyagának biztosítása az adatvédelmi tisztviselő feladata, melyet a jogi szakterülettel együttműködésben lát el.

Az adatvédelmi oktatás keretében biztosított képzésen részt vevők körét az adatvédelmi tisztviselő az Emberi Erőforrás és Szabályozási Megfelelés szakterületekkel egyetértésben határozza meg.

Az adatvédelmi oktatás szakmai tartalmát az adatvédelmi tisztviselő határozza meg. Ennek ki kell terjednie a GDPR Bankra alkalmazható rendelkezéseire és a NAIH, az Európai Adatvédelmi Testület (EDPB) olyan gyakorlatára, amely a Banki adatkezelés szempontjából releváns.

3.13 Az adatvédelmi kontrollok

Az Adatvédelmi tisztviselő az alábbi területek felett gyakorol másodszintű kontrollt:

3.13.1 Az adatkezelések támogatása

Az Adatvédelmi tisztviselő az Konzultáció az adatvédelmi tisztviselővel szerint a vezérigazgató előtt beszámol a Társaság adatvédelmi szempontból jelentős tevékenységeiről, kiemelve az esetleges adatvédelmi kockázatokat.

3.13.2 Belső, más kontroll alá nem eső adatátadás workflow

A Belső, más kontroll alá nem eső adatátadás workflow használatával kell igényelni olyan Bankcsoporton belüli adatátadást, adattovábbítást, melynél az adatot igénylő szervezeti egység (dolgozója) az igényelt adatot tartalmazó rendszerhez nem rendelkezik hozzáféréssel. Az adatigénylésben a kért adatok azonosító adatain kívül meg kell jelölni, hogy az igénylő mely munkafolyamatához van szükség az igényelt adatokra. Az igénylő az átadott adatok biztonságos kezeléséért felelősséget vállal.

Az Adatvédelmi tisztviselő az érintett hozzáférési jogát, hatósági adatszolgáltatást, belső munkaügyi vizsgálatot érintő adattovábbítás engedélyezését végzi el. Ennek keretében szükség esetén az igénylőt nyilatkoztatja az adatigénylés okáról, az igényelt adatok kezeléséről. Ha szabálytalan adatigénylést, jelen Szabályzat rendelkezéseinek be nem tartását tapasztalja, az adatigénylő szervezeti egységének vezérigazgató közvetlen alárendeltségében működő vezetőjét értesíti. Az ellenőrzés eredményéről a vezérigazgató előtt legalább negyedévente beszámol.

3.13.3 Adatvédelmi riportok ellenőrzése

Az adatvédelmi tisztviselő áttekinti a Panaszkezelés, IT incidens menedzsment napi – adatvédelmi vonatkozású – riportjait. Adatvédelmi incidens gyanú észlelése esetén értesíti a beküldő szervezeti egységet, felkéri adatvédelmi incidens rögzítésére

3.14 Központi Hitelinformációs Rendszerre vonatkozó szabályok

A KHR-ben kezelt adatokkal, a Bankcsoport munkatársainak feladatairól a részletes szabályokat a mindenkor hatályos Ügyviteli utasítás (Információszolgáltatás a Központi hitelinformációs rendszer részére) tartalmazza.

4 Mellékletek:

1 - KHR Tájékoztatóval kapcsolatos tudnivalókat tartalmazó Belső Segédlet

2 - Az un. *prospective* (leendő) ügyfelek adatkezelési hozzájárulását tartalmazó minta
3 – Incidens kockázati besorolása
4 – Példák adatvédelmi incidensre