TANSEGÉDLET

ADATVÉDELMI (GDPR) TÉMAKÖRBEN

Szerző:	**Hegyi Zsolt**
	Dr. Csillag Eszter
Szakmai (adatvédelmi) lektor:	**Molnár Gábor**
Nyelvi lektor:	**Köntös Mihály**
Szerkesztő:	**Kamrás Nikolett**
Készült:	**2018. október**

I. kiadás

TARTALOMJEGYZÉK

I.

BEVEZETÉS

2018. május 25-ével a magyar adatvédelemben olyan szabályozás lépett életbe, amely a hozzá kapcsolódó kényszerintézkedések és az eddig példátlanul magas összeget is elérő büntetési tételek fenyegetése miatt komoly hatással bír minden gazdasági szereplőre, aki személyes adatokat kezel.

A vagyonvédelmi / magánbiztonsági területek mindegyike alanyi jogon (a saját alkalmazottak, illetve munkatársak kapcsán) és a szolgáltatásai miatt is egyszerre érintett ezen a területen.

A vagyonvédelmi / magánbiztonsági vállalkozások különösen kiemelt érintettsége azért igényel sürgős kezelést, a tájékoztatástól a jogszabályi megfelelésig, mert a megbízói, megrendelői kör ezen vállalkozásokat és munkatársait tartja szakembereknek, természetesnek veszi, hogy napi munkájuk során az adatvédelmi rendelkezéseknek megfelelően járnak el, így a rájuk bízott területen a már említett hatalmas méretű bírságokkal szemben a szolgáltatásokat igénybe vevő megbízó védett.

A rendészeti feladatokat ellátó személyek, a segédfelügyelők, valamint a személy- és vagyonőrök képzéséről és vizsgáztatásáról szóló 68/2012. (XII. 14.) BM rendelet, amely a vagyonvédelmi ágazat számára előírja az ötévente tartandó kötelező képzést, azért jött létre, hogy a vagyonvédelem minden területén dolgozó, szolgáltatást biztosító vállalkozások munkatársainak szakmai tudása naprakész legyen.

A köznyelvben adatvédelemi, GDPR[1], valamint Infotörvényi[2] szabályozásként elterjedt rendelkezések tartalmával, a szabályozásoknak a szakmai követelmények szerinti napi gyakorlati szintű alkalmazásával alapszinten rendelkeznie kell a 16 órás kiegészítő képzésen résztvevőknek.

Ennek a célnak a megvalósítása érdekében a BM VTTF (Belügyminisztérium Vezetőképzési, Továbbképzési és Tudományszervezési Főosztály) a jogszabályi megfelelés érdekében az

1 Az Európai Parlament és Európai Tanács 2016/679 számú rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről)

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

alábbi adatvédelmi tájékoztatót adja ki az Adatvédelmi Rendeletnek (GDPR) való naprakész megfelelés érdekében.

Az Európai Parlament és Európai Tanács 2016. április 27-én hatályba léptette az Adatvédelmi Rendeletet.

Az Adatvédelmi Rendelet célja, hogy a természetes személyek legfontosabb értékeinek egyikét, a rájuk vonatkozó adatokat, a személyes adatokat védje. Ennek érdekében az EU területére vonatkozóan olyan szabályozást hoztak létre, amelyet minden tagállamban minden külön aktus nélkül alkalmazni kell.

Az alkalmazásra való felkészülésre 2 év állt rendelkezésre, vagyis 2018. május 25-étől kell a rendelkezéseknek megfelelni, azokat alkalmazni. Ide értve a büntetési tételeket is, ami kisebb fokú szabálysértés esetén a cég előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-a vagy 10 millió €, súlyos szabálysértés esetén az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-a vagy 20 millió € is lehet (a nagyobb összeg az irányadó).

A szabályokat a magyar jogalkotó implementálta, vagyis átvezette a magyar szabályozáson, és az adatvédelmet, adatkezelést szabályozó ún. Infotörvénybe beültette. Ennek megfelelően az Adatvédelmi Rendelet előírásait az Infotörvény rendelkezéseivel kiegészítve kell alkalmazni Magyarországon.

A szabályozás lényege, hogy minden természetes személy tudja, hogy az adatait ki kezeli, hogyan kezeli, kinek adja tovább. Erről mindig megfelelő tájékoztatást kapjon és a kezelt adataival kapcsolatban legyen lehetősége rendelkezni.

II.

ÁLTALÁNOS RÉSZ

1. Személyes adatok

A védelem a természetes személyek (érintettek) azon adatait érinti, amely információ alapján közvetlen vagy közvetett módon azonosítható. Ilyen személyes adat különösen: név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó

egy vagy több tényező. Különleges adat a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Egyéb azonosító hiányában nem tartozik önmagában a személyes adatok közé a kép- és hangfelvétel, név, vagy rendszám. Mindezen adat azonban azonnal személyes adattá válik, amint annak alapján egy konkrét természetes személy egyértelműen beazonosíthatóvá válik.

2. Az adatkezelés résztvevői

Adatkezelő az, aki személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja. Az adatfeldolgozó az adatkezelő megbízásából vagy rendelkezése alapján kezeli a személyes adatokat.

Adatkezelésről akkor beszélünk, ha az alkalmazott eljárástól függetlenül az adaton műveletet vagy műveletek összességét hajtják végre, így különösen gyűjtik, felveszik, rögzítik, rendszerezik, tárolják, megváltoztatják, felhasználják, lekérdezik, továbbítják, nyilvánosságra hozzák, összehangolják vagy összekapcsolják, zárolják, törlik és megsemmisítik, valamint az adat további felhasználását megakadályozzák, fénykép-, hang- vagy képfelvétel készítenek, valamint a személy azonosítására alkalmas fizikai jellemzőket (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítik.

A fenti rendelkezések alapján a személy- és vagyonvédelmi tevékenységet végző vállalkozásnak vagy személynek lehet és van olyan tevékenysége, amikor annak végzése során a birtokába került személyes adatot kezeli. Az adatkezelést pedig csak úgy végezheti, ha annak során eleget tesz a jogszabály előírásainak.

Példa: Adatkezelő az a vagyonőr céget megbízó intézmény vagy vállalkozás, amely saját döntése alapján kiszervezi a biztonsági feladatok ellátását egy vállalkozás számára, meghatározva a vállalkozó tevékenységét (őrzés-védelem), feladatainak az ellátását (személyes tevékenység, kamerahasználat).

Nem minősül személyes adatok kezelésének az, amikor a tevékenység végzése során a természetes személy azonosítását lehetővé nem tevő módon kezelnek adatokat. Ilyen eset lehet, amikor a ruhatárban elhelyezett kabát sorszámmal kerül átadás-átvételre.

Adatfeldolgozó az a természetes vagy jogi személy, amely az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.

Példa: Amikor a recepciós tevékenységet ellátó vagyonőr a megbízó informatikai rendszerében rögzíti a belépő személyek adatait.

Címzett az a természetes vagy jogi személy, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz. A címzett a személyes adatot nem használhatja fel.

Példa: Amikor egy elektronikus vagyonvédelmi rendszer felvételét a felügyelet érdekében egy vagyonőr megtekinti, de nem végez adatkezelési tevékenységet.

Harmadik fél az a természetes vagy jogi személy, aki nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek.

Példa: a vagyonőr hibaelhárítást végez a kamerákkal kapcsolatban, de a felvételeket nem tekinti meg.

Az adatkezelési folyamat során egy tevékenység végzése közben egy szereplő akár több adatkezelési szerepkört (adatkezelő, adatfeldolgozó, címzett, harmadik fél) is betölthet.

3. Adatkezelés jogalapja

Személyes adatot csak akkor lehet kezelni, ha annak megvan az alapja:

- az adatkezelés szerződés teljesítéséhez, vagy szerződés megkötéséhez szükséges, ha az érintett az egyik fél,
- az adatkezelés jogi kötelezettség teljesítéséhez szükséges, vagyis jogszabály írja elő,
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges,
- az adatkezelés közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges,
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges (kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett jogai, amelyek személyes adatok védelmét teszik szükségessé),
- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.

A rendelkezésére bocsátott személyes adatot nem lehet önkényesen harmadik személynek továbbadni, csak abban az esetben, ha az adatokat kifejezetten ezzel a céllal kezelik és az érintettet megfelelően tájékoztatták. Ez azt jelenti, hogy pl. a beléptetésnél felírt nevet a megbízó részére át lehet adni (hiszen a megbízó az adatkezelő, akinek a megbízása alapján a vagyonőr adatfeldolgozóként az adatot kezeli, és ebből a célból gyűjti és rögzíti az adatot, amiről a belépésnél az érintett megfelelő tájékoztatást is kell, hogy kapjon), de a következő belépő személynek már nem lehet megmutatni a korábbi belépők adatait.

4. Érintett jogai

Az adatkezeléssel kapcsolatban az érintettnek a következő jogai vannak:

Előzetes tájékozódáshoz való jog: jogosult az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapni.

Ennek keretében az érintett részére az adatkezelő köteles a személyes adatok kezelésére vonatkozó valamennyi információt és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal nyújtani.

Az adatkezelő az alábbi információkat kell az érintett részére megadja:

- az adatkezelő és – ha valamely adatkezelési műveletet adatfeldolgozó végez – az adatfeldolgozó megnevezését és elérhetőségeit,
- a tervezett adatkezelés célját,
- az érintettet megillető jogok, valamint azok érvényesítési módjának ismertetését,
- az adatkezelés jogalapját,
- a kezelt személyes adatok megőrzésének időtartamát, ezen időtartam meghatározásának szempontjait,
- a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek körét,
- a kezelt személyes adatok gyűjtésének forrását,
- az adatkezelés körülményeivel összefüggő minden további érdemi tényt,
- ha az adatokat nem az érintettől gyűjtötték be, akkor a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak,
- azt, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az

érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.

Hozzáféréshez való jog: jogosult arra, hogy kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa.
Az érintettet kérelmére, az adatkezelő tájékoztatja az alábbiakról:

- a kezelt személyes adatok forrása,
- az adatkezelés célja és jogalapja,
- a kezelt személyes adatok köre,
- a kezelt személyes adatok továbbítása esetén az adattovábbítás címzettjeinek köre,
- a kezelt személyes adatok megőrzésének időtartama, ezen időtartam meghatározásának szempontjai,
- az érintettet megillető jogok, valamint azok érvényesítési módja,
- profilalkotás alkalmazásának esetén annak ténye és
- az érintett személyes adatainak kezelésével összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményei, azok hatásai és az azok kezelésére tett intézkedések.

Helyesbítéshez való jog: jogosult arra, hogy kérelmére személyes adatait az adatkezelő helyesbítse, illetve kiegészítse.
Ha az adatkezelő által kezelt személyes adatok pontatlanok, helytelenek vagy hiányosak, azokat – különösen az érintett kérelmére – haladéktalanul pontosítja vagy helyesbíti, illetve ha az az adatkezelés céljával összeegyeztethető, az érintett által rendelkezésére bocsátott további személyes adatokkal vagy az érintett által a kezelt személyes adatokhoz fűzött nyilatkozattal kiegészíti.

Adatkezelés korlátozásához való jog: jogosult arra, hogy kérelmére személyes adatai kezelését az adatkezelő korlátozza.
Az adatkezelő korlátozza az adatkezelést,

- ha az érintett vitatja az adatkezelő által kezelt személyes adatok pontosságát, helytállóságát vagy hiánytalanságát, és a kezelt személyes adatok pontossága, helytállósága vagy hiánytalansága kétséget kizáróan nem állapítható meg, a fennálló kétség tisztázásának időtartamára.

- ha az adatok törlésének lenne helye, de az érintett írásbeli nyilatkozata vagy az adatkezelő rendelkezésére álló információk alapján megalapozottan feltételezhető, hogy az adatok törlése sértené az érintett jogos érdekeit, a törlés mellőzését megalapozó jogos érdek fennállásának időtartamára.
- ha az adatok törlésének lenne helye, de az adatkezelő vagy más közfeladatot ellátó szerv által vagy részvételével végzett, jogszabályban meghatározott vizsgálatok vagy eljárások – így különösen büntetőeljárás – során az adatok bizonyítékként való megőrzése szükséges, ezen vizsgálat vagy eljárás végleges, illetve jogerős lezárásáig.
- ha az adatok törlésének lenne helye, de dokumentációs kötelezettség teljesítése céljából az adatok megőrzése szükséges.
- az érintett 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.

Az adatkezelés korlátozásának időtartama alatt az adatokkal az adatfeldolgozó a tároláson túl egyéb adatkezelési műveletet kizárólag az érintett jogos érdekének érvényesítése céljából vagy jogszabályban meghatározottak szerint végezhet.

Törléshez való jog: jogosult arra, hogy kérelmére személyes adatait az adatkezelő törölje.
Az adatkezelő haladéktalanul törli az érintett személyes adatait, ha

- az adatkezelés jogellenes, így különösen, ha az adatkezelés
  - az alapelvekkel ellentétes,
  - célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához,
  - jogszabályban meghatározott időtartama eltelt, vagy
  - jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja.
- az érintett az adatkezeléshez adott hozzájárulását visszavonja – és az adatkezelésnek nincs más jogalapja – vagy személyes adatainak törlését kérelmezi.
- az adatok törlését jogszabály, a Hatóság vagy a bíróság elrendelte, vagy
- a korlátozásra meghatározott időtartam eltelt.
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre.
- a személyes adatok gyűjtésére gyerekekhez kapcsolódó információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

5. Információbiztonság

Mivel az általunk kezelt adatok egy részét, informatikai környezetben tároljuk, és a GDPR is tartalmaz információbiztonsági előírásokat, fontos, hogy ezen a területen is rendelkezzünk megfelelő ismeretekkel. A vagyonvédelmi / magánbiztonsági vállalkozások fontos feladata ezen előírások közül a fizikai biztonsági előírások betartása, betartatása. Az informatikai környezetben tárolt adatok többféle módon kerülhetnek illetéktelen kezekbe, például:

- Az informatikai eszközök eltulajdonításával (lopás)
- Az adatok jogosulatlan lemásolásával (informatikai bűncselekmény)
- Jogosulatlan hozzáféréssel (illetéktelen személy jut az informatikai eszköz közelébe)

A fent felsorolt eseményeket - az informatikai környezet - megbízó / megrendelő előírásai szerinti kiemelt védelemmel megnehezíthetjük, illetve megakadályozhatjuk.
Kiemelt figyelmet kell fordítani a központi informatikai helyiségek felügyeletére. Ezek például:

- Szervertermek
- Informatikai raktárak
- Telekommunikációs helyiségek
- Elektromos helyiségek (fogadó, elosztó, akkumulátor terem, áramfejlesztő)

A fent felsorolt helyiségekben meg kell akadályozni az illetéktelen, és az engedély nélküli belépést - a megbízó előírásai szerint -, továbbá lehetőség szerint folyamatos felügyeleti és jelzőberendezésekkel kell ellátni ezeket (riasztó, fizikai belépést naplózó rendszer (belépőkártya) – az adatvédelmen túli fizikai védelem: tűzjelző, oltórendszer, hő- és páratartalom ellenőrző).

Magasabb védelmi előírások esetén a megbízó korlátozhatja az informatikai eszközök védett területre történő be- illetve kivitelét. Ilyen előírások esetén a vagyonvédelemi szervezetre hárul ennek az előírásnak a betartatása.

6. Adatvédelmi incidens

Fontos megemlíteni még az adatvédelmi incidens fogalmát és a teendőket. Az adatvédelmi incidens az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt

személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az ilyen incidens esetén az adatkezelőnek haladéktalanul intézkednie kell. Ha az adat jelentős sérelmével járt, akkor az adatkezelőnek 72 órán belül be kell jelentenie az adatvédelmi hatóság, a NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) részére. Ezért fontos, hogy amennyiben adatvédelmi incidens gyanújával kerül szembe, akkor haladéktalanul jelentse azt felettesének, megbízójának, hogy a szükséges intézkedéseket meg lehessen tenni!

III.

SZAKMAI RÉSZ

Vagyonvédelem

1. Kulcskezelés

Amennyiben az irodák kulcsait is a vagyonőrök adják ki a megbízó utasításából, akkor annak nincsen akadálya, hogy egy lapon szerepeljen minden kulcs, és így minden személy lássa a többi kulcs státuszát, mivel ez egy olyan munkáltatói döntés/szabály alapján történik, ami az adatkezelés ezen módját lehetővé teszi (és remélhetőleg a munkáltató ezt megfelelően szabályozta munkavállalói felé). Ebben az esetben a vagyonőr adatfeldolgozó.

2. Beléptetés - recepciós tevékenység

Papíralapú beléptetőrendszer

Az a megoldás nem alkalmazható, amikor egy lapon történik a személyek beléptetése úgy, hogy az adott papírt minden belépő kezébe adják, pl. aláírásra, mivel ebben az esetben minden későbbi belépő láthatja a korábban belépők személyes adatait.

Papíralapú beléptetés csak úgy történhet, hogy a beléptetőpapírt

a) amennyiben aláíratják a belépővel akkor minden belépő vonatkozásában külön készítik el;

b) a beléptetőpapírt nem íratják alá, nem adják át a belépőnek, akkor akár egy lapon is történhet az adminisztráció.

A papíralapú beléptető rendszer esetében a vagyonőr adatfeldolgozó, amennyiben azt a megbízó utasítására és utasítása szerint végzi.

Belépésnél a belépési feltételeket az határozza meg, akihez a belépés történik. Ő határozza meg, hogy a belépő személyt azonosítani kell-e és ha igen, miként, pl. személyi igazolvánnyal. Ebben az esetben a belépéskor a vagyonőr tájékoztatja a belépőt a feltételekről (pl. elkéri személyi igazolványát), és amennyiben a belépő a feltételeknek való megfelelést megtagadja, akkor nem engedi be. Ha a feltételeket teljesíti a belépő (pl. átadja a személyi igazolványát), akkor az adatkezeléshez hozzájárult.

3. Elektronikus beléptetőrendszer

Ha a belépők adatait elektronikus rendszerben rögzítik, akkor a vagyonőr adatfeldolgozó, amennyiben a rendszerben a megbízó utasításából történik a rögzítés.

Biztonságtechnikai tervezés és a telepített rendszerek felügyelete

1. Biztonsági rendszer tervezése, kiépítése, karbantartása

A tervezés, kiépítés során adatkezelés nem valósul meg, a tevékenység végzése önmagában a GDPR szerinti harmadik fél státuszának minősül a kiépített rendszerre nézve, mivel annak üzemeltetésébe, az abban feldolgozott adatokra nézve a tervezőnek és kiépítőnek semmiféle rálátása nincs.

A karbantartás során amennyiben a felvételekbe, vagy az adatokba betekint a vagyonőr, akkor címzetté válik, a megtekintett adatok vonatkozásában a megtekintés idejére.

2. Mechanikai védelem

Mechanikai védelem esetén kizárható, hogy a vagyonőrnek személyes adatok kerüljenek a birtokába, így adatkezelés nem valósul meg.

3. Megfigyelőrendszerek

Amíg a megfigyelőrendszer nem rögzít és nem továbbít semmilyen adatot, csak megfigyel, addig nem történik adatkezelés.

Amennyiben a rendszer rögzít vagy továbbít adatot, akkor az adatkezelésre az általános szabályok az irányadóak.

4. Rögzítőrendszerek

Mindig az az Adatkezelő, aki a rendszert üzemelteti. Amennyiben erre más adott utasítást (megbízó), akkor közös adatkezelés történik. A felvételt visszanéző személy címzett, mivel csak megnézi a felvételt, de nem végez adatkezelési tevékenységet.

Amennyiben a felvételekkel kapcsolatban intézkedésre kerül sor, akkor az adatkezelési státusz a következőképpen alakul: a vagyonőr amennyiben

- a felvételeket rögzíti a megbízó utasításából, akkor adatfeldolgozó,
- a felvételt kimenti a megbízó utasításából, akkor adatfeldolgozó,
- a felvételt továbbítja a megbízó utasításából, akkor adatfeldolgozó,
- a felvételen látott esemény vonatkozásában intézkedik, akkor az intézkedés vonatkozásában adatkezelő.

Ha a kamerák kihelyezéséről, használatáról a vagyonőr döntött, és nem a megbízó, akkor a megbízónak nincs joga a felvételeket megtekinteni, tehát ebben az esetben csak megfelelő indokkal mutathatja meg részére a felvételeket a vagyonőr. A megbízó csak címzett.

5. Behatolásvédelmi rendszerek, személy mozgásának visszaazonosítására alkalmas rendszerek, nyomkövetésre alkalmas egyéb rendszerek

A belépési kódok, belépőkártya kibocsátója és nyilvántartója, a nyomkövetésre alkalmas rendszer üzemeltetője az adatkezelő (általában a megbízó), a vagyonőr szerepe lehet:

- harmadik fél, ha a személyhez rendelt kódokat, a személyhez rendelt belépőkártya személyre vonatkozó személyes adatait, illetve a nyomkövető rendszer vonatkozásában a személyre vonatkozó személyes adatokat nem ismeri és nem is tudja a személlyel összerendelni,
- címzett, ha
    - személyhez rendelten kapja meg a kódokat, a belépőkártya adatait, a helyzeti adatokat, de azokkal semmilyen további tevékenységet nem végez, csak őrzi azokat,
    - a megbízó elektronikus rendszerében a mozgásokat nyomon követi (a képernyőn felvillanó személyes adatok megtekintésével, „élőben”), de azokkal semmilyen további tevékenységet nem végez,
- adatfeldolgozó, ha a belépéseket rögzíti a megbízó utasítása szerint;
- adatkezelő, ha a rögzítés a vagyonőr döntése alapján történik.

ÖNELLENŐRZŐ KÉRDÉSEK

Általános kérdések:

1. Ismertesse, hogy mely jogszabály rendelkezik az adatvédelemről!
2. Ismertesse az adatkezelési folyamatban részt vevő személyeket!
3. Ismertesse az adatkezelési jogalapokat, vagyis mi alapján lehet személyes adatot kezelni!
4. Ismertesse, hogy mikor kell hozzájárulást kérnie az érintett személy adatainak kezeléséhez!
5. Ismertesse az érintett jogait!
6. Ismertesse, hogy mi a teendő, ha az érintett személyes adatainak helyesbítését kéri!
7. Ismertesse, milyen információkat kell az érintett részére megadni, ha tájékoztatást kér a kezelt adatokról!
8. Ismertesse, mit jelent az adatkezelés korlátozása!
9. Ismertesse, hogy milyen jogorvoslati lehetőségei vannak az érintettnek az adatkezelés kapcsán!
10. Ismertesse, mi az adatvédelmi incidens és milyen kötelezettségek keletkeznek általa!
11. Ismertesse, hogy mely informatikai helyiségek kiemelt védelme szükséges!
12. Ismertesse, hogy mi a teendő, ha az őrzött területen egy pendrive-ot, laptopot, telefont, külső merevlemezt (winchestert), személyes adatot tartalmazó dokumentumot, iratot talál!

Vagyonvédelemi kérdések:

1. Ismertesse adatkezelési szempontból, hogy miként kell eljárni a belépők ellenőrzése során!
2. Ismertesse adatkezelési szempontból, hogy miként kell eljárnia akkor, ha a látogatókat regisztrálni szükséges!
3. Ismertesse adatkezelési szempontból, hogy miként kell eljárnia akkor, ha a behajtó gépjárműveket és azok vezetőit ellenőriznie kell!

4. Ismertesse adatkezelési szempontból, hogy miként kell eljárnia akkor, ha a behajtó gépjárműveket és azok vezetőit regisztrálnia kell!
5. Ismertesse adatkezelési szempontból, hogy miként kell a rendszámokat és a gépjárművezetők adatait nyilvántartani!
6. Ismertesse adatkezelési szempontból, hogy milyen szabályokat kell betartania, ha a bevásárlóközpont üzlethelyiségében olyan vásárlót észlel, aki az árut fizetés nélkül a hátizsákjába rejti!
7. Ismertesse adatkezelési szempontból, hogy mire kell tekintettel lenni egy kamera kihelyezésénél!
8. Ismertesse adatkezelési szempontból, hogy a kamerafelvételt kinek lehet megtekintenie és milyen feltételekkel!
9. Ismertesse adatkezelési szempontból, hogy a kamerafelvételt kinek lehet átadni és milyen feltételekkel!
10. Ismertesse adatkezelési szempontból, hogy milyen szabályokat kell betartania, ha egy adott esemény kapcsán tanúval találkozik!
11. Ismertesse adatkezelési szempontból, hogy milyen szabályokat kell betartania, ha munkavégzés közben karambolozik!
12. Ismertesse adatkezelési szempontból, hogy milyen szabályokat kell betartania, ha a rendezvény helyszínén egy személy belépőkártya nélkül kíván a helyszínre bemászni!

MELLÉKLET

Információbiztonság keretében érintett, adatvédelmi incidens alapját képező eszközök bemutatása

Pendrive:






Laptop:



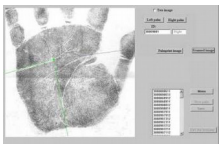
Telefon:


Külső merevlemez:

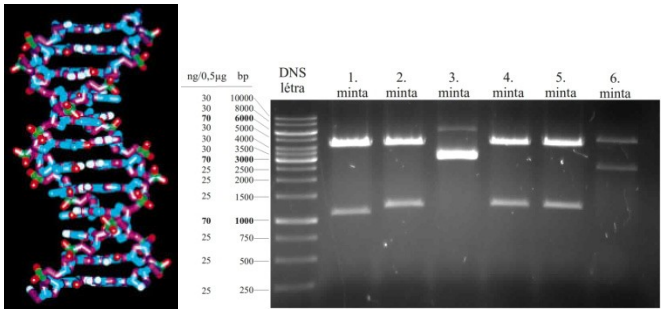

Személyes adatot tartalmazó dokumentum:


Személy azonosítására alkalmas fizikai jellemzők

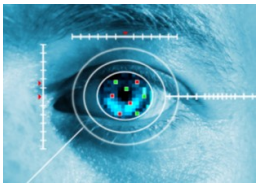
Ujj- vagy tenyérnyomat:

DNS-minta:



Íriszkép:



Felügyeleti és jelzőberendezések

Riasztó:

Fizikai belépést naplózó rendszer (belépőkártya):

Kamera: