WP29

2/2017-es vélemény a munkahelyi adatkezelésről (részlet)

5. Forgatókönyvek (a közösségi médiahasználat munkáltató általi megfigyeléséről)

Ez a fejezet olyan munkahelyi adatkezelési forgatókönyveket vázol fel, melyek során új technológiák vagy már meglévő technológiák továbbfejlesztése magas kockázatú hatással bír a munkavállalók magánéletére. Minden ilyen esetben a munkáltatóknak fontolóra kell venniük a következőket:

- az adatkezelési tevékenységre szükség van-e, és amennyiben igen, meg van-e a kellő jogalap;
- a személyes adatok tervezett kezelése tisztességes a munkavállalókra nézve;
- az adatkezelési tevékenység arányos a felmerült aggályokhoz képest;
- az adatkezelési tevékenység transzparens.

5.1. Adatkezelési műveletek a felvételi eljárás során

A közösségi média használata elterjedt az adatalanyok körében, és viszonylag gyakori, hogy a felhasználói profilok bárki által nyilvánosan megtekinthetők (beállításoktól függően). Ennek eredményeképpen a munkáltatók úgy gondolják, hogy a jelöltek profiljának vizsgálata a munkaerő-toborzási folyamataik során indokoltak. Ez lehet más, nyilvánosan elérhető információ is a potenciális alkalmazottról.

A munkáltatók azonban nem feltételezheti azt, hogy pusztán azért, mert az egyén közösségi média profilja nyilvánosan hozzáférhető, akkor ezeket az adatokat saját céljaikra felhasználhatják. Ehhez az adatkezeléshez jogalap szükséges, például a munkáltató jogos érdeke. Ebben az összefüggésben a munkáltatónak - a közösségi profil ellenőrzését megelőzően - figyelembe kell vennie, hogy a kérelmező közösségi profilja üzleti vagy magáncélhoz kötődik-e, mivel ez fontos információval szolgálhat az adatok ellenőrzésének jogi elfogadhatósága szempontjából. Ezenkívül a munkáltatók annyiban gyűjthetik és kezelhetik a munkakeresők személyes adatait, amennyiben ezeknek az adatoknak a gyűjtése szükséges és releváns azon munka szempontjából, melyre az egyén jelentkezik.

A felvételi eljárás során összegyűjtött adatokat általában törölni kell, amint világossá válik, hogy nem adnak konkrét munkavégzésre vonatkozó ajánlatot, vagy a jelölt azt nem fogadja el.[1] Az egyént is megfelelően tájékoztatni kell minden ilyen adatkezelésről, mielőtt a munkaerő-felvételi folyamat megkezdődik.

A munkáltatónak nincs jogalapja arra, hogy megkövetelje a potenciális munkavállalóktól, hogy ”ismerősnek jelölje” a potenciális munkáltatót, vagy más módon hozzáférést biztosítson az egyén a profiljához.

Példa
„Új munkatársak felvétele során a munkáltató ellenőrzi a jelöltek profilját a különféle közösségi hálózatokon, és az ezekről a hálózatokról szerzett információkat beépíti a szűrési folyamatba.

A fenti eljárás csak annyiban lehetséges, amennyiben a munkakör betöltése különleges funkcióval bír, az egyén alkalmazása különleges kockázattal jár és ezt szükséges előzetesen felmérni, és a pályázó

[1] Lásd még a témakörben: Recommendation CM/Rec(2015)5of the Committee of Ministers to member Stateson the processing of personal data in the context of employment (https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a)

megfelelően tájékoztatva van erről (pl. a hirdetés szövegében). Így a munkáltatónak meg lehet a jogalapja az Adatvédelmi Irányelv 7. Cikk (f) pontja szerint arra, hogy a pályázó nyilvánosan elérhető profilján található személyes adatokat áttekintése."

5.2. Adatkezelési műveletek munkahelyi átvilágítások során

A közösségi média profilokon, valamint az új analitikus technikák kifejlesztése révén a munkáltatóknak meg van a lehetőségük arra, hogy folyamatosan ellenőrizzék alkalmazottaikat barátaikon keresztül, nyomon kövessék véleményeiket, hitüket, érdekeiket, szokásaikat, tartózkodási helyüket továbbá viselkedésükkel kapcsolatos egyéb információkat gyűjthetnek. A személyes és családi életre vonatkozó adatok - ideértve a szenzitív adatokat is - rögzíthetnek.

A munkavállalók közösségi médiaprofiljainak munkahelyi átvilágítása nem szabad, hogy általános művelet legyen.

Továbbá a munkáltatóknak tartózkodniuk kell a munkavállalónak vagy pályázónak az arra való felkérésétől, hogy biztosítsanak hozzáférést olyan információhoz, amelyeket megosztottak másokkal a közösségi hálózatokon keresztül.

Példa
„A munkáltató figyelemmel kíséri azon korábbi alkalmazottak LinkedIn profiljait, akik részt vesznek a munkáltatóval korábban kötött versenytilalmi megállapodásban. A megfigyelés célja az ilyen megállapodások betartásának ellenőrzése. A megfigyelés csak ezekre a korábbi alkalmazottakra korlátozódik.

Amíg a munkáltató bizonyítani tudja, hogy az ilyen jellegű ellenőrzés jogos érdekeinek védelméhez szükséges, valamint nincs más, kevésbé invazív eszköz, és hogy a korábbi munkavállalók megfelelően tájékoztatva lettek a jövőbeni, megállapodás idejére korlátozódó megfigyelésről, hivatkozhat az Adatvédelmi Irányelv 7. cikk f) pontjában rögzített jogalapra.

Ezenkívül a munkavállalóknak nem szabad szükségszerűen igénybe venniük azon közösségi média profilt, amelyet a munkáltatójuk biztosít számukra. Még akkor is, ha ez kifejezetten a feladataik (pl. egy szervezeten belüli szószóló) vonatkozásában került előírásra, meg kell tartaniuk a "nem a munkahelyhez kapcsolódó" nem publikus profilt, elválasztva a "hivatalos", a munkáltatóval kapcsolatos profiltól, és ezt a munkaszerződésben is meg kell határozni."

5.3. Az infokommunikációs technológia alkalmazásának megfigyelésével kapcsolatos adatkezelési műveletek

Hagyományosan az elektronikus kommunikáció (pl. telefon, internetes böngészés, e-mail, azonnali üzenetküldés, VOIP stb.) megfigyelése, nyomon követése volt a legfőbb fenyegetés a munkatársak magánéletére. Az elektronikus hírközlés munkahelyi megfigyeléséről szóló 2001. évi WP29-es Munkadokumentumban a WP29 számos következtetést vont le az e-mail és internethasználat ellenőrzésével kapcsolatban. Bár e a következtetések továbbra is érvényesek, figyelembe kell venni azokat a technológiai fejlesztéseket, amelyek lehetővé tették az újabb, potenciálisan behatolóbb és átfogóbb megfigyelési módszereket. Ilyen fejlesztések közé tartozik többek között:

- adatvesztés-megelőzésére (DLP) szolgáló eszközök, melyek felügyelik a kimenő kommunikációt a lehetséges visszaélések felderítésének megelőzésére;
- az új generációs tűzfalak (NGFWs) és az Unified Threat Management (UTM) rendszerek, amelyek számos megfigyelési technológiát kínálhatnak, beleértve a TLS lehallgatást, weboldal szűrést, tartalomszűrést, „on-appliance" jelentéstételt, felhasználói azonosító adatokat és

(amint azt fentebb leírtuk) adatvesztés-megelőzést figyelő programok. Az ilyen technológiákat a munkáltatótól függően egyénileg is fel lehet használni;
- biztonsági alkalmazások és intézkedések, amelyek magukban foglalják a munkavállalók hozzáférésének a munkáltatói rendszerbe való bejutását;
- az eDiscovery technológia, amely minden olyan folyamatra utal, amelyben az elektronikus adatokat keresik annak érdekében, hogy azokat bizonyítékként felhasználhassák;
- az alkalmazás és az eszközhasználat nyomon követése láthatatlan szoftveren keresztül, akár az asztalon, akár a felhőben;
- office alkalmazások felhőszolgáltatásként történő biztosítása a munkahelyen, amely elméletileg lehetővé teszi az alkalmazottak tevékenységének nagyon részletes naplózását;
- a személyes eszközök (pl. PC-k, mobil eszközök, telefonok, táblagépek) megfigyelése, amelyeket az alkalmazottak egy adott felhasználási irányelvnek megfelelően használnak, például a Bring-Your-Own-Device (BYOD), valamint a Mobile Device Management (MDM) technológia alkalamzásán keresztül, és más hordozható eszközök (például egészségügyi és fitnesz eszközök) megfigyelése.

Lehetséges, hogy a munkaadó egy "all-in-one" felügyeleti megoldást valósít meg, amely lehetővé teszi, hogy figyelemmel kísérje minden infokommunikációs technológia munkahelyen történő alkalmazását A WP55-ben elfogadott következtetések bármely olyan rendszerre vonatkoznak, amely lehetővé teszi az ilyen jellegű átfogó ellenőrzést.[2]

Példa
„A munkáltató egy TLS (Transport Layer Security, titkosítási protokoll) ellenőrző készülék telepítését tervezi, hogy visszafejtsék és ellenőrizzék a biztonságos adatfolyamot, azzal a céllal, hogy bármilyen esetleges rosszindulatú beavatkozást észleljenek. A készülék képes továbbá rögzíteni és elemezni a munkavállaló online tevékenységének egészét a szervezet hálózatán.

A titkosított kommunikációs protokollok használatát egyre inkább a személyes adatok lehallgatás elleni védelme érdekében alkalmazzák. Azonban ez is problémákat vethet fel, mivel a titkosítás lehetetlenné teszi a bejövő és kimenő adatok ellenőrzését. A TLS megfigyelő eszköz dekódolja az adatfolyamot, biztonsági célból ellenőrzi a tartalmat, majd utána újra titkosítja a folyamatot.

Ebben a példában a munkáltató jogos érdekeire hivatkozik - a hálózat védelmének szükségessége, valamint az e hálózatban tárolt alkalmazottak és ügyfelek személyes adataihoz való illetéktelen hozzáférés vagy adatszivárgás megelőzése. Azonban a munkavállaló minden online tevékenységének figyelemmel kísérése aránytalan reakció és a magántitokhoz való jogot is sértheti. A munkáltatónak először meg kell vizsgálnia más, kevésbé invazív eszközök alkalmazásának lehetőségét is.

Amennyiben a TLS forgalom bizonyos szintű lehallgatását feltétlenül szükségesnek ítélik, a készüléket oly módon kell beállítani, hogy megakadályozza a munkavállalói tevékenység időkorlát nélküli naplózását, például a gyanús bejövő vagy kimenő forgalom blokkolásával és a felhasználó átirányításával egy információs portálra, ahol kérheti az ilyen típusú automatizált döntés felülvizsgálatát. Ha bizonyos általános naplózást szigorúan szükségesnek ítélünk meg, a készüléket úgy is beállíthatjuk, hogy ne tárolja a naplóadatokat, hacsak a készülék nem jelzi az esemény bekövetkezését, és minimálisra csökkenti az összegyűjtött információkat."

Jó gyakorlatként a munkáltató alternatív, nem ellenőrzött hozzáférést kínálhat a munkavállalóknak. Ez biztosítható lehet ingyenes WiFi, vagy önálló eszközök vagy terminálok (megfelelő biztosítékokkal a kommunikáció titkosságának biztosításával) rendelkezésre bocsátásával, ahol a munkavállalók

[2] Lásd még a témakörben: Copland v United Kingdom, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (http://www.bailii.org/eu/cases/ECHR/2007/253.html)

gyakorolhatják az őt megillető jogaikat, nevezetesen hogy munkahelyi eszközöket bizonyos magáncélra használhassák.[3] Ezen kívül a munkáltatóknak figyelemmel kell lenniük bizonyos típusú forgalmakra, amelynek monitorozása veszélyezteti a munkáltatói jogos érdek és a munkavállalók magánélet védelméhez való jogának megfelelő egyensúlyát - például a magán email használatát, az online banki és egészségügyi weboldalak látogatását - azzal a céllal, hogy megfelelően állítsa be az eszközöket úgy, hogy ne történjen megfigyelés olyan körülmények esetén, melyek nem arányosak a munkáltató-munkavállaló viszonyát illetően. Az alkalmazottaknak tudomására kell hozni, hogy a munkahelyi készülékek milyen jellegű használata kerül rögzítésre vagy megfigyelésre.

Szükség van egy kidolgozott szabályzatra, mely a gyanús naplózás adatokhoz való hozzáférés jogait szabályozza, és egyszerű és tartós hozzáférhetőség kell minden munkavállaló számára annak érdekében, hogy a hálózat elfogadható és elfogadhatatlan használatát is megismertesse velük. Ez lehetővé teszi az alkalmazottak számára, hogy megfelelően alkalmazkodjanak, és tudják, mely magatartásuk kerül rögzítésre és mely nem. Így a munkahelyen jogszerűen használhatják az informatikai eszközöket magáncélra. Jó gyakorlatként egy ilyen munkahelyi szabályozást legalább évente felül kell vizsgálni annak érdekében, hogy a választott megfigyelési megoldás hozza-e a tervezett eredményeket, és van-e más, kevésbé invazív eszköz ugyanarra a célra.

Az adott technológia vagy az általa biztosított technológiai megoldástól függetlenül az Adatvédelmi Irányelv 7. cikk f) pontjában található jogalap csak akkor lehetséges, ha az adatkezelés bizonyos feltételeknek megfelel. Először is, a munkaadóknak ezekkel az eszközökkel kapcsolatban figyelembe kell venniük az arányosság kritériumát, és hogy tesznek-e további lépéseket az adatkezelés mértékének és hatásának mérséklésére vagy csökkentésére. A helyes gyakorlat példájaként ezt a megfontolást egy DPIA-n, azaz adatvédelmi hatásvizsgálat útján lehet végrehajtani, mielőtt bármilyen monitoring technológia bevezetésre kerülne. Másodszor, a munkaadóknak létre kell hozniuk bizonyos felhasználási politikákat, szabályzatokat az adatvédelmi szabályzatokkal együtt, amelyek körvonalazzák a szervezet hálózatának és felszerelésének megengedett felhasználását, és részletezik a feldolgozást.

Néhány országban egy ilyen szabályzat létrehozása jogilag megköveteli a munkavállalók érdekcsoportjának vagy a munkavállalók hasonló képviseletének jóváhagyását. A gyakorlatban az ilyen szabályzatokat többnyire az IT-ért felelős személyzet dolgozza ki. Mivel a fő hangsúlyt leginkább a biztonságra és nem a munkavállalók magánéletének védelmére, jogaik biztosítására helyezik, a WP29 azt ajánlja, hogy minden esetben a munkavállalók bizonyos reprezentatív száma vegyen részt ezek kialakításában, valamint ezek rendszeres értékelése során is.

Példa
„A munkáltató egy adatvesztést megelőző eszközt telepít a kimenő e-mailek automatikus ellenőrzésére a tulajdonosi adatok (pl. az ügyfelek személyes adatainak) illetéktelen átvitelének megakadályozása céljából, függetlenül attól, hogy egy ilyen művelet véletlenszerű-e vagy sem. Amennyiben egy e-mailt adatvédelmi incidens potenciális forrásának tekintik, további vizsgálatot végeznek.

Ismét megjegyezzük, hogy ebben az esetben is a munkáltató a jogos érdekére hivatkozik az ügyfelek személyes adatainak védelme, valamint eszközeinek jogosulatlan hozzáférés vagy adatszivárgás elleni védelme esetén. Ilyen adatvesztést megelőző eszköz azonban szükségessé teheti a személyes adatok kezelését, feldolgozását – például egy "hamis" riasztás jogosulatlan hozzáférést eredményezhet olyan e-mailekhez, amelyeket az alkalmazottak küldtek (például személyes, magánélethez köthető e-mailekhez).

[3] Lásd bővebben: Halford v. United Kingdom, [1997] ECHR 32, (http://www.bailii.org/eu/cases/ECHR/1997/32.html)

Ezért az adatvesztést megelőző eszköz szükségessége és annak telepítése teljes mértékben indokoltnak kell lennie, hogy megfelelő egyensúlyt teremtsen jogos érdek és a munkavállalók személyes adatainak védelméhez való alapvető jog között. Annak érdekében, hogy a munkáltató jogos érdekei támaszkodhasson, bizonyos intézkedéseket kell hozni kockázatok enyhítésére. Például a szabályok, melyek alapján a rendszer egy e-mailt potenciális adatvédelmi incidens forrásának tekinti, teljes mértékben átláthatónak kell lennie a felhasználók számára, és abban az esetben, ha az eszköz felismeri a problémás e-mailt, figyelmeztető üzenetet kell küldenie a küldőnek, hogy visszafordíthassa a küldési folyamatot."

Bizonyos esetekben az alkalmazottak megfigyelése nemcsak az adott technológiák telepítése miatt lehetséges, hanem egyszerűen azért, mert a munkavállalóktól elvárás, hogy a munkáltató által rendelkezésre bocsátott online alkalmazásokat használják, amely személyes adatokat kezel. Ilyen például a cloud-szolgáltatás alapú eszközök (például dokumentumszerkesztők, naptárak, közösségi hálózatok) használata. Biztosítani kell, hogy az alkalmazottak bizonyos privát tereket jelölhessenek ki maguknak, amelyekhez a munkáltató csak kivételes körülmények között férhet hozzá. Erre példa a naptárak használata, amelyeket gyakran alkalmaznak a privát, magánélethez kapcsolódó találkozók szervezésére is. Ha a munkatárs beállítja a "Privát" jelzést bizonyos bejegyzésekhez, a munkáltatónak (és más alkalmazottainak) nem szabad engedélyezni a hozzáférést.

A szubszidiaritás követelménye ebben az összefüggésben néha azt jelenti, hogy egyáltalán nem lehet megfigyelést végezni. Például ez az eset áll fenn akkor, amikor a kommunikációs (Chat, Messenger stb.) használatát bizonyos webhelyek letiltásával korlátozzák. Amennyiben van lehetőség arra, hogy munkáltató weboldalakat blokkoljon, az összes kommunikáció folyamatos nyomon követése helyett, a szubszidiaritás követelményének való megfelelés érdekében ezt kell választani.

Ezen túlmenően a megelőzésnek sokkal nagyobb súlyt kell kapnia, mint a felderítésnek - a munkáltató érdekeit jobban szolgálja az internet nem megfelelő használatának technikai eszközökkel való megelőzése, nem pedig erőforrások kiszélesítésével hogy felderítsék a szabályellenes felhasználást.