GOBERT ÉS TÁRSA
ÜGYVÉDI IRODA

Róbert Károly krt. 70-74., B ép. 8. em.
1134 Budapest
MAGYARORSZÁG
Telefon + 36 (1) 270 9900
Telefax + 36 (1) 270 9990
office@gfplegal.com

A BWSP GOBERT ÉS TÁRSA ÜGYVÉDI IRODA

GDPR HÍRLEVELE

KÜLÖNKIADÁS

Budapest

2018

A GDPR ALKALMAZÁSA A GYAKORLATBAN - ITT AZ IDŐ A TERVEZÉSRE!

Felkészülés az új európai általános adatvédelmi rendeletre Magyarországon

A privát szféra védelme különösen kiemelt szerepet fog kapni a közvetlenül alkalmazandó Európai Parlament és Tanács 2016/679 általános adatvédelmi rendeletével (**GDPR**). Az új rendelet a személyes adatok kezelését nem szabályozza kevésbé szigorúan és csekélyebb jelentőséggel, mint egyfajta új gazdasági erőforrás birtoklását. Hasonlóan vélekedik erről a magyar hatóság, ugyanis a Nemzeti Adatvédelmi és Információbiztonsági Hatóság (**NAIH**) munkatársai szakmai berkeken belül tartott előadásaikon rendszerint úgy nyilatkoznak, hogy „az adat nem más, mint az információs társadalom olaja". Az EU 28 tagországában közvetlenül alkalmazandó és nemzeti jogszabályokat felülíró GDPR-t Magyarországon az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (**Infotv.**) rendelkezéseivel, más ágazati jogszabályokkal, valamint a magyar adatvédelmi hatóság gyakorlatával együtt értelmezve kell alkalmazni 2018. május 25-étől minden Magyarországon székhellyel rendelkező vállalkozás napi működése során a digitalizált és papír alapú rendszerbe foglalt adatkezeléseknél. A GDPR rendelkezései azonban nem csak az EU tagállamaiban tevékenységi központtal rendelkező vállalkozásokat érintik, a GDPR hatálya ugyanis kiterjed azon EU-n kívüli tevékenységi központtal rendelkező adatkezelő vállalkozásokra is, amelyek adatkezelési tevékenysége áruknak vagy szolgáltatásoknak az EU bármely tagállamának területén tartózkodó érintettek számára történő nyújtásához kapcsolódik, vagy amely vállalkozások adatkezelési tevékenysége természetes személyek EU területén belüli viselkedésének megfigyeléséhez kapcsolódik (pl. profilalkotás, személyes preferenciák előrejelzése, netes nyomon követés stb.).

Az új európai adatvédelmi szabályozásra való **felkészülés komplex jogi és információtechnikai intézkedéseket igényel**, amit nem lehet elég korán kezdeni. A hatályba lépés napjától az európai adatvédelmi hatóságok példátlanul magas, akár 20 millió euró vagy a cég előző éves világpiaci forgalma 4%-ának megfelelő összegű bírság kiszabására is jogosultak lesznek. Mindez azt jelenti, hogy gyökeresen meg fog növekedni a jogszabályoknak való nem megfelelés pénzügyi kockázata az EU területére kiterjedően adatkezelést végző vállalkozások számára.

I. MIT TARTALMAZ EGY HATÉKONY AKCIÓTERV A GDPR-RA FELKÉSZÜLÉS SORÁN?

Felmerül a kérdés, pontosan mit tehetünk a GDPR-nak megfelelő adatvédelmi és adatbiztonsági szint eléréséhez a következő pár hónapban és hogyan minimalizálhatjuk cégünk pénzügyi kockázatát? Irodánk vezető partnerei az alábbi akció tervet javasolják, melyet irodánk adatvédelmi szakértői a GDPR-ra felkészítő szolgáltatáscsomagunk keretében dolgoztak ki:

1. A jelenlegi céges adatkezelési gyakorlat és adatvédelmi dokumentáció adatvédelmi szempontú átvilágítása (auditálás, hatásvizsgálat, informatikai átvilágítás, adattérkép);

2. Megfelelőségi vizsgálatok, érdekmérlegelési tesztek, adatvédelmi szintek kialakítása az új GDPR szerinti adatkezelési jogalapokra, az adatkezeléshez való hozzájárulásokra, érintettek jogainak biztosítására, incidensek kezelésére, álnevesítésre és egyéb adatvédelmet érintő céges gyakorlatokra vonatkozóan;

3. A GDPR-nak megfelelő jogi dokumentációk elkészítése (pl. munkavállalói és ügyfél szabályzatok, tájékoztatók, hozzájárulási nyilatkozatok, formanyomtatványok, incidenskezelési terv, információbiztonsági szabályzat, stb.);

4. Az érintettek megfelelő tájékoztatását biztosító jogi dokumentáció és eljárások kidolgozása, adattérkép aktualizálása és folyamatos monitoringja;

5. A cég honlapjának adatvédelmi szempontú felülvizsgálata, átdolgozása és kialakítása;

6. A „Privacy by Design" alapelv jogszabály által elvárt adatvédelmi biztonsági gyakorlatok beépítése a cég működésébe és IT rendszerébe;

7. Adatfeldolgozói szerződés minta és kockázatértékelési eljárások kialakítása a szerződéses partnerek kiválasztási folyamatára vonatkozóan;

8. Felhő alapú adattárolások jogi megfelelőségének vizsgálata és GDPR megfelelőség kialakítása;

9. Gyermekek jogainak különös védelmét szolgáló eljárások, intézkedések kidolgozása;

10. Adatvédelmi tisztviselő kinevezéséről való intézkedés, amennyiben ezt a GDPR kötelezően előírja a vállalkozás esetében;

11. Bejelentési kötelezettség alá eső adatkezelések bejelentése a NAIH-hoz az új szabályozásnak megfelelően 2018. május 25. előtt és után;

12. Cégvezetők és adatkezelést végző munkavállalók oktatásának biztosítása cégen belül, adatvédelmi tudatosság fokozása, cégen belül felhasználható e-learning tesztek és vizsgaanyag kialakítása;

13. A NAIH-hal folyamatos kapcsolattartás, érdekmérlegelési tesztek jóváhagyatása, előzetes hatásvizsgálatok lefolytatása;

14. Kötelező belső adatvédelmi nyilvántartások kidolgozása;

15. Cégcsoporton belüli Kötelező Erejű Szervezeti Szabályozás kidolgozása; a Privacy Shield-ben résztvevő cégek ellenőrzése;

16. Céges működés folyamatos monitorozása az adatvédelmi szabályozásnak való megfelelés szempontjából.

II. MIT ÉRDEMES MINDENKINEK TUDNI A GDPR RENDELKEZÉSEIRŐL?

Személyes adatok kezelőjének, ún. „adatkezelőnek" minősül és így a GDPR szabályainak betartására köteles minden vállalkozás, amely természetes személyektől bármilyen kapcsolat során személyes adatokat vesz fel, gyűjt, felhasznál vagy tárol, vagyis a működő vállalkozások 99%-a. Ha egy cég a GDPR-ban meghatározott bármely adatkezelési tevékenységet végzi Magyarországra kiterjedően, szem előtt kell tartania a GDPR szabályait, a nemzeti adatvédelmi jogszabályokat és a szigorú NAIH gyakorlatot.

A GDPR a „személyes adat" fogalmát az eddigi Európai irányelvnél és a nemzeti szabályozásnál tágabban értelmezi. A GDPR szerint ugyanis **személyes adat bármilyen természetes személyre vonatkozó információ, amivel a személy közvetlen vagy közvetett módon azonosítható lehet**. Személyes adatnak minősül ennek megfelelően nemcsak bármely természetes magánszemély (**érintett**) neve, személyi igazolvány száma, születési helye, e-mail elérhetősége, képmása vagy hangfelvétele, hanem az érintettek szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó bármely ismeret, az érintettek által használt gépjárművek GPS vagy a telefonjaik adatai, mint helymeghatározó adatok, vagy a munkahelyi böngészési adataik, sőt még az IP címek, cookie-k is. **A GDPR-ral jelentősen bővült személyes adatok adatvédelem-tudatos kezelését hogyan végezhetjük gyakorlatban úgy, hogy az előírásoknak maradéktalanul megfeleljünk?** – kérdezik tőlünk rendszeresen ügyfeleink. Mindezen személyes adatoknak még a megtekintéséhez (azaz megismeréséhez) is vállalaton belüli adatkezelési szabályzatra, a munkavállalói monitoring (pl. internethasználat, céges telefon, kamera használat, GPS) formáira vonatkozó tájékoztatásra és szabályzatokra, adatkezelési nyilvántartásra, illetve egy jogszerű célra és utólagos igazolhatóságra lesz szükség, amely követelmények betartása 2018. május 25-től kritikus fontosságú lesz.

Az új adatvédelmi szabályozás egyik központi eleme az adatkezelések célszerűsége, a célhoz kötöttség alapelve. Ez azt jelenti, hogy minden egyes adatkezelés valamilyen konkrét célt kell szolgáljon, vagyis ha egy cég nem tudja utólag is igazolni a konkrét, körülhatárolt jogszabályoknak megfelelő célt a személyes adatok gyűjtésére, tárolására vonatkozóan, jelentős a veszélye, hogy adatkezelési gyakorlata jogi aggályokat vet fel. **A GDPR-ra való felkészülés egyik első kulcsfontosságú lépése, hogy a vállalkozások egyes adatfelvételeinek jelenlegi céljait felül kell vizsgálni a GDPR-ban rögzített elvek szerint.** A célhoz kötöttség alapelve mellett a szükségesség és céllal arányosság követelménye is kiemelt szerepet kap. Ezen felül kiemelten kell vizsgálni a GDPR-ban új,

különösen érzékeny adatkörök, így pl. az egészségügyi vagy a biometrikus (pl. arckép, ujjlenyomat), illetve a genetikai adatok kezelését. A NAIH szerint az ilyen adatok kezelése kizárólag különösen fontos érdekből történhet modern beléptető rendszerek esetén is, ami a NAIH jelenlegi álláspontja szerint nem lehet csekélyebb, mint hogy a beléptető mögötti helyiségben „halálos vírust vizsgálnak".

A GDPR-ra való felkészülés során kiemelt figyelmet kell szentelni az adatkezelési gyakorlat megfelelő jogalapok szerinti felülvizsgálatára is. **Az új szabályozás szerint az adatkezelések jogalapja az érintett önkéntes hozzájárulása vagy jogszabályi előírás, illetve egyéb új jogalapok pl. jogos érdek, közérdekű, közhatalmi jogosítványuk gyakorlása egyike lehet.** Az új jogalapok közül kiemelendő a jogos érdek, azaz a GDPR szerint az adatkezelő vagy harmadik fél jogos érdeke is indokolhatja az adatkezelést. A gyakorlatban várhatóan gyakran alkalmazandó ezen jogalap munkaviszonnyal összefüggésben, illetve szerződés megkötéséhez, illetve teljesítéséhez szükséges adatkezelésnél.

A GDPR alkalmazása alatt a vállalkozások vezetőinek és adatkezelést végző munkavállalóinak kifejezetten tisztában kell majd lenniük az érintettek jogaival (tájékoztatási, helyesbítési, törlési jog stb.), hiszen az érintetti jogok tiszteletben tartása a vállalkozás, mint adatkezelő oldalán továbbra is kötelezettségként jelenik meg.

III. MILYEN TIPIKUS ADATKEZELÉSI TEVÉKENYSÉGEKKEL TALÁLKOZHAT EGY VÁLLALKOZÁS?

Az alábbiakban kifejtett valamennyi vállalkozás által végzett mindennapi műveletek adatkezelésnek minősülnek, ezért az alábbiakban összefoglaltuk praktikus és gyakorlati tanácsainkat 2018. május 25-e utánra GDPR megfelelőség szempontjából.

1. Információkérés, ajánlatkérés, időpontfoglalás kezelése, állásra pályázók önéletrajzai

Az adatkezelések teljes folyamatára és az időtartamára is vonatkozik a célhoz kötöttség, a szükségesség és céllal arányosság követelménye. A NAIH gyakorlata szerint, ha pl. akár egy információkérést, ajánlatkérést, időpontfoglalást (és ezzel az ügyfelek személyes adatait), vagy állásra pályázó önéletrajzát tartalmazó e-maillel nincs már több teendője egy vállalkozásnak, azokat azonnal törölni szükséges a cég összes adatbázisából. Bár egy-egy időpontfoglalás esetén az ügyfél nevét, illetve telefonszámát rendszerint felírjuk, a rendeltetésük megszűnésével ezeket a személyes adatokat is elvileg azonnal törölni kell az adatbázisokból, kivéve, ha igazolni tudjuk, hogy a vállalkozásnak jogos érdeke fűződik az adatok megtartásához, vagy kifejezetten hozzájárult kérésünkre az érintett, hogy megtartsuk az adatokat a cél megszűnése után is.

2. Kamerarendszer üzemeltetése

Fontos tudni, hogy kamerarendszer jelenleg és a GDPR hatályba lépésétől közterületen, magánterületen, illetve munkahelyen a munkavállalók megfigyelésére kizárólag garanciális szabályok betartása és az érintettek, munkavállalók megfelelő tájékoztatása mellett építhető ki. Munkahelyi kamerarendszerrel különösen nem megengedett a magánéletét megfigyelés alatt tartani (tilos pl. munkahelyi pihenőhelyre, dohányzásra kijelölt helyre kamerákat építeni), vagy a munkavégzésüket befolyásolni a kamerákkal.

A kamerarendszerek kiépítésekor azért kell különösen figyelemmel lenni az adatvédelmi szabályoknak való megfelelésre, mert a NAIH az adatkezelésekhez kapcsolódó szükségesség és arányosság elvét a gyakorlatban alkalmazva az ,,aránytalanul túlfigyeltnek" minősített területből vagy helyiségből is, így pl. egy hotel recepciójáról bírság kiszabása mellett leszereltetheti az általa a cél eléréséhez már nem szükséges, feleslegesnek ítélt kamerákat (pl. 4 kamerából csak 2 kamera megtartását engedélyezi a helyiségben). A kamerafelvételek felhasználás hiányában 3 napig őrizhetőek meg, speciális esetekben ez 30 vagy 60 napig lehetséges a személy- és

vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény szerinti feltételek fennállása esetén.

Amennyiben egy vállalkozás mégis használ kamerákat, erre vonatkozóan minden esetben szükséges a kamerázott területre belépő érintetteknek szóló és megfelelő a NAIH által javasolt mellékletekkel ellátott kameraszabályzat létrehozása. A NAIH szerint mindenkinek, tehát minden épületbe belépő személynek, ügyfélnek és munkavállalónak joga van megismerni belépés előtt a rá vonatkozó kameraszabályzatot. További kérdést vethet fel a gyakorlatban és az egyes esetek konkrét körülményeinek függvényében mérlegelendő, hogy a kamerák által belátott képek (pl. egy bank belső helyiségei) üzleti titoknak minősülhetnek-e.

A GDPR-nak megfelelő adatkezelés kialakításának emellett részét kell képezze egy ún. „**érdekmérlegelési-megfelelőségi teszt**”. Az érdekmérlegelési-megfelelőségi teszt lényege, hogy az adatkezelőnek fel kell tennie magának a kérdést különösen a jogos érdekből végzett adatkezeléseknél, hogy az adatkezelésre ténylegesen szükség van-e és össze kell vetnie saját érdekeit az érintettek érdekeivel. A tesztet igazolhatóan kiálló és a NAIH által is jóváhagyott adatkezelési eljárások megvalósítása ajánlott a gyakorlatban.

Az adatkezelés megkezdése előtt az érintetteknek mindenképpen elérhetővé kell tenni a tájékoztatókat, szabályzatokat a vállalkozás honlapján vagy akár papír alapon. Kamerahasználat esetén a megfigyelt helyiségeken belül minden egyes területen matricával, tájékoztató táblával kell jelezni, hogy az kamera látóterében van. A munkahelyen való kamerás megfigyelőrendszer üzemeltetése esetén a NAIH szigorúan megköveteli a munkavállalók részletes előzetes tájékoztatását a konkrét megnevezett cél (semmiképpen sem az ő megfigyelésükre!) közlésével.

3. Panaszkezelés

A jelenleg hatályos fogyasztóvédelmi jogszabályok szerint 5 évig kötelező tárolni a panaszkezeléssel kapcsolatban kezelt adatokat. Ezen időtartamon azonban a közeljövőben változtathat a magyar Országgyűlés által jelenleg tárgyalt törvénymódosítási javaslat.

4. Hírlevél küldése

A hírlevelek küldésének jogalapja az önkéntes és kifejezett hozzájárulás lehet, amelyet az érintettek a hírlevélre való feliratkozáskor adnak meg. A GDPR rendelkezései szerint a vállalkozásoknak tudni kell majd bizonyítaniuk az egyes hozzájárulások megtörténtének tényét, ezért a hozzájárulások megadásának elektronikus vagy papír alapú dokumentációját minden esetben meg kell őrizni.

A hírlevelekkel kapcsolatban Magyarországon EU-s viszonylatban is szigorú a magyar adatvédelmi hatóság álláspontja. A NAIH állásfoglalása szerint a cégek a szükségesség-arányosság elvének megfelelve az ügyfelek nevét, e-mail címét gyűjthetik és tarthatják nyilván hírlevelek küldésének céljából a hozzájárulás időpontjával párosítva. Kivételt képezhet ez alól, ha a hírlevélben közzétett tartalmat csak 18 éven felüliek tekinthetik meg, ilyen esetben a születési dátum is kezelhető. Ha a vállalat hírlevelek küldésével kapcsolatban ennél több adatot kezelt, 2018. május 25-ig tisztázni ajánlott az eddig alkalmazott hírlevél-adatbázist.

A NAIH állásfoglalása alapján további jogi és gyakorlati kérdéseket vet fel egy honlapot működtető vállalkozásnál, hogy pl. weboldalon elektronikus feliratkozás esetén a jelölőnégyzetet („checkbox”) minden esetben megfelelő formátumú-e, biztosított-e a leiratkozás, beleértve a postai úton történő leiratkozást is az adatkezelő által megadott címen, rendszeres-e a NAIH szerint javasolt adatbázis frissítés.

5. Nyereményjáték

A nyereményjátékot indító cégek általában adatkezelőnek, míg pl. a nyereményjáték lebonyolításával megbízott marketinges cégek rendszerint az adatkezelők utasítása alapján az adatokkal dolgozó szervezeteknek, ún.

„adatfeldolgozónak" minősülnek. Az adatfeldolgozókat a GDPR rendelkezései alapján az adatkezelőkhöz hasonló szintű felelősség, illetve bírság kockázata fogja terhelni az adatvédelmi szabályok betartásával kapcsolatban. A nyereményjátékok jelenleg bejelentés köteles adatkezelési tevékenységek, amelyeket elektronikus úton minden esetben regisztrálni kell a NAIH on-line nyilvánosan elérhető adatvédelmi nyilvántartásában. Szükséges emellett kialakítani egy adatvédelmi és egy nyereményjáték-szabályzatot is, amelyeket nyilvánosan hozzáférhetővé kell tenni (pl. weboldalon vagy oda vezető linken).

6. Állásra pályázók és munkavállalók adatainak kezelése

A céghez állásra pályázók, illetve a cégnél munkát vállalók adatainak kezelésének megkezdése előtt minden esetben az érintettek előzetes, részletes, körültekintő írásbeli tájékoztatása szükséges. Hangsúlyozni kell, hogy a GDPR fényében a munkáltató cégek a pályázók kifejezett előzetes hozzájárulása hiányában a sikertelen jelentkezők önéletrajzát nem tárolhatják a kiválasztás lezárulása után. A munkáltatók szintén nem kérhetnek be különleges adatokat (pl. erkölcsi bizonyítvány) a jelentkező hozzájárulása hiányában amennyiben a munkakör jellegéhez az nem kifejezetten indokolt. A munkáltatóknak különös fokozott körültekintése javasolt az adatkezelés során, amely megfelel az alábbiakban részletezett, az adatkezelő kötelezettségeivel, illetve az érintettek jogainak érvényesítésével kapcsolatos követelményeknek.

IV. MILYEN KÖTELEZETTSÉGEI VANNAK AZ ADATKEZELŐNEK?

Az adatkezelők kötelezettségei és az érintettek jogai a GDPR-ral jelentősen bővülni fognak 2018. május 25-től. Alábbi összefoglalónkban összegyűjtöttük azokat a lényeges adatkezelői kötelezettségeket, amelyeket az adatkezelők kötelesek betartani a GDPR szerint.

1. Előzetes tájékoztatás kötelezettsége

Az érintetteket megillető előzetes tájékoztatáshoz való jog nem új keletű, azonban a GDPR fokozottan megkívánja, hogy az minden adatkezelésnél teljes körű legyen kiterjedve többek között a célra, jogalapra, adattárolás idejére, jogorvoslati jogokra, adatbiztonságra, adatvédelmi tisztviselő kapcsolattartási adataira, adattovábbításra és adatfeldolgozókra vonatkozó információra. Az adatkezelőnek tudnia kell igazolnia egy esetleges hatósági vizsgálat esetén azt, hogy az adatkezelést megelőzően megtörtént az érintett részletes, előírásoknak megfelelő tájékoztatása az adatkezeléssel kapcsolatban.

Hozzájáruláson alapuló adatkezelésnél a GDPR egyik újdonsága, hogy a személyes adatok kezeléséhez az érintett „**önkéntes és kifejezett**", bármikor visszavonható aktív magatartással tett hozzájárulását írja elő, mint követelményt. Az előírás gyakorlati alkalmazására vonatkozóan általános gyakorlati javaslatunk az adatkezelő vállalkozások számára, hogy az adatfelvétel előtt az érintettek lehető legrészletesebb, lehetőleg írásbeli, utólag igazolható módon történő tájékoztatása mellett szerezzék be az írásbeli hozzájárulásukat, illetve őrizzék is meg azt egy esetleges adatvédelmi hatósági vizsgálat esetére. A GDPR mellett a NAIH is szigorú gyakorlati követelményeket támaszt az előzetes tájékoztatáson alapuló hozzájárulás tekintetében, különösen a weboldalas „checkbox" módszer és hangfelvételek esetén.

A GDPR-nak való megfelelés egyik kulcsa a megfelelő tájékoztatók, illetve szabályzatok készítése. A GDPR-nak megfelelő tájékoztatók, szabályzatok tartalmának lényeges, irodánk adatvédelmi szakértői által javasolt minimális elemei:

- Ha NAIH bejelentés köteles az adatkezelés, mi az adatkezelés bejelentésének száma?
- Ki az adatkezelő?
- Mi az adatkezelés célja?
- Mi az adatkezelés jogalapja?
- Mennyi ideig kezeli az adatkezelő az adatokat?

- Hogyan, milyen módon zajlik az adatok kezelése?
- Kik és mely munkavállalók férnek hozzá az adatokhoz és pontosan mikor, milyen esetekben jogosultak a hozzáférésre?
- Az adatkezelő milyen adatfeldolgozókat használ?
- Történik-e EU-n kívüli adattovábbítás?
- Az érintettnek milyen jogai vannak és azokat milyen módon érvényesítheti?
- Van-e Adatvédelmi Tisztviselő és milyen esetekben fordulhat hozzá az érintett?
- Milyen adatbiztonsági intézkedések és eljárások vannak hatályban az adatkezelőnél?
- Mi az incidenskezelési eljárás folyamata az adatkezelőnél?

2. NAIH nyilvántartásba vételi kötelezettség és az adatkezelések belső nyilvántartása

Jelenleg bizonyos típusú adatkezeléseket, néhány kivétellel, kötelező bejelenteni a NAIH által vezetett adatvédelmi nyilvántartásba. Ettől függetlenül a GDPR kötelezettségként előírja az adatkezelők, illetve adatfeldolgozók számára, hogy vezessenek az adatkezelésekről belső nyilvántartást is.

A 250 munkavállalónál kevesebbet foglalkoztató szervezetek nem kötelesek nyilvántartást vezetni, kivéve, ha kockázatos vagy nem alkalmi jellegű adatkezelést folytatnak, vagy ha ún. „**különleges adatokat**" (így pl. faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra vonatkozó, genetikai, biometrikus, esetleg egészségügyi adatokat) vagy büntetőjogi felelősségre vonatkozóadatokat kezelnek.

3. Adattovábbítások nyilvántartása

A GDPR a jelenleg is hatályos szabályokhoz hasonlóan, megfelelő adatbiztonsági szintet biztosító garanciális feltételek teljesülése esetén teszi lehetővé az adattovábbítást harmadik országba vagy nemzetközi szervezet részére. Változatlan a nemzeti adatvédelmi jogszabályok alapján, hogy az adatokat továbbító adatkezelőknek automatikusan vagy munkavállaló által vezetett naplóval minden esetben nyilván kell tartaniuk.

A GDPR szerint az adattovábbítás tagállami hatósági jóváhagyása nem szükséges speciális GDPR szerinti adattovábbítási garanciák (pl. nemzeti hatóságok által jóváhagyott Kötelező Szervezeti Szabályozás) megléte esetén. Egyéb, adatkezelő és harmadik országbeli vagy nemzetközi szervezeten belüli adatfeldolgozó szervezetek közötti megállapodások alapján is biztosítható a jogszerű adattovábbítás, amennyiben a nemzeti adatvédelmi hatóság külön engedéllyel jóváhagyja ezen szerződéses rendelkezéseket az adatbiztonsági szint garanciájaként.

Ezen garanciák és a GDPR szerinti további garanciák hiányában, amennyiben a Bizottság hivatalosan megállapítja, hogy egy adott ország megfelelő adatvédelmi szintet biztosít, nincs szükség ilyen engedély kérése, azonban ilyen minősítésű ország egyelőre nem létezik.

4. Adatvédelmi incidensek nyilvántartása

A GDPR bevezeti az adatvédelmi incidens fogalmát, lényege az adatkezelési rendszer biztonságának olyan sérülése, amely az adatokhoz való jogosulatlan hozzáférést, vagy az adatok jogellenes megsemmisítését eredményez (pl. a cég nyilvántartását hackerek törik fel; ha máshoz jut el egy e-mail vagy egy levél; eltűnik egy munkahelyi laptop). Adatvédelmi incidens esetén az adatkezelőket bejelentési, nyilvántartási és tájékoztatási kötelezettség is terhelni fogja a GDPR szerint az alábbi időrendben:

1. **Gyors hatásvizsgálat**, amelynek eredményeképpen, ha megállapításra kerül, hogy a biztonság sérülése az érintetteknek potenciálisan jelentős sérelmet okozhat, illetve az adatvédelmi incidens jelentős adatvédelmi kockázatot jelent, a vállalkozás köteles megtenni az alábbi második és harmadik lépést.

2. **72 órán belül bejelentés a NAIH felé** arról, hogy az adatkezelő biztonsági rendszere sérült. A bejelentésnek tartalmaznia kell az adatvédelmi incidens leírásán kívül azt is, hogy mit tett az adatkezelő a kockázatok és károk elhárítása, illetve a későbbi hasonló adatvédelmi incidensek megelőzése érdekében.

3. **Érintettek tájékoztatása** a valószínűsíthetően magas kockázattal járó adatvédelmi incidens megtörténtéről. Az adatkezelőnek minden érintettet tájékoztatnia kell világos és közérthető módon, amely magában hordozza azt a jogi kockázatot az adatkezelők számára, hogy az érintettek személyes adataik védelméhez való joguk megsértése miatt sérelemdíjat követelnek a vállalkozástól bíróság előtti polgári peres eljárásban.

5. Belső adatvédelmi tisztviselő kinevezése

A GDPR szerint egyes esetekben kötelező lesz az adatvédelem területén szakértelemmel rendelkező, független ún. „adatvédelmi tisztviselő" alkalmazása a vállalkozásoknál 2018. május 25-étől:

1. ha az adatkezelést közhatalmi, közfeladatot ellátó szervek végzik,
2. **ha az adatkezelő, illetve adatfeldolgozó fő tevékenysége összefügg személyes adatok rendszeres és szisztematikus, nagymértékű megfigyelésével**, vagy
3. ha különleges adatokat, vagy az érintettek büntetőjogi felelősségének megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatokat kezel a szervezet.

A fenti esetkörök közül kiemelendő a második, amely különösen rugalmasan értelmezhető és a vállalkozások jelentős részét érintően felveti a kérdést, hogy pontosan milyen típusú adatkezelést végző vállalkozásokra vonatkozik. A második esetkörben annak eldöntésében, hogy az adott adatkezelés a vállalkozás fő tevékenységéhez kapcsolódik-e, a cégjegyzékben megtalálható tevékenységi körök szolgálnak iránymutatásul, így ezen GDPR előírásnak a mentén biztosítani köteles lesz adatvédelmi tisztviselőt foglalkoztatnia pl. a marketing ügynökségeknek, bankoknak, biztosítóknak, a telefon- és internet-szolgáltatóknak.

6. Kötelező Erejű Szervezeti Szabályozás (Binding Corporate Rules, BCR), Svájc/EU-USA Adatvédelmi Pajzs

Az EU tagállamain kívüli országba történő adattovábbítások előfeltétele, hogy a két ország között garanciák biztosítsák a megfelelő adatvédelmi szintet. A megfelelő adatvédelmi szintet biztosító garanciák egyike cégcsoportok számára a helyi adatvédelmi hatóságok által engedélyezett Kötelező erejű Szervezeti Szabályozás elfogadása, amely alapján a cégcsoport vállalatai vállalják a GDPR megfelelést, tehát gyakorlatilag magukra kötelezőnek fogadják a GDPR rendelkezéseit.

A fentihez hasonlóan hatékony eszköz lehet a Svájc/EU-USA adatvédelmi pajzshoz (**Privacy Shield**) való csatlakozás, amely a transzatlanti kereskedelmi kapcsolatok esetében megoldást jelenthet az üzleti partnereknek a Svájcból / EU-ból Amerikába való adattovábbításoknál. A Privacy Shield-hez csatlakozó amerikai vállalatoknak tehát akkor továbbítható adat az EU-ból vagy Svájcból, ha a GDPR megfelelést biztosító Privacy Shield alapelveket magukra nézve kötelező erejűnek elismerik. A Privacy Shield-ben résztvevő vállalatok listája itt ellenőrizhető: www.privacyshield.gov/welcome.

7. Adatvédelmi szabályoknak megfelelő napi működés folyamatos biztosítása, Privacy by Design alapelv

A GDPR újdonságként bevezeti a sajtóban ma már sokat hallott „Privacy by Design" gondolkodásmód általános követelményét, az adat minimalizálás elve mellett. Ezen elvek megvalósításához folyamatosan monitorozni szükséges a vállalat működését adatvédelmi és adatbiztonsági szempontból. **Mindez folyamatos adatvédelmi hatásvizsgálat futtatását fogja jelenteni különösen pl. új termékek, szolgáltatások kifejlesztésekor,**

tervezésekor, kiválasztásakor vagy felhasználásakor. **A gyakorlatban ezen a követelmények a vállalatok működésének folyamatos auditálását fogja jelenteni.**

V. MILYEN JOGOK SEGÍTIK ELŐ AZ ÉRINTETTI JOGGYAKORLÁST?

A GDPR az érintettek számára az alábbi új és megújult jogosultságokat biztosítja, amelyek érvényesíthetőségének elősegítése szintén az adatkezelők és adatfeldolgozók kötelezettsége lesz.

1. Tájékoztatás és hozzáférés joga

Az érintettek jogosultak lesznek az adatkezelőktől részletes dokumentációt kérni a rájuk vonatkozó, illetve az általuk az adatkezelők rendelkezésére bocsátott adatok kezeléséről. Az érintettnek átadott dokumentációnak tartalmaznia kell, hogy történt-e személyes adatkezelés és amennyiben igen, az érintettre vonatkozó konkrét adatokon kívül, többek között az egyes adatkezelési célokat, az adatkezelés időtartamát, adatfeldolgozókat, esetleges adattovábbítás esetén a címzetteket, jogorvoslati jogokat, illetve amennyiben ilyen történt, az automatizált profilalkotás tényét is. Az érintettek kérése esetén a személyes adataiknak legalább egy másolatát ingyenesen a rendelkezésükre kell bocsátani.

2. Elfeledtetés joga

A GDPR szerinti „elfeledtetés joga" a törléshez való joghoz képest többletjogosultságot fog jelenteni az érintettek számára, amely értelmében az adatkezelő köteles késedelem nélkül törölni a személyes adatokat, ha a GDPR-ban meghatározott esetek valamelyike fennáll. Eszerint, az adatkezelő az érintett kérésére még a biztonsági mentésekből, illetve esetleges másodpéldányokból is köteles lesz törölni a személyes adatokat, különösen pl. akkor, ha az adatkezeléshez való hozzájárulást az érintett még gyermekként adta meg, vagy az adat elavult és kezelése már nem szükséges vagy az adatkezelés jogellenes.

Az érintettet a kérésére történt intézkedésekről tájékoztatni kell. Ha az adatkezelő esetleg nyilvánosságra hozta vagy más adatkezelőnek vagy adatfeldolgozónak továbbította a személyes adatokat, nem elég az adatokat a saját adatbázisaiból törölnie, hanem köteles ezeket az adatkezelőket, illetve adatfeldolgozókat is tájékoztatni az érintett kéréséről és intézkedni a személyes adatok maradéktalan törlése érdekében. A GDPR által bevezetett elfeledtetés joga az adatkezelők ezzel kapcsolatos széleskörű kötelezettségei miatt hatékony eszközt fog jelenteni valamennyiünknek, de pl. azon munkavállalók a számára, akik az általuk még gyermek- vagy ifjú korukban on-line közzétett képeket, információkat szeretnék maradéktalanul eltávolítani.

3. Adathordozhatóság joga

Automatizált adatkezelés esetén egyes esetekben (ha a vállalkozás által végzett adatkezelés jogalapja önkéntes hozzájárulás vagy szerződés teljesítéséhez szükséges a kezelt adat) az érintetteket megilleti az adathordozhatóság joga. Az adathordozhatóság joga alapján az érintettek kérhetik az adatkezelőtől, hogy a rájuk vonatkozó adatokat, illetve az általuk az adatkezelők rendelkezésére bocsátott adatokat küldje el számukra, illetve azt, hogy az adatkezelő továbbítsa azokat egy másik, az érintett által meghatározott adatkezelőnek pl. egyik bank a másiknak fiókváltás esetén. Az adatokat az érintett, illetve a címzett szervezet számára géppel olvasható formátumban, strukturáltan kell kiadnia vagy továbbítania. A GDPR az adathordozhatóság jogának érvényesítését azzal segíti elő, hogy bevezeti az „interoperatibilitás", azaz a szervezetek közötti adatkezelési együttműködést mint új általános követelményt az automatizált adatkezelést végző adatkezelőkkel szemben.

4. A GDPR fellép a profilalkotás ellen

A GDPR egyik újdonsága, hogy kifejezetten fellép a profilalkotás, vagyis az ellen a jelenség ellen, hogy egyes adatkezelők a közösségi oldalakról és más adatbázisokból automatikusan gyűjtött viselkedésre, preferenciákra utaló

információkból következtetéseket vonnak le érintettekre vonatkozóan, azaz profilt alkotnak, illetve ez alapján hajtanak végre műveleteket. Profilalkotásnak fog minősülni a GDPR rendelkezései szerint pl. amikor biztosítók, bankok, fejvadászok betáplálják az általuk közösségi oldalakról (Facebook, LinkedIn) begyűjtött információkat a rendszereikbe és ezek automatikus feldolgozásának eredményeként megállapítják, hogy mekkora összegű biztosítást, hitelt adjanak az érintetteknek vagy eldöntik, milyen típusú állásokra lehetnek alkalmasak. A GDPR alkotói a profilalkotás szabályozása során számoltak azzal, hogy ezek a profilalkotásra alkalmas informatikai rendszerek, algoritmusok folyamatosan fejlődnek és a jelenlegi alkalmazásuknál jóval nagyobb szerepük lehet a jövőben. Éppen ezért a GDPR hatályba lépésétől a profilalkotás csak megfelelő garanciák mellett lesz végezhető, az adatkezelőnek biztosítania kell nemcsak a profilalkotást megelőző tájékoztatást az érintettek számára, hanem a tiltakozás, illetve a törlés lehetőségét is az érintettek erre vonatkozó kérése esetén.

A HR célú profilalkotási gyakorlattal kapcsolatban fontos szem előtt tartani, hogy a NAIH arra az álláspontra helyezkedett az utóbbi években, hogy a munkavállalók, állásra jelentkezők monitorozása a Facebook profiljukon, egyéb közösségi oldalakon keresztül csak akkor megengedett, ha ennek a tényét a munkaadó előzetesen feltüntette az álláshirdetésben, illetve ha a profilalkotás tényéről a munkakereső, illetve munkavállaló előzetesen tájékoztatva volt. Gyakorlati javaslatunk ezzel kapcsolatban, hogy mindenképpen érdemes pl. e-mailben megerősítést kérni az adatok kezelésére és tárolására vonatkozóan.

A GDPR által bevezetett egyik új adatkezelési jogalap a „jogos érdek", amelyre hivatkozással szintén lehetőség nyílik egyes esetekben szűkebb keretek között jogszerű módon a profilalkotásra és amelynek kulcs eleme az adatkezelőnek a profilalkotás konkrét céljához mint adatkezelési célhoz fűződő jogos érdekének szem előtt tartása. Ennek egyik gyakorlati példája, amikor fejvadász cégek üzletszerzési célból kezelhetnek személyes adatokat (pl. az érintett által a LinkedIn profilján közzétett, korábbi munkahelyekre és szakmai tapasztalatokra vonatkozó személyes adatokat). Ennek azonban szintén előfeltétele, hogy a profilalkotást végző vállalkozás köteles az érintettek figyelmét felhívni az adatkezelés tényére, illetve biztosítani az érintettek jogai érvényesítésének lehetőségét.

5. Álnevesítés: ajánlott adatvédelmi gyakorlat a GDPR szerint

Az „álnevesítés" a GDPR rendelkezéseiben egyik tételesen szereplő ajánlott adatvédelmi gyakorlat, amellyel az adatkezelő, illetve adatfeldolgozó csökkentheti az adatkezelés kockázatát, illetve eleget tehet GDPR szerinti kötelezettségeinek. Az álnevesítési művelet lényege, hogy az érintett egy további, külön tárolt adat hiányában nem azonosítható be többé a személyes adat alapján. Eszerint, az adatkezelő az egyes személyes adatokat egy kóddal pl. „JGH789" azonosítja, illetve kapcsolja össze. A személyes adatokat az összekapcsolás után csak a kóddal helyettesíti az egyes nyilvántartásokban vagy dokumentumokban, és az összekapcsolást tartalmazó, „dekódoló" nyilvántartáshoz - így pl. akár egy Excel táblázathoz, amelynek egyik oszlopában a személyes adatok, másik oszlopában a kódok vannak - a hozzáférési jogosultságokat a lehető legminimálisabb mértékre, pl. egyetlen illetékes munkavállalóra vagy az adatvédelmi tisztviselőre szorítja.

6. Az adatkezelő vállalkozások elszámoltathatósága és átláthatósága a GDPR alapján

Gyakran fordulnak irodánk ügyfelei adatvédelmi szakértő kollégáinkhoz azzal a kérdéssel, hogy mit fog jelenteni a gyakorlatban a GDPR által az adatkezelők részére előírt elszámoltathatóság és átláthatóság követelménye. Az adatkezelőknek az elszámoltathatóság követelménye alapján mindenkor tudniuk kell majd bizonyítani pl. dokumentumokkal és nyilvántartásokkal az adatvédelmi hatóság esetleges vizsgálata esetén, hogy az adatkezelés jogszerűen történt. Az adatkezelők ennek érdekében kötelesek a „megfelelő technikai és szervezési intézkedések" végrehajtására, vagyis a dokumentációs és jogi kötelezettségeket az információ technológiai eljárások bevonásával kell teljesíteni.

Az adatkezelések átláthatóságát egyszerű, tömör és jól érthető tájékoztatók, szabályozások, illetve szükség esetén ábrák, a NAIH által is támogatott táblázatok, szabványosított ikonok kell elősegítsék, amelyek könnyen elérhetővé

teszik az érintettek számára az adatkezelés folyamatát és jellemzőit. Az átláthatóság követelményének betartása kulcsfontosságú lesz, ha az adatkezelő kifejezetten gyermekekre vonatkozó adatokat gyűjt.

VI. MI ELLEN VÉDI A VÁLLALATOKAT A GDPR SZERINTI MEGFELELŐSÉGI TANÚSÍTVÁNY?

A GDPR lehetőséget ad a tagállamok adatvédelmi hatóságainak, illetve meghatalmazott szervezeteinek - Magyarországon a NAIH-nak -, hogy olyan ún. tanúsító szervezeteket akkreditáljanak, amelyek a piaci igényekhez alkalmazkodva vállalják a vállalatok működésének adatvédelmi szempontú átvilágítását, és az átvilágítás eredményeként tanúsítványt állítsanak ki a GDPR-nak megfelelő működésről. Ilyen szervezetek, vállalkozások várhatóan lesznek Magyarországon is. Jelenleg még egy ilyen akkreditált GDPR megfelelőségi tanúsítványt kiállító szervezet sem jelent meg a piacon, amelyet irodánk folyamatosan figyelemmel kísér.

A tanúsítvánnyal kapcsolatban fontos kiemelni, hogy annak vállalat általi megszerzése pusztán azt fogja garantálni, hogy a NAIH nem indít hivatalból, azaz külön érintetti panasz nélkül is vizsgálatot az adatkezelő ellen. Mindez már nem teljesül, ha érintetti panasz érkezik a tanúsítvánnyal rendelkező cég ellen. Nem lesz tehát elegendő a tanúsítvány megszerzése és mindenkor a GDPR-nak megfelelő működést kell fenntartani.

VII. KÖTELEZŐ HATÁSVIZSGÁLAT ÉS KÖTELEZŐ ELŐZETES KONZULTÁCIÓ A NAIH-HAL?

Kötelező lesz konzultálniuk a Magyarországon adatkezelést végző vállalkozásoknak a NAIH-hal abban az esetben, ha egy-egy adatkezelés előtti - szintén kötelező - belső hatásvizsgálat eredménye azt mutatja, hogy a még nem bevezetett adatkezelés figyelemmel annak jellegére, hatókörére, körülményére és céljaira valószínűsíthetően magas kockázattal járna az érintett személyek jogai és szabadságai szempontjából. Az előzetes adatvédelmi hatósági konzultációnak mint új, GDPR által bevezetett jogintézménynek még egyáltalán nincs gyakorlata Magyarországon.

Fontos tudni emellett az előzetes konzultáció hordozta kockázatokról is. A GDPR rendelkezései alapján az előzetes konzultáció során a NAIH nemcsak tanácsot adhat írásban a vállalkozásoknak, hanem az előzetes konzultáció eredeti tárgyával kapcsolatban akár más adatkezelésekre is kiterjedő vizsgálatot indíthat a vállalkozás ellen, illetve a vizsgálat lefolytatása után utasíthatja, figyelmeztetheti vagy bírságolhatja is a vállalkozást bármilyen jogsértés észlelése esetén.

VIII. HOGYAN KERÜLJE EL CÉGE A REKORD ÖSSZEGŰ BÍRSÁGOKAT?

A GDPR 2018. május 25-től lehetőséget fog biztosítani minden tagállami adatvédelmi hatóságnak, így a NAIH-nak is, hogy hatósági vizsgálatot követően a vállalkozásra jogsértés észlelése esetén az adatvédelmi szabályok megsértésének súlyosságát, a jogsértés szándékos vagy gondatlan jellegét, időtartalmát és más szempontokat viszonylag szabadon, a GDPR biztosította tág keretek között mérlegelve bírságot szabjon ki. A NAIH **egyes enyhébb esetekben 10 millió euró (több, mint 3 milliárd forint) vagy a vállalat teljes előző éves világpiaci forgalma 2 %-ának** megfelelő összegű bírságot szabhat majd ki (pl. ha elmulasztja a vállalkozás az adatvédelmi incidens bejelentését a NAIH felé, vagy megsérti a Privacy by Design követelményét a működése során), **illetve egyes súlyosabb esetekben 20 millió euró (több, mint 6 milliárd forint) vagy a vállalat teljes előző éves világpiaci forgalma 4 %-ának megfelelő összegű bírság** megfizetésére kötelezheti a vizsgált vállalatot (pl. ha megsérti a GDPR alapelvi rendelkezéseit, az érintettek hozzájárulását nem az előírásoknak megfelelően szerzi be, ha nem megfelelő jogalapra hivatkozással, esetleg jogalap hiányában kezel adatokat). A GDPR ezzel lehetőséget biztosít a tagállami adatvédelmi hatóságoknak olyan rendkívüli mértékű bírság vagy bírságok kiszabására is, amely komoly következményekkel járhat akár a világpiaci nagyvállalatok működésére is. Különböző adatkezelési eljárások nem megfelelősége esetén ugyanis bírság akár többször is kiszabható.

A FENTIEK ALAPJÁN UGYE ÖNNEK SEM KÉRDÉS, HOGY ELJÖTT A FELKÉSZÜLÉS IDEJE?

A bírság kockázata elkerülésének érdekében még mindig nem késő elkezdeni, illetve felgyorsítani az akár hónapokat is igénylő felkészülést az új európai adatvédelmi rezsimre. De mit lehet, mit kell tenni pontosan ennek érdekében? – teszi fel magának a kérdést a következő hónapokban minden felelős vállalatvezető.

Cégcsoportok esetén, amennyiben a GDPR implementáció az anyavállalat országából kerül lebonyolításra (pl. US, Németország), a helyi adatvédelmi jogi szakértői tanácsadás ebben az esetben is megkerülhetetlen. Magyarországon az új IT rendszerek, szabályzatok, érdekmérlegelési-tesztek, Kötelező Szervezeti Szabályozás és az adatkezelés valamennyi aspektusa meg kell feleljen a GDPR-nak, a szigorú Infotv.-nek és a még szigorúbb NAIH gyakorlatnak. **A GDPR rendelkezései alapján tehát, ha új IT rendszerek, új adatkezelési- feldolgozási módszerek kerülnek bevezetésre, a multinacionális cégek hazai leányvállalatainak 99%-a nem tudja elkerülni az adatvédelmi hatásvizsgálatot és a kötelező előzetes NAIH konzultációt.**

Az első javasolt lépés mindenképpen a vállalat működésének adatvédelmi szempontú átvilágítása: meg kell vizsgálni a vállalatnak nemcsak az alkalmazott adatkezelési eljárásait, a ténylegesen végzett adatkezelési műveleteit és adatbiztonsági intézkedéseit, hanem a rendelkezésre álló adatvédelmi dokumentációt is (milyen szabályzatokkal és tájékoztatókkal rendelkezik már az adatkezelő, vannak-e eljárásrendek adatbiztonsági okokból, az adatvédelmi szabályoknak mennyire megfelelőek a munkaszerződések stb.).

A GDPR alkalmazására való felkészüléshez emellett fel kell térképezni informatikai oldalt is. Be kell építeni az egyes adatkezelési műveletekhez illeszkedő megfelelő garanciákat a szabályzatok betartására, szükség esetén új szabályzatokat és eljárásokat kell kialakítani.

Ha kötelező, adatvédelmi tisztségviselőt kell kinevezni a vállalatnál. A szabályzatok kialakítása után azokat nemcsak publikálni kell, hanem oktatás keretében meg is kell ismertetni a munkavállalókkal.

Összességében: eleget kell tenni a jogszabályi kötelezettségeknek és általában növelni kell az adatvédelmi jogi tudatosságot a vállalat mindennapi működése során annak érdekében, hogy egy érintett se nyújtson be panaszt a NAIH-hoz a személyes adataik nem megfelelő kezelése miatt, vagy ha panasz kerül benyújtásra is kerül, megfelelő válaszokat tudjunk adni a hatóságnak a vizsgálat folyamán és az bírság kiszabása nélkül záruljon. A GDPR rendelkezéseinek való nem megfelelés valós és jelentős anyagi kockázatokat hordoz az adatkezelő vállalatok számára. **A kockázatok azonban elkerülhetőek, amelynek érdekében irodánk vezető partnerei és adatvédelmi szakértői együtt dolgoznak azon, hogy a lehető legtöbb vállalatnál minél hamarabb megtörténjen a kockázatok felmérése adatvédelmi audittal, és ügyfeleink a lehető legmagasabb felkészültségi szintre jussanak 2018. május 25-ig.**

A GDPR alkalmazására való felkészüléssel kapcsolatban felmerülő bármilyen kérdés esetén adatvédelmi jogi szakértőink bármikor szívesen állnak vállalkozása rendelkezésére az alábbi elérhetőségeken:

Dr. Arne Gobert
Irodavezető Partner, Ügyvéd
arne.gobert@gfplegal.com

Dr. Réka Ipacs
Partner, Ügyvéd, Képzett Adatvédelmi Tisztviselő
réka.ipacs@gfplegal.com

Dr. Francis-Hegedűs Veronika
Ügyvéd, Adatvédelmi Csoport Vezetője
veronika.francis-hegedus@gfplegal.com