

A KKV-k tapasztalatai a GDPR alkalmazásával kapcsolatban

I. Felkészülés az új adatvédelmi rendelkezések alkalmazására

1. A felkészülés időszakai

a) A felkészülés előzményei és a GDPR alkalmazásának kezdete körüli időszak; 2016-2018

A GDPR rendelkezéseinek alkalmazására történő felkészülés - a viszonylag hosszú, két éves időintervallum ellenére – csak viszonylag lassan indult. A GDPR rendelet 2016. május 25-i hatályba lépését követő időszakban a vállalkozások vagy nem is értesültek megfelelően ezen kötelezettségükről vagy bizonytalanok voltak abban, hogy pontosan mit is kellene tenniük a felkészülés érdekében, ráadásul még nagyon távolinak tűnt az az időszak, amikor ténylegesen számon kérhetőek lesznek ezen kötelezettségek. Emellett nem minden esetben látták át, hogy valójában a tevékenységük mely részét érinti a rendelet, mi számít személyes adatnak és milyen esetekben, milyen körben kell foglalkozniuk a kérdéssel. A bizonytalanságuk fő oka elsősorban az ismerethiányból alakult ki.

A kamarai hálózat közvetlen kapcsolatban áll a vállalkozásokkal és folyamatosan igyekeznek megfelelő tájékoztatással, képzésekkel segíteni a KKV-k tevékenységét. Ezért a felkészülési időszakban is számos GDPR rendelettel kapcsolatos képzést, konferenciát szerveztek, ahol számos visszajelzés érkezett a vállalkozások részéről az ezen kötelezettségükhöz való viszonyulásukról, és magáról a felkészültségükről. Tapasztalataik szerint a KKV-k jelentős része ekkor még úgy gondolta, hogy:

- Az ő cége nem is kezel személyes adatokat.
- Náluk minden rendben van az adatkezelés terén.
- Illetve voltak olyanok is, akik az adatvédelmi szabályok bevezetését csak egy újabb feladatként, kötelezettségként élték meg, amelyet a vállalkozásokra rónak.
- Szélsőséges esetben pedig néhányan úgy ítélték meg, hogy ez egy olyan költség, kiadás, amellyel büntetni akarják a vállalkozásokat.

b) A 2018 májusa körüli időszak

A 2018. májusi „élesedés” környékén azonban robbanásszerű igény történt a GDPR-ral kapcsolatos információkra, az olyan tájékoztatókra, amely segít tájékozódni abban, hogy hogyan tudnak megfelelni a hatályba lépő rendeletnek. 2017 év végétől ugyanis egyre több KKV ébredt rá arra, hogy újfajta jogi kötelezettségeik vannak az adatvédelem terén, ezért igyekeztek minden lehetséges forrásból információt nyerni ezen kötelezettségeikről. Azonban a felkészülési folyamatot továbbra is számos bizonytalanság, tisztázatlan jogszabályi és értelmezési kérdések nehezítették.

Mi okozta a bizonytalanságot?

1. Beazonosítás:

- Elsősorban az okozott problémát – jellemzően a mikro-vállalkozói körnek –, hogy beazonosítsák, hogy egyáltalán rájuk vonatkozik-e a rendelet.
- Ha ez sikerült, akkor ezt követően annak a felmérése, hogy melyek azok az adattartalmak, amelyek vonatkozásában a GDPR rendelet szabályait alkalmazniuk kell. Milyen adatokat tart nyilván a vállalkozásában és az a rendelet hatálya alá tartozik-e, illetve melyek azok a személyes adatok, tartalmak, amelyek nyilvántartását a megfelelő biztonsági intézkedések megtételével meg kell oldaniuk.

2. Ennek során ugyanakkor komoly gondot okozott számukra, hogy egyáltalán hogyan kezdjenek hozzá? Milyen dokumentumokat kell előállítaniuk, hogyan kell rendszerezniük, és az egyes tevékenységeket milyen időbeli ütemezésben kell tenni, azaz milyen tevékenységeket kell elvégezniük lépésről-lépésre.

3. és ha már elkészült a dokumentáció, az is problémaként merült fel, hogy azokat hol és hogy tárolja?

Jellemző volt erre az időszakra, hogy a KKV-k egymás között információs csoportokat hoztak létre, ahol megosztották a „tudnivalókat”. Számos ilyen jellegű csoport a mai napig is, meglehetősen jelentős létszámmal működik.

A későbbiekben azonban egyre több szerv, így a NAIH által szervezett konferenciák, rendezvények, tájékoztató anyagok segítették a megfelelő előkészületeket. Azonban a hirtelen nagy mennyiségben érkező szabályozási anyag nagy kihívások elé állította a KKV-kat.

c) 2018 májusa után

Néhány hónappal 2018 májusa után a KKV-k felkészülési kedve csökkent, a korábbi ugrásszerű érdeklődés egyre kevésbé volt jelen. Jellemző és a mai napig fennálló probléma ugyanakkor az is, hogy számos esetben a KKV-k 2018 májusára megfelelően felkészültek a GDPR rendeletnek való megfelelésre, azonban az adatvédelmi értelmezésben, és sokszor a saját működésükben történt változásokat az adatvédelmi rendszerükön már nem vezették át, nem aktualizálják.

A NAIH joggyakorlata és később összefoglalói, továbbá a DPO-k számára tartott konferenciái, értelmezései kimondottan hatékony segítséget nyújtottak a KKV-k számára. Mindezzel egy időben azonban a tájékoztató és információs képzések és előadások iránti kereslet folyamatosan csökkent, és a vállalkozások egyre inkább „biztos minták”, „bevált módszerek” alapján igyekeztek megoldásokat keresni.

II. A felkészülés módszertanai

„Mintás” megoldások

Korábban, és jelenleg is jellemző felkészülési módja a vállalkozásoknak, hogy általuk alkalmazható GDPR dokumentációs csomagot vásárolnak, vagy töltenek le az internetről és a sablon szerinti dokumentáció gépies alkalmazását gondolják célravezetőnek. Nem gondolják végig, hogy minden egyes vállalkozásnak, szervezetnek, az egyedi adatkezelési tevékenységeire és körülményeire figyelemmel, egyedi dokumentációval kell rendelkeznie. Ezek elkészítéséhez pedig a konkrét vállalkozás működésének és tevékenységének mélységi ismerete szükséges, így nem elegendő egy sablont letölteni az internetről, vagy megrendelni a GDPR szakértőtől, hanem a saját folyamatait kell szabályoznia. A mikro-vállalkozói szektor azonban gazdasági okokból rákényszerül arra, hogy minta szerinti, vagy saját maga által elkészített irattalajjal igyekezzen a kötelezettségeit teljesíteni.

„Szakértői” felkészülések

A KKV-k egy jelentős része külső szakértő segítségével készült fel, illetve igyekszik jelenleg is megfelelni a rendeletnek. Az elmúlt két évben rengeteg „adatvédelmi szakértő” lett (teremt) hazánkban, ha az internet keresőprogramjába beütjük, rengeteg adatvédelemmel foglalkozó szakembert, vállalkozást találunk, ezért a vállalkozásoknak nehéz eldöntenie, hogy valójában melyik is, ki az az igazi szakértő, aki megfelelő felkészítést biztosít a számára. Ráadásul előfordult, hogy egyes szakértők túlmisztifikálták a kérdéskört, próbálták elrettenteni a hallgatóságot - arra törekedve, hogy őket bízzák meg a vállalkozások a felkészítésére. Éppen ezért gyakori igény a vállalkozások részéről, hogy megfelelő, megbízható szakértőt ajánljanak a számukra és többször jelezték azt is, hogy jó lenne, ha lenne egyfajta minőségbiztosítási rendszer, „tanúsítvány”, amely valamiféle eligazítást nyújtana számukra az adatvédelmi szakértő felkészültségéről.

A vállalkozások sok esetben jelezték azt is, hogy a megbízott külső partnereik a szükséges dokumentumokat elkészítik, de a legritkább esetben tartanak tényleges képzést számukra. Tény ugyanakkor, ha a vállalkozásnak van kijelölt adatvédelmi tisztviselője, akkor ez a képzés szinte minden esetben megtörténik.

Autodidakta módon készül fel

Nagyon sok vállalkozó – legtöbbször gazdasági megfontolásból – saját maga igyekszik felkészülni az adatvédelmi feladataira, jellemzően tájékoztatók, konferenciák útján, információs csoportokon keresztül.

A KKV-k felkészülése azonban sok esetben felemásra sikerült. Inkább az irattalajokra, a tájékoztatók, szabályzatok elkészítésére fókuszáltak, és kevésbé gyakori az, hogy folyamatszemplélet alapján, ténylegesen a vállalati működést is az új követelményekhez igazítsák. Így pl. nem alakultak ki a mindennapi operatív működés során alkalmazandó szttenderdek, elmaradt az IT rendszer tényleges áttekintése és a szükséges védelmi intézkedések megtétele, a weblap, a levelezőrendszer áttekintése, a mentések beütemezése stb. A másik hiányzó lépés az adatok és adattovábbítások feltérképezésének hiánya, melyet „időhiányra” hivatkozva ki szoktak hagyni a feladataik közül.

A folyamatszmlélet hiánya azonban eredményezheti azt, hogy bár az iratanyag szempontjából megfelelnek a kritériumoknak, a gyakorlati oldal hiányosságai miatt azonban a megfelelés csak látszólagos. Mindezek miatt a KKV-knak további segítségre lenne szükségük ahhoz, hogy a követelményeket teljesíteni tudják.

Meg kell jegyezni ugyanakkor azt is, hogy a KKV szektorban kedvezőbb helyzetben vannak azok a vállalkozások, akik eleve valamilyen ISO vagy egyéb tanúsítási rendszer keretein belül dolgoznak, hiszen ezek esetében számos átfedés van az adatvédelmi szabályokkal.

III. A GDPR rendelkezéseinek napi szintű tényleges alkalmazásával kapcsolatos problémák

A tényleges alkalmazás kérdésköre nehezkesebb, mint a felkészüléssel fentebb leírtak.

A KKV-k ugyan felismerték, hogy a felkészülés szükséges, és igyekeznek is megfelelni a követelményeknek (részben sikeresen), azonban az adatvédelem, mint napi szintű szempont kevésbé épült be az üzleti folyamatokba. Maga a GDPR nem csupán elkészítendő iratanyag, hanem folyamat- és cégmenedzsment témakörébe tartozó kérdés. Főként a kisebb vállalkozásoknak azonban az ügymenete számos esetben nem tervszerű és preventív, hanem inkább napi reaktív tevékenységeket fed le, a folyamatszabályozás ritkán jelenik meg a tevékenységeikben. A kialakult folyamatok és gyakorlatok hiánya az adatvédelem témakörét is érinti, ennek okán az adatvédelem sok esetben csupán „megírandó irat”-ként csapódott le a vállalkozói szférában, nem pedig mindennapi operatív feladatként.

Külön kiemelendő a KKV szektor kapcsán az **adatvédelmi incidensek** kérdésköre. Számos KKV nem tudja pontosan, hogy mi is az adatvédelmi incidens (leegyszerűsítik a „hekkertámadásra”), és részben e miatt, részben pedig a magas büntetési fenyegetettség okán kifejezetten ritkán jelentik azt be a Hatóságnak (gyakran esetleg teljesen elzárkóznak ettől). Bár tény, hogy előfordul az, hogy az adatkezelő hibája miatt fordul elő incidens, amely azonban sok esetben ez az adatkezelő kellő gondossága mellett is megtörténhet. A KKV szektorban gyakran találkozni azzal az elképzeléssel, hogy ha szabályszerűen bejelentené az incidenst, akkor az azonnal (megléhetősen magas) összegű bírsággal járna. Ennek okán tehát egyrészt az incidens fel nem ismerése, másrészt a gazdasági okokból történő félelem komoly akadálya az incidensek nyilvántartásának és bejelentésének. Ez az elképzelés – véleményem szerint – csak további tájékoztatásokkal módosítható. Természetesen ebben az esetben is előnyösebb helyzetben vannak az adatvédelmi tisztviselőt kijelölő KKV-k, hiszen ebben az esetben kifejezett segítségük van mind a tájékozódás, mind a tényleges intézkedések terén.

További észrevétel, hogy több KKV nem tudja, hogy mikor is szükséges az **adatvédelmi tisztviselő** kijelölése (különösen „mintás” felkészülésnél), vagy ha be is azonosítja, hogy számára kötelező, akkor is vagy összeférhetetlen személyt jelöl ki a feladatra, vagy egyszerűen nem jelöl senkit ki. Vannak olyan KKV-k, akik a saját alkalmazottaikat igyekeztek rövidebb képzés segítségével felkészíteni az új munkakörre/feladatra, ennek sikere azonban változó, bár kifejezetten előre mutató tendencia.

III. A GDPR felkészülés aránya a KKV-k körében

A 2018 környéki nagy felkészülési hullám, valamint mindazok ellenére, hogy az adatvédelmi tudatosság 2018. óta láthatóan növekszik, azonban még mindig nagy lehet azoknak a KKV-nak a száma, amelyek nem gondolják, hogy a GDPR rendelkezései őket is érintik és igen sok KKV még egyáltalán nem tett lépéseket a felkészülés tekintetében. Százalékos arányt igen nehéz mondani, de talán kb. 60%-a készülhetett fel valamilyen módon, és kb. 40% az, aki eddig még semmilyen lépést sem tett, vagy még csak fontolgatja.

Előnyben vannak azok az KKV-k, akik valamilyen pályázatokon indulnak, mert ott kötelező bemutatni ezeket a dokumentumokat, illetve akik a partnereik miatt, mert pl. multinacionális céggel állnak aktív gazdasági kapcsolatban és emiatt kénytelenek voltak az adatvédelemmel magas szinten foglalkozni. Egyes beszállítói szektoroknál ez kifejezetten lényeges volt.

Még mindig gyakori érvelés az, hogy „szerintem ez nekünk nem kell, nem kezelünk személyes adatot”. Ez a képzés, a megfelelő tájékoztatás hiányára visszavezethető érvelés, mely természetesen nem állja meg a helyét.

IV. A jelenlegi helyzet, a felkészülés akadályai ma a KKV oldaláról

A felkészülés és a tényleges alkalmazás akadályait az alábbiakban próbáltam meg összefoglalni:

1. A KKV még mindig nincsen tisztában a GDPR szerinti kötelezettségeivel/feladataival, vagy úgy véli, hogy rá ez a kötelezettség nem terjed ki;
2. A KKV felkészült és tett ilyen intézkedéseket, azonban nem tudja, hogy megfelelően vezette-e be a GDPR szabályokat, nem tudja, mi hiányzik még vagy mit csinál rosszul. Igazából a hétköznapiakban nem tudja jól működtetni, és jól alkalmazni a GDPR-t;
3. A KKV valamilyen mintát tölt ki, az operatív folyamatait azonban nem igazítja hozzá;
4. Előfordul az is, hogy jogszabályi vagy fogalmi pontatlanságok és kérdések akadályozzák a precíz felkészülést és az operatív alkalmazást;
5. A KKV az iratanyag elkészítés során nem készít adattérképet, nem méri fel az adatállományát és adattovábbításait, vagy csak részben teszi ezt meg;
6. A KKV alkalmazottai nem tudják a (már elkészült) anyagot értelmezni, vagy meg sem ismerik;
7. A KKV alkalmazottai nem tudják az iratanyagban (különösen szabályzatokban) foglaltakat alkalmazni;
8. Gazdaságilag nem engedheti meg magának az iratanyag szintű felkészülést;
9. Fontos probléma, hogy a cégvezetők többnyire nem ismerik fel az informatikai adatbiztonság jelentőségét, illetve nem áll rendelkezésükre megfelelő anyagi forrás annak megteremtésére;
10. Ritkább esetben az informatikai vagy a webfejlesztő partner nem megfelelő felkészültségű;
11. Általánosságban elmondható, hogy az adatvédelmi kérdéseket, feladataikat jogi témakörnek tartják és a jogászoktól, esetleg a könyvelőjüktől várják rá a megfelelő megoldást.

Továbbra is folyamatos kérdés a KKV-k részéről, a kamerás megfigyelés jogszerű gyakorlata, az ügyfeleknek szánt adatkezelési tájékoztató kialakítása, a munkahelyi adatkezelések

Itt külön szeretném kiemelni, hogy a KKV-k egy része nem követte le a pandémia miatt előállt helyzetet. Igen nagy – anyagi és humán erőforrásbeli – kihívás ez az időszak számukra, hiszen sok helyen, ahol home office került bevezetésre, ez a fajta munkatevékenység csak kísérleti, vagy először alkalmazzák a működésük során. Viszonylag nehéz rövid időn belül megfelelő rendszert kiépíteni, emellett egyes esetekben a rendszer kiépítésének költsége elbocsátásokhoz vezetne. További gond a KKV-k számára, hogy a pandémia miatt hirtelen gyors változások álltak be mind az operatív működésben, mind az ügymenetben, sokáig pedig bizonytalanok voltak, akár olyan kérdések tekintetében is, hogy szabad-e a munkavállaló testhőmérsékletét mérni? A munkáltató által finanszírozott COVID szűrés eredményeit kezelheti-e a munkáltató, és ha igen, akkor hogyan? A pandémiás szabályok megírása a kapkodásban vagy elmaradt, vagy ha volt is, az adatvédelem tükrében nem került átgondolásra. E tekintetben is útmutatásra vártak a KKV-k, továbbá ebben az esetben is keresik az alkalmazható mintákat.

A GDPR releváns szakirodalmának és a tisztázott fogalmi kérdéseknek köszönhetően azonban egyre több valóban hatékony felkészülés zajlott és zajlik ma is.