Adatfeldolgozási megállapodás

CÉL ÉS PRIORITÁSI SORREND

A jelen Adatfeldolgozási megállapodás, annak mellékleteivel és a kifejezetten kereszthivatkozott dokumentumokkal együtt (a „**DPA**”) az Iron Mountain és az Ügyfél között létrejött szolgáltatási megállapodás (a „**Megállapodás**”) részét képezi. A Megállapodás feltételei és kikötései a felek jelen DPA szerinti jogaira és kötelezettségeire vonatkoznak és azokra irányadók.

Ha a jelen DPA-ban foglalt bármely feltétel és kikötés ellentétes a Megállapodásban meghatározott feltételekkel, a jelen DPA-ban meghatározott feltételeket kell irányadónak tekinteni a jelen DPA tárgyára vonatkozóan. A jelen DPA hatályon kívül helyez minden korábbi adatfeldolgozási megállapodást, illetve adatvédelmi vagy magánélet védelmére vonatkozó záradékot a felek között a Megállapodás alapján nyújtott Szolgáltatásokkal kapcsolatban, illetve azok helyébe lép.

ÁLTALÁNOS FELTÉTELEK

1. FOGALOMMEGHATÁROZÁSOK

Hacsak a jelen dokumentum kifejezetten másként nem rendelkezik, minden nagybetűs kifejezés jelentése megegyezik a Megállapodásban megadott jelentéssel.

„**Adatkezelő**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb testület, amely a Személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza;

„**Ügyfél személyes adatok”**: az Ügyfélhez vagy annak valamely társvállalatához tartozó vagy általuk gyűjtött Személyes adatok, amelyeket a Szolgáltatások részeként kezelnek;

„**Érintett**”: azonosított vagy azonosítható természetes személy;

„Adatvédelmi jogszabályok”: a Személyes adatok kezelésére vonatkozó összes alkalmazandó jogszabály és előírás, amely az adott joghatóságokban létezhet, beleértve többek között: az EU GDPR rendelete ((EU) 2016/679 rendelet), az Egyesült Királyság GDPR rendelete (a GDPR az Egyesült Királyság belföldi jogszabályainak részeként alkalmazandó, az Európai Unió 2018. évi (kilépési) törvényének 3. szakasza alapján, és a 2019. évi Adatvédelmi, magánélet-védelmi és elektronikus hírközlési (módosítások stb.) (EU kilépés) rendeletek) (módosításokkal együtt)), a 2018. évi adatvédelmi törvény, az FADP (Svájci szövetségi adatvédelmi törvény), az Egyesült Államok állami adatvédelmi jogszabályai, a LGPD (brazil általános adatvédelmi törvény), a PIPL (a Kínai Népköztársaság személyes adatok védelmére vonatkozó törvénye), valamint az ezek alapján végrehajtott vagy hozott bármely jogszabály és/vagy előírás, illetve amely módosítja, helyettesíti, újra bevezeti vagy összevonja ezek bármelyikét, beleértve adott esetben a felügyeleti hatóságok által kiadott iránymutatásokat és gyakorlati kódexeket;

„**Személyes adatok**”: az Érintettekre vonatkozó bármely információ;

„**Adatfeldolgozó**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy egyéb szerv, amely az Adatkezelő nevében Személyes adatokat kezel;

„**Adatfeldolgozás**”: a Személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

„**Biztonsági incidens**”: az Iron Mountain, annak személyzete vagy alvállalkozói által kezelt Személyes ügyféladatok bármely olyan véletlen vagy jogellenes sérülése, megsemmisítése, elvesztése, megváltoztatása vagy jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés a Szolgáltatások nyújtása során;

„**Szolgáltatások**”: az Iron Mountain vagy annak társvállalatai által az Ügyfél vagy annak társvállalatai részére a Megállapodás alapján nyújtott bármely szolgáltatás;

Az „**Egyesült Államok állami adatvédelmi jogszabályai**” az Egyesült Államok minden olyan adatvédelmi és adatbiztonsági jogszabályát jelenti, amely a Személyes adatok Megállapodás szerinti kezelésére vonatkozik, beleértve korlátozás nélkül a következőket, és amelyeket időről időre módosíthatnak, hatályon kívül helyezhetnek vagy helyettesíthetnek: (1) a kaliforniai fogyasztói adatvédelmi törvény (California Consumer Privacy Act), a kaliforniai adatvédelmi törvény által módosított formában, és az ezekhez kapcsolódó bármely végrehajtási rendelet (együttesen: „**CCPA**”); (2) a coloradoi adatvédelmi törvény (Colorado Privacy Act, „**CPA**”), (3) a virginiai fogyasztói adatvédelmi törvény (Virginia Consumer Data Protection Act, „**CDPA**”); (4) a utahi fogyasztói adatvédelmi törvény (Utah Consumer Privacy Act, „**UCPA**”); és (5) a connecticuti adatvédelmi törvény („**CTDPA**”).

2. AZ ADATFELDOLGOZÁS TERJEDELME ÉS RÉSZLETEI

2.1 A jelen Adatfeldolgozási megállapodás az Iron Mountain által Adatfeldolgozóként kezelt Személyes ügyféladatokra vonatkozik a Szolgáltatásoknak az Ügyfél nevében a Megállapodás szerint történő nyújtása során.

2.2 Az Iron Mountain adatkezelőként gyűjtheti és kezelheti az Ügyfél és társvállalatai alkalmazottainak Személyes adatait jogszerű üzleti célokból, például szerződés- és ügyfélkapcsolat-kezelés céljából, az adatvédelmi jogszabályokkal és az Iron Mountain weboldalain elérhető adatvédelmi nyilatkozattal és más alkalmazandó adatvédelmi szabályzatokkal összhangban. Az Iron Mountain jelen DPA-ban meghatározott kötelezettségei nem vonatkoznak az ilyen Személyes adatok kezelésére.

2.3 A Személyes adatok feldolgozásának tárgya a Szolgáltatások teljesítése. Az Ügyfél és az Iron Mountain jogait és kötelezettségeit a jelen Adatfeldolgozási megállapodás határozza meg. A jelen Adatfeldolgozási megállapodás 1. melléklete meghatározza az Adatfeldolgozás jellegét, időtartamát és célját, az Iron Mountain által kezelt Személyes ügyféladatok típusait és azon Érintettek kategóriáit, akiknek a Személyes adatait kezelik.

2.4 Amikor az Iron Mountain a Szolgáltatások nyújtása során Személyes ügyféladatokat dolgoz fel, az Iron Mountain:

2.4.1 A Személyes ügyféladatokat kizárólag az Ügyfél dokumentált utasításainak megfelelően kezelheti. Ha az Iron Mountainnek az Iron Mountainre vonatkozó jogszabályok által előírt bármely más célból kezelnie kell Személyes ügyféladatokat, akkor először az Iron Mountain tájékoztatja az Ügyfelet erről a követelményről, kivéve, ha az ilyen jogszabály(ok) fontos közérdekből tiltja (tiltják) ezt; és

2.4.2 Mindig betartja az alkalmazandó Adatvédelmi jogszabályokat, és azonnal értesíti az Ügyfelet, ha az Iron Mountain véleménye szerint az Ügyfél által megadott, a Személyes ügyféladatok feldolgozására vonatkozó utasítás sérti az alkalmazandó Adatvédelmi jogszabályokat.

2.5 Az Ügyfél utasításai kötelező érvényűek az Iron Mountainre nézve, kivéve, ha az utasítások teljesítése a Megállapodás szerinti szolgáltatás nyújtását teszi szükségessé, és az Ügyfél nem vállalja, hogy az ilyen szolgáltatások szolgáltatási díját megfizeti.

2.6 Az Iron Mountain köteles biztosítani, hogy feladatai teljesítéséhez a Személyes ügyféladatokhoz hozzáférést igénylő személyzetre titoktartási kötelezettség vonatkozzon az ilyen Személyes ügyféladatok tekintetében, és észszerű lépéseket kell tennie annak érdekében, hogy biztosítsa az Iron Mountain azon személyzetének megbízhatóságát és kompetenciáját, akik a Személyes ügyféladatokhoz hozzáférnek.

3. ÜGYFÉLSZOLGÁLAT BIZTOSÍTÁSA

3.1 Az Iron Mountain segítséget nyújt az Ügyfélnek, mindenkor figyelembe véve az Adatfeldolgozás jellegét:

3.1.1 megfelelő technikai és szervezési intézkedésekkel és amennyire lehetséges, az Ügyfél azon kötelezettségeinek teljesítése érdekében, hogy megválaszolja a jogaikat gyakorló Érintettektől érkező kérelmeket;

3.1.2 az Ügyfél kötelezettségeinek való megfelelés biztosítása (például az Adatfeldolgozás biztonsága, az Adatvédelmi incidens bejelentése a felügyeleti hatóság felé, az Adatvédelmi incidens közlése az Érintettel, adatvédelmi hatásvizsgálat és a felügyeleti hatóságokkal való előzetes konzultáció, amennyiben az Adatfeldolgozás magas kockázatot jelentene, ha az Adatkezelő nem tesz megfelelő intézkedéseket a kockázat csökkentése érdekében), figyelembe véve az Iron Mountain számára elérhető információkat; és

3.1.3 azáltal, hogy az Ügyfél rendelkezésére bocsát minden olyan információt, amelyet az Ügyfél ésszerűen kér annak érdekében, hogy az Ügyfél bizonyíthassa, hogy az Iron Mountain kiválasztására és kinevezésére vonatkozó kötelezettségei teljesültek.

4. BIZTONSÁGI INTÉZKEDÉSEK

4.1 Figyelembe véve a szokásos működési eljárásokat, a megvalósítás költségeit, és az Adatfeldolgozás jellegét, hatókörét, kontextusát és céljait, az Iron Mountain megfelelő és észszerű technikai és

szervezési intézkedéseket hajt végre a titoktartás, az integritás és a Személyes ügyféladatok elérhetőségének védelme érdekében, valamint a Személyes ügyféladatok védelmére jogosulatlan vagy jogellenes Adatfeldolgozással, illetve véletlen elvesztéssel, megsemmisítéssel, károsodással, módosítással, vagy nyilvánosságra hozatallal szemben. Az Iron Mountain biztonsági szabványait a jelen DPA 2. melléklete tartalmazza.

4.2 Az Ügyfél kizárólagos felelőssége annak felmérése, hogy ezek a technikai és szervezési intézkedések megfelelnek-e az Ügyfél követelményeinek.

5. JOGSZABÁLYOK BETARTÁSA

Az Ügyfél és annak társvállalatai kötelesek: (i) a Személyes ügyféladatokat az Adatvédelmi jogszabályoknak megfelelően kezelni; (ii) írásbeli utasításokat adni az Iron Mountain számára a Személyes ügyféladatok Szolgáltatásokkal kapcsolatos Kezelésére vonatkozóan (beleértve bármely olyan harmadik fél szervezet nevében történő adatfeldolgozást, amely a Személyes ügyféladatok Adatfeldolgozója); és (iii) a Személyes ügyféladatok feletti Adatkezeléssel kapcsolatos ellenőrzést és hatáskört mindenkor fenntartani.

6. TOVÁBBI ADATFELDOLGOZÓK

6.1 Az Ügyfél tudomásul veszi és elfogadja, hogy az Iron Mountain igénybe veheti anyavállalatát, társvállalatait és más harmadik fél további adatfeldolgozókat (beleértve az Iron Mountain társvállalatai vagy anyavállalata által megbízott harmadik fél további adatfeldolgozókat is) a Személyes ügyféladatok jelen DPA szerinti kezelése céljából, az alábbi 6.2. pont szerint.

6.2 Az Ügyfél által a jelen DPA keltének napján jóváhagyott további adatfeldolgozók listája itt[1] érhető el. Az Iron Mountain bármikor lecserélhet vagy kinevezhet egy új további adatfeldolgozót, feltéve, hogy az Ügyfél erről tizenöt (15) napos előzetes írásbeli értesítést kap, és az Ügyfél nem tiltakozik az ilyen változások ellen az adatvédelemmel kapcsolatos bizonyítható okokból ezen időkereten belül. Ahhoz, hogy ilyen e-mail értesítéseket kapjon, az Ügyfélnek ezen a weboldalon[2] keresztül kell feliratkoznia az Iron Mountain értesítési szolgáltatására és kezelnie a meglévő előfizetéseket.

6.3 Ha az Ügyfél nem iratkozik fel az értesítési szolgáltatásra, az Iron Mountain nem vállal felelősséget a további adatfeldolgozóra vonatkozó értesítés elmulasztásáért, és minden ilyen kijelölést az Ügyfél által engedélyezettnek kell tekinteni**.** Ha az Ügyfél írásban tiltakozik az adatvédelemhez kapcsolódó bizonyítható okok miatt egy helyettesítő vagy új további adatfeldolgozó kinevezése ellen a tizenöt (15) napos előzetes írásbeli értesítés keretén belül, akkor az Iron Mountain minden észszerű erőfeszítést megtesz annak érdekében, hogy az Ügyfél számára elérhetővé tegye a Szolgáltatások módosítását, vagy változtatásokat javasoljon az Ügyfél konfigurációját vagy a Szolgáltatások használatát illetően, minden esetben annak elkerülése érdekében, hogy a kifogásolt további adatfeldolgozó az Ügyfél megfontolása és jóváhagyása érdekében Személyes ügyféladatokat kezeljen. Ha az Ügyfél tizenöt (15) napon belül nem hagyja jóvá az Iron Mountain által javasolt módosításokat, az Iron Mountain az Ügyfél írásbeli értesítése mellett azonnali hatállyal felmondhatja a Szolgáltatást vagy a Szolgáltatás azon részét, amelyet az Iron Mountainnak a kifogásolt további adatfeldolgozó igénybevétele nélkül nem áll módjában nyújtani. Az ilyen felmondás nem érinti a felek megszerzett jogait és kötelezettségeit, feltéve, hogy az Iron Mountain vagy az Iron Mountain társvállalatai nem fizetnek felmondási díjat, költséget vagy egyéb kompenzációt az ilyen felmondással kapcsolatban, és az Ügyfél haladéktalanul megszerzi az Iron Mountain számára a megszüntetett Szolgáltatások részeként átadott eszközök tulajdonjogát, a Megállapodás feltételeinek megfelelően, az Ügyfél saját költségén.

6.4 Az Iron Mountain köteles biztosítani, hogy a jelen DPA hatálya alá tartozó további adatfeldolgozókkal kötött szerződések olyan rendelkezéseket tartalmazzanak, amelyek lényegi rendelkezéseket tekintve hasonlók a jelen DPA rendelkezéseihez, és amelyeket az alkalmazandó Adatvédelmi jogszabályok előírnak. Ha az Iron Mountain további adatfeldolgozója miatt az Iron Mountain a jelen DPA vagy bármely alkalmazandó Adatvédelmi jogszabály szerinti kötelezettségeit megszegi, az Iron Mountain továbbra is teljes felelősséggel tartozik az Ügyfél felé az Iron Mountain jelen feltételek szerinti kötelezettségeinek teljesítéséért.

7. BIZTONSÁGI INCIDENSEK

7.1 Biztonsági incidens gyanúja esetén az Iron Mountain:

7.1.1 azonnal intézkedik a gyanított Biztonsági incidens kivizsgálása, valamint a gyanított Biztonsági incidens hatásainak azonosítása, megelőzése és enyhítése, valamint a Biztonsági incidens orvoslása érdekében;

---

[1] https://www.ironmountain.com/-/media/files/Utility/Legal/GLOBAL-Personal-Data-Subprocessors-List.xlsx?la=en

[2] https://urldefense.proofpoint.com/v2/url?u=https-3A__reach.ironmountain.com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFIot0PGng&r=JTlzF2zjI-gYEq5GmWmZcbgd--hgyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKIzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

7.1.2 indokolatlan késedelem nélkül értesíti az Ügyfelet, amint elvárható mértékben megbizonyosodott arról, hogy Biztonsági incidens történt, és az Ügyfélnek részletesen beszámol a Biztonsági incidensről, beleértve azokat az információkat is, amelyek ésszerűen szükségesek az Ügyfél számára az Adatvédelmi jogszabályok szerinti bejelentési kötelezettségek teljesítéséhez.

7.2 Az Ügyfél elfogadja, hogy az Iron Mountain a 7.1.2. pont alapján szakaszosan is átadhatja az információkat. Azokban az esetekben, amikor az Iron Mountain nem fér hozzá a 7.1.2. pontban felsorolt bizonyos információkhoz, vagy azokat nem tudja az Ügyfél rendelkezésére bocsátani, az Iron Mountain erről tájékoztatja az Ügyfelet, és az Iron Mountain nem vállal felelősséget az ilyen információk megadásának elmulasztásáért.

8. AUDITOK

Az Iron Mountain lehetővé teszi az Ügyfél és annak auditorai vagy meghatalmazott képviselői számára, hogy a Szerződés időtartama alatt - az Iron Mountain legalább tíz (10) munkanappal korábban történő értesítését követően - ellenőrzéseket vagy vizsgálatokat végezzenek, azzal a feltétellel, hogy az Iron Mountain nem köteles hozzáférést biztosítani vagy engedni a következőkre vonatkozó információkhoz: (i) az Iron Mountain más ügyfelei; (ii) az Iron Mountain nem nyilvános külső jelentései; és (iii) az Iron Mountain belső ellenőrzési vagy megfelelőségi funkciója által készített belső jelentések. A jelen pont szerinti audit vagy ellenőrzés célja annak vizsgálatára korlátozódik, hogy az Iron Mountain a jelen DPA szerinti kötelezettségeinek megfelelően kezeli-e a Személyes ügyféladatokat. Tizenkét (12) hónapos időszakon belül legfeljebb egy ilyen auditra kerülhet sor, kivéve, ha Biztonsági incidens történt.

9. NEMZETKÖZI ADATTOVÁBBÍTÁS (KORLÁTOZOTT ADATTOVÁBBÍTÁS)

9.1. Az Ügyfél ezennel hozzájárul és engedélyezi a Személyes ügyféladatok nemzetközi továbbítását a 6.2. pontban meghatározott szervezetek részére, a 3. mellékletnek megfelelően a Szolgáltatások nyújtása céljából, illetve az Ügyfél és az Iron Mountain vállalják, hogy:

9.1.1 betartják az ilyen adattovábbításokra vonatkozó alkalmazandó Adatvédelmi jogszabályokat;

9.1.2 korlátozás nélkül figyelembe véve i) az Ügyfél személyes adatok kategóriáit, ii) azokat az országokat, amelyek nemzeti jogszabályai esetleg nem biztosítanak az EU/Egyesült Királyság jogszabályaihoz hasonló szintű védelmet a Személyes adatok számára („**Harmadik ország**"), iii) a 7. pontban meghatározott vonatkozó technikai és szervezési intézkedéseket és iv) a Személyes ügyféladatok kezelésében részt vevő érintett feleket, elvégezték az itt elfogadott vonatkozó adattovábbítási mechanizmus megfelelőségének értékelését, amennyiben azt a jogszabályok megkövetelik, és megállapították, hogy az ilyen adattovábbítási mechanizmus megfelelően kialakításra került annak biztosítása érdekében, hogy a jelen DPA-val összhangban továbbított Személyes adatok a célországban olyan szintű védelemben részesüljenek, amely lényegében egyenértékű az adatvédelmi jogszabályok által garantált védelemmel.

10. FELELŐSSÉG ÉS KÁRTALANÍTÁS

10.1 A Megállapodásban foglalt bármely ellenkező értelmű rendelkezés ellenére, amennyiben a jelen DPA szerinti kötelezettségeinek Iron Mountain általi megszegése Biztonsági incidenst okoz, az Iron Mountain az alkalmazandó jogszabályok által megengedett mértékben megtéríti az Ügyfélnek az Ügyfélnél közvetlenül, igazolhatóan, szükséges és észszerű módon felmerült harmadik feleknek fizetendő költségeket (a) az ilyen Biztonsági incidens kivizsgálása során, (b) az ilyen Érintettek és a szabályozó hatóságok értesítéseinek előkészítése és postázása tekintetében az Adatvédelmi jogszabályok által előírtak szerint, (c) a jogszabályok által előírt hitelfelügyeleti szolgáltatások nyújtása során ilyen személyek számára tizenkét (12) hónapot meg nem haladó időtartamra, és (d) a felügyeleti hatóság által kiszabott bírságok, büntetések vagy szankciók azon részének kifizetését illetően, amelyekért a felügyeleti hatóság szerint az Iron Mountain közvetlenül felelős.

10.2 Amennyiben az Érintett az Adatvédelmi jogszabályok állítólagos megsértése miatt keresetet nyújt be bármelyik vagy mindkét féllel szemben („**Érintetti követelések**"), amennyiben ez megengedett, a felek mindegyike maga határozza meg az ilyen követeléssel szembeni saját védekezését (vagy a védekezés egy részét), és kizárólagos felelősséggel tartozik a saját költségeiért, az ezzel kapcsolatos kiadásaiért és kötelezettségeiért, ideértve a jogi díjakat vagy a bíróság által vele szemben megítélt vagy általa egyezség formájában megállapított összegeket, feltéve azonban, hogy ha mindkét fél felelős egy részért, vagy bármelyik fél felelős az Érintett által ugyanazon esemény vagy eseménysorozat miatt elszenvedett kár teljes összegéért, és az Érintett csak az egyik féltől kapott teljes kártérítést (a „**Kártalanító fél**"), akkor a Kártalanító fél jogosult a másik féltől a másik fél által okozott kárnak megfelelő kártalanításnak azt a részét visszaigényelni. A Kártalanító fél az eseményt követő 12 hónapon belül csak az alkalmazandó jogszabályok által megengedett mértékben nyújthat be követelést a másik fél felé.

10.3. Az alkalmazandó jogszabályok által megengedett legteljesebb mértékig a Megállapodásban foglalt felelősségkorlátozások és a károkért való felelősség korlátozása vagy kizárása vonatkozik az Ügyfél

jelen DPA-ból és/vagy az Iron Mountain elleni Megállapodásból eredő vagy azzal kapcsolatos összes követelésével kapcsolatos együttes felelősségre is. A felelősség ezen korlátozása és a kártérítés kizárása minden jelen DPA-ból vagy a Megállapodásból fakadó követelésre vonatkozik, függetlenül attól, hogy az szerződésből, szerződésen kívüli károkozásból vagy bármely más felelősségi elméletből ered-e, és az Iron Mountain felelősségére való hivatkozás az Iron Mountain és az Iron Mountain társvállalatának együttes felelősségét jelenti az Ügyfél és az Ügyfél összes többi társvállalata által támasztott követelések tekintetében. Az alkalmazandó jogszabályok által előírtak szerint a jelen pontnak nem célja (i) a felek felelősségének módosítása vagy korlátozása olyan féllel szemben támasztott Érintetti követelések tekintetében, amely egyetemleges felelősség fennállása esetén merül fel, vagy (ii) bármely fél felelősségének korlátozása a szabályozó hatóság által az adott félre kiszabott büntetések kifizetésére.

10.4 A 10.1–10.3. pontok rögzítik mindkét fél egyedüli és kizárólagos jogorvoslati lehetőségét, valamint mindegyik fél kizárólagos felelősségét a jelen DPA-val kapcsolatos bármely veszteség, kár, kiadás vagy felelősség tekintetében.

11. HATÓSÁGI KÉRELEMEK

11.1 Amennyiben a jogszabályok megengedik, és az alábbi 11.2 - 11.5 feltételek az adott esetre irányadóak, az Iron Mountain vállalja, hogy értesíti az Ügyfelet, ha:

11.1.1 jogilag kötelező érvényű kérést kap valamely hatóságtól, ideértve a bírósági hatóságokat is, a célország jogszabályai szerint a Megállapodás alapján továbbított Személyes ügyféladatok közlésére vonatkozóan; vagy

11.1.2 tudomást szerez arról, hogy hatóságok közvetlenül hozzáférnek a Megállapodás alapján továbbított Személyes ügyféladatokhoz a rendeltetési ország jogszabályainak megfelelően..

11.2 Amennyiben a célország jogszabályai alapján az Iron Mountain nem értesítheti az Ügyfelet, az Iron Mountain vállalja, hogy minden tőle telhetőt megtesz annak érdekében, hogy a lehető leghamarabb mentesüljön a tilalom alól, annak érdekében, hogy a lehető legtöbb információt közölje.

11.3 Az Iron Mountain vállalja, hogy felülvizsgálja a közzétételi kérelem jogszerűségét, különösen azt, hogy a megkereső hatóság rendelkezik-e hatáskörrel, és megtámadja a kérelmet, ha arra a következtetésre jut, hogy megalapozottan feltételezhető, hogy a kérelem a célország jogszabályai szerint jogellenes. A kért Személyes ügyféladatokat nem adja ki mindaddig, amíg erre az alkalmazandó eljárási szabályok alapján nem köteles.

11.4 Az Iron Mountain vállalja, hogy a közzétételi kérelemre adott válasz során a kérelem észszerű értelmezése alapján a lehető legkevesebb információt biztosítja.

11.5 Az Iron Mountain vállalja, hogy a jelen pont szerinti információkat a Megállapodás időtartama alatt megőrzi, és kérésre az illetékes felügyeleti hatóság rendelkezésére bocsátja.

12. VEGYES RENDELKEZÉSEK

12.1 Az Iron Mountain által nyújtott Szolgáltatások jellegétől függően, a Megállapodás megszűnésekor/lejáratakor, az Ügyfél konkrét utasításai és a Megállapodás feltételei alapján, az Iron Mountain köteles törölni/megsemmisíteni vagy visszajuttatni az Ügyfél vagy az Ügyfél által kijelölt harmadik fél részére az összes Személyes ügyféladatot. Az Iron Mountain által az Ügyfél nevében tárolt, az Ügyfél eszközében található Személyes ügyféladatokat a megállapodás szerinti kilépési vagy átállási tervnek megfelelően kell visszajuttatni az Ügyfélnek, a Megállapodás szerinti költségek mellett, a Megállapodásban vagy más vonatkozó szerződéses dokumentumban meghatározottak szerint. Minden egyéb esetben, ha a Megállapodás nem rendelkezik a Személyes ügyféladatok törléséről/megsemmisítéséről vagy visszajuttatásáról, és az Ügyfél nem ad semmilyen utasítást a Személyes ügyféladatok törlésével/megsemmisítésével vagy visszajuttatásával kapcsolatban a Megállapodás megszűnésétől/lejáratától számított tizenöt (15) napon belül, az Iron Mountain írásos értesítést küld az Ügyfélnek, amelyben 15 (tizenöt) napon belül konkrét utasításokat kér arra vonatkozóan, hogy törölje-e/megsemmisítse-e vagy küldje-e vissza a Személyes ügyféladatokat, és tájékoztatja az Ügyfelet az Ügyfél által fizetendő összes vonatkozó biztonságos megsemmisítési vagy egyéb díjakról. Amennyiben az Ügyfél ezen tizenöt (15) napos határidőn belül nem ad írásbeli utasításokat, és nem fizeti meg az alkalmazandó díjakat ugyanezen időszakon belül, akkor az Ügyfél ezennel felhatalmazza az Iron Mountaint, hogy a Megállapodás felmondása után, az Iron Mountain választása szerint és az Ügyfél költségére, az összes Személyes ügyféladatot tovább kezelje, törölje vagy megsemmisítse.

12.2 A 12.1. pontban foglaltak ellenére, az Iron Mountain nem szegi meg a biztonsági szalagokon tárolt Személyes ügyféladatok törlésével kapcsolatos kötelezettségeit, amennyiben az ilyen biztonsági szalagokat felülírják (és ezáltal törlik a Személyes ügyféladatokat) a szokásos üzletmenet során.

12.3 Az Általános szerződési feltételek (a jelen DPA 3. mellékletében meghatározottak szerint) kivételével a jelen DPA, valamint a jelen DPA-ból, illetve annak megszegéséből, megszűnéséből vagy érvényességéből eredő vagy azzal kapcsolatos bármely jogvita, követelés vagy ellentmondás tekintetében a Megállapodás jogválasztásra vonatkozó rendelkezése az irányadó; és a jelen DPA-ból

eredő vagy azzal kapcsolatos minden jogvita, ellentmondás vagy követelés elsődlegesen a Megállapodásban foglalt bármely meghatározott vitarendezési eljárás útján rendezendő.

12.4 Mindegyik fél időről időre írásban értesítheti a másik felet a jelen DPA bármely olyan módosításáról, amelyet a fél ésszerűen szükségesnek tart az Adatvédelmi jogszabályok követelményeinek, illetve a felügyeleti hatóságok vagy egy illetékes bíróság bármely döntésének a kezelése érdekében. Minden ilyen módosítás csak akkor lép hatályba, ha és amilyen mértékben azt a jelen DPA mindkét fél által aláírt, kölcsönösen elfogadott módosítása tartalmazza, kivéve, ha az egyik fél a másik felet bármely új jogszabályi követelményről tájékoztatja, és olyan módosítást küld, amely csak a szükséges változásokat tartalmazza, és amely formális hozzájárulás nélkül is elfogadható, azaz azáltal, hogy egy adott határidőn belül nem emelnek ellene kifogást, a jelen DPA kölcsönösen elfogadott módosításának minősül.

1. MELLÉKLET

Az adatfeldolgozás és az adattovábbítás részletei (amennyiben alkalmazandó)

A. A FELEK LISTÁJA:

A jelen DPA szerződő feleit, valamint az Adatátadó és az Adatátvevő feladatait a Megállapodás és a 3. melléklet (Nemzetközi adattovábbítások) határozza meg, ha van ilyen.

B. AZ ADATFELDOLGOZÁS/ADATTOVÁBBÍTÁS LEÍRÁSA (ha van):

Azon Érintettek kategóriái, akiknek a Személyes adatait feldolgozzák/továbbítják:

Az Iron Mountain Szolgáltatásainak természetétől és az Ügyfél tevékenységétől függően az Ügyfél az Érintettek különböző kategóriáihoz tartozó Személyes adatokat elküldheti az Iron Mountainnak, amelynek körét az Ügyfél saját belátása szerint határozza meg és ellenőrzi. Így az Érintettek kategóriái a következők lehetnek: korábbi és jelenlegi alkalmazottak; korábbi és jelenlegi vállalkozók vagy tanácsadók; ügynökség által biztosított vállalkozók vagy tanácsadók és külső megbízottak; állásra jelentkezők és jelöltek; hallgatók és önkéntesek; az alkalmazottak vagy nyugdíjasok által kedvezményezettként azonosított személyek, házastárs, egy háztartásban élő/élettárs, eltartottak és vészhelyzeti kapcsolattartók; nyugdíjasok; korábbi és jelenlegi igazgatók és tisztségviselők; részvényesek; kötvénytulajdonosok; számlatulajdonosok; végfelhasználók/fogyasztók (felnőttek, gyermekek); betegek (felnőttek, gyermekek); járókelők (CCTV kamerák); és a weboldal felhasználói.

A feldolgozott/továbbított személyes adatok kategóriái:

Az Iron Mountain Szolgáltatásainak természetétől és az Ügyfél tevékenységétől függően az Ügyfél a Személyes adatok különböző kategóriáihoz tartozó Személyes adatokat elküldheti az Iron Mountainnak, amelynek körét az Ügyfél saját belátása szerint határozza meg és ellenőrzi. Ennek értelmében a kategóriák magukban foglalhatják az Ügyfélre és/vagy az Ügyfél saját ügyfeleire, alkalmazottaira stb. vonatkozó személyes adatokat.

Továbbított érzékeny adatok (ha vannak):

Az Iron Mountain szolgáltatásainak természetétől és az Ügyfél tevékenységétől függően az Ügyfél érzékeny adatokat küldhet az Iron Mountainnak, amelynek körét az Ügyfél saját belátása szerint határozza meg és ellenőrzi.

Adott esetben az adattovábbítás gyakorisága (pl. az adatok egyszeri vagy folyamatos továbbítása):

Az átadás folyamatos jelleggel történik.

Az adatfeldolgozás jellege:

Gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Az adatfeldolgozás /adattovábbítás és a további adatfeldolgozás (amennyiben alkalmazandó) célja(i):

A Szolgáltatások Megállapodásban rögzítettek szerinti nyújtása.

Adatmegőrzési kötelezettség:

A Személyes adatokat az Iron Mountain az Ügyfélnek nyújtott Szolgáltatások időtartama alatt megőrzi, addig az időpontig, amíg a Személyes adatokat vissza nem szolgáltatják vagy meg nem semmisítik a jelen DPA 12.1. pontjában meghatározottak szerint.

Adott esetben a (további) Adatfeldolgozók részére történő adattovábbítások esetén, határozza meg az Adatfeldolgozás tárgyát, jellegét és időtartamát is:

Az Ügyféllel kötött Megállapodás időtartama alatt a további adatfeldolgozók többek között informatikai (IT) és tanácsadási szolgáltatásokat nyújtanak, beleértve a globális informatikai támogatást, eseményjelentési és -kezelési szolgáltatásokat.

C. ILLETÉKES FELÜGYELETI HATÓSÁG

A 3. mellékletben (Nemzetközi adattovábbítások) meghatározottak szerint, ha van ilyen.

2. MELLÉKLET

TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK („BIZTONSÁGI INTÉZKEDÉSEK”)

1. INFORMÁCIÓBIZTONSÁGI PROGRAM ÉS SZABÁLYZAT

Az Iron Mountainnak megfelelő fizikai, technikai és adminisztratív szabályozásokat tartalmazó információbiztonsági programot kell fenntartania, amely megfelel az iparági szabványoknak. Az információbiztonsági programnak a következőket kell tartalmaznia:

1.1 Az Iron Mountain információbiztonsági szabályzatainak, szabványainak és eljárásainak dokumentálása, belső közzététele és kommunikációja;

1.2 Az információbiztonsági program létrehozásával és fenntartásával kapcsolatos felelősség és hatáskör dokumentált, egyértelmű hozzárendelése;

1.3. Az információbiztonsági program legfontosabb ellenőrzéseinek, rendszereinek és eljárásainak rendszeres tesztelése;

1.4. Adminisztratív, technikai és működési intézkedések, amelyek célja az összes Személyes ügyféladat védelme a jelen Biztonsági mellékletben leírt gyakorlatok, folyamatok és eljárások alkalmazásával, amennyiben azok relevánsak és alkalmazandóak a Személyes ügyféladatok megőrzésének formátumát illetően.

2. KOCKÁZATÉRTÉKELÉS

Az Iron Mountain információbiztonsági kockázatértékelési programot tart fenn, amelynek célja azon ésszerűen előre látható belső és külső kockázatok és sebezhetőségek azonosítása és értékelése, amelyek befolyásolhatják a Személyes ügyféladatok biztonságát, titkosságát és/vagy integritását. Az Iron Mountain évente, vagy amikor a Személyes ügyféladatokat érintő kockázatot vagy sebezhetőséget érintően lényeges változás következik be, értékeli és - amennyiben szükséges, ésszerűen és megfelelő módon - frissíti az ilyen kockázatok korlátozására szolgáló jelenlegi információbiztonsági program hatékonyságát.

3. INFORMÁCIÓKEZELÉSI ESZKÖZÖK ÉS FIZIKAI ADATHORDOZÓK KEZELÉSE

3.1 Információkezelési eszközök kezelése. Az Iron Mountain eszközleltár-kezelési programot tart fenn az Iron Mountain információkezelő eszközeire (például számítógépekre, szerverekre, tárolóeszközökre, kommunikációs hálózatokra, személyi számítógépekre, laptopokra és perifériás eszközökre) vonatkozó fizikai, technikai és adminisztratív ellenőrzések kezelésére.

Az eszközkleltár-kezelési program a következőket tartalmazza:

3.1.1 Az eszköz tulajdonjogának dokumentált átruházása az Iron Mountain személyzetére az információk megfelelő besorolásának biztosítása, a hozzáférési korlátozások meghatározása és a hozzáférési ellenőrzések felülvizsgálata érdekében.

3.1.2 Az eszközök fertőtlenítése azok ártalmatlanítása előtt, az NIST 800-88 szerint.

3.1.3 A vezetőség engedélyének szükségessége olyan berendezések vagy szoftverek eltávolítása előtt, amelyeket nem egy adott személyhez rendeltek hozzá az Iron Mountain létesítményeiből.

3.2 Ellenőrzések. Az Iron Mountain ellenőrzései a következőket tartalmazzák:

3.2.1 Operatív eljárások és műszaki ellenőrzések, amelyek célja a dokumentumok, a számítógépes adathordozók, a bemeneti/kimeneti/biztonsági adatok és a rendszerdokumentáció illetéktelen közzétételtől, módosítástól és megsemmisítéstől való védelme.

3.2.2 Az Ügyfél személyes adatokat tartalmazó elektronikus vagy fizikai adathordozók biztonságos megsemmisítésére vonatkozó eljárások.

3.2.3 Kialakított folyamat az Ügyfél összes fizikai adathordozójának nyomon követésére az Iron Mountain kezdeti felügyeletétől a végleges visszavonásig vagy megsemmisítésig.

4. MUNKAERŐ-BIZTONSÁGI INTÉZKEDÉSEK

4.1 Titoktartás. Az Iron Mountain észszerű mértékben megköveteli, hogy az Iron Mountain minden alkalmazottja, beleértve az ideiglenes és szerződéses alkalmazottakat is, vállalja a Személyes ügyféladatok bizalmas kezelését, és betartsa az Iron Mountain belső információbiztonsági és elfogadható felhasználási követelményeit.

4.2 Háttérvizsgálati szabályzat. Az Iron Mountain az alkalmazottjaira kiterjedően háttérvizsgálati szabályzattal és kábítószer-tesztelési szabályzattal rendelkezik (csak az Egyesült Államokban). Az Iron Mountain a Megállapodás időtartama alatt továbbra is fenntartja ezeket a szabályzatokat. A szabályzat többek között a következő követelményeket tartalmazza: drogszűrés (csak az Egyesült Államokban), a személyzet személyazonosságának ellenőrzése, bűnügyi nyilvántartásban végzett keresések, foglalkoztatási ellenőrzések, kormányzati/terrorista megfigyelési lista keresések, valamint bizonyos alkalmazottak iskolai végzettségének ellenőrzése, illetve járművezetői engedélyek és jogsértési előzmények a járművezetők jelöltjei és a meglévő járművezetők esetében. Ha a háttérellenőrzés során terhelő információkat azonosítanak, az Iron Mountain személyre szabott értékelést végez, az alkalmazandó munkaügyi jogszabályoknak és bevált gyakorlatoknak megfelelően.

4.3 Alvállalkozók bevonásával végzett munka. Az Iron Mountain megköveteli, hogy a Megállapodás alapján Szolgáltatásokat nyújtó alvállalkozók a jelen pontban meghatározottakhoz hasonló korlátozásokat

tartsanak be az alvállalkozók azon személyzete tekintetében, akik a Megállapodás alapján Szolgáltatásokat fognak nyújtani, és amelyek magukban foglalják a Személyes ügyféladatok kezelését.

4.4 Biztonságtudatossági képzés. Az Iron Mountain legalább évente általános biztonsági tudatosságnövelő képzést és konkrét szerepkörre vonatkozó biztonsági képzést tart az Iron Mountain minden olyan alkalmazottja számára, aki a Személyes ügyféladatokhoz hozzáfér. Az Iron Mountain nyilvántartást vezet, amelyben feltünteti a jelen lévő Iron Mountain alkalmazottak nevét és az egyes biztonsági tudatosságnövelő képzések dátumát. Az Iron Mountain rendszeresen felülvizsgálja és frissíti biztonsági tudatosságnövelő képzési programját.

4.5 Az Iron Mountain személyzet eltávolítása. Az Iron Mountain vállalatnál fegyelmi eljárás van érvényben, amelyet az Iron Mountain azon alkalmazottjai esetében alkalmaz, akik megsértik az itt leírt biztonsági követelményeket.

4.6 A hozzáférés megszüntetése megszüntetés/átruházás esetén. A felmondást vagy az olyan szerepkörbe való áthelyezést követően, amely nem igényel hozzáférést a Személyes ügyféladatokhoz, az Iron Mountain alkalmazottjának a Személyes ügyféladatokhoz való hozzáférését azonnal vissza kell vonni.

5. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

5.1 Fizikai biztonsági ellenőrzések. Az Iron Mountain létesítményei olyan fizikai ellenőrzéseket alkalmaznak, amelyek észszerű módon korlátozzák a Személyes ügyféladatokhoz való hozzáférést, beleértve - az Iron Mountain által megfelelőnek ítélt módon - a hozzáférés-ellenőrzési protokollokat, fizikai akadályokat, például zárt létesítményeket és területeket, az alkalmazottak belépési kártyáit, látogatói naplókat, látogatói belépési kártyákat, kártyaolvasókat, videokamerákat és behatolásjelző riasztó rendszereket. Minden látogatónak mindig be kell jelentkeznie és a látogatókhoz kíséretet kell biztosítani.

5.2 Közművek támogatása. Az Iron Mountain olyan intézkedéseket alkalmaz, amelyek célja, hogy megvédje a Személyes ügyféladatokat és rendszereket tartalmazó létesítményeit az áramellátás, a távközlés, a vízellátás, a szennyvíz, a fűtés, a szellőztetés és a légkondicionálás esetleges meghibásodásaitól.

5.3 Átviteli rendszer biztonsága. Az Iron Mountain olyan intézkedéseket alkalmaz, amelyek célja hálózati infrastruktúrája és távközlési rendszerei fizikai biztonságának védelme az átvitel lehallgatásával és károsodásával szemben.

5.4 Telephelyen kívüli berendezések. Abban az esetben, ha az Iron Mountain kiszervezi azokat a funkciókat, amelyek a szolgáltatások támogatása érdekében telephelyen kívüli berendezések használatát igénylik, a Személyes ügyféladatokat tároló telephelyen kívüli berendezéseket ugyanolyan biztonsági védelemmel kell védeni, mint az ugyanazon célra használt telephelyi berendezésekét.

5.5 Információkezelési eszközökhöz való fizikai hozzáférés. Az Iron Mountain egy évig nyilvántartást vezet az Iron Mountain által ellenőrzött számítógépes környezet(ek)hez való fizikai hozzáférésre felhatalmazott Iron Mountain alkalmazottakról, amelyeket az Iron Mountain használ a Szolgáltatások nyújtására, és az Ügyfél kérésére Biztonság incidens esetén, és az Iron Mountain biztonsági szabályzatainak megfelelően hozzáférést biztosít az Ügyfél számára az ilyen Iron Mountain alkalmazottak ellenőrizhető nyilvántartásainak megtekintéséhez.

5.6 Korlátozott fizikai hozzáférés. Az Iron Mountainnak a Személyes ügyféladatokat kezelő, Iron Mountain által ellenőrzött létesítményekhez való fizikai hozzáférést azokra az Iron Mountain alkalmazottakra és felhatalmazott személyekre kell korlátoznia, akiknek üzleti szempontból szükségük van az ilyen hozzáférésre. Az Iron Mountainnak rendelkeznie kell egy jóváhagyási eljárással az ilyen létesítményekhez való fizikai hozzáférésre vonatkozó kérelmek engedélyezésére és nyomon követésére.

5.7 Javítások és módosítások. Az Iron Mountainnak rögzítenie kell a biztonsággal kapcsolatos javításokat és módosításokat bármely fizikai összetevőn, beleértve a hardvert, a falakat, az ajtókat és a biztonságos területek zárait azon létesítményekben, ahol Személyes ügyféladatokat tárolnak.

5.8 Nyilvántartások. Nyilvántartás vezetése a hardverek és az elektronikus adathordozók mozgásáról, valamint minden felelős személyről.

6. KOMMUNIKÁCIÓS ÉS INFORMÁCIÓKEZELÉSI MŰVELETEK KEZELÉSE

6.1 Eszközkonfigurációs szabványok. Az Iron Mountain az iparági szabványoknak megfelelő rendszeradminisztrációs eljárásokat hoz létre, vezet be és tart fenn, beleértve többek között a rendszerkeményítést, a rendszer- és eszközjavítást (operációs rendszer és alkalmazások), valamint a megfelelő vírusirtó telepítést és a frissítéseket.

6.2 Információkezelő rendszerek változásellenőrzése. Az Iron Mountain belső, formális változáskezelési folyamattal rendelkezik az információkezelési és kommunikációs hálózati rendszerekre vonatkozóan, és az Iron Mountain változáskéréseit dokumentálják, tesztelik és jóváhagyják az új információkezelési vagy hálózati kommunikációs képességek, rendszerjavítások vagy a meglévő rendszerek módosításainak bevezetése előtt.

6.3 A feladatok elkülönítése. Az Iron Mountain elkülöníti a feladatokat és felelősségi területeket, hogy egyetlen személy se tudja módosítani a Személyes ügyféladatokhoz hozzáférő információkezelő rendszereket.

6.4 A fejlesztési és termelési környezetek különválasztása. Az Iron Mountain információkezelésirendszerekre vonatkozó fejlesztési, tesztelési és termelési környezeteit logikailag vagy fizikailag el kell különíteni egymástól.

6.5 Műszaki architektúra-menedzsment. Az Iron Mountainnek létre kell hoznia egy konfigurációkezelési folyamatot a Szolgáltatások nyújtásához használt információkezelési rendszer összetevőinek és az ilyen összetevők műszaki infrastruktúrájának meghatározására, kezelésére és ellenőrzésére.

6.6 Behatolásészlelés. Az Iron Mountain folyamatosan figyelemmel kíséri a számítógépes rendszereket és folyamatokat a megkísérelt vagy tényleges biztonsági behatolások vagy jogsértések tekintetében, és értesíti az Ügyfelet a Személyes ügyféladatokhoz való jogosulatlan hozzáférésről.

6.7 Hálózati biztonság. Az Iron Mountainnak biztosítania kell a következőket:

6.7.1 A Szolgáltatások nyújtására használt Iron Mountain által üzemeltetett környezet(ek)re vonatkozóan a hálózati behatolásérzékelő rendszer („IDS") és a behatolás-megelőzési érzékelők („IPS") naplózásra kerülnek, és a napi jelentéseket kiadják felülvizsgálatra (együttesen „IDS/IPS");

6.7.2 A Szolgáltatások nyújtásához használt Iron Mountain által üzemeltetett környezet(ek) tekintetében legalább heti rendszerességgel, de a frissítések beérkezését követően a lehető legrövidebb időn belül frissített IDS/IPS rendszerek, valamint a legújabb fenyegetés-jelzések vagy szabályok azonnali futtatása;

6.7.3 A külső rendszerek nagy kockázatú portjai nem érhetők el az internetről;

6.7.4 Az Iron Mountain hálózati kapcsolatait naplózza és naplófájlokban rögzíti;

6.7.5 Tűzfal(ak) telepítése, amelyek célja a meghatározott hálózati pontok közötti összes bejövő és kimenő hálózati szolgáltatás forgalom védelme és ellenőrzése;

6.7.6 Az információbiztonsági program keretében dokumentált és engedélyezett valamennyi, az Iron Mountain tulajdonában lévő vagy felügyelt rendszer bejövő és kimenő hálózati portjainak vagy szolgáltatási forgalmának meghatározására vonatkozó szabályzatok kidolgozása;

6.7.7 Megfelelően védett hálózati és diagnosztikai portok; és

6.7.8 Az Iron Mountain információs rendszereit érintő rosszindulatú kódok vagy ismert támadások megelőzésére, észlelésére és eltávolítására szolgáló szabályzatok, eljárások és műszaki ellenőrzések.

6.8 Titkosított hitelesítő adatok. Az Iron Mountainnek gondoskodnia kell arról, hogy az Iron Mountain hálózati eszközein továbbított hitelesítő adatok titkosítva legyenek a továbbítás során.

6.9 Biztonságos hálózati adminisztráció. Az Iron Mountain hálózatokat észszerű módon kell kezelni és ellenőrizni az ismert fenyegetésektől való védelem, valamint a hálózaton lévő vagy a hálózaton áthaladó adattovábbítás során kezelt összes Iron Mountain alkalmazás és adat biztonságának a fenntartása érdekében. Technikai ellenőrzéseket és biztonságos kommunikációs protokollokat kell bevezetni a nem megbízható hálózatokhoz vagy nyilvánosan elérhető szerverekhez való korlátlan csatlakozás tiltása érdekében.

6.10 Vírusvédelem. Az Iron Mountain vírusirtó programot vezet be és tart fenn, ideértve a kártevők elleni védelmet, a naprakész aláírásfájlokat vagy a felmerülő fenyegetések, javítások és vírusdefiníciók elleni alternatív védelmet, az Iron Mountain által kezelt szerverek és munkaállomások számára, amelyeket a Személyes ügyféladatok tárolására vagy elérésére használnak.

6.11 Weboldal – Ügyféltitkosítás. Az Iron Mountainnek biztosítania kell, hogy minden egyes weboldala esetében engedélyezve legyen a Secure Sockets Layering (SSL), és azok tartalmazzanak egy érvényes SSL tanúsítványt, amely titoktartási, hitelesítési vagy engedélyezési ellenőrzést igényel.

6.12 Információk biztonsági mentése. Az Iron Mountainnek megfelelő biztonsági másolatokat kell készítenie a rendszerfájlokról. Ezenkívül az Iron Mountainnek katasztrófa-helyreállítási eljárásokat kell kidolgoznia és fenntartania, további részletekért lásd az alábbi „Katasztrófa-helyreállítás" című pontot.

6.13 Továbbítás alatt álló elektronikus információk. Az Iron Mountain az Iron Mountain által üzemeltetett infrastruktúrából származó, nyilvános hálózatokon keresztül továbbított Személyes ügyféladatok védelme érdekében legalább 128 bites kulcshosszúságú, ipari szabványú algoritmussal történő titkosítást alkalmaz.

6.14 Kriptográfiai ellenőrzések. Az Iron Mountainnek követnie kell a titkosítási ellenőrzések használatára vonatkozó dokumentált szabályzatot. Az Iron Mountain kriptográfiai ellenőrzései(t):

6.14.1 Úgy kell kialakítani, hogy azok a Megállapodás feltételeinek megfelelően észszerűen védjék az Iron Mountain által a megosztott hálózati környezetben feldolgozott, továbbított vagy tárolt Személyes ügyféladatok titkosságát és integritását;

6.14.2 az Iron Mountain által üzemeltetett, a szolgáltatások nyújtásához használt környezet(ek)ben kell alkalmazni a „nem megbízható" hálózatokon (azaz az Iron Mountain által jogilag nem ellenőrzött hálózatokon) keresztül vagy azokba történő átvitel során a Személyes ügyféladatokra, beleértve az Iron Mountain hálózatáról az Ügyfél vállalati hálózatára történő adatküldésre használt hálózatokat is, minden esetben az Ügyfélnek az Ügyfél által fogadott adattovábbítások titkosításának megszüntetéséhez szükséges titkosítási kulcsok kezelésében való együttműködése mellett; és

6.14.3 Ide tartoznak a kriptográfiai technológiák biztonságát támogató, dokumentált titkosítási kulcskezelési gyakorlatok.

6.14.4 Magukba foglalják a laptopokon vagy más hordozható eszközökön tárolt összes Személyes ügyféladat titkosítását.

6.15 Bejelentkezési követelmények. Az Iron Mountain köteles biztosítani a következőket:

6.15.1 Jelentős biztonsági és rendszeresemények naplózása és ellenőrzése;

6.15.2 Az Iron Mountain által a szolgáltatások nyújtásához használt, az Iron Mountain által hosztolt környezet(ek)ben lévő rendszerek ellenőrzési naplóinak legalább egy évig történő megőrzése;

6.15.3 A rendszer auditálási naplóinak felülvizsgálata rendellenességek szempontjából; és

6.15.4 A naplózási létesítményekre és rendszerekre vonatkozó információk észszerű védelmet élveznek a manipuláció és az illetéktelen hozzáférés ellen.

6.16 Hálózati időszinkronizálás. Az Iron Mountain az összes információkezelési rendszer óráit közös, hiteles időforrás segítségével szinkronizálja.

6.17 Hálózati elkülönítés. Az Iron Mountain megfelelően elkülöníti az információs szolgáltatások, felhasználók és információs rendszerek kapcsolódó csoportjait a hálózatokon.

7. HOZZÁFÉRÉS-ELLENŐRZÉS

7.1 Hozzáférés-ellenőrzési szabályzat. Az Iron Mountain hozzáférés-ellenőrzési szabályzatokat tart fenn az Iron Mountain által hivatalosan jóváhagyott, közzétett és megvalósított információkezelési eszközök tekintetében.

7.2 Logikai hozzáférés engedélyezése. Az Iron Mountainnek rendelkeznie kell egy jóváhagyási eljárással a Személyes ügyféladatokhoz való logikai hozzáférési kérelmekre, valamint a Szolgáltatásokban való használatra kijelölt Iron Mountain rendszerekhez való hozzáférési kérelmekre vonatkozóan.

7.3 Hozzáférés-ellenőrzés és hozzáférés-áttekintés. Az Iron Mountain kizárólag az Iron Mountain azon aktív alkalmazottai számára biztosít hozzáférést a Személyes ügyféladatokhoz, ideértve az ideiglenes és szerződéses alkalmazottakat, valamint az aktív felhasználói fiókokat, akiknek munkakörük ellátásához szükségük van ilyen hozzáférésre. Minden privilegizált hozzáférést felül kell vizsgálni és meg kell erősíteni olyan szempontból, hogy az megfelel-e a jelenlegi munkakörnek, és azt legalább negyedévente dokumentálni kell.

7.4 Harmadik felek általi hozzáférés ellenőrzése. Mielőtt hozzáférést biztosítana az Iron Mountain azon információs rendszereihez, amelyek hozzáférnek a Személyes ügyféladatokhoz, az Iron Mountainnek biztosítania kell a megfelelő ellenőrzések meglétét.

7.5 Működési rendszerek hozzáférés-ellenőrzése. Az Iron Mountainnek az operációs rendszerekhez (szoftver- és hardveralapú operációs rendszerekhez egyaránt) való hozzáférést egy olyan biztonságos bejelentkezési folyamattal kell ellenőriznie, amely egyedileg azonosítja az operációs rendszerhez hozzáférő személyt.

7.6 Mobil számítástechnikai eszközök. Az Iron Mountainnek olyan szabályzattal vagy eljárással kell rendelkeznie, amely megvédi az Iron Mountain mobil számítástechnikai eszközeit a jogosulatlan hozzáféréstől. Az ilyen szabályzatoknak vagy eljárásoknak a fizikai védelmet, a hozzáférés-ellenőrzést és a biztonsági ellenőrzéseket, például a titkosítást, a vírusvédelmet és az eszköz biztonsági mentését kell kezelniük.

7.7 Ügyfélrendszerek leválasztása. Az Iron Mountain a Szolgáltatások nyújtására használt, tárolt környezet(ek)ben logikailag elválasztja és elkülöníti a Személyes ügyféladatokat minden egyéb információtól.

7.8 Fiókok. Az Iron Mountain a következőket teszi a fiókok tekintetében:

7.8.1 A személyes adatokat kezelő Iron Mountain rendszerekhez való hozzáférést kereső és a megosztott felhasználói fiókok vagy általános hitelesítő adatokkal (azaz azonosítókkal) rendelkező felhasználói fiókok használatát megtiltó Iron Mountain alkalmazottak személyazonosságának hitelesítését igényli a Személyes ügyféladatokhoz vagy a rendszereihez való hozzáféréshez.

7.8.2 Előírja, hogy minden felhasználói fiók azonosítóját, beleértve a kiváltságos fiókokat is, közvetlenül egy személyhez (és ne egy pozícióhoz) kössék.

7.8.3 Ha az alapértelmezett rendszergazdai fiókok nincsenek letiltva vagy eltávolítva, előírja ideiglenes jelszavak, kijelentkezési azonosítók vagy hasonló ellenőrzések használatát az alapértelmezett adminisztrációs fiókokhoz való hozzáféréshez.

7.8.4 Előírja az inaktív rendszeres fiókok 90 napos inaktivitás utáni zárolását vagy letiltását.

7.8.5 Megtiltja a fiókhoz való hozzáférést több sikertelen hozzáférési kísérlet után.

7.8.6 Egyedi azonosítókat és erős jelszavakat ír elő, amelyek legalább a következőket tartalmazzák: legalább 8 karakter; 90 naponta kötelező módosítás; és bonyolultsági követelmények.

7.8.7 Megtiltja az alkalmazottaknak, hogy jelszavakat osszanak meg vagy írjanak le.

7.9 A felügyelet nélküli rendszerek ellenőrzése. Az Iron Mountainnak jelszóval védett képernyővédőt kell használnia minden olyan rendszer esetében, amelyet felügyelet nélkül hagynak és amelyen 30 percig nem végeztek tevékenységet.

8. INFORMÁCIÓS RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA

8.1 Rendszerfejlesztési biztonság. Az Iron Mountainnak biztosítania kell, hogy a biztonság részét képezze minden információs rendszer fejlesztésének és azok műveleteinek, és az alkalmazásfejlesztés biztonsági szabványai alapján közzé kell tenni és be kell tartani a belső biztonságos kódolási módszereket.

8.2 Szoftverbiztonság-kezelés. Az Iron Mountain információs rendszereit (beleértve az operációs rendszereket, infrastruktúrát, üzleti alkalmazásokat, szolgáltatásokat és a felhasználó által kifejlesztett alkalmazásokat) úgy kell megtervezni, hogy azok megfeleljenek az információbiztonsági szabványoknak.

8.3 Hálózati diagramok. Az Iron Mountainnak a hálózati eszközökről és a forgalomról fizikai és logikai diagramokat kell kidolgoznia, dokumentálnia és fenntartania.

8.4 Alkalmazás-sebezhetőségi értékelés/Etikus hackelés. Az Iron Mountain legalább évente sebezhetőségi felméréseket végez a tárolt környezetében (környezeteiben) található alkalmazásokon, amelyeket a

Személyes ügyféladatok kezelésére szolgáló szolgáltatások nyújtására használnak. A részletes eredmények az Iron Mountain bizalmas és védett információi, amelyek nem kerülnek átadásra.

8.5 Változás tesztelése és felülvizsgálata. Az Iron Mountain a telepítés előtt felülvizsgálja és teszteli az alkalmazások és operációs rendszerek változásait annak biztosítása érdekében, hogy az ne legyen káros hatással a Személyes ügyféladatokra vagy a rendszereire.

9. KATASZTRÓFA-HELYREÁLLÍTÁS

Az Iron Mountain katasztrófa utáni helyreállítási tervet tart fenn, amely magában foglalja a Szolgáltatások biztonsági mentési adatközpontba történő támogatásához használt rendszerek és elektronikus adatok replikációját. A rendszerek és elektronikus adatok reprodukálása nem terjed ki az Iron Mountain létesítményében fizikailag tárolt Személyes ügyféladatokra. Az Iron Mountain üzleti folytonossági tervet tart fenn a kritikus üzleti funkciók helyreállítása érdekében. Az Iron Mountain legalább tizenkét (12) havonta egyszer elvégzi a katasztrófa utáni helyreállítási tesztelést.

10. KÜLSŐ AUDITOK ÉS ÉRTÉKELÉSEK

Az Iron Mountain biztonsági protokolljait úgy tervezték meg, hogy azok megfeleljenek az iparági szabványoknak. Az Iron Mountain az Ügyfél rendelkezésére bocsátja az általa megrendelt, harmadik féltől származó független ellenőrzési jelentéseket (pl. PCI, ISO27001, SOC2 stb.), amelyek a Szolgáltatásokra vonatkoznak abban a régióban, ahol az ilyen Szolgáltatásokat nyújtják („Auditjelentés”). Az Iron Mountain minden ilyen jelentést azzal a céllal bocsát rendelkezésre, hogy azok az ügyfelek számára elérhetőek legyenek, függetlenül a jelentés eredményeitől. Az Iron Mountain nem köteles átadni azon belső auditok eredményeit vagy más független értékelések eredményeit, amelyeket azzal a szándékkal rendeltek meg, hogy az Iron Mountain számára bizalmasak legyenek. Az Ügyfél és annak külső auditorai kérésre megkapják az Auditjelentés másolatait. A jelen pontban előírt tesztek vagy auditok során létrehozott bármely Auditjelentés vagy egyéb eredmény az Iron Mountain Bizalmas információjának minősül. Az Ügyfélnek jogában áll az ilyen Auditjelentés egy példányát átadni az Ügyfél bármely érintett ügyfele vagy szabályozó hatósága részére, az e dokumentumban foglaltakkal megegyező mértékben korlátozó jellegű titoktartási rendelkezések mellett. Az Ügyfél kérésére az Iron Mountain írásban megerősíti, hogy az ilyen Auditjelentés elkészítése óta nem történt változás a vonatkozó szabályzatokban, eljárásokban és belső ellenőrzésekben, és ez nem haladhatja meg az Auditjelentésben szereplő bejelentési időszak végétől számított három hónapot.

3. MELLÉKLET

Nemzetközi adattovábbítások

1. FOGALOMMEGHATÁROZÁSOK

„**2021. évi EU-s általános szerződési feltételek**”: a személyes adatok harmadik országokba történő továbbítására vonatkozó, a GDPR szerinti általános szerződési feltételek, amelyeket az Európai Bizottság a Bizottság (EU) 2021/914 végrehajtási határozatával fogadott el, és amely itt[3] érhető el.

„**2022. évi egyesült királyságbeli kiegészítés”**: az Egyesült Királyság Információs Biztosának Hivatala által kiadott és a Parlament elé a 2018. évi adatvédelmi törvény 119A szakaszának megfelelően 2022. február 2-án benyújtott B.1.0 minta-kiegészítés, amely annak 18. szakasza alapján felülvizsgálható, és amely itt[4] érhető el.

„**EU-s személyes ügyféladatok**”: a Személyes ügyféladatok olyan jellegű kezelése, amelyre az Iron Mountain általi adatkezelést megelőzően az Európai Unió, illetve az Európai Unió vagy az Európai Gazdasági Térség valamely tagállamának adatvédelmi jogszabályai vonatkoztak;

A „**Védett terület**” jelentése:

i. EU-s személyes ügyféladatok esetén az Európai Unió és az Európai Gazdasági Térség tagállamai, valamint minden olyan ország, terület, ágazat vagy nemzetközi szervezet, amelyre vonatkozóan a GDPR 45. cikke szerinti megfelelőségi határozat van hatályban;

ii. egyesült királyságbeli személyes ügyféladatok esetében, az Egyesült Királyság és minden olyan ország, terület, ágazat vagy nemzetközi szervezet, amelyek tekintetében az Egyesült Királyság megfelelőségi szabályai szerinti megfelelőségi határozat van hatályban;

iii. svájci személyes ügyféladatok esetében bármely ország, terület, ágazat vagy nemzetközi szervezet, amelyet Svájc jogszabályai szerint megfelelőnek ismernek el;

iv. bármely más, EU-s, egyesült királyságbeli vagy svájci személyes ügyféladatok vonatkozásában hasonló védelmet nyújtó joghatóságon kívülre továbbított Személyes ügyféladatok esetében bármely olyan ország, terület, ágazat vagy nemzetközi szervezet, amelyet az adott joghatóság jogszabályai megfelelőnek ismernek el;

„**Általános szerződési feltételek**”: együttesen a 2021. évi EU-s általános szerződési feltételek és a 2022. évi egyesült királyságbeli kiegészítés.

„**Svájci személyes ügyfél**adatok”: a Személyes ügyféladatok olyan kezelése, amelyre Svájc adatvédelmi jogszabályai vonatkoznak az Iron Mountain általi kezelés előtt;

„**Egyesült királyságbeli személyes ügyfél**adatok”: a Személyes ügyféladatok olyan kezelése, amelyre az Egyesült Királyság adatvédelmi jogszabályai vonatkoznak az Iron Mountain általi kezelés előtt;

2. VEGYES RENDELKEZÉSEK

2.1 A jelen 3. melléklet a következő részekre terjed ki: (i) A. rész – EU-s személyes ügyféladatok továbbítása; (ii) B. rész – svájci személyes ügyféladatok továbbítása; (iii) C. rész – egyesült királyságbeli személyes ügyféladatok továbbítása, amelyek a Személyes ügyféladatoknak az Iron Mountain által a Szolgáltatásokkal kapcsolatban történő továbbítása tekintetében alkalmazandók.

2.2 Az Általános szerződési feltételek az Iron Mountainre és annak társvállalataira mint „adatátvevőkre”, valamint az Ügyfélre és annak társvállalataira mint „adatátadókra” vonatkoznak.

2.3 A Megállapodás aláírása és keltezése az általános szerződési feltételekhez szükséges összes aláírást és keltezést is magában foglalja.

2.4 Abban az esetben, ha a felek EU-s, egyesült királyságbeli vagy svájci személyes ügyféladatokat védett területen kívülre továbbítanak, és az Európai Bizottság vonatkozó határozata vagy az alkalmazandó adatvédelmi jogszabályok szerinti más érvényes megfelelőségi módszer, amelyre az Iron Mountain az adattovábbítás során támaszkodott, érvénytelennek minősül, vagy ha bármely felügyeleti hatóság a Személyes adatok ilyen határozat alapján végrehajtott továbbításának a felfüggesztését követeli meg, a felek együttműködnek és elősegítik egy alternatív továbbítási mechanizmus alkalmazását. A felek megállapodnak abban is, hogy a jelen 3. mellékletben a nemzetközi adattovábbítások elősegítésére alkalmazott megfelelő garanciák nem kizárólagosak, és hogy a felek további adattovábbítási mechanizmusokat alkalmazhatnak, ilyen például az EU-USA Adatvédelmi Keretrendszer.

A. RÉSZ – AZ EU-S SZEMÉLYES ÜGYFÉLADATOK TOVÁBBÍTÁSA

Ha és amennyiben az Ügyfél vagy Társvállalatai a Védett területen kívülre továbbítják az EU-s személyes ügyféladatokat az Iron Mountain vagy Társvállalatai részére a Megállapodás szerinti Iron Mountain

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[4] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

Szolgáltatásokkal kapcsolatban, a 3. melléklet jelen A. része alkalmazandó, és a Felek a következőkben állapodnak meg:

1. **Általános szerződési feltételek kiválasztása.** A 2021. évi EU-s általános szerződési feltételek MÁSODIK MODULJÁNAK szövege abban az esetben alkalmazandó, ha az Ügyfél vagy annak bármely Társvállalata adatkezelő, és az Iron Mountain vagy annak bármely Társvállalata adatfeldolgozó; a 2021. évi EU-s általános szerződési feltételek HARMADIK MODULJÁNAK szövege abban az esetben alkalmazandó, ha az Ügyfél vagy annak bármely Társvállalata adatfeldolgozó, és az Iron Mountain vagy annak bármely Társvállalata további adatfeldolgozó. A 2021. évi EU-s általános szerződési feltételek vonatkozó rendelkezései hivatkozás útján beépülnek a jelen DPA-ba és a jelen DPA szerves részét képezik. A 2021. évi EU-s általános szerződési feltételekben lehetőségként megjelölt egyéb modulok vagy záradékok nem alkalmazandók. A 2021. évi EU-s általános szerződési feltételek mellékleteinek céljaihoz szükséges információkat az 1. melléklet – Az adatkezelés/továbbítás leírása, a 2. melléklet – Technikai és szervezési intézkedések, valamint a DPA 6.2. pontja – További adatfeldolgozók listája tartalmazza.

2. **További adatfeldolgozók alkalmazása.** A 2021. évi EU-s általános szerződési feltételek 9. feltétele alkalmazásában a további adatfeldolgozók Szolgáltatások teljesítéséhez történő használatára vonatkozó 2. opció (Általános írásos engedély) alkalmazandó. Az Ügyfél tudomásul veszi és elfogadja, hogy az Iron Mountain a jelen DPA 6. pontjában megállapított mechanizmuson keresztül új további adatfeldolgozókat vehet igénybe, és hogy a további adatfeldolgozók módosítási kérelmeinek benyújtására tizenöt (15) nap áll rendelkezésre.

3. **Az eljáró bíróság és a joghatóság megválasztása.** A 2021. évi EU-s általános szerződési feltételek 17. feltétele (Irányadó jog) alkalmazásában a 2. lehetőség szerinti irányadó jog az alkalmazandó, és ezekre a feltételekre azon EU tagállam joga vonatkozik, amelyben az adatátadó székhelye található, amennyiben az lehetővé teszi a harmadik fél kedvezményezetti jogait. A 2021. évi EU-s általános szerződési feltételek (Az eljáró bíróság és a joghatóság megválasztása) 18. feltétele alkalmazásában ezek annak az EU tagállamnak a bíróságai, amelyben az adatátadó székhelye található.

4. **Törlés igazolása.** A 2021. évi EU-s általános szerződési feltételek 8.5. feltétele és a 16. feltételének (d) pontja alkalmazásában az Iron Mountain kizárólag az Ügyfél írásbeli kérésére köteles igazolni a Személyes adatok törlését az Ügyfél számára.

5. **Adatvédelmi incidensek.** A 2021. évi EU-s általános szerződési feltételek 8.6. feltételének (c) pontja alkalmazásában az adatvédelmi incidenseket a DPA 7. pontjában megállapított mechanizmusnak megfelelően kell kezelni.

6. **Auditok.** A 2021. évi EU-s általános szerződési feltételek 8.9. feltétele alkalmazásában e feltételek ellenőrzését a Megállapodásban megállapított ellenőrzési mechanizmusnak megfelelően kell elvégezni.

7. **Panaszok.** A 2021. évi EU-s általános szerződési feltételek 11. feltétele alkalmazásában az Iron Mountain tájékoztatja az Ügyfelet, ha az Érintettől az EU személyes ügyféladatokkal kapcsolatban panasz érkezik be hozzá, és a panaszt a Megállapodásban megállapodott mechanizmusnak megfelelően közli az Ügyféllel.

8. **Felügyeleti hatóság.** A 2021. évi EU-s általános szerződési feltételek tekintetében az illetékes felügyeleti hatóságot az EU általános szerződési feltételek 13. feltételével összhangban kell meghatározni.

B. RÉSZ – SVÁJCI SZEMÉLYES ÜGYFÉLADATOK TOVÁBBÍTÁSA

Ha és amennyiben az Ügyfél vagy társvállalatai a Védett területen kívülre továbbítják a svájci személyes ügyféladatokat az Iron Mountain vagy társvállalatai részére a Megállapodás szerinti Iron Mountain Szolgáltatásokkal kapcsolatban, a 3. melléklet jelen B. része alkalmazandó, és a Felek a következőkben állapodnak meg:

1. **Általános szerződési feltételek kiválasztása.** A 2021. évi EU-s általános szerződési feltételek és az A. rész vonatkozó rendelkezései abban az esetben alkalmazandók, ha az Ügyfél vagy annak bármely Társvállalata Adatkezelő, és az Iron Mountain vagy annak bármely Társvállalata Adatfeldolgozó, és/vagy az Ügyfél vagy annak bármely Társvállalata Adatfeldolgozó, és az Iron Mountain vagy annak bármely Társvállalata További Adatfeldolgozó, kivéve, hogy:

   a. a 2021. évi EU-s általános szerződési feltételek 13. feltétele szerinti illetékes felügyeleti hatóság a Svájci Szövetségi Adatvédelmi és Információs Bizottság;

   b. a 2021. évi EU-s általános szerződési feltételek 17. feltétele szerinti szerződéses követelésekre vonatkozó alkalmazandó jogszabály a svájci jog, és a felek közötti, a 18. feltétel (b) pontja szerinti intézkedések joghatóságának helye a svájci bíróság.

2. A 2021. évi EU-s általános szerződési feltételekben az EU GDPR-re való hivatkozások az FADP-re való hivatkozásokként értelmezendők.

3. A 2021. évi EU-s általános szerződési feltételekben szereplő „tagállam” kifejezés nem értelmezhető úgy, hogy az kizárja a Svájcban élő Érintetteket a szokásos tartózkodási helyük (Svájc) szerinti jogaik miatti perindítás lehetőségéből a 2021. évi EU-s általános szerződési feltételek 18. feltételének (c) pontja szerint.

C. RÉSZ – EGYESÜLT KIRÁLYSÁGBELI SZEMÉLYES ÜGYFÉLADATOK TOVÁBBÍTÁSA

Ha és amennyiben az Ügyfél vagy Társvállalatai a Védett területen kívülre továbbítják az egyesült királyságbeli személyes ügyféladatokat az Iron Mountain vagy Társvállalatai részére a Megállapodás szerinti Iron Mountain Szolgáltatásokkal kapcsolatban, a 3. melléklet jelen C. része alkalmazandó, és a Felek a következőkben állapodnak meg:

1. **Általános szerződési feltételek kiválasztása.** A 2021. évi EU-s általános szerződési feltételek A. részének vonatkozó rendelkezései és a 2022. évi egyesült királyságbeli kiegészítés alkalmazandó, ha az Ügyfél vagy annak bármely Társvállalata adatkezelő, és az Iron Mountain vagy annak bármely Társvállalata adatfeldolgozó, és/vagy az Ügyfél vagy annak bármely Társvállalata adatfeldolgozó, és az Iron Mountain vagy annak bármely Társvállalata további adatfeldolgozó.

2. **1. rész: A 2022. évi egyesült királyságbeli kiegészítés 1-3. táblázata:** A Felekre vonatkozó információk – 1. táblázat; Kiválasztott ÁSZF-ek, modulok és kiválasztott feltételek; és függelék információk, beleértve az 1A mellékletet: A Felek listája, 1B melléklet: Az adattovábbítás leírása és 1C melléklet: Az adatok biztonságát garantáló technikai és szervezési intézkedések - 3. táblázat, a jelen 3. mellékletre hivatkozva teljesítettnek tekintendők, beleértve az egyesült királyságbeli kiegészítés A. rész, 4. táblázatot is: Az Ügyfél és az Iron Mountain tudomásul veszi és elfogadja, hogy az egyesült királyságbeli kiegészítését bármelyik Fél felmondhatja.

3. **2. rész:** Az egyesült királyságbeli kiegészítés kötelező feltételei: Az Ügyfél és az Iron Mountain tudomásul veszi és elfogadja az egyesült királyságbeli kiegészítés kötelező feltételeit.

4. **Felügyeleti hatóság.** Az Egyesült Királyság Információs Biztosának Hivatala illetékes felügyeleti hatóságként jár el.

D. RÉSZ – EGYÉB SZEMÉLYES ÜGYFÉLADATOK TOVÁBBÍTÁSA

Ha és amennyiben az Ügyfél vagy társvállalatai olyan Személyes ügyféladatokat továbbítanak az Iron Mountain vagy társvállalatai részére, amelyekre nem terjed ki az A-C. RÉSZ hatálya, a Megállapodás szerinti Iron Mountain Szolgáltatásokkal kapcsolatban a 3. melléklet A. része alkalmazandó az irányadó Adatvédelmi jogszabályok szerinti releváns és alkalmazandó mértékig. Egyébként, amennyiben az Adatvédelmi jogszabályok értelmében bármely helyettesítő vagy további megfelelő biztosíték vagy továbbítási mechanizmus szükséges a Személyes ügyféladatok olyan országba történő továbbításához, amely az adatátadó szempontjából nem biztosít megfelelő szintű védelmet a Személyes adatok számára, a felek megállapodnak abban, hogy a lehető leghamarabb bevezetik azokat, és dokumentálják az ilyen végrehajtási követelményeket a jelen DPA mellékletében.

4. MELLÉKLET

HIPAA – Üzlettársi megállapodás (Business Associate Agreement, „BAA")

A jelen BAA kiegészíti és módosítja az Iron Mountain és társvállalatai, valamint az Ügyfél és társvállalatai között létrejött valamennyi jelenlegi vagy jövőbeli Megállapodást, amelyek alapján az Iron Mountain vagy társvállalatai bizonyos Szolgáltatásokat nyújtanak az Ügyfél vagy társvállalatai számára, és amelyek Szolgáltatások megkövetelik az Üzlettárstól, hogy az Érintett szervezet nevében felhasználja és/vagy közzétegye a védett egészségügyi adatokat. A jelen BAA-ban módosítottak kivételével a Megállapodásban rögzített valamennyi feltétel teljes mértékben érvényes és hatályos marad, és irányadó az Iron Mountain által az Ügyfélnek nyújtott Szolgáltatások tekintetében.

Az Iron Mountain és az Ügyfél azért kötik meg a jelen BAA-t, hogy mindkét fél eleget tegyen a vonatkozó kötelezettségeiknek, amint azok hatályba lépnek és kötelező erejűek lesznek a felekre nézve a HIPAA Adatvédelmi, biztonsági és jogsértés bejelentésére vonatkozó szabályai szerint, beleértve az Omnibus-szabály részeként bevezetett szabályokat is (együttesen „HIPAA-szabályok"), amely alapján az Ügyfél és társvállalatai „Érintett szervezet" vagy „Üzlettárs", az Iron Mountain és társvállalatai pedig az Ügyfél „Üzlettársa". A jelen Megállapodás alkalmazásában a továbbiakban az Üzlettársra történő hivatkozások az Iron Mountainre vagy annak megfelelő társvállalatára történő hivatkozásoknak tekintendők.

1. FOGALOMMEGHATÁROZÁSOK

A jelen BAA-ban használt, de itt másként meg nem határozott nagybetűs kifejezések jelentése megegyezik a HIPAA-szabályokban vagy a Megállapodásban meghatározott jelentéssel, esettől függően.

„**Incidens-értesítési szabály**": a nem biztonságos védett egészségügyi adatokkal kapcsolatos incidens-értesítésre vonatkozó szabályt jelenti a 45 CFR §164 D alpontjában.

„**Üzlettárs**": a fent megnevezett Üzlettárs szervezetét jelenti, amennyiben Védett egészségügyi információkat kap, tart fenn vagy továbbít az Ügyfeleknek nyújtott Szolgáltatások során.

„**HIPAA**": az egészségbiztosítás hordozhatóságáról és elszámoltathatóságáról szóló 1996. évi törvény.

„**HITECH törvény**": a 2009. évi amerikai helyreállításról és új befektetésekről szóló törvénybe beépített, a gazdasági és klinikai egészséget szolgáló egészségügyi információs technológiáról szóló törvény vonatkozó rendelkezései, beleértve az esetleges végrehajtási rendelkezéseket is.

„**Adatvédelmi szabály**": a 45 CFR 160.§ és 164.§, A és E alpontokban található, egyénileg azonosítható egészségügyi adatok adatvédelmi normái.

„**Védett egészségügyi adatok**" vagy „**PHI**": jelentése megegyezik a 45 CFR 160.103. § „védett egészségügyi adatok" kifejezésével, és az Üzlettárs által az Ügyfél nevében létrehozott vagy az Ügyféltől vagy annak nevében a Megállapodás alapján kapott védett egészségügyi adatokra korlátozódik.

„**Biztonsági szabály**": az elektronikus védett egészségügyi adatok védelmére vonatkozó biztonsági szabványokat jelenti a 45 CFR 160.§ és 164.§, A és C alpontokban.

2. AZ ÜZLETTÁRS KÖTELEZETTSÉGEI ÉS TEVÉKENYSÉGEI

2.1. Az Üzlettárs vállalja, hogy nem használ fel vagy ad ki további védett egészségügyi adatokat a jelen BAA által megengedett vagy előírt, illetve a jogszabályok által előírt eseteken kívül.

2.2. Az Üzlettárs vállalja, hogy megfelelő biztosítékokat alkalmaz, és adott esetben megfelel a 45 CFR 164.§ C alpontjának az elektronikus PHI tekintetében, hogy megakadályozza a PHI-nek a jelen BAA-ban vagy a Megállapodásban előírtaktól eltérő felhasználását vagy nyilvánosságra hozatalát; azonban a felek elismerik és megállapodnak abban, hogy az Ügyfél és nem az Üzlettárs felelőssége, hogy megfeleljen a 45 CFR 164.312.§ szerinti követelményeknek a titkosítási vagy dekódolási mechanizmusok alkalmazása tekintetében a fizikai adathordozókon (pl. szalagokon) tárolt elektronikus PHI-re vonatkozóan, amelyet az Ügyfél az Üzlettársnál tárol.

2.3. Az Üzlettárs vállalja, hogy haladéktalanul jelenti az Ügyfélnek a védett egészségügyi adatok olyan biztonsági incidensét, megsértését vagy egyéb felhasználását vagy közzétételét, amelyről tudomást szerez, és amelyet a jelen BAA vagy a Megállapodás nem engedélyez vagy ír elő. Incidens előfordulása esetén az ilyen értesítést a HIPAA-szabályoknak megfelelően és az adott üzlettárs által megkövetelt módon kell megtenni, beleértve többek között a 45 CFR 164.410-et, de semmiképpen sem több mint három (3) munkanappal azt követően, hogy az Üzlettárs befejezte a belső vizsgálatot, és megerősítette az Incidens megtörténtét. Az Üzlettárs köteles észszerű segítséget és együttműködést nyújtani az ilyen Incidens kivizsgálásában, és dokumentálni a veszélyeztetett konkrét Betéteket, bármely jogosulatlan harmadik fél azonosítását, aki hozzáférhetett vagy megkaphatja a védett egészségügyi adatokat, ha az ismert, és minden olyan intézkedést, amelyet az Üzlettárs tett az ilyen jogsértés hatásainak enyhítése érdekében.

2.4. Az Üzlettárs a 45 CFR 164.502(e)(1)(ii) és a 164.308(b)(2) rendelkezéseivel összhangban köteles gondoskodni arról, hogy minden olyan üzlettárs, aki alvállalkozóként PHI-t hoz létre, kap, tart fenn vagy továbbít az Üzlettárs nevében a Megállapodás szerinti Szolgáltatások nyújtásának elősegítése céljából, elfogadja ugyanazokat a korlátozásokat, feltételeket és követelményeket, amelyek az Üzlettársra vonatkoznak az ilyen PHI-k tekintetében a jelen BAA-n keresztül.

2.5. Ha az Üzlettárs PHI-t őriz egy Kijelölt nyilvántartási készletben az egyénekre vonatkozóan, és ha az Ügyfél ezt kéri, az Üzlettárs beleegyezik abba, hogy hozzáférést biztosít az ilyen PHI-hoz az Ügyfélnek azáltal, hogy visszakeresi és átadja az ilyen PHI-t a Megállapodás feltételeinek megfelelően, így az Ügyfél válaszolhat egy Egyénnek a 45 CFR 164.524.§ követelményeinek teljesítése érdekében.

2.6. Az Üzlettárs elfogadja, hogy amennyiben az Üzlettárs felügyelete alá tartozó Kijelölt nyilvántartási készletben a PHI módosítására van szükség, és ha az Ügyfél arra utasítja az Üzlettársat, hogy a Megállapodásnak megfelelően szerezze be az ilyen PHI-t, akkor az Üzlettársnak el kell végeznie azt a szolgáltatást annak érdekében, hogy az Ügyfél a 45 CFR 164.526.§ alapján az Ügyfél vagy egy Egyén által megkövetelt módon bármilyen módosítást elvégezhessen az ilyen PHI-ken.

2.7. Az Üzlettárs vállalja, hogy dokumentálja és az Ügyfél rendelkezésére bocsátja a PHI közzétételek elszámolásához szükséges információkat, feltéve, hogy az Ügyfél elegendő információt adott az Üzlettársnak ahhoz, hogy az Üzlettárs meghatározhassa, mely nyilvántartások vagy adatok tartalmaznak PHI-t az Ügyféltől vagy az Ügyfél nevében az Üzlettárs által. A Közzétételek dokumentációjának tartalmaznia kell olyan információkat, amelyek szükségesek ahhoz, hogy az Ügyfél válaszolhasson egy Egyénnek a PHI közzétételek elszámolására vonatkozó kérésére a 45 CFR 164.528.§ vagy a HIPAA-szabályok egyéb rendelkezései szerint.

2.8. Hacsak a Megállapodás kifejezetten másként nem rendelkezik, az Üzlettárs haladéktalanul értesíti az Ügyfelet a védett egészségügyi adatokhoz való hozzáférésre, azok ismeretére vagy helyesbítésére vonatkozó kérelmekről, az ilyen kérelmek megválaszolása nélkül, és az Ügyfél felel az ilyen kérelmek átvételéért és megválaszolásáért.

2.9. Amennyiben az Üzlettárs a 45 CFR 164.§ E alpontja értelmében egy vagy több Ügyfél kötelezettséget teljesít, az Üzlettárs köteles betartani az E alpont azon követelményeit, amelyek az Ügyfélre vonatkoznak az ilyen kötelezettség(ek) teljesítése során.

2.10. Az Üzlettárs vállalja, hogy belső gyakorlatait, könyveit és nyilvántartásait elérhetővé teszi a Titkár számára a HIPAA-szabályok betartásának meghatározása céljából.

3. ÜZLETTÁRS ÁLTALI ENGEDÉLYEZETT FELHASZNÁLÁSOK ÉS KÖZZÉTÉTELEK

3.1. Az Üzlettárs a Megállapodásban meghatározott Szolgáltatások teljesítéséhez szükséges mértékben felhasználhatja vagy közölheti a védett egészségügyi adatokat.

3.2. Az Üzlettárs a védett egészségügyi adatokat a jogszabályok által előírtak szerint használhatja fel vagy teheti közzé.

3.3. Az Üzlettárs vállalja, hogy észszerű erőfeszítéseket tesz annak érdekében, hogy a védett egészségügyi adatokat a felhasználás, közzététel vagy kérelem szándékolt céljának eléréséhez szükséges minimumra korlátozza.

3.4. Az Üzlettárs nem használhatja fel és nem adhatja ki a védett egészségügyi adatokat olyan módon, amely az Ügyfél által elkövetett cselekmény esetén sértené a 45 CFR 164.§ E alpontját.

3.5. Az Üzlettárs az Üzlettárs megfelelő kezelése és adminisztrációja, illetve az Üzlettárs jogi kötelezettségeinek teljesítése érdekében közölheti a védett egészségügyi adatokat, feltéve, hogy a Közzétételt jogszabály írja elő, vagy az Üzlettárs észszerű biztosítékot kap attól a személytől, akivel az információt közlik, hogy az információ bizalmas marad, és azt csak a jogszabályok által előírt módon vagy azon célokból használják fel vagy teszik a továbbiakban közzé, amelyek érdekében azt a személlyel közölték, és a személy értesíti az Üzlettársat minden olyan esetről, amelyről tudomást szerez azzal kapcsolatban, hogy az információk titkosságát megsértették.

4. AZ ÜGYFÉL KÖTELEZETTSÉGEI

4.1. Az Ügyfél nem utasíthatja az Üzlettársat arra, hogy olyan módon járjon el, amely nem felelne meg a HIPAA-szabályoknak.

4.2. Az Ügyfél köteles értesíteni az Üzlettársat a 45 CFR 164.520.§ szerinti adatvédelmi gyakorlatra vonatkozó értesítésében foglalt korlátozás(ok)ról, amennyiben az ilyen korlátozás hatással lehet az Üzlettárs PHI-nak felhasználására vagy közzétételére.

4.3. Az Ügyfél köteles értesíteni az Üzlettársat a védett egészségügyi adatok felhasználásához vagy közzétételéhez adott engedélyének bármely változásáról vagy visszavonásáról, amennyiben az ilyen változások befolyásolhatják a védett egészségügyi adatok Üzlettárs általi felhasználását vagy közzétételét.

4.4. Az Ügyfél köteles írásban értesíteni az Üzlettársat a védett egészségügyi adatok felhasználására vagy közzétételére vonatkozó minden olyan korlátozásról, amelyet az Ügyfél a 45 CFR 164.522.§ szerint elfogadott, amennyiben az ilyen korlátozás hatással lehet a védett egészségügyi adatok Üzlettárs általi felhasználására vagy közzétételére.

5. IDŐTARTAM ÉS MEGSZŰNÉS

5.1. A jelen BAA időtartama a Hatálybalépés napján kezdődik, és automatikusan megszűnik a következők közül a későbbi időpontban: (i) a Megállapodás lejárta, vagy (ii) amikor az Ügyfél által az Üzlettársnak átadott összes PHI megsemmisül vagy visszakerül az Ügyfélhez.

5.2. Ha valamelyik fél tudomást szerez a BAA másik fél általi súlyos megsértéséről, a nem szerződésszegő fél lehetőséget biztosít a szerződésszegés orvoslására. Ha a szerződésszegést elkövető fél nem orvosolja a szerződésszegést harminc (30) napon belül azt követően, hogy a szerződésszegést elkövető fél megkapta az ilyen lényeges szerződésszegés részleteit ismertető írásos értesítést, akkor a nem szerződésszegő fél jogosult a jelen BAA-t és a Megállapodást a Megállapodás feltételei szerint felmondani, vagy ha a felmondás nem kivitelezhető, köteles a problémát a Titkárnak vagy bármely más illetékes hatóságnak jelenteni.

5.3. A megszűnés joghatása:

5.3.1.1. Az alábbi 5.3.2. pontban foglaltak kivételével a jelen BAA bármely okból történő megszűnésekor az Üzlettárs köteles az Ügyféltől kapott összes PHI-t a Megállapodásnak megfelelően visszaszolgáltatni vagy megsemmisíteni. Ez a rendelkezés az Üzlettárs alvállalkozóinak vagy megbízottjainak birtokában lévő PHI-kre vonatkozik. Az Üzlettárs nem őrizheti meg a PHI-k egyetlen példányát sem.

5.3.1.2. Abban az esetben, ha az Üzlettárs megállapítja, hogy a PHI-k visszaszolgáltatása vagy megsemmisítése kivitelezhetetlen, az Üzlettárs értesíti az Ügyfelet azokról a feltételekről, amelyek a visszaszolgáltatást vagy megsemmisítést kivitelezhetetlenné teszik. Az Ügyfél értesítése után az Üzlettárs köteles a jelen BAA védelmét az ilyen PHI-kre kiterjeszteni, és az ilyen PHI-k további felhasználását és közlését azokra a célokra korlátozni, amelyek a visszajuttatást vagy megsemmisítést megvalósíthatatlanná teszik, mindaddig, amíg az Üzlettárs az ilyen védett egészségügyi adatokat a Megállapodás feltételei szerint fenntartja.

6. VEGYES RENDELKEZÉSEK

6.1. Kártalanítás. Az Üzlettárs vállalja, hogy mentesíti az Ügyfelet minden olyan bírság vagy büntetés alól, amelyet az Ügyfélre a Titkár által indított végrehajtási eljárás vagy egy állami főügyész által az Ügyfél ellen indított polgári per eredményeként szabnak ki, amely eljárás vagy per közvetlenül és kizárólag az Üzlettárs olyan tevékenységéből vagy mulasztásából ered, amely vagy a HIPAA-szabályok megsértése, vagy a jelen BAA lényeges megsértése („Követelés”). Az Üzlettárs nem köteles kártalanítani az Ügyfelet az ilyen bírságok vagy büntetések bármely olyan része tekintetében, amelyek (i) a HIPAA-szabályoknak vagy a jelen BAA Ügyfél általi megsértéséből, vagy (ii) az Ügyfél gondatlan vagy szándékos tevékenységeiből vagy mulasztásaiból erednek. A fenti kártalanítási kötelezettség kifejezetten feltétele annak, hogy az Ügyfél az Üzlettárs választása szerint és költségén, valamint saját választása szerinti ügyvéddel gyakoroljon jogot az ilyen Követelés ellenőrzésére vagy az azzal szembeni védekezésben való részvételre, feltéve azonban, hogy amennyiben az ilyen Követelés egy nagyobb eljárás vagy intézkedés része, az Üzlettársnak az ellenőrzésre vagy részvételre vonatkozó joga a Követelésre, és nem a nagyobb eljárásra vagy intézkedésre korlátozódik. Abban az esetben, ha az Üzlettárs él a védekezési lehetőséggel, akkor (i) az Üzlettárs az Ügyfél előzetes írásbeli hozzájárulása nélkül nem rendezhet semmilyen olyan követelést, amely a hiba beismerését igényli, (ii) az Ügyfél jogosult saját költségén részt venni a követelésben vagy a perben, és (iii) az Ügyfél köteles észszerűen igényelt módon együttműködni az Üzlettárssal. A fentiek rögzítik az Ügyfél egyedüli és kizárólagos jogorvoslati lehetőségét, valamint az Üzlettárs kizárólagos felelősségét a jelen BAA-val kapcsolatos bármely Követeléssel kapcsolatban az Ügyfél részéről felmerülő bármely veszteség, kár, költség vagy felelősség tekintetében.

6.2. Ideiglenes intézkedés. Az Üzlettárs tudomásul veszi, hogy a védett egészségügyi adatok Üzlettárs általi jogosulatlan használata vagy közzététele helyrehozhatatlan kárt okozhat az Ügyfélnek, amelyért az Ügyfél – amennyiben úgy dönt – ideiglenes intézkedést vagy más méltányos jogorvoslatot kérhet.

6.3. Szabályozói hivatkozások. A jelen BAA-ban a HIPAA-szabályok egy részére történő hivatkozás a HIPAA, az Adatvédelmi szabály, a Biztonsági szabály, a HITECH ACT vagy a végleges Omnibus-szabályok módosított és hatályos szakaszát jelenti, amelyek betartása kötelező

6.4. Módosítás. A felek vállalják, hogy jóhiszeműen tárgyalnak a jelen BAA minden olyan módosításáról, amely időről időre szükséges ahhoz, hogy az Ügyfél vagy az Üzlettárs megfeleljen a HIPAA-szabályok követelményeinek. Ha a felek nem tudnak kölcsönösen megállapodni bármely ilyen módosítás feltételeiről az Ügyfél által az Üzlettárshoz intézett ilyen írásbeli kérelem kézhezvételétől számított hatvan (60) napon belül, akkor bármelyik fél jogosult a jelen BAA-t és a Megállapodást felmondani, a másik fél részére legalább harminc (30) nappal korábban megküldött írásbeli értesítéssel.

6.5. Harmadik fél kedvezményezettek kizárása. A jelen BAA-ban foglalt, kifejezett vagy hallgatólagos egyetlen rendelkezés sem biztosít semmilyen jogot, jogorvoslatot, kötelezettséget vagy felelősséget az Ügyfélen, az Üzlettárson és azok jogutódain vagy engedményesein kívül senki más részére.

6.6. Független vállalkozó. Az Üzlettárs, beleértve annak igazgatóit, tisztviselőit, alkalmazottait és ügynökeit, független vállalkozónak minősül, és nem az Ügyfél képviselője vagy az Ügyfél munkaerő-állományának tagja (a szövetségi általános ügynökségi törvény meghatározása szerint). A fentiek általános jellegének korlátozása nélkül az Ügyfél nem jogosult az Üzlettársnak a szolgáltatások nyújtása során tanúsított magatartását ellenőrizni, irányítani vagy más módon befolyásolni, a jelen BAA vagy a Megállapodás érvényesítésén, illetve kölcsönös módosításán kívül.

6.7. Elsőbbség; A megállapodás teljessége. A jelen BAA-ban előforduló bármely kétértelműséget oly módon kell feloldani, hogy a felek betarthassák a HIPAA-szabályokat. A jelen BAA képezi a felek között annak

tárgyában létrejött teljes megállapodást, és hatályon kívül helyez a HIPAA-szabályokkal kapcsolatos minden korábbi közlést, nyilatkozatot, megállapodást és megegyezést, beleértve a felek között létrejött minden korábbi üzleti partneri megállapodást is.