Споразумение за обработване на данни

ЦЕЛ И ЙЕРАРХИЯ НА ДОКУМЕНТИТЕ

Настоящото Споразумение за обработване на данни, заедно с приложенията към него и всеки документ, към който има изрични препратки („**СОД**“), се счита за част от договора за услуги между Iron Mountain и Клиента („**Договорът**“). Правилата и условията на Договора се прилагат и се отнасят към правата и задълженията на страните по настоящото СОД.

Ако някои от правилата и условията, съдържащи се в настоящото СОД, са в противоречие с правилата и условията, изложени в Договора, правилата и условията, изложени в настоящото СОД, са управляващи правила и условия по отношение на предмета на настоящото СОД. Настоящото СОД отменя и заменя всички предишни споразумения за обработване на данни или клаузи за защита на данните или клаузи за поверителност между страните във връзка с Услугите, предоставяни съгласно Договора.

ОБЩИ УСЛОВИЯ

1. ОПРЕДЕЛЕНИЯ

Освен ако не е изрично посочено в настоящия документ, всички термини с главни букви имат същото значение, което им е дадено в Договора.

„**Администратор**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни;

„**Лични данни на Клиента**“ означава лични данни, принадлежащи или събрани от Клиента или негови свързани лица, обработвани като част от Услугите;

„**Субект на данни**“ означава идентифицирано или подлежащо на идентифициране физическо лице;

„Законодателство за защита на данните“ означава всички приложими закони и регламенти, свързани с обработването на лични данни, които могат да съществуват в съответните юрисдикции, включително, но не само ОРЗД на ЕС (Регламент (ЕС) 2016/679), ОРЗД на Обединеното кралство (ОРЗД, както е приложим като част от националното законодателство на Обединеното кралство по силата на раздел 3 от Закона за Европейския съюз (закон за оттеглянето) от 2018 г. и както е изменен от Закона за защита на данните, поверителността и електронните съобщения (с изменения и т.н.) Регламенти 2019 (за излизане от ЕС) (с изменения)), Закон за защита на данните от 2018 г., FADP (Швейцарски федерален закон за защита на данните), Щатските закони за защита на личните данни в САЩ, LGPD (Общ закон за защита на данните на Бразилия), PIPL (Закон за защита на личната информация на Китайската народна република) и всяко законодателство и/или регламент, внедрен или изработен в следствие на тях или който изменя, замества, възобновява или консолидира всеки от тях, включително, където е приложимо, насоки и кодекси за поведение, издадени от надзорните органи;

„**Лични данни**“ означава всяка информация, свързана със субект на данни;

„**Обработващ лични данни**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

„**Обработване**“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства, като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

„**Нарушение на сигурността**“ означава всяко случайно или неправомерно увреждане, унищожаване, загуба, промяна или неразрешено разкриване или достъп до Личните данни на Клиента, които Iron Mountain, неговите служители или подизпълнители обработват в процеса на предоставяне на Услугите;

„**Услуги**“ означава всички услуги, предоставяни от Iron Mountain или негови свързани лица към Клиента или негови свързани лица съгласно Договора;

„**Щатски закони за защита на личните данни в САЩ**“ означава всички щатски закони за защита на личните данни в САЩ, приложими към обработването на лични данни съгласно Договора, включително, без ограничение и както може да бъдат изменяни, заместване или заменяни от време на време: (1) Закон за поверителност на потребителите в Калифорния, изменен от Закона за правата за поверителност на Калифорния и всички регламенти за изпълнение, свързани със същия (заедно наричани „**CCPA**“), (2) Закон за поверителност на Колорадо („**CPA**“), (3) Закон за защита на данните на потребителите във Вирджиния („**CDPA**“), (4) Закон за поверителност на потребителите в Юта („**UCPA**“) и (5) Закон за защита на личните данни в Кънектикът („**CTDPA**“).

2. ОБХВАТ И ПОДРОБНОСТИ ЗА ОБРАБОТВАНЕТО НА ДАННИ

2.1 Това СОД се прилага към Личните данни на Клиента, обработвани от Iron Mountain като Обработващ лични данни, в хода на предоставянето на Услугите съгласно Договора от името на Клиента.

2.2 Iron Mountain може да събира и обработва лични данни на служителите на Клиента и на негови свързани лица като Администратор за легитимни бизнес цели, като управление на договорни и клиентски отношения, и в съответствие със законодателството за защита на данните и известието за поверителност на Iron Mountain, налично на уебсайтовете на Iron Mountain, и други приложими политики за поверителност. Задълженията на Iron Mountain, посочени в настоящото СОД, не се прилагат към обработването на такива Лични данни.

2.3 Предметът на обработването на лични данни е изпълнение на Услугите. Правата и задълженията на Клиента и Iron Mountain са посочени в настоящото СОД. Приложение 1 към настоящото СОД определя естеството, продължителността и целта на обработването, видовете лични данни на Клиента, които Iron Mountain обработва, и категориите субекти на данни, чиито лични данни се обработват.

2.4 Когато Iron Mountain обработва лични данни на Клиента в хода на предоставяне на Услугите, Iron Mountain ще:

2.4.1 Обработва личните данни на Клиента само в съответствие с документираните инструкции от Клиента. Ако законодателството, на което е подчинена Iron Mountain, изисква от него да обработва личните данни на Клиента за каквато и да е друга цел, Iron Mountain първо ще информира Клиента за това изискване, освен ако този закон/тези закони не забранява(т) това на важни основания от обществен интерес, и

2.4.2 Се съобразява по всяко време с приложимото законодателство за защита на данните и незабавно ще уведоми Клиента, ако по мнение на Iron Mountain дадена от Клиента инструкция за обработване на лични данни на Клиента нарушава приложимото законодателство за защита на данните.

2.5 Инструкциите на Клиента ще бъдат обвързващи за Iron Mountain, освен ако изпълнението на инструкциите не изисква предоставянето на услуга по Договора и Клиентът не се съгласява да плати възнаграждението за тази услуга.

2.6 Iron Mountain гарантира, че персоналът, на който е необходим достъп до Личните данни на Клиента, подлежи на обвързващо задължение за поверителност по отношение на тези Лични данни на Клиента, и предприема разумни стъпки, за да гарантира надеждността и компетентността на персонала на Iron Mountain, който има достъп до Личните данни на Клиента.

3. ПРЕДОСТАВЯНЕ НА СЪДЕЙСТВИЕ НА КЛИЕНТА

3.1 Iron Mountain ще оказва съдействие на Клиента, като винаги взема предвид естеството на Обработването:

3.1.1 чрез подходящи технически и организационни мерки и, доколкото е възможно, при изпълнение на задълженията на Клиента да отговори на искания от Субекти на данни, упражняващи правата си;

3.1.2 при осигуряване на спазването на задълженията на Клиента (като сигурност на обработването, уведомяване на надзорния орган за нарушение на сигурността на личните данни, съобщаване на субекта на данни за нарушение на сигурността на личните данни, оценка на въздействието върху защитата на данните и предварителна консултация с надзорните органи, когато обработването би довело до висок риск при липса на мерки, предприети от Администратора с цел намаляване на риска), като взема предвид информацията, с която разполага Iron Mountain, и

3.1.3 чрез предоставяне на Клиента на цялата информация, която Клиентът основателно поиска, за да позволи на Клиента да докаже, че са изпълнени задълженията му при избора и назначаването на Iron Mountain.

4. МЕРКИ ЗА СИГУРНОСТ

4.1 Като вземе предвид обичайните оперативни процедури, разходите за изпълнение и естеството, обхвата, контекста и целите на обработването, Iron Mountain ще приложи подходящи и разумни технически и организационни мерки, предназначени за защита на поверителността, цялостността и наличието на Личните данни на Клиента, както и за защита на Личните данни на Клиента срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване, повреждане, промяна или разкриване. Стандартите за сигурност на Iron Mountain са изложени в Приложение 2 към настоящото СОД.

4.2 Единствено Клиентът носи отговорност да прецени дали тези технически и организационни мерки отговарят на изискванията на Клиента.

5. СЪОТВЕТСТВИЕ СЪС ЗАКОНИТЕ

Клиентът и неговите свързани лица трябва: (i) да обработват Личните данни на Клиента в съответствие със Законодателството за защита на данните, (ii) да бъдат упълномощени да дават писмени инструкции на Iron Mountain за обработването на Лични данни на Клиента във връзка с Услугите (включително от името на трета страна, която е Администратор на Личните данни на Клиента) и (iii) по всяко време да запазват контрола и властта върху Личните данни на Клиента във връзка с Обработването.

6. ПОДОБРАБОТВАНЕ

6.1 Клиентът потвърждава и се съгласява, че Iron Mountain може да ангажира своята компания майка, нейните свързани лица и други подобработващи трети страни (включително подобработващи трети страни, ангажирани от свързаните лица или компанията майка на Iron Mountain) за целите на обработването на Лични данни на Клиента съгласно това СОД, предмет на клауза 6.2 по-долу.

6.2 Списък на подобработващите, одобрени от Клиента към датата на настоящото СОД, е наличен тук[1] . Iron Mountain може по всяко време да замени или назначи нов подобработващ, при условие че Клиентът получи петнадесет (15) дни предварително писмено уведомление и в рамките на този срок Клиентът не възрази срещу тези промени с доказуемо основание, свързано със защитата на данните . За да получава тези известия по имейл, Клиентът се абонира и управлява всеки съществуващ абонамент за услугата за известия на Iron Mountain чрез тази уеб страница[2].

6.3 Ако Клиентът не се абонира за тази услуга за известия, Iron Mountain не носи отговорност за липсата на известяване относно подобработващи лица и всички такива договорки ще се считат за позволени от Клиента**.** Ако Клиентът възрази срещу назначаването на заместник или нов подобработващ в писмена форма с доказуемо основание, свързано със защитата на данните, в рамките на петнадесет (15) дни от предварителното писмено уведомление, тогава Iron Mountain ще положи разумни усилия, за да осигури на Клиента промяна в Услугите или да препоръча промяна в конфигурацията или използването на Услугите от Клиента, във всеки случай с цел да се избегне обработването на Лични данни на Клиента от страна на подобработващия, който е обект на възражение, за разглеждане и одобрение от страна на Клиента. Ако Клиентът не одобри промените, предложени от Iron Mountain в рамките на петнадесет (15) дни, Iron Mountain може след предоставено на Клиента писмено уведомление незабавно да прекрати Услугата или част от Услугата, която не може да бъде предоставена от Iron Mountain без помощта на подобработващия, който е обект на възражение. Такова прекратяване не засяга полагаемите права и задължения на страните, при условие че няма да бъдат дължими такси, разходи или друга компенсация от страна на Iron Mountain или свързани лица на Iron Mountain във връзка с такова прекратяване и Клиентът незабавно придобива активите, които е предоставил на Iron Mountain като част от прекратените Услуги, при спазване на условията на Договора и за собствена сметка и разходи на Клиента.

6.4 Iron Mountain гарантира, че всеки договор с подобработващи лица в обхвата на настоящото СОД съдържа разпоредби, които във всички съществени аспекти са същите като тези в настоящото СОД и са съобразени с изискванията на приложимото законодателство за защита на данните. Когато подобработващо лице на Iron Mountain стане причина Iron Mountain да наруши задълженията си, възникващи от настоящото СОД или от приложимото законодателство за

[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=JTlzF2zjl-gYEq5GmWmZcbgd--hgyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

защита на данните, Iron Mountain ще остане изцяло отговорна пред Клиента за изпълнението на задълженията на Iron Mountain по настоящите условия.

7. НАРУШЕНИЯ НА СИГУРНОСТТА

7.1 В случай на предполагаемо нарушение на сигурността Iron Mountain ще:

7.1.1 предприеме незабавно действие за разследване на предполагаемото нарушение на сигурността и за идентифициране, предотвратяване и смекчаване на последиците от предполагаемото нарушение на сигурността и за отстраняване на нарушението на сигурността;

7.1.2 уведоми Клиента без ненужно забавяне, след като има разумна степен на сигурност, че е настъпило нарушение на сигурността, и ще предостави на Клиента подробно описание на нарушението на сигурността, включително информация, която е разумно необходима на Клиента, за да изпълни задълженията за докладване съгласно Законодателството за защита на данните.

7.2 Клиентът се съгласява, че Iron Mountain може да предоставя информацията по клауза 7.1.2 на етапи. В такива случаи, когато Iron Mountain няма достъп или не може да предостави на Клиента определена информация, посочена в клауза 7.1.2, Iron Mountain ще информира Клиента по съответния начин и Iron Mountain не носи отговорност за непредоставянето на такава информация.

8. ОДИТИ

При предоставяне на Iron Mountain на най-малко десет (10) работни дни предизвестие Iron Mountain ще позволи на Клиента и съответните му одитори или упълномощени представители да проведат одити или инспекции по време на срока на Договора, при условие че от Iron Mountain не се изисква да предоставя или да разрешава достъп до информация относно: (i) други клиенти на Iron Mountain, (ii) който и да е от външните доклади на Iron Mountain, които не са публични, и (iii) всички вътрешни доклади, изготвени от служители на Iron Mountain, отговорни за вътрешните одити или съответствието. Целите на одита или инспекцията съгласно тази клауза се ограничават до проверка дали Iron Mountain обработва Личните данни на Клиента в съответствие със задълженията си по настоящото СОД. С изключение на случаите на настъпило нарушение на сигурността, не трябва да се извършва повече от един такъв одит на всеки дванадесет-(12)-месечен период.

9. МЕЖДУНАРОДНИ ПРЕДАВАНИЯ НА ДАННИ (ОГРАНИЧЕНИ ПРЕДАВАНИЯ)

9.1 Доколкото е приложимо, с настоящото Клиентът се съгласява и разрешава международни предавания на Лични данни на Клиента към юридически лица, както е посочено в Раздел 6.2 и в съответствие с Приложение 3 за предоставянето на Услугите, и Клиентът и Iron Mountain се съгласяват:

9.1.1 да спазват приложимото законодателство за защита на данните по отношение на такива предавания;

9.1.2 че, като се имат предвид, без това да бъде изчерпателно, i) категориите лични данни на Клиента, ii) страните, чиито национални закони може да не предоставят ниво на защита на личните данни, сравнимо с това на законодателството на ЕС/Обединеното кралство, („**Трета държава**“), iii) съответните технически и организационни мерки, посочени в Раздел 7, и iv) съответните страни, участващи в обработването на такива Лични данни на Клиента, са извършили оценка на целесъобразността на съответния механизъм за предаване, приет по силата на настоящото споразумение, когато това се изисква от закона, и са установили, че този механизъм за предаване е подходящо изработен, за да гарантира, че за Личните данни, прехвърлени в съответствие с настоящото СОД, се осигурява ниво на защита в държавата на местоназначение, което по същество е еквивалентно на това, гарантирано съгласно Законодателството за защита на данните.

10. ОТГОВОРНОСТ И ОБЕЗЩЕТЕНИЕ

10.1 Независимо от каквото и да е противоречие, съдържащо се в Договора, в случай на нарушение на сигурността, причинено пряко от нарушение на задълженията на Iron Mountain по настоящото СОД, Iron Mountain ще възстанови на Клиента до степента, позволена от приложимото законодателство, извършените преки, подлежащи на проверка, необходими и разумно направени разходи за трети страни на Клиента при (а) разследването на такова нарушение на сигурността, (б) изготвянето и изпращането на уведомления до такива Субекти на данни и регулаторни органи, както се изисква от Законодателството за защита на данните, (в) предоставянето на услуги за кредитен мониторинг на такива лица, както се изисква от закона, за период, не по-дълъг от дванадесет (12) месеца, и (г) заплащането на частта от нормативните глоби, наказания или

санкции, наложени от надзорен орган, за която надзорният орган посочва, че Iron Mountain е пряко отговорна.

10.2 В случай че Субект на данни предяви иск срещу едната или срещу двете страни за предполагаемо нарушение на Законодателството за защита на данните („**Искания на субекта на данни**"), когато това е разрешено, всяка страна ще ръководи собствената си защита при всеки такъв иск (или своята част от защитата) и ще остане единствено отговорна за собствените си разноски, разходи и задължения, свързани с този иск, включително хонорари за правна помощ или суми, присъдени от съда да бъдат заплатени или възникнали поради сключено споразумение, при условие обаче, че когато всяка страна е отговорна за част или една от страните е отговорна за пълната сума на щетите, претърпени от Субекта на данни за същия инцидент или серия от инциденти, и Субектът на данни е получил пълната компенсация само от едната страна („**Обезщетяващата страна**"), тогава Обезщетяващата страна има право да поиска обратно от другата страна тази част от компенсацията, съответстваща на щетите, причинени от тази друга страна. Обезщетяващата страна може да предяви иска си към другата страна само в рамките на 12 месеца след инцидента, доколкото е разрешено от приложимото законодателство.

10.3 До максималната степен, позволена от приложимото законодателство, ограниченията на отговорността и всички изключения от щетите, посочени в Договора, уреждат общата отговорност за всички искове на Клиента срещу Iron Mountain, произтичащи или свързани с настоящото СОД и/или Договора. Тези ограничения на отговорността и изключенията от щетите се прилагат за всички искове, независимо дали възникват по договор, закононарушение или друга теоретична отговорност, и всяко посочване на отговорността на Iron Mountain означава колективната отговорност на Iron Mountain и всички свързани лица на Iron Mountain заедно за искове от страна на Клиента и всички други свързани лица на Клиента. До степента, изисквана от приложимото законодателство, този раздел не е предназначен да (i) променя или ограничава отговорността на страните за искове на субект на данни, направени срещу дадена страна, когато са налични съвместни и няколко отговорности, или (ii) да ограничава отговорността на която и да е от страните да заплаща глоби, наложени на тази страна от регулаторен орган.

10.4 Клаузи от 10.1 до 10.3 посочват единственото и изключително правно средство за защита на всяка страна и единствената отговорност на всяка страна за всяка загуба, щета, разход или отговорност във връзка с настоящото СОД.

11. ИСКАНИЯ ОТ ПУБЛИЧЕН ОРГАН

11.1 До степента, позволена от закона и представляваща предмет на клаузи от 11.2 до 11.5 по-долу, Iron Mountain се съгласява да уведоми Клиента, ако:

11.1.1 получи правно обвързващо искане от публичен орган, включително съдебни органи, съгласно законите на държавата на местоназначение за разкриване на Лични данни на Клиента, пренасяни съгласно Договора, или

11.1.2 научи за всеки пряк достъп от страна на публични органи до Личните данни на Клиента, пренасяни съгласно Договора в съответствие със законите на държавата на местоназначение.

11.2 Ако на Iron Mountain е забранено да уведомява Клиента съгласно законите на страната на местоназначение, Iron Mountain се съгласява да положи всички усилия, за да получи отказ от забраната, с цел да съобщи възможно най-много информация възможно най-скоро.

11.3 Iron Mountain се съгласява да разгледа законността на искането за разкриване, по-специално дали то е в рамките на правомощията на изискващия публичен орган, и да оспори искането, ако заключи, че има основателни причини да се смята, че искането е незаконно съгласно законите на държавата на местоназначение. Iron Mountain няма да разкрива исканите Лични данни на Клиента, докато не бъде принудена да го направи съгласно приложимите процедурни правила.

11.4 Iron Mountain се съгласява да предостави минималното допустимо количество информация, когато отговаря на искане за разкриване, въз основа на разумно тълкуване на искането.

11.5 Iron Mountain се съгласява да съхранява информацията съгласно тази клауза за срока на Договора и да я предоставя на компетентния надзорен орган при поискване.

12. РАЗНИ

12.1 В зависимост от естеството на Услугите, предоставяни от Iron Mountain, при прекратяване/изтичане на Договора според специфичните инструкции на Клиента и при спазване на условията на Договора Iron Mountain трябва или да изтрие/унищожи, или да върне на Клиента или на трета страна, определена от Клиента, всички Лични данни на Клиента. Всички Лични данни на Клиента, съдържащи се в актива на Клиента, съхраняван от Iron Mountain от името на Клиента, ще бъдат върнати на Клиента в съответствие с договорен план за излизане или преход и при спазване на съгласуваните разходи, както е посочено в Договора или друг приложим договорен документ. Във всички останали случаи, ако Договорът не съдържа информация за изтриването/унищожаването или връщането на Лични данни на Клиента и Клиентът не даде никакви инструкции относно изтриването/унищожаването или връщането на Лични данни на

Клиента в рамките на петнадесет (15) дни от прекратяването/изтичането на Договора, Iron Mountain ще изпрати писмено уведомление до Клиента с искане за получаване в рамките на 15 (петнадесет) дни на конкретни инструкции дали да изтрие/унищожи, или да върне Личните данни на Клиента, и с информация за Клиента относно всички приложими възнаграждения за безопасното унищожаване или други възнаграждения, дължими от Клиента. Ако Клиентът не предостави писмени инструкции в рамките на този срок от петнадесет (15) дни и не заплати приложимите възнаграждения в рамките на същия период, Клиентът упълномощава с настоящото Iron Mountain да продължи да обработва, изтрива, унищожава всички Лични данни на Клиента след прекратяване на Договора по преценка на Iron Mountain и за сметка на Клиента.

12.2 Независимо от клауза 12.1 Iron Mountain не трябва да нарушава задълженията си по отношение на изтриването на Личните данни на Клиента, съхранявани на резервни записи, докато такива резервни записи не бъдат отхвърлени (и по този начин личните данни на Клиента бъдат изтрити) в нормалния ход на работата.

12.3 С изключение на Стандартните договорни клаузи (както са определени в Приложение 3 към настоящото СОД), настоящото СОД и всеки спор, иск или противоречие, произтичащи или свързани с настоящото СОД или с нарушението, прекратяването или изтичането на валидността му, се уреждат съгласно клаузата в Договора за избор на законодателство; и за всеки спор, противоречие или иск, произтичащи или свързани с настоящото СОД, преди всичко ще бъде търсено разрешаване чрез определен процес за разрешаване на спорове, съдържащ се в Договора.

12.4 Всяка страна може да уведомява другата страна в писмена форма от време на време за всякакви промени в настоящото СОД, които страната основателно смята за необходими за изпълнение на изискванията на законодателството за защита на данните или на решение на надзорен орган или компетентен съд. Всички такива промени ще влязат в сила само при взаимно договорено изменение на настоящото СОД, сключено от двете страни, и до степента, посочена в него, освен когато едната страна информира другата за всяко ново правно изискване и изпрати такова изменение, което включва само необходимите промени и което може да бъде прието без официално съгласие с него, т.е. при липса на отправено възражение в рамките на определен срок те се считат за взаимно договорени изменения на настоящото СОД.

ПРИЛОЖЕНИЕ 1

Подробности за обработването и предаването на данни (ако е приложимо)

А. СПИСЪК НА СТРАНИТЕ:

Страните по настоящото СОД и ролите на Износител на данни и Вносител на данни са посочени в Договора и Приложение 3 (Международни предавания на данни), ако е приложимо.

Б. ОПИСАНИЕ НА ОБРАБОТВАНЕТО/ПРЕДАВАНЕТО (ако е приложимо):

Категории Субекти на данни, чиито Лични данни се обработват/предават:

В зависимост от естеството на Услугите на Iron Mountain и сферата на дейност на Клиента Клиентът може да предостави на Iron Mountain Лични данни, принадлежащи на различни категории Субекти на данни, обхватът на които се определя и контролира от Клиента по негова преценка. Такива категориите Субекти на данни могат да включват: бивши и настоящи служители; бивши и настоящи изпълнители или консултанти; предоставени от агенции изпълнители или консултанти и външни служители; кандидати и претенденти за работа; студенти и доброволци; лица, определени от служители или пенсионирани служители за бенефициери, съпрузи, съвместно съжителстващи лица/партньори, зависещи лица и лица за контакт при спешни случаи; пенсионирани служители; бивши и настоящи директори и длъжностни лица; акционери; облигационери; титуляри на сметки; крайни потребители/клиенти (възрастни, деца); пациенти (възрастни, деца); преминаващи (камери за видеонаблюдение) и потребители на уебсайтове.

Категории обработвани/предавани Лични данни:

В зависимост от естеството на Услугите на Iron Mountain и сферата на дейност на Клиента, Клиентът може да предостави на Iron Mountain Лични данни, спадащи към различни категории Лични данни, обхватът на които се определя и контролира от Клиента по негова преценка. Такива категории могат да включват лични данни, свързани с Клиента и/или неговите собствени клиенти, служители и т.н.

Предавани чувствителни данни (ако е приложимо):

В зависимост от естеството на услугите на Iron Mountain и сферата на дейност на Клиента, Клиентът може да предостави на Iron Mountain чувствителни данни, обхватът на които се определя и контролира от Клиента по негова преценка.

Ако е приложимо, честота на предаване (напр. дали данните се предават еднократно или непрекъснато):

Предаването се извършва непрекъснато.

Естество на обработването:

Събиране, записване, организиране, структуриране, съхранение, адаптиране или изменяне, извличане, консултиране, използване, разкриване чрез предаване, разпространение или по друг начин предоставяне, съпоставяне или комбиниране, ограничаване, изтриване или унищожаване.

Цел(и) на обработването/предаването на данни (ако е приложимо) и по-нататъшно обработване:

Предоставянето на Услуги, както е посочено в Договора.

Запазване на данни:

Личните данни ще бъдат запазени от Iron Mountain за срока на Услугите, предлагани на Клиента, и до момента, в който Личните данни бъдат върнати или унищожени, както е определено в съответствие с клауза 12.1 от настоящото СОД.

Ако е приложимо, за предавания към (под)обработващи лични данни, посочете също предмета, естеството и продължителността на Обработването:

За срока на Договора с Клиента подобработващите лица предоставят, наред с другото, информационни технологии (ИТ) и консултантски услуги, включително глобална ИТ поддръжка, докладване на събития и услуги за управление.

В. КОМПЕТЕНТЕН НАДЗОРЕН ОРГАН

Както е посочено в Приложение 3 (Международни предавания на данни), ако е приложимо.

ПРИЛОЖЕНИЕ 2

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ („МЕРКИ ЗА СИГУРНОСТ“)

1. ПРОГРАМА И ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Iron Mountain ще поддържа програма за информационна сигурност с подходящи физически, технически и административни средства за контрол, изготвени така, че да отговарят на стандартите в областта. Програмата за информационна сигурност включва:

1.1 Документация, вътрешно публикуване и съобщаване на политиките, стандартите и процедурите за информационна сигурност на Iron Mountain;

1.2. Документирано ясно възлагане на отговорност и правомощия за изготвяне и поддържане на програмата за информационна сигурност;

1.3 Редовно тестване на ключовите средства за контрол, системи и процедури на програмата за информационна сигурност;

1.4 Административни, технически и оперативни мерки, изготвени така, че да защитават всички Лични данни на Клиента, като прилагат практиките, процедурите и процесите, описани в настоящото Приложение за сигурност, доколкото са подходящи и приложими за формата, в който се поддържат Личните данни на Клиента.

2. ОЦЕНКА НА РИСКА

Iron Mountain ще поддържа програма за оценка на риска за информационната сигурност, изготвена така, че да идентифицира и оцени разумно предвидими вътрешни и външни рискове и уязвимости, които биха могли да повлияят на сигурността, поверителността и/или целостта на личните данни на Клиента. За да се ограничат такива рискове, Iron Mountain ще оценява и актуализира, когато е необходимо, разумно и подходящо, ефективността на текущата програма за информационна сигурност на годишна база или когато има съществена промяна в риска или уязвимостта на Личните данни на Клиента.

3. УПРАВЛЕНИЕ НА АКТИВИ ЗА ОБРАБОТВАНЕ НА ИНФОРМАЦИЯ И ФИЗИЧЕСКИ НОСИТЕЛИ

3.1 Управление на активи за обработване на информация. Iron Mountain поддържа програма за управление на наличностите от активи, за да управлява физическите, техническите и административните средства за контрол по отношение на активите на Iron Mountain за обработване на информация (като компютри, сървъри, устройства за съхранение, комуникационни мрежи, персонални компютри, лаптопи и периферни устройства).
Програмата за управление на наличностите от активи включва следното:

- 3.1.1 Документирано приписване на собствеността върху активите на персонала на Iron Mountain, за да се осигури подходящо класифициране на информацията, определяне на ограниченията за достъп и преглед на средствата за контрол на достъпа.
- 3.1.2 Почистване на цялата информация от активите преди тяхното изхвърляне в съответствие с NIST 800-88.
- 3.1.3 Изискване за разрешение за управление преди отстраняването на оборудване или софтуер, който не е предназначен за конкретно лице, от помещенията на Iron Mountain.

3.2 Средства за контрол. Средствата за контрол на Iron Mountain включват следното:

- 3.2.1 Работни процедури и технически средства за контрол, предназначени за защита на документи, компютърни носители, входни/изходни/резервни данни и системна документация от неразрешено разкриване, модификация и унищожаване.
- 3.2.2 Процедури за надеждно изхвърляне на електронни или физически носители, съдържащи Лични данни на Клиента.
- 3.2.3 Установен процес за проследяване на всички физически носители на Клиента от първоначалното им предоставяне под грижите на Iron Mountain до окончателното им оттегляне или унищожаване.

4. МЕРКИ ЗА СИГУРНОСТ НА РАБОТНАТА СИЛА

4.1 Поверителност. Iron Mountain ще изисква в разумна степен от всички служители на Iron Mountain, включително от временни служители и служители на договор за изпълнение, да се съгласят да спазват поверителността на Личните данни на Клиента и да действат в съответствие с изискванията на Iron Mountain за вътрешна информационна сигурност и допустима употреба.

4.2 Политика за проверка на служителите. Iron Mountain има политика за проверка на служителите и политика за тестване за наркотични вещества (само за САЩ), която е в сила за неговите служители. Iron Mountain ще продължи да поддържа такива политики за срока на Договора. Изискванията на политиката включват, но не се ограничават само до скрининг за наркотични вещества (само за САЩ), проверка на самоличността на персонала, търсене в криминалните досиета, проверка на предишните работни места, търсене в правителствения списък за наблюдение/списъка за наблюдение на терористи, както и проверки на образователната степен за определени служители и правоспособността за управление на МПС за шофьори и история на нарушенията за кандидати за шофьори и настоящи шофьори. Когато при проверката на

служителите бъде идентифицирана компрометираща информация, Iron Mountain провежда индивидуализирана оценка в съответствие с приложимите трудови закони и най-добри практики.

4.3 Работа с подизпълнители. Iron Mountain ще изисква от всеки подизпълнител, извършващ Услуги по Договора, да спазва подобни ограничения като тези, посочени в настоящия раздел, по отношение на целия персонал на подизпълнителя, който ще извършва Услуги по Договора, включващи Обработване на Лични данни на Клиента.

4.4 Обучение за осведоменост по отношение на сигурността. Най-малко веднъж годишно Iron Mountain ще провежда обучение за осведоменост по отношение на общата сигурност и обучение за специфичната за дадена роля сигурност на всички служители на Iron Mountain с достъп до Лични данни на Клиента. Iron Mountain ще поддържа документация с имената на присъстващите служители на Iron Mountain и датата на всяко обучение за осведоменост по отношение на сигурността. Iron Mountain редовно ще преглежда и актуализира своята програма за обучение за осведоменост по отношение на сигурността.

4.5 Отстраняване на персонал на Iron Mountain. Iron Mountain поддържа дисциплинарна процедура, която се прилага към служителите на Iron Mountain, нарушаващи изискванията за сигурност, посочени в настоящия документ.

4.6 Прекратяване на достъпа при прекратяване/преназначаване. При прекратяване или преназначаване на друга позиция, която не изисква достъп до Лични данни на Клиента, достъпът на служител на Iron Mountain до Лични данни на Клиента се оттегля незабавно.

5. ФИЗИЧЕСКА И ЕКОЛОГИЧНА СИГУРНОСТ

5.1 Средства за контрол на физическата сигурност. Помещенията на Iron Mountain разполагат със средства за физически контрол, които разумно ограничават достъпа до Личните данни на Клиента, включително, както Iron Mountain счете за подходящо, протоколи за контрол на достъпа, физически бариери, като заключени помещения и зони, баджове за достъп за служители, регистри на посетителите, баджове за достъп за посетители, четци на карти, камери за видеонаблюдение и аларми за откриване на проникване. Всички посетители трябва да се регистрират и да бъдат придружавани по всяко време.

5.2 Помощни съоръжения. Iron Mountain ще прилага мерки, предназначени да защитят неговите помещения, съдържащи лични данни и системи на Клиента, от повреди в електрозахранването, телекомуникациите, водоснабдяването, канализацията, отоплението, вентилацията и климатизацията, както е приложимо.

5.3 Сигурност на системата за пренос. Iron Mountain ще прилага мерки, предназначени да защитят физическата сигурност на неговата мрежова инфраструктура и телекомуникационни системи от прихващане и повреда на сигнала.

5.4 Оборудване извън обекта. В случай че Iron Mountain възлага функции, които изискват използване на оборудване извън обекта в помощ на услугите, всяко оборудване извън обекта, съхраняващо Лични данни на Клиента, ще бъде защитено със сигурност, еквивалентна на тази, използвана за оборудването на място, използвано за същата цел.

5.5 Физически достъп до активи за обработване на информация. Iron Mountain ще съхранява за една година документация за служители на Iron Mountain, упълномощени за физически достъп до контролирана от Iron Mountain компютърна(и) среда(и), използвана(и) от Iron Mountain за предоставяне на Услуги, и по искане на Клиента, свързано с Нарушение на сигурността, и в съответствие с политиките за сигурност на Iron Mountain, ще осигури достъп на Клиента за преглед на подлежащата на одит документация за такива служители на Iron Mountain.

5.6 Ограничен физически достъп. Iron Mountain ще ограничава физическия достъп до контролирани от Iron Mountain помещения, в които се обработват Лични данни на Клиента, за тези служители на Iron Mountain и упълномощени лица, които имат служебна необходимост от такъв достъп. Iron Mountain ще има процедура за одобрение за упълномощаване и проследяване на искания за физически достъп до такива помещения.

5.7 Ремонти и модификации. Iron Mountain ще документира всички свързани със сигурността ремонти и модификации на всички физически компоненти, включително хардуер, стени, врати и ключалки на защитени зони, в помещенията, където се съхраняват Личните данни на Клиента.

5.8 Документация. Ще поддържа документация за движението на хардуера и електронните носители и за всяко лице, отговорно за това.

6. УПРАВЛЕНИЕ НА ОПЕРАЦИИТЕ ЗА КОМУНИКАЦИЯ И ОБРАБОТВАНЕ НА ИНФОРМАЦИЯ

6.1 Стандарти за конфигуриране на устройства. Iron Mountain ще създаде, внедри и поддържа процедури за системна администрация, които отговарят на стандартите в областта, включително, без това да бъде изчерпателно, подсилване на защитата на системата, коригиране на системата и устройството (операционна система и приложения) и правилна антивирусна инсталация и актуализации.

6.2 Контрол на промените на системите за обработване на информация. Iron Mountain ще има въведена вътрешна официална процедура за управление на заявките за промяна за системите за обработване на информация и комуникационните мрежи, а заявките за промяна на Iron Mountain ще бъдат документирани, тествани и одобрявани преди внедряването на нови мощности за обработване на информация или мрежови комуникации, системни корекции или промени в съществуващите системи.

6.3 Разделяне на задълженията. Iron Mountain ще разделя задълженията и областите на отговорност, така че никой човек да няма възможност самостоятелно да променя системите за обработване на информация, които имат достъп до Личните данни на Клиента.

6.4 Разделяне на средите за развойна и производствена дейност. Развойната, тестовата и производствената среда на Iron Mountain за системите за обработване на информация трябва да бъде логически или физически отделена.

6.5 Управление на техническата архитектура. Iron Mountain ще внедри процедура на управление на конфигурирането, за да дефинира, управлява и контролира компонентите на системата за обработване на информация, използвани за предоставяне на Услугите, и техническата инфраструктура на тези компоненти.

6.6 Откриване на проникване. Iron Mountain ще следи непрекъснато компютърните системи и процеси за опити или за действителни нарушения на сигурността и ще уведомява Клиента за всеки неразрешен достъп до Личните данни на Клиента.

6.7 Сигурност на мрежата. Iron Mountain ще осигури наличието на следното:

6.7.1 По отношение на хостваната(ите) от Iron Mountain среда(и), използвана(и) за предоставяне на Услугите, мрежовата система за откриване на проникване („IDS“) и сензорите за предотвратяване на проникване („IPS“) предупреждават за регистрирани събития с дневни доклади, издавани за преглед (наречени общо „IDS/IPS“);

6.7.2 По отношение на хостваната(ите) от Iron Mountain среда(и), използвана(и) за предоставяне на Услугите, IDS/IPS, които се актуализират не по-рядко от веднъж седмично, но възможно най-скоро след получаване на актуализациите и незабавно изпълнение на най-новите подписи или правила за заплахи;

6.7.3 Високорисковите портове на обърнатите навън системи не са достъпни през интернет;

6.7.4 Мрежовите връзки на Iron Mountain се регистрират и документират в регистрационни файлове;

6.7.5 Поставяне на защитна(и) стена(и), предназначена(и) да защитава(т) и инспектира(т) целия трафик на входящи и изходящи мрежови услуги между определени мрежови точки;

6.7.6 Политики за подсилване на защитата за определяне на входящи и изходящи мрежови портове или трафик на услуги за всички системи, притежавани или управлявани от Iron Mountain, които са документирани и разрешени в рамките на програмата за информационна сигурност;

6.7.7 Мрежови и диагностични портове, които са правилно обезопасени, и

6.7.8 Политики, процедури и технически средства за контрол, предназначени за предотвратяване, откриване и отстраняване на злонамерен код или известни атаки срещу информационните системи на Iron Mountain.

6.8 Криптирани идентификационни данни за удостоверяване. Iron Mountain ще гарантира, че идентификационните данни за удостоверяване, предавани през мрежовите устройства на Iron Mountain, се криптират при пренос.

6.9 Администрация на мрежата за сигурност. Мрежите на Iron Mountain трябва да бъдат разумно управлявани и контролирани, за да има защита от известни заплахи и за да се поддържа сигурността на всички управлявани приложения и данни на Iron Mountain в мрежата или при пренос по мрежата. Ще бъдат внедрени технически средства за контрол и протоколи за сигурна комуникация, за да се забранят неограничените връзки с ненадеждни мрежи или публично достъпни сървъри.

6.10 Защита от вируси. Iron Mountain ще внедри и поддържа програма за управление на защитата от вируси, включително защита от злонамерен софтуер, актуализирани файлове с подписи или алтернативна защита срещу възникващи заплахи, корекции и дефиниции за вируси, за сървърите и работните станции, управлявани от Iron Mountain и използвани за съхраняване или достъп до Лични данни на Клиента.

6.11 Криптиране уебсайт–клиент. Iron Mountain ще гарантира, че за всеки от неговите уебсайтове е активиран протокол „Secure Sockets Layering“ („SSL“) и се съдържа валиден SSL сертификат, изискващ контрол на поверителността, удостоверяването или оторизацията.

6.12 Архивиране на информация. Iron Mountain ще създаде подходящи резервни копия на системните файлове. Освен това Iron Mountain ще разработи и ще поддържа процедури за аварийно възстановяване, вижте раздела „Аварийно възстановяване“ по-долу за повече подробности.

6.13 Електронна информация при пренос. Iron Mountain ще използва криптиране със стандартен за областта алгоритъм с минимална дължина от 128 бита, за да защити Личните данни на Клиента, предавани в публични мрежи, когато произхождат от инфраструктура, хоствана от Iron Mountain.

6.14 Криптографски средства за контрол. Iron Mountain ще следва документирана политика за използване на криптографски средства за контрол. Криптографските средства за контрол на Iron Mountain:

6.14.1 ще бъдат проектирани за разумна защита на поверителността и целостта на Личните данни на Клиента, които се обработват, предават или съхраняват от Iron Mountain във всяка споделена мрежова среда, в съответствие с условията на Договора;

6.14.2 ще се прилагат в среда(и), хоствана(и) от Iron Mountain, използвана(и) за предоставяне на услуги, към Лични данни на Клиента, които се прехвърлят през или към „ненадеждни“ мрежи (т.е. мрежи, които Iron Mountain не контролира законно), включително тези, използвани за изпращане на данни към корпоративната мрежа на Клиента от мрежата на Iron Mountain, като във всеки случай ще зависят от сътрудничеството на Клиента при

управлението на криптиращи ключове, необходими за дешифриране на предавания, получени от Клиента, и

6.14.3 ще включват документирани практики за управление на ключове за криптиране в помощ на сигурността на криптографските технологии.

6.14.4 ще включват криптиране на всички Лични данни на Клиента на лаптопи или други преносими устройства.

6.15 Изисквания за вход. Iron Mountain ще осигури следното:

6.15.1 Значителните събития, свързани със сигурността и системите, се регистрират и преглеждат;

6.15.2 Регистрите на одитите се съхраняват за минимум една година за системи в среда(и), хоствана(и) от Iron Mountain, които се използват от Iron Mountain за предоставяне на услуги;

6.15.3 Регистрите за системен одит се преглеждат за аномалии и

6.15.4 Информацията за съоръженията и системите за регистриране е разумно защитена срещу подправяне и неразрешен достъп.

6.16 Синхронизиране на мрежовото време. Iron Mountain ще синхронизира системните часовници на всички системи за обработване на информация, като използва общ достоверен източник на точно време.

6.17 Разделяне в мрежите. Iron Mountain ще разделя по подходящ начин свързани групи от информационни услуги, потребители и информационни системи в мрежите.

7. КОНТРОЛ НА ДОСТЪПА

7.1 Политика за контрол на достъпа. Iron Mountain поддържа политики за контрол на достъпа по отношение на активите за обработване на информация, които Iron Mountain официално одобрява, публикува и внедрява.

7.2 Разрешение за логически достъп. Iron Mountain ще има процедура за одобрение за заявки за логически достъп до Личните данни на Клиента и искания за достъп до системите на Iron Mountain, предназначени за използване в Услугите.

7.3 Контрол на достъпа и преглед на достъпа. Iron Mountain ще предоставя достъп до Личните данни на Клиента само на активни служители на Iron Mountain, включително на временни служители и служители на договор за изпълнение, както и на активни потребителски акаунти, които се нуждаят от такъв достъп, за да изпълняват служебните си функции. Целият привилегирован достъп ще бъде преглеждан и потвърждаван, за да съответства на настоящата длъжност, и ще бъде документиран най-малко на тримесечна основа.

7.4 Контрол на достъпа на трети страни. Преди да предостави достъп на външни страни до информационните системи на Iron Mountain, които имат достъп до Лични данни на Клиента, Iron Mountain ще гарантира, че са въведени подходящи средства за контрол.

7.5 Контрол на достъпа до операционните системи. Iron Mountain ще контролира достъпа до операционните системи (както софтуерни, така и хардуерни операционни системи), като изисква сигурен процес на влизане, който уникално идентифицира лицето, което има достъп до операционната система.

7.6 Мобилни компютърни устройства. Iron Mountain ще има въведена политика или процедура, предназначена да защити мобилните компютърни устройства на Iron Mountain от неоторизиран достъп. Тези политики или процедури трябва да предоставят физическа защита, контрол на достъпа и контрол на сигурността, като криптиране, защита от вируси и архивиране на устройства.

7.7 Изолация на системите на клиента. В рамките на своята хоствана(и) среда(и), използвана(и) за предоставяне на Услугите, Iron Mountain логически отделя и изолира личните данни на Клиента от цялата друга информация.

7.8 Акаунти. Iron Mountain ще направи следното по отношение на акаунтите:

7.8.1 Ще изисква удостоверяване на самоличността на всеки служител на Iron Mountain, който иска достъп до системите на Iron Mountain, които обработват Лични данни на Клиента, и ще забранява използването на споделени потребителски акаунти или потребителски акаунти с общи идентификационни данни (т.е. ИД), за достъп до Лични данни на Клиента или системи.

7.8.2 Ще изисква всички ИД на потребителски акаунти, включително привилегировани акаунти, да бъдат свързани директно с дадено лице (а не с работна позиция).

7.8.3 Ако акаунтите за администриране по подразбиране не са деактивирани или премахнати, ще изисква използването на временни пароли, ИД за проверка или подобни средства за контрол за достъп до акаунта за администриране по подразбиране.

7.8.4 Ще изисква неактивните редовни акаунти да бъдат заключени или деактивирани след 90 дни бездействие.

7.8.5 Ще забрани достъпа до акаунт след няколко неуспешни опита за достъп.

7.8.6 Ще изисква уникални идентификатори и силни пароли, които включват най-малко следното: минимален брой знаци – 8; изискване за смяна на всеки 90 дни и изисквания за сложност.

7.8.7 Ще забрани на служителите да споделят или записват пароли.

7.9 Средства за контрол за ненаблюдавани системи. Iron Mountain ще използва защитен с парола скрийнсейвър за всички системи, които са оставени без надзор и не са имали дейност в продължение на 30 минути.

8. РАЗРАБОТВАНЕ И ПОДДРЪЖКА НА ИНФОРМАЦИОННИ СИСТЕМИ

8.1 Сигурност на разработването на системи. Iron Mountain ще гарантира, че сигурността е част от разработването и дейностите на всички информационни системи, и ще публикува и да се придържа към вътрешни методологии за сигурно кодиране, базирани на стандартите за сигурност за разработване на приложения.

8.2 Управление на софтуерната сигурност. Информационните системи на Iron Mountain (включително операционни системи, инфраструктура, бизнес приложения, услуги и разработени от потребителите приложения) трябва да бъдат проектирани така, че да отговарят на стандартите за информационна сигурност.

8.3 Мрежови диаграми. Iron Mountain ще разработва, документира и поддържа физически и логически диаграми на мрежови устройства и трафик.

8.4 Оценка на уязвимостта на приложението/Етично хакерство. Най-малко веднъж годишно Iron Mountain ще извършва оценки на уязвимостта на приложения в своята(ите) хоствана(и) среда(и), използвана(и) за предоставяне на услуги, които обработват Лични данни на Клиента. Подробните резултати са поверителна и собствена информация на Iron Mountain и няма да бъдат предоставяни.

8.5 Тестване и преглед на промените. Iron Mountain ще преглежда и тества промените в приложенията и операционните системи преди внедряването, за да гарантира, че няма неблагоприятен ефект върху Личните данни на Клиента или системите.

9. АВАРИЙНО ВЪЗСТАНОВЯВАНЕ

Iron Mountain ще поддържа план за аварийно възстановяване, включително репликация на системи и електронни данни, използвани за поддръжка на Услугите, в архивен център за данни. Репликацията на системи и електронни данни не включва Лични данни на Клиента, които физически се съхраняват в помещение на Iron Mountain. Iron Mountain ще поддържа план за непрекъснатост на работата за възстановяване на критичните работни функции. Iron Mountain ще извършва тестове за аварийно възстановяване не по-рядко от веднъж на всеки дванадесет (12) месеца.

10. ВЪНШНИ ОДИТИ И ОЦЕНКИ

Протоколите за сигурност на Iron Mountain са изготвени така, че да съответстват на стандартите в областта. Iron Mountain ще предостави на Клиента всички доклади от независими одити от трети страни, които е възложил (напр. PCI, ISO27001, SOC2 и т.н.), свързани с Услугите, в региона, в който се предоставят тези Услуги („Доклад от одит“). Iron Mountain ще предостави всички такива доклади, възложени с намерението да бъдат предназначени за клиентите, независимо от резултатите от доклада. От Iron Mountain няма да се изисква да предоставя резултати от вътрешен одит или резултати от други независими оценки, възложени с намерението да бъдат поверителни за Iron Mountain. При поискване на Клиента и на неговите външни одитори ще бъдат предоставени копия от Доклада от одита. Всеки Доклад от одит или друг резултат, получен от тестове или одити, изисквани съгласно настоящия раздел, ще се счита за Поверителна информация на Iron Mountain. Клиентът ще има право да предостави копие от този Доклад от одит на всички заинтересовани клиенти или регулаторни органи на Клиента, при спазване на клаузи за поверителност, толкова рестриктивни, колкото изложените в настоящия документ. По искане на Клиента Iron Mountain ще потвърди писмено, че няма настъпили промени в съответните политики, процедури и вътрешни средства за контрол след попълването на всеки такъв Доклад от одит, но не повече от три месеца след края на отчетния период на Доклада от одита.

ПРИЛОЖЕНИЕ 3

Международни предавания на данни

1. ОПРЕДЕЛЕНИЯ

„**Стандартни договорни клаузи на ЕС от 2021** г.“ означава стандартните договорни клаузи за предаването на лични данни на трети държави съгласно ОРЗД, приети от Европейската комисия съгласно Решение за изпълнение (ЕС) 2021/914 на Комисията, достъпно тук[3] .

„**Допълнение за Обединеното кралство от 2022** г.“ означава образец на Допълнение B.1.0, издадено от Службата на комисаря по информацията на Обединеното кралство и внесено в Парламента в съответствие с раздел 119A от Закона за защита на данните от 2018 г. на 2 февруари 2022 г., с редакции съгласно Раздел 18 настоящия документ, достъпно тук[4] .

„**Лични данни на Клиента от ЕС**“ означава обработването на Лични данни на Клиента, за които са приложими законите за защита на данните на Европейския съюз или на държава членка на Европейския съюз или Европейската икономическа зона преди обработването им от Iron Mountain;

„**Защитена зона**“ означава:

i. в случай на Лични данни на Клиент от ЕС, държавите членки на Европейския съюз и Европейското икономическо пространство и всяка държава, територия, сектор или международна организация, по отношение на които е в сила решение относно адекватността на защитата съгласно член 45 от ОРЗД;

ii. в случай на Лични данни на Клиент от Обединеното кралство, Обединеното кралство и всяка държава, територия, сектор или международна организация, по отношение на която е в сила решение относно адекватността на защитата съгласно разпоредбите за адекватност на Обединеното кралство;

iii. в случай на Лични данни на Клиент от Швейцария, всяка държава, територия, сектор или международна организация, за която е призната адекватност на защитата съгласно законите на Швейцария;

iv. в случай на други Лични данни на Клиент, предавани извън юрисдикция, предлагаща защита, подобна на тази на Личните данни на Клиент от ЕС, Обединеното кралство или Швейцария, всяка държава, територия, сектор или международна организация, за която е призната адекватност на защитата съгласно законите на тази юрисдикция;

„**Стандартни договорни клаузи**“ означават заедно Стандартните договорни клаузи на ЕС за 2021 г. и Допълнението за Обединеното кралство от 2022 г.

„**Лични данни на Клиент от Швейцария**“ означава обработването на Лични данни на Клиент, за което са приложими законите за защита на данните на Швейцария преди обработването им от Iron Mountain;

„**Лични данни на Клиент от Обединеното кралство**“ означава обработването на Лични данни на Клиент, за което са приложими законите за защита на данните на Обединеното кралство преди обработването им от Iron Mountain;

2. РАЗНИ

2.1 Настоящото Приложение 3 включва следните части: (i) Част А – Предавания на Лични данни на Клиент от ЕС; (ii) Част Б – Предавания на Лични данни на Клиент от Швейцария; (iii) Част В – Предаване на Лични данни на Клиент от Обединеното кралство, които ще се прилагат според случая за предаване на Лични данни на Клиент от Iron Mountain във връзка с Услугите.

2.2 Стандартните договорни клаузи се прилагат за Iron Mountain и неговите свързани лица като „вносители на данни“ и за Клиента и неговите свързани лица като „износители на данни“.

2.3 Подписът и датирането на Договора представляват всички необходими подписи и дати за Стандартните договорни клаузи.

2.4 В случай че страните пренасят Лични данни на Клиент от ЕС, от Обединеното кралство или Швейцария извън защитената зона и съответно решение на Европейската комисия или друг валиден метод за определяне на адекватност на защитата съгласно приложимото законодателство за защита на данните, на което Iron Mountain се позовава за прехвърлянето на данни, бъде сметнато за невалидно, или в случай че който и да е надзорен орган изисква предаването на Лични данни, направено съгласно такова решение, да бъде преустановено, страните ще си сътрудничат и ще улеснят използването на алтернативен механизъм за предаване. Страните също така се съгласяват, че подходящите предпазни мерки, използвани в настоящото приложение 3 за улесняване на международните предавания, не са изключителни и

[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

страните могат да следват допълнителни механизми за предаване, като например Рамката за защита на личните данни между ЕС и САЩ.

ЧАСТ А – ПРЕДАВАНИЯ НА ЛИЧНИ ДАННИ НА КЛИЕНТ ОТ ЕС

Ако и доколкото Клиентът или неговите Свързани лица предават Лични данни на Клиент от ЕС извън защитената зона към Iron Mountain или негови Свързани лица във връзка с Услугите на Iron Mountain съгласно Договора, се прилага тази част А на Приложение 3 и Страните се съгласяват, както следва:

1. **Избор на стандартни договорни клаузи.** Текстът от МОДУЛ ДВЕ от Стандартните договорни клаузи на ЕС от 2021 г. се прилага, когато Клиентът или някое от неговите Свързани лица е Администратор, а Iron Mountain или някое от неговите Свързани лица е Обработващ лични данни; текстът от МОДУЛ ТРИ от Стандартните договорни клаузи на ЕС от 2021 г. се прилага, когато Клиентът или някое от неговите Свързани лица е Обработващ лични данни, а Iron Mountain или някое от неговите Свързани лица е подобработващ лични данни. Съответните разпоредби, съдържащи се в Стандартните договорни клаузи на ЕС от 2021 г., са включени чрез позоваване в настоящото СОД и са неразделна част от настоящото СОД. Не се прилагат други модули или клаузи, маркирани като незадължителни в Стандартните договорни клаузи на ЕС от 2021 г. Информацията, необходима за целите на Приложенията към Стандартните договорни клаузи на ЕС за 2021 г., е посочена в Приложение 1 – Описание на обработването/предаването, Приложение 2 – Технически и организационни мерки, и Клауза 6.2 от СОД – Списък на подобработващите лични данни.

2. **Използване на подобработващи лица.** За целите на клауза 9 от Стандартните договорни клаузи на ЕС от 2021 г. се прилага вариант 2 (Общо писмено разрешение) за използването на подобработващи за изпълнението на Услугите. Клиентът потвърждава и се съгласява, че Iron Mountain може да ангажира нови подобработващи лица чрез механизма, договорен в клауза 6 от настоящото СОД, и че срокът за подаване на искания за промени към подобработващи лица е петнадесет (15) дни.

3. **Приложимо законодателство и избор на юрисдикция.** За целите на клауза 17 от Стандартните договорни клаузи на ЕС от 2021 г. (Приложимо право) се прилага вариант 2 относно приложимото право и тези клаузи се уреждат от правото на държавата членка на ЕС, в която е установен износителят на данни, доколкото позволяват правата на трета страна бенефициер. За целите на клауза 18 от Стандартните договорни клаузи на ЕС от 2021 г. (Избор на съд и юрисдикция) това са съдилищата на държавата членка на ЕС, в която е установен износителят на данни.

4. **Сертифициране на изтриването.** За целите на Клауза 8.5 и 16(г) от Стандартните договорни клаузи на ЕС от 2021 г. Iron Mountain предоставя на Клиента сертификат за изтриване на Лични данни само при писмено искане от страна на Клиента.

5. **Нарушения на сигурността на личните данни.**За целите на клауза 8.6(в) от Стандартните договорни клаузи на ЕС от 2021 г. нарушенията на сигурността на личните данни се обработват в съответствие с механизма, договорен в клауза 7 от СОД.

6. **Одити.**За целите на клауза 8.9 от Стандартните договорни клаузи на ЕС от 2021 г. одитите на тези клаузи се извършват в съответствие с механизма за одит, договорен в Договора.

7. **Оплаквания.** За целите на клауза 11 от Стандартните договорни клаузи на ЕС от 2021 г. Iron Mountain информира Клиента, ако получи оплакване от Субект на данни по отношение на Личните данни на Клиент на ЕС, и съобщава за оплакването на Клиента в съответствие с механизма, договорен в Договора.

8. **Надзорен орган.** За Стандартните договорни клаузи на ЕС от 2022 г. съответният компетентен надзорен орган се определя в съответствие с клауза 13 от Стандартните договорни клаузи на ЕС.

ЧАСТ Б – ПРЕДАВАНИЯ НА ЛИЧНИ ДАННИ НА КЛИЕНТ ОТ ШВЕЙЦАРИЯ

Ако и доколкото Клиентът или неговите свързани лица предават Лични данни на Клиент от Швейцария извън защитената зона към Iron Mountain или негови свързани лица във връзка с Услугите на Iron Mountain съгласно Договора, се прилага тази част Б на Приложение 3 и Страните се съгласяват, както следва:

1. **Избор на стандартни договорни клаузи.** Стандартните договорни клаузи на ЕС от 2021 г. и съответните разпоредби съгласно Част А се прилагат, когато Клиентът или някое от неговите Свързани лица е Администратор, а Iron Mountain или някое от неговите Свързани лица е Обработващ лични данни и/или Клиентът или някое от неговите Свързани лица е Обработващ лични данни, а Iron Mountain или някое от неговите Свързани лица е подобработващ лични данни, с изключение на случаите, в които:

а. компетентният надзорен орган съгласно Клауза 13 от Стандартните договорни клаузи на ЕС от 2021 г. е Швейцарската федерална комисия за защита на данните и информацията;

б. приложимото право за договорни искове съгласно клауза 17 от Стандартните договорни клаузи на ЕС от 2021 г. е швейцарското право, а мястото на юрисдикция за искове между страните съгласно клауза 18 (б) са швейцарските съдилища.

2. Позоваванията на ОРЗД на ЕС в Стандартните договорни клаузи на ЕС от 2021 г. трябва да се разбират като позоваванията на FADP.

3. Терминът „държава членка“ в Стандартните договорни клаузи на ЕС от 2021 г. не трябва да се тълкува по начин, който изключва Субектите на данни от Швейцария от възможността да заведат дело за своите права по обичайното си местопребиваване (Швейцария) в съответствие с Клауза 18 (в) от Стандартните договорни клаузи на ЕС от 2021 г.

ЧАСТ В – ПРЕДАВАНИЯ НА ЛИЧНИ ДАННИ НА КЛИЕНТ ОТ ОБЕДИНЕНОТО КРАЛСТВО

Ако и доколкото Клиентът или неговите Свързани лица предават Лични данни на Клиент от Обединеното кралство извън защитената зона към Iron Mountain или негови Свързани лица във връзка с Услугите на Iron Mountain съгласно Договора, се прилага тази част В на Приложение 3 и Страните се съгласяват, както следва:

1. **Избор на стандартни договорни клаузи.** Стандартните договорни клаузи на ЕС от 2021 г., съответните разпоредби съгласно Част А и Допълнението за Обединеното кралство от 2022 г. се прилагат, когато Клиентът или някое от неговите Свързани лица е Администратор, а Iron Mountain или някое от неговите Свързани лица е Обработващ лични данни и/или Клиентът или някое от неговите Свързани лица е Обработващ лични данни, а Iron Mountain или някое от неговите Свързани лица е подобработващ лични данни.

2. **Част 1: Таблица 1 – 3 от Допълнението за Обединеното кралство от 2022 г.:** Информация за Страните – Таблица 1; Избрани СДК, модули и избрани клаузи; Приложение Информация, включително Приложение 1А: Списък на страните, Приложение 1В: Описание на предаването, и Приложение 1С: Технически и организационни мерки за гарантиране на сигурността на данните – Таблица 3, се считат за завършени чрез позоваване на настоящото Приложение 3, включително Част А. Таблица 4 от Допълнението за Обединеното кралство: Клиентът и Iron Mountain потвърждават и се съгласяват, че Допълнението за Обединеното кралство може да бъде прекратено от всяка от Страните.

3. **Част 2:** Задължителни клаузи на Допълнението за Обединеното кралство: Клиентът и Iron Mountain потвърждават и се съгласяват със Задължителните клаузи на Допълнението за Обединеното кралство.

4. **Надзорен орган.** Службата на комисаря по информацията на Обединеното кралство действа като компетентен надзорен орган.

ЧАСТ Г – ПРЕДАВАНИЯ НА ЛИЧНИ ДАННИ НА ДРУГИ КЛИЕНТИ

Ако и до степента, до която Клиентът или неговите свързани лица предават Лични данни на Клиента, които не са обхванати от ЧАСТ А – В, към Iron Mountain или негови свързани лица във връзка с Услугите на Iron Mountain съгласно Договора, Част А от Приложение 3 се прилага до степента, подходяща и приложима съгласно приложимото законодателство за защита на данните. В противен случай, доколкото са необходими заместващи или допълнителни подходящи предпазни мерки или механизми за предаване съгласно законодателството за защита на данните, за да се предават Лични данни на Клиент към държава, която не осигурява адекватно ниво на защита на Личните данни от гледна точка на износителя на данни, страните се съгласяват да приложат същото възможно най-скоро и да документират тези изисквания за изпълнение в приложение към настоящото СОД.

ПРИЛОЖЕНИЕ 4

HIPAA – Споразумение за бизнес сътрудничество („Business Associate Agreement“, „BAA“)

Настоящото BAA допълва и изменя всички настоящи или бъдещи споразумения, сключени между Iron Mountain и негови свързани лица и Клиента и негови свързани лица, съгласно които Iron Mountain или негови свързани лица предоставят определени Услуги за Клиента или неговите свързани лица, които Услуги изискват бизнес сътрудникът да използва и/или разкрива защитена здравна информация от името на осигурено юридическо лице. До степента, променена в настоящото BAA, всички условия, посочени в Договора, остават в пълна сила и действие и уреждат Услугите, предоставяни от Iron Mountain на Клиента.

Iron Mountain и Клиентът сключват настоящото BAA, за да могат и двете страни да изпълнят съответните си задължения, тъй като те стават ефективни и обвързващи за страните съгласно правилата за поверителност, сигурност и уведомяване при нарушение на HIPAA, заедно с всички правила за прилагане, включително тези, въведени като част от правилото „Omnibus“ (наричани общо „Правилата на HIPAA“), по силата на което Клиентът и неговите свързани лица са „Защитено юридическо лице“ или „Бизнес сътрудник“, а Iron Mountain и неговите свързани лица са „Бизнес сътрудник“ на Клиента. За целите на настоящия Договор всички споменавания на бизнес сътрудник по-долу ще се смятат за назовавания на Iron Mountain или на съответното свързано лице.

1. ОПРЕДЕЛЕНИЯ

Използваните термини с главни букви, които не са дефинирани по друг начин в настоящото BAA, имат същото значение, като това, което е дадено на тези термини в Правилата на HIPAA или в Договора, както е приложимо.

„**Правило за уведомяване за нарушение**“ означава правилото за уведомяване за нарушение за непредпазена защитена здравна информация в 45 CFR §164 подраздел Г.

„**Бизнес сътрудник**“ означава юридическото лице, посочено по-горе, доколкото получава, поддържа или предава защитена здравна информация при предоставяне на Услуги на Клиенти.

„**HIPAA**“ означава Закона за преносимостта и отчетността на здравното осигуряване (Health Insurance Portability and Accountability Act) от 1996 г.

„**Закон HITECH**“ означава приложимите разпоредби на Закона за здравните информационни технологии за икономическото и клиничното здраве (Health Information Technology for Economic and Clinical Health Act), както са включени в Американския закон за възстановяване и реинвестиране (American Recovery and Reinvestment Act) от 2009 г., включително всички приложими разпоредби.

„**Правило за поверителност**“ означава Стандартите за поверителност на индивидуално идентифициращата здравна информация в 45 CFR §160 и §164, подраздели А и Д.

„**Защитена здравна информация**“ или „**ЗЗИ**“ има същото значение като термина „защитена здравна информация“ в 45 CFR §160.103 и се ограничава до ЗЗИ, създадена от бизнес сътрудник от името на Клиента или получена от Клиента или от негово име съгласно Договора.

„**Правило за сигурност**“ означава Стандартите за сигурност за защита на електронната защитена здравна информация на 45 CFR §160 и §164, подраздели А и В.

2. ЗАДЪЛЖЕНИЯ И ДЕЙНОСТИ НА БИЗНЕС СЪТРУДНИКА

2.1. Бизнес сътрудникът се съгласява да не използва и да не разкрива допълнително ЗЗИ, освен както е разрешено или изисквано от настоящото BAA или както се изисква от закона.

2.2. Бизнес сътрудникът се съгласява да прилага подходящи предпазни мерки и да спазва, както е приложимо, подрадел В от 45 CFR §164 по отношение на електронната ЗЗИ, за да се предотвратят употреби или оповестявания на ЗЗИ, различни от предвидените в настоящото BAA или Договора; Въпреки това страните признават и се съгласяват, че Клиентът, а не Бизнес сътрудникът, носи отговорност да спазва изискванията на 45 CFR §164.312 за прилагане на механизми за криптиране или декриптиране на електронна ЗЗИ, поддържани на физически носители (напр. записи), съхранявани от Клиент с Бизнес сътрудник.

2.3. Бизнес сътрудникът се съгласява незабавно да докладва на Клиента за всеки инцидент, нарушение или друго използване или разкриване на ЗЗИ, за което научи, че не е разрешено или изисквано от това BAA или Договора. В случай на Нарушение такова уведомление трябва да бъде направено в съответствие и както се изисква от бизнес сътрудник съгласно Правилата на HIPAA, включително, без това да бъде изчерпателно, съгласно 45 CFR 164.410, но в никакъв случай повече от три (3) работни дни след като Бизнес сътрудникът е завършил своето вътрешно разследване и е потвърдил нарушението, както е настъпило. Бизнес сътрудникът ще окаже разумна помощ и сътрудничество при разследването на всяко такова Нарушение и ще документира конкретните Депозити, които са били компрометирани, самоличността на всяка

неупълномощена трета страна, която може да е осъществила достъп или да е получила ЗЗИ, ако е известна, и всички действия, предприети от Бизнес сътрудника за смекчаване на последиците от такова Нарушение.

2.4. У съответствие с 45 CFR 164.502(e)(1)(ii) и 164.308(b)(2), както е приложимо, Бизнес сътрудникът трябва да гарантира, че всеки бизнес сътрудник, който е подизпълнител и който създава, получава, поддържа или предава ЗЗИ от името на Бизнес сътрудника с цел помощ при предоставянето на Услуги съгласно Договора, се съгласява със същите ограничения, условия и изисквания, които се прилагат за Бизнес сътрудника по отношение на такава ЗЗИ чрез това ВАА.

2.5. Ако Бизнес сътрудникът отговаря за ЗЗИ в определен набор от записи по отношение на физически лица и ако Клиентът поиска това, Бизнес сътрудникът се съгласява да предостави на Клиента достъп до тази ЗЗИ чрез извличане и предоставяне на такава ЗЗИ в съответствие с условията на Договора, така че Клиентът да може да отговори на физическо лице, за да спази изискванията на 45 CFR §164.524.

2.6. Бизнес сътрудникът се съгласява, че ако се изисква изменение на ЗЗИ в определен набор от записи под отговорността на Бизнес сътрудника и ако Клиентът инструктира Бизнес сътрудника да извлече такава ЗЗИ в съответствие с Договора, Бизнес сътрудникът трябва да извърши такава услуга, така че Клиентът да може да направи всяко изменение на такава ЗЗИ, което може да се изисква от Клиента или от физическо лице съгласно 45 CFR §164.526.

2.7. Бизнес сътрудникът се съгласява да документира и да осигурява на Клиента информацията, необходима за предоставяне на отчетност на Оповестяванията на ЗЗИ, при условие че Клиентът е предоставил на Бизнес сътрудника достатъчно информация, за да даде възможност на Бизнес сътрудника да определи кои записи или данни, които Бизнес сътрудникът е получил от Клиента или от негово име, съдържат ЗЗИ. Документацията за Оповестяванията трябва да съдържа такава информация, каквато би била необходима на Клиента, за да отговори на искане от физическо лице за отчитане на Оповестяванията на ЗЗИ в съответствие с 45 CFR §164.528 или други разпоредби на Правилата на HIPAA.

2.8. Освен ако не е изрично договорено друго в Договора, Бизнес сътрудникът трябва незабавно да уведоми Клиента за всякакви искания от страна на Физически лица за достъп, запознаване или корекция на ЗЗИ, без да отговаря на такива искания, и Клиентът носи отговорност за получаването и отговарянето на такива искания от физическо лице.

2.9. До степента, до която Бизнес сътрудникът трябва да изпълни едно или повече от задълженията на Клиента съгласно подраздел E от 45 CFR §164, Бизнес сътрудникът трябва да спазва изискванията на подраздел E, които се прилагат за Клиента при изпълнението на такова(ива) задължение(я).

2.10. Бизнес сътрудникът се съгласява да предостави своите вътрешни практики, книжа и документация на разположение на секретаря с цел определяне на спазването на правилата на HIPAA.

3. РАЗРЕШЕНИ УПОТРЕБИ И РАЗКРИВАНИЯ ОТ БИЗНЕС СЪТРУДНИК

3.1. Бизнес сътрудникът може да използва или разкрива ЗЗИ, както е необходимо за изпълнение на Услугите, посочени в Договора.

3.2. Бизнес сътрудникът може да използва или разкрива ЗЗИ, както се изисква от закона.

3.3. Бизнес сътрудникът се съгласява да положи разумни усилия, за да ограничи ЗЗИ до минимума, необходим за постигане на предназначението на използването, разкриването или искането.

3.4. Бизнес сътрудникът не може да използва или разкрива ЗЗИ по начин, който би нарушил подраздел E от 45 CFR §164, ако се извършва от Клиента.

3.5. Бизнес сътрудникът може да разкрива ЗЗИ за правилното управление и администрация на Бизнес сътрудника или за изпълнение на правните отговорности на Бизнес сътрудника, при условие че Оповестяванията се изискват от закона или Бизнес сътрудникът получава разумни гаранции от лицето, на което се разкрива информацията, че информацията ще остане поверителна и ще се използва или ще се разкрива по-нататък само както се изисква от закона или за целите, за които е била разкрита на лицето, и лицето уведомява Бизнес сътрудника за всички случаи, за които е известно, че е нарушена поверителността на информацията.

4. ЗАДЪЛЖЕНИЯ НА КЛИЕНТА

4.1. Клиентът няма да нарежда на Бизнес сътрудника да действа по начин, който не би бил в съответствие с Правилата на HIPAA.

4.2. Клиентът трябва да уведоми Бизнес сътрудника за всяко ограничение в известието си за практиките за поверителност на Клиента в съответствие с 45 CFR §164.520, доколкото това ограничение може да засегне използването или разкриването на ЗЗИ от Бизнес сътрудника.

4.3. Клиентът трябва да уведоми Бизнес сътрудника за всякакви промени или отмяна на разрешението от страна на дадено физическо лице за използване или разкриване на неговата ЗЗИ, доколкото тези промени могат да засегнат използването или разкриването на ЗЗИ от страна на Бизнес сътрудника.

4.4. Клиентът трябва да уведоми Бизнес сътрудника писмено за всяко ограничение на използването или разкриването на ЗЗИ, с което Клиентът се е съгласил в съответствие с 45 CFR §164.522, доколкото това ограничение може да засегне използването или разкриването на ЗЗИ от Бизнес сътрудника.

5. СРОК И ПРЕКРАТЯВАНЕ

5.1. Срокът на това ВАА започва от Датата на влизане в сила и се прекратява автоматично при това събитие, което настъпи по-късно: (i) изтичането на Договора или (ii) когато цялата ЗЗИ, предоставена от Клиента на Бизнес сътрудника, бъде унищожена или върната на Клиента.

5.2. При знанието на една от страните за съществено нарушение на ВАА от другата страна, изправната страна предоставя възможност на нарушаващата страна да поправи нарушението. Ако нарушаващата страна не поправи нарушението в рамките на тридесет (30) дни след получаване от нарушаващата страна на писмено уведомление от изправната страна, в което се посочват подробностите за такова съществено нарушение, тогава изправната страна има право да прекрати настоящото ВАА и Договора съгласно условията на Договора или ако прекратяването не е осъществимо, трябва да докладва за проблема на секретаря или на друг компетентен орган.

5.3. Настъпване на прекратяване:

5.3.1.1. С изключение на предвиденото в 5.3.2 по-долу, при прекратяване на това ВАА по каквато и да е причина Бизнес сътрудникът трябва да върне или унищожи цялата ЗЗИ, получена от Клиента, в съответствие с Договора. Тази разпоредба се прилага за ЗЗИ, която е във владение на подизпълнители или представители на Бизнес сътрудник. Бизнес сътрудникът няма да съхранява копия на ЗЗИ.

5.3.1.2. В случай че Бизнес сътрудникът определи, че връщането или унищожаването на ЗЗИ е невъзможно, Бизнес сътрудникът трябва да предостави на Клиента известие за условията, които правят връщането или унищожаването невъзможни. След уведомление до Клиента Бизнес сътрудникът трябва да разшири защитата на това ВАА до такава ЗЗИ и да ограничи по-нататъшните употреби и оповестявания на такава ЗЗИ до тези цели, които правят връщането или унищожаването невъзможни, докато Бизнес сътрудникът поддържа такава ЗЗИ съгласно условията на Договора.

6. РАЗНИ

6.1. Обезщетение. Бизнес сътрудникът се съгласява да обезщети Клиента в случай на всякакви глоби или санкции, наложени на Клиента в резултат на изпълнително производство, започнато от Секретаря, или граждански иск, предявен от щатски главен прокурор срещу Клиента, което производство или иск произтичат пряко и единствено от каквото и да е действие или пропуск от страна на Бизнес сътрудника, което е в нарушение на Правилата на HIPAA или в съществено нарушение на това ВАА („Иск“). Бизнес сътрудникът не е задължен да обезщети Клиента за каквато и да е част от такива глоби или санкции, произтичащи от (i) нарушение от страна на Клиента на Правилата на HIPAA или на това ВАА или (ii) небрежни или умишлени действия или пропуски от страна на Клиента. Горепосоченото задължение за обезщетяване изрично зависи от това Клиентът да предостави на Бизнес сътрудника правото – по избор и за сметка на Бизнес сътрудника и с адвокат по негов собствен избор – да води или да участва в защитата на всеки такъв Иск, при условие обаче, че доколкото такъв Иск е част от по-мащабно производство или действие, правото на Бизнес сътрудника да контролира или участва ще бъде ограничено до Иска, а не до по-мащабното производство или действие. В случай че Бизнес сътрудникът упражни правото си да води защитата, тогава (i) Бизнес сътрудникът няма да урежда иск, изискващ признаване на вина от страна на Клиента без неговото предварително писмено съгласие, (ii) Клиентът има право да участва за своя сметка в иска или делото и (iii) Клиентът трябва да сътрудничи на Бизнес сътрудника, както може да бъде основателно поискано. Горепосоченото посочва единственото и изключително правно средство за защита на Клиента и единствената отговорност на Бизнес сътрудника за всяка загуба, повреда, разход или отговорност на Клиента за всякакви Искове във връзка с това ВАА.

6.2. Поставяне под възбрана. Бизнес сътрудникът потвърждава, че всяко неразрешено използване или разкриване на ЗЗИ от Бизнес сътрудника може да причини непоправима вреда на Клиента, за която Клиентът има право, ако реши това, да търси налагане на възбрана или друго справедливо обезщетение.

6.3. Нормативни препратки. Позоваването в настоящото BAA на раздел от Правилата на HIPAA означава този раздел от HIPAA, Правилото за поверителност, Правилото за сигурност, Закона HITECH или окончателните правила „Omnibus“, както са изменени и в сила и за които се изисква съответствие.

6.4. Изменение. Страните се съгласяват да договарят добросъвестно всяко изменение на това BAA, което може да се изисква от време на време, както е необходимо за Клиента или Бизнес сътрудника, за да се спазят изискванията на Правилата на HIPAA. Ако страните не могат да постигнат взаимно съгласие относно условията на такова изменение в рамките на шестдесет (60) дни след датата на получаване на такова писмено искане, отправено от Клиента до Бизнес сътрудника, тогава всяка от страните има право да прекрати настоящото BAA и Договора, след като предостави на другата страна писмено предизвестие със срок не по-малко от тридесет (30) дни.

6.5. Без трети страни бенефициери. Нищо, изрично или подразбиращо се в този BAA, няма за цел да предостави, нито нещо в настоящият документ ще предостави на друго лице, освен на Клиента, Бизнес сътрудника и съответните им наследници или правоприемници, каквито и да било права, средства за защита, задължения или отговорности.

6.6. Независим изпълнител. Бизнес сътрудникът, включително неговите директори, длъжностни лица, служители и представители, е независим изпълнител, а не представител (както е определено от Федералния общ закон за представителството) на Клиента или член на неговата работна сила. Без да се ограничава общият характер на гореизложеното, Клиентът няма право да контролира, насочва или по друг начин да влияе върху поведението на Бизнес сътрудника в хода на извършване на услугите, освен чрез прилагането на това BAA или Договора или на взаимно договорено изменение на същия.

6.7. Йерархия; Цялостност на споразумението. Всяка неяснота в това BAA ще бъде разрешена, за да позволи на страните да спазват правилата на HIPAA. Настоящото BAA представлява цялото споразумение между страните по отношение на предмета на настоящия документ и заменя всички предишни съобщения, декларации, споразумения и договорености, свързани с Правилата на HIPAA, включително всички предишни споразумения за бизнес партньори между страните.