Avtal om databehandling

SYFTE OCH PRIORITETSORDNING

Detta databehandlingsavtal, tillsammans med dess bilagor och alla dokument som uttryckligen korshänvisas (”**DPA**”), anses vara en del av tjänsteavtalet mellan Iron Mountain och Kunden (”**Avtalet**”). Villkoren i Avtalet gäller för, och reglerar, parternas rättigheter och skyldigheter enligt detta DPA.

Om några villkor i detta DPA står i konflikt med de villkor som anges i Avtalet ska de villkor som anges i detta DPA vara de styrande villkoren med avseende på föremålet för detta DPA. Detta DPA ersätter alla tidigare databehandlingsavtal eller dataskydds- eller sekretessklausuler mellan parterna i förhållande till de tjänster som tillhandahålls enligt avtalet.

ALLMÄNNA VILLKOR

1. DEFINITIONER

Om det inte specifikt definieras häri ska alla termer med versaler ha samma betydelse som de ges i Avtalet.

”**Personuppgiftsansvarig**” avser den fysiska eller juridiska person, myndighet, byrå eller annat organ som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

”**Kundens personuppgifter**” avser Personuppgifter som tillhör eller samlas in av Kunden eller dess dotterbolag som behandlas som en del av Tjänsterna.

”**Registrerad**” avser en identifierad eller identifierbar fysisk person.

”Dataskyddslagstiftning” avser alla tillämpliga lagar och förordningar som rör behandling av personuppgifter som kan finnas i relevanta jurisdiktioner, inklusive men inte begränsat till EU:s GDPR (förordning (EU) 2016/679), Storbritanniens GDPR (GDPR enligt vad som är tillämpligt som en del av brittisk inhemsk lagstiftning enligt avsnitt 3 i EU:s (Utträde) lag 2018 och i dess lydelse enligt dataskydds-, integritets- och elektronisk kommunikation (ändringar osv.) (EU-förordningar om utträde) 2019 (i dess ändrade lydelse)), Dataskyddslagen 2018, FADP (den schweiziska federala dataskyddslagen), Amerikanska delstatliga sekretesslagar, LGPD (Brasiliens allmänna dataskyddslag), PIPL (lagen om skydd av personuppgifter i Folkrepubliken Kina) och alla lagar och/eller förordningar som implementerar eller upprättas i enlighet med dem, eller som ändrar, ersätter, återinför eller konsoliderar någon av dem, inklusive, i förekommande fall, de riktlinjer och uppförandekoder som utfärdats av tillsynsmyndigheterna.

”**Personuppgifter**” avser all information som rör en registrerad.

”**Personuppgiftsbiträde**” avser en fysisk eller juridisk person, offentlig myndighet, byrå eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

”**Behandling**” avser alla åtgärder eller uppsättningar av åtgärder som utförs på personuppgifter eller på uppsättningar av personuppgifter, oavsett om de utförs automatiskt eller inte, såsom insamling, registrering, organisering, strukturering, lagring, anpassning eller ändring, hämtning, konsultation, användning, utlämnande genom överföring, spridning eller på annat sätt tillgängliggörande, anpassning eller kombination, begränsning, radering eller förstörelse.

”**Säkerhetsöverträdelse**” avser oavsiktlig eller olaglig skada, förstörelse, förlust, ändring eller obehörigt avslöjande av eller åtkomst till Kundens Personuppgifter som Iron Mountain, dess personal eller underleverantörer Behandlar i samband med tillhandahållandet av Tjänsterna.

”**Tjänster**” avser alla tjänster som tillhandahålls av Iron Mountain eller dess dotterbolag till Kunden eller dess dotterbolag enligt Avtalet.

”**Amerikanska delstatliga sekretesslagar**” avser alla amerikanska delstatliga sekretess- och dataskyddslagar som är tillämpliga på behandling av personuppgifter enligt avtalet, inklusive, utan begränsning, och som kan komma att ändras, avskaffas eller ersättas från tid till annan: (1) California Consumer Privacy Act, i dess lydelse enligt California Privacy Rights Act, och alla tillämpningsföreskrifter som rör dessa (sammantaget, ”**CCPA**”) (2)

Colorado Privacy Act (”**CPA**”), (3) Virginia Consumer Data Protection Act (”**CDPA**”) (4) Utah Consumer Privacy Act (”**UCPA**”) och (5) Connecticut Data Privacy Act (”**CTDPA**”).

2. OMFATTNING OCH INFORMATION OM DATABEHANDLING

2.1. Detta DPA ska gälla för Kundens Personuppgifter som behandlas av Iron Mountain som Personuppgiftsbiträde i samband med tillhandahållandet av Tjänsterna i enlighet med Avtalet för Kundens räkning.

2.2. Iron Mountain kan samla in och behandla Personuppgifter om Kundens och dess dotterbolags anställda som Personuppgiftsansvarig för legitima affärsändamål, såsom hantering av avtal och kundrelationer, och i enlighet med Dataskyddslagstiftningen och Iron Mountains integritetsmeddelande som finns tillgängligt på Iron Mountains webbplatser och andra tillämpliga integritetspolicyer. Iron Mountains skyldigheter som anges i detta DPA ska inte gälla för behandling av sådana personuppgifter.

2.3. Föremålet för Personuppgiftsbehandlingen är utförandet av tjänsterna. Kundens och Iron Mountains rättigheter och skyldigheter anges i detta DPA. Bilaga 1 till detta DPA beskriver behandlingens art, varaktighet och syfte, de typer av Kunders Personuppgifter som Iron Mountain Behandlar och de kategorier av Registrerade vars Personuppgifter behandlas.

2.4. När Iron Mountain Behandlar Kundens Personuppgifter i samband med tillhandahållandet av Tjänsterna kommer Iron Mountain att:

2.4.1. Behandla Kundens Personuppgifter endast i enlighet med dokumenterade instruktioner från Kunden. Om Iron Mountain är skyldigt att behandla Kundens Personuppgifter för något annat ändamål enligt lagstiftning som Iron Mountain är föremål för kommer Iron Mountain att informera Kunden om detta krav först, såvida inte sådan(-a) lag(/lagar) förbjuder detta på viktiga grunder av allmänt intresse.

2.4.2. Alltid följa tillämplig Dataskyddslagstiftning och meddela Kunden omedelbart om Iron Mountain anser att en instruktion för behandling av Kundens Personuppgifter som ges av Kunden bryter mot tillämplig Dataskyddslagstiftning.

2.5. Kundens instruktioner är bindande för Iron Mountain såvida inte slutförandet av instruktionerna kräver tillhandahållande av en tjänst enligt Avtalet och Kunden inte samtycker till att betala serviceavgifterna för sådana tjänster.

2.6. Iron Mountain ska säkerställa att personal som måste få tillgång till Kundens Personuppgifter omfattas av en bindande sekretessplikt avseende sådana Kunders Personuppgifter och vidta rimliga åtgärder för att säkerställa tillförlitligheten och kompetensen hos Iron Mountains personal som har tillgång till Kundens Personuppgifter.

3. TILLHANDAHÅLLA KUNDSUPPORT

3.1. Iron Mountain ska tillhandahålla Kunden assistans, alltid med hänsyn till behandlingens art:

3.1.1. genom lämpliga tekniska och organisatoriska åtgärder och i den mån det är möjligt för att uppfylla Kundens skyldigheter att svara på förfrågningar från Registrerade som utövar sina rättigheter,

3.1.2. för att säkerställa efterlevnad av Kundens skyldigheter (t.ex. säkerhet vid behandling, anmälan av en Personuppgiftsöverträdelse till tillsynsmyndigheten, kommunikation av en Personuppgiftsöverträdelse till den Registrerade, konsekvensbedömning avseende dataskydd och föregående samråd med tillsynsmyndigheter där Behandlingen skulle leda till en hög risk i avsaknad av åtgärder som vidtagits av den personuppgiftsansvarige för att minska risken), med beaktande av den information som finns tillgänglig för Iron Mountain, och

3.1.3. genom att för Kunden tillgängliggöra all information som Kunden skäligen begär för att Kunden ska kunna visa att dess skyldigheter att välja och utse Iron Mountain har uppfyllts.

4. SÄKERHETSÅTGÄRDER

4.1 Med beaktande av sedvanliga operativa förfaranden, kostnaderna för genomförandet och arten, omfattning, sammanhang och ändamål med Behandlingen ska Iron Mountain vidta lämpliga och rimliga tekniska och organisatoriska åtgärder för att skydda sekretessen, integritet, och tillgängligheten av Kundens Personuppgifter och för att skydda Kundens Personuppgifter mot obehörig eller olaglig behandling och mot oavsiktlig förlust, förstörelse, skada, ändring, eller avslöjande. Iron Mountains säkerhetsstandarder anges i Bilaga 2 till detta DPA.

4.2 Det är Kundens eget ansvar att bedöma om dessa tekniska och organisatoriska åtgärder uppfyller Kundens krav.

5. EFTERLEVNAD AV LAGAR

Kunden och dess dotterbolag ska: (i) Behandla Kundens Personuppgifter i enlighet med Dataskyddslagstiftningen (ii) ha rätt att ge skriftliga instruktioner till Iron Mountain om Behandlingen av

Kundens Personuppgifter i samband med Tjänsterna (inklusive på uppdrag av en tredje part som är Personuppgiftsansvarig för Kundens Personuppgifter), och (iii) alltid behålla kontrollen och myndigheten över Kundens Personuppgifter i samband med Behandlingen.

6. UNDERBEHANDLING

6.1 Kunden bekräftar och samtycker till att Iron Mountain får anlita sitt moderbolag, sina dotterbolag och andra tredjepartspersonuppgiftsbiträden (inklusive tredjepartspersonuppgiftsbiträden som anlitats av Iron Mountains dotterbolag eller moderbolag) för behandling av Kunders Personuppgifter enligt detta DPA med förbehåll för klausul 6.2 nedan.

6.2 En lista över under-personuppgiftsbiträden som godkänts av Kunden per datumet för detta DPA finns tillgänglig här[1] . Iron Mountain kan när som helst ersätta eller utse ett nytt under-personuppgiftsbiträde, förutsatt att Kunden får femton (15) dagars skriftligt varsel och att Kunden inte motsätter sig sådana ändringar på bevisbara grunder relaterade till dataskydd inom den tidsramen. För att få dessa e-postmeddelanden ska Kunden teckna och hantera eventuella befintliga abonnemang på Iron Mountains meddelandetjänst via denna webbsida[2].

6.3 Om Kunden inte registrerar sig för denna anmälningstjänst ska Iron Mountain inte hållas ansvarigt för bristen på under-personuppgiftsbiträdeanmälan och alla sådana utnämningar ska anses vara godkända av Kunden**.** Om Kunden motsätter sig skriftligt avseende påvisbara grunder relaterade till dataskydd vid utnämningen av en ersättare eller ny under-personuppgiftsbiträde inom femton (15) dagar föregående skriftligt varsel ska Iron Mountain vidta rimliga åtgärder för att göra en ändring av Tjänsterna tillgänglig för Kunden eller rekommendera en ändring av Kundens konfiguration eller användning av Tjänsterna, i varje enskilt fall för att undvika behandling av Kundens Personuppgifter av den invända underbiträdet för Kundens övervägande och godkännande. Om Kunden inte godkänner sådana ändringar som föreslås av Iron Mountain inom femton (15) dagar kan Iron Mountain genom skriftligt meddelande till Kunden omedelbart säga upp Tjänsten eller en del av Tjänsten som inte kan tillhandahållas av Iron Mountain utan att använda den invända under-personuppgiftsbiträden. Sådan uppsägning ska inte påverka eventuella upplupna rättigheter och skyldigheter för parterna, förutsatt att inga uppsägningsavgifter, utgifter eller annan ersättning ska betalas av Iron Mountain eller Iron Mountains dotterbolag i samband med sådan uppsägning och att Kunden omedelbart ska ta över tillgångar som tillhandahålls Iron Mountain som en del av de uppsagda Tjänsterna, med förbehåll för villkoren i Avtalet och på Kundens egen bekostnad.

6.4 Iron Mountain ska säkerställa att alla avtal med under-personuppgiftsbiträden som omfattas av detta DPA innehåller bestämmelser som i alla väsentliga avseenden är desamma som i detta DPA och som krävs enligt tillämplig Dataskyddslagstiftning. Om ett under-personuppgiftsbiträde till Iron Mountain orsakar att Iron Mountain bryter mot sina skyldigheter enligt detta DPA eller någon tillämplig Dataskyddslagstiftning kommer Iron Mountain att förbli fullt ansvarigt gentemot Kunden för uppfyllandet av Iron Mountains skyldigheter enligt dessa villkor.

7. SÄKERHETSÖVERTRÄDELSER

7.1 Vid misstänkt säkerhetsöverträdelse kommer Iron Mountain att:

7.1.1 vidta åtgärder omedelbart för att utreda den misstänkta säkerhetsöverträdelsen och för att identifiera, förhindra och mildra effekterna av den misstänkta säkerhetsöverträdelsen och för att åtgärda säkerhetsöverträdelsen;

7.1.2 meddela Kunden utan onödigt dröjsmål när denne har en rimlig grad av säkerhet om att en Säkerhetsöverträdelse har inträffat och ge Kunden en detaljerad beskrivning av Säkerhetsöverträdelsen inklusive information som rimligen är nödvändig för att Kunden ska kunna uppfylla anmälningsskyldigheter enligt Dataskyddslagstiftningen.

7.2 Kunden samtycker till att Iron Mountain kan tillhandahålla informationen enligt klausul 7.1.2 i etapper. I de fall då Iron Mountain inte har tillgång till eller inte kan tillhandahålla Kunden viss information som anges i klausul 7.1.2, kommer Iron Mountain att informera Kunden om detta och Iron Mountain har inget ansvar för underlåtenhet att tillhandahålla sådan information.

8. REVISIONER

Iron Mountain kommer att tillåta Kunden och dess respektive revisorer eller auktoriserade ombud, efter att ha lämnat minst tio (10) arbetsdagars varsel till Iron Mountain, genomföra revisioner eller inspektioner under Avtalets löptid, förutsatt att Iron Mountain inte är skyldigt att tillhandahålla eller tillåta tillgång till information om: (i) andra Kunder till Iron Mountain; (ii) någon av Iron Mountains icke-offentliga externa rapporter; och (iii) eventuella interna rapporter som utarbetats av Iron Mountains interna

[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=NB4wIISphmYGggvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

revisions- eller efterlevnadsfunktion. Syftet med en revision eller inspektion enligt denna klausul ska begränsas till att verifiera att Iron Mountain Behandlar Kundens Personuppgifter i enlighet med sina skyldigheter enligt detta DPA. Förutom när en säkerhetsöverträdelse har inträffat ska högst en sådan revision genomföras under en tolvmånadersperiod (12).

9. INTERNATIONELLA DATAÖVERFÖRINGAR (BEGRÄNSADE ÖVERFÖRINGAR)

9.1 I den utsträckning det är tillämpligt samtycker Kunden härmed till och godkänner internationella överföringar av Kundens Personuppgifter till enheter enligt vad som anges i Avsnitt 6.2 och i enlighet med Bilaga 3 för tillhandahållandet av Tjänsterna och Kunden och Iron Mountain samtycker till:

9.1.1 för att följa tillämplig Dataskyddslagstiftning med avseende på sådana överföringar;

9.1.2 att utan begränsning beakta i) kategorierna av Kundens Personuppgifter, ii) de länder vars nationella lagar kanske inte tillhandahåller en skyddsnivå för Personuppgifter som är jämförbar med EU/Storbritanniens lagstiftning (”**tredje land**”) i omfattning, iii) de relevanta tekniska och organisatoriska åtgärder som anges i avsnitt 7 och iv) de relevanta parter som deltar i Behandlingen av sådana Kundpersonuppgifter, genomfört en bedömning av lämpligheten av den relevanta överföringsmekanism som antagits härunder där så krävs enligt lag och har fastställt att sådan överföringsmekanism är lämpligt utformad för att säkerställa att Personuppgifter som överförs i enlighet med detta DPA ges en skyddsnivå i destinationslandet som i huvudsak motsvarar den som garanteras enligt Dataskyddslagstiftningen.

10. ANSVAR OCH ERSÄTTNING

10.1 Oaktat något som strider mot Avtalet ska Iron Mountain, i händelse av en säkerhetsöverträdelse som direkt orsakas av Iron Mountains åsidosättande av sina skyldigheter enligt detta DPA, ersätta Kunden i den utsträckning som tillåts enligt gällande lag för direkt, verifierbar, nödvändiga och skäligen uppkomna tredjepartskostnader för Kunden i (a) utredningen av sådan säkerhetsöverträdelse, (b) förberedelse och utskick av meddelanden till sådana Registrerade och tillsynsmyndigheter enligt vad som krävs av Dataskyddslagstiftningen, (c) tillhandahållande av kreditövervakningstjänster till sådana personer som krävs enligt lag under en period som inte överstiger tolv (12) månader, och (d) betalning av den del av lagstadgade böter, påföljder, eller sanktioner som ålagts av en tillsynsmyndighet för vilken tillsynsmyndigheten anger att Iron Mountain är direkt ansvarigt.

10.2 Om en registrerad väcker talan mot endera eller båda parter för påstådd överträdelse av Dataskyddslagstiftningen (”**registrerade personers anspråk**”) ska varje part, där detta är tillåtet, kontrollera sitt eget försvar av sådana anspråk (eller dess del av försvaret) och förbli ensam ansvarig för sina egna kostnader, kostnader och skulder relaterade till dessa, inklusive rättsliga avgifter eller eventuella belopp som en domstol har tilldelat den eller som den har gjort i förlikning, förutsatt dock, att om varje part är ansvarig för en del eller endera parten är ansvarig för hela beloppet av de skador som en registrerad lidit för samma incident eller serie av incidenter och den registrerade har återvunnit full ersättning från endast en part (”**ersättningsparten**”), då ska ersättnignsparten ha rätt att från den andra parten kräva tillbaka den del av ersättningen som motsvarar den skada som den andra parten orsakat. Ersättningsparten kan endast framställa sitt anspråk gentemot den andra parten inom 12 månader efter incidenten, i den utsträckning som tillåts enligt tillämplig lag.

10.3 I den maximala utsträckning som tillåts enligt gällande lagar styr ansvarsbegränsningarna och eventuella undantag från skador som anges i Avtalet det sammanlagda ansvaret för alla Kundens anspråk som uppstår på grund av eller i samband med detta DPA och/eller Avtalet mot Iron Mountain. Dessa ansvarsbegränsningar och uteslutningar av skador gäller för alla anspråk, oavsett om de uppstår under avtal, skadestånd eller någon annan ansvarsteori, och alla hänvisningar till Iron Mountains ansvar avser det sammanlagda ansvaret för Iron Mountain och alla Iron Mountains dotterbolag tillsammans för anspråk från Kunden och alla andra Kunddotterbolag. I den utsträckning som krävs enligt gällande lagar är detta avsnitt inte avsett att (i) ändra eller begränsa parternas ansvar för registrerades anspråk som görs mot en part där det finns ett gemensamt och solidariskt ansvar, eller (ii) begränsa endera partens ansvar att betala påföljder som åläggs sådan part av en tillsynsmyndighet.

10.4 Klausulerna 10.1 till 10.3 anger varje parts enda och exklusiva gottgörelse och varje parts enda ansvar för förlust, skada, utgift eller ansvar i samband med detta DPA.

11. BEGÄRAN OM ALLMÄN AUKTORITET

11.1 I den utsträckning det är tillåtet enligt lag och med förbehåll för klausulerna 11.2 till 11.5 nedan samtycker Iron Mountain till att meddela Kunden om det:

11.1.1 får en rättsligt bindande begäran från en offentlig myndighet, inklusive rättsliga myndigheter, enligt lagstiftningen i destinationslandet för utlämnande av Kundens Personuppgifter som överförs i enlighet med Avtalet, eller

11.1.2 får kännedom om eventuell direkt åtkomst från offentliga myndigheter till Kundens Personuppgifter som överförs i enlighet med Avtalet i enlighet med lagarna i destinationslandet.

11.2 Om Iron Mountain är förbjudet att meddela Kunden enligt lagarna i destinationslandet samtycker Iron Mountain till att göra sitt bästa för att få ett avstående från förbudet, i syfte att kommunicera så mycket information som möjligt, så snart som möjligt.

11.3 Iron Mountain samtycker till att se över lagligheten i begäran om utlämnande, särskilt om det ligger inom de befogenheter som beviljats den begärande offentliga myndigheten, och att bestrida begäran om det konstateras att det finns rimliga skäl att anse att begäran är olaglig enligt lagstiftningen i destinationslandet. Den ska inte lämna ut de begärda Kundpersonuppgifterna förrän den måste göra det enligt tillämpliga procedurregler.

11.4 Iron Mountain samtycker till att tillhandahålla den minsta mängd information som är tillåten när man svarar på en begäran om utlämnande, baserat på en rimlig tolkning av begäran.

11.5 Iron Mountain samtycker till att bevara informationen i enlighet med denna klausul under avtalets löptid och göra den tillgänglig för den behöriga tillsynsmyndigheten på begäran.

12. MISCELLANEOUS

12.1 Med förbehåll för arten av de tjänster som tillhandahålls av Iron Mountain, vid uppsägning/utgång av Avtalet, baserat på Kundens specifika instruktioner och med förbehåll för villkoren i Avtalet, ska Iron Mountain antingen radera/förstöra eller returnera alla Kundens Personuppgifter till Kunden eller till en tredje part som utsetts av Kunden. Alla Kundpersonuppgifter som ingår i Kundens tillgång som lagras av Iron Mountain på uppdrag av Kunden kommer att returneras till Kunden i enlighet med en överenskommen exit- eller övergångsplan och med förbehåll för överenskomna kostnader, enligt vad som anges i Avtalet eller annat tillämpligt avtalsdokument. I alla andra fall om Avtalet är tyst om radering/destruktion eller återlämnande av Kundens Personuppgifter och Kunden inte ger några instruktioner om radering/destruktion eller återlämnande av Kundens Personuppgifter inom femton (15) dagar efter Avtalets upphörande/utgång ska Iron Mountain inom 15 (femton) dagar skicka ett skriftligt meddelande till Kunden med begäran om att få specifika instruktioner om att radera/förstöra eller återlämna Kundens Personuppgifter och informera Kunden om all tillämplig säker förstörelse eller andra avgifter som ska betalas av Kunden. Om Kunden inte tillhandahåller skriftliga instruktioner inom sådana femton (15) dagar och betalar tillämpliga avgifter inom samma period, godkänner Kunden härmed att Iron Mountain vidare Behandlar, raderar, förstör alla Kundens Personuppgifter efter uppsägning av Avtalet på Iron Mountains val och Kundens bekostnad.

12.2 Oaktat vad som framgår av punkt 12.1 ska Iron Mountain inte bryta mot sina skyldigheter med avseende på radering av Kundens Personuppgifter som lagras på backupband så länge sådana backupband åsidosätts (och Kundens Personuppgifter därmed raderas) i den normala verksamheten.

12.3 Med undantag för standardavtalsklausulerna (enligt definitionen i bilaga 3 till detta DPA), detta DPA och alla tvister, anspråk eller kontroverser som uppstår genom eller i samband med detta DPA, eller brottet, uppsägningen eller giltigheten därav, styrs av valet av lagbestämmelse i avtalet; och alla tvister, kontroverser eller anspråk som uppstår genom eller i samband med detta DPA kommer i första hand att försöka lösas genom en definierad tvistlösningsprocess som ingår i avtalet.

12.4 Varje part kan från tid till annan skriftligen meddela den andra parten om eventuella ändringar av detta DPA som parten rimligen anser vara nödvändiga för att uppfylla kraven i dataskyddslagstiftningen eller beslut av en tillsynsmyndighet eller behörig domstol. Alla sådana ändringar ska endast träda i kraft om och i den utsträckning som anges i en ömsesidigt överenskommen ändring av detta DPA som utförs av båda parter, förutom när en part informerar den andra parten om eventuella nya rättsliga krav och skickar en sådan ändring som endast omfattar nödvändiga ändringar och som kan accepteras utan formellt samtycke till det, dvs. genom att inte göra någon invändning inom en viss tidsfrist, betraktas som ömsesidigt överenskomna ändringar av detta DPA.

BILAGA 1

Uppgifter om behandling och dataöverföring (om tillämpligt)

A. LISTA ÖVER PARTER:

Parterna i detta DPA och rollerna som Uppgiftsutgivare och Uppgiftsinförare anges i Avtalet och Bilaga 3 (Internationella dataöverföringar), om tillämpligt.

B. BESKRIVNING AV BEHANDLING/ÖVERFÖRING (om tillämpligt):

Kategorier av registrerade vars personuppgifter behandlas/överförs:

Beroende på typen av Iron Mountains tjänster och Kundens verksamhet kan Kunden skicka Personuppgifter som tillhör olika kategorier av Registrerade till Iron Mountain, vars omfattning bestäms och kontrolleras av Kunden efter eget gottfinnande. Som sådana kan kategorier av Registrerade omfatta: tidigare och nuvarande anställda, tidigare och nuvarande leverantörer eller konsulter, entreprenörer eller konsulter som tillhandahålls av agenturer och externa utstationerade; arbetssökande och kandidater, studenter och volontärer, personer som identifierats av anställda eller pensionärer som förmånstagare, make/maka, inhemsk/civil partner, anhöriga och nödkontakter, pensionärer, tidigare och nuvarande direktörer och tjänstemän, aktieägare, obligationsinnehavare, kontoinnehavare, slutanvändare/konsumenter (vuxna, barn), patienter (vuxna, barn), förbipasserande (CCTV-kameror), och webbplatsanvändare.

Kategorier av personuppgifter som behandlas/överförs:

Beroende på typen av Iron Mountains Tjänster och Kundens verksamhet kan Kunden skicka Personuppgifter som tillhör olika kategorier av Personuppgifter till Iron Mountain, vars omfattning bestäms och kontrolleras av Kunden efter eget gottfinnande. Därför kan kategorier omfatta Personuppgifter som rör Kunden och/eller Kundens egna Kunder, anställda osv.

Känsliga uppgifter som överförs (om tillämpligt):

Beroende på typen av Iron Mountains tjänster och Kundens verksamhet kan Kunden skicka känsliga uppgifter till Iron Mountain, vars omfattning bestäms och kontrolleras av Kunden efter eget gottfinnande.

Om tillämpligt, regelbundenheten i överföringen (t.ex. om uppgifterna överförs på engångsbasis eller löpande):

Överföringen sker löpande.

Behandlingens art:

Insamling, registrering, organisering, strukturering, lagring, anpassning eller ändring, hämtning, konsultation, användning, avslöjande genom överföring, spridning eller på annat sätt tillgängliggörande, anpassning eller kombination, begränsning, radering eller förstörelse.

Syfte(-n) med databehandlingen/överföringen (om tillämpligt) och ytterligare behandling:

Tillhandahållande av Tjänster enligt Avtalet.

Lagring av data:

Personuppgifterna kommer att behållas av Iron Mountain under de tjänster som erbjuds Kunden och fram till dess att Personuppgifterna returneras eller förstörs enligt vad som fastställs i klausul 12.1 i detta DPA.

Om tillämpligt, för överföringar till (under-)Behandlare, specificera även ämnet, arten och varaktigheten av Behandlingen:

Under avtalets löptid tillhandahåller under-personuppgiftsbiträden bland annat informationsteknik (IT) och konsulttjänster, inklusive global IT-support, evenemangsrapportering och hanteringstjänster.

C. BEHÖRIG TILLSYNSMYNDIGHET

Enligt vad som framgår av Bilaga 3 (Internationella dataöverföringar), om tillämpligt.

BILAGA 2

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER (”SÄKERHETSÅTGÄRDER”)

1. INFORMATIONSSÄKERHETSPROGRAM OCH POLICY

Iron Mountain ska upprätthålla ett informationssäkerhetsprogram med lämpliga fysiska, tekniska och administrativa kontroller som är utformade för att uppfylla branschstandarder. Informationssäkerhetsprogrammet ska omfatta:

1.1 Dokumentation, intern publicering och kommunikation av Iron Mountains policyer, standarder och procedurer för informationssäkerhet.

1.2. Dokumenterad, tydlig ansvarsfördelning och behörighet för upprättande och underhåll av informationssäkerhetsprogrammet.

1.3 Regelbunden testning av de viktigaste kontrollerna, systemen och förfarandena i informationssäkerhetsprogrammet.

1.4 Administrativa, tekniska och operativa åtgärder som är utformade för att skydda alla Kundpersonuppgifter med hjälp av de metoder, procedurer och processer som beskrivs i denna Säkerhetsbilaga, i den utsträckning de är relevanta och tillämpliga på det format i vilket Kundpersonuppgifterna upprätthålls.

2. RISKBEDÖMNING

Iron Mountain ska upprätthålla ett program för riskbedömning av informationssäkerhet som är utformat för att identifiera och bedöma rimligen förutsebara interna och externa risker och sårbarheter som kan påverka säkerheten, sekretessen och/eller integriteten för Kundens Personuppgifter. Iron Mountain ska utvärdera och uppdatera, vid behov, rimligt och lämpligt, effektiviteten hos det aktuella informationssäkerhetsprogrammet för att begränsa sådana risker, på årsbasis eller när det sker en väsentlig förändring av risker eller sårbarheter för Kundens Personuppgifter.

3. HANTERING AV TILLGÅNGAR FÖR INFORMATIONSBEHANDLING OCH FYSISKA MEDIER

3.1 Hantering av tillgångar för informationsbehandling. Iron Mountain upprätthåller ett program för hantering av tillgångar för hantering av fysiska, tekniska och administrativa kontroller avseende Iron Mountains informationsbehandlingstillgångar (t.ex. datorer, servrar, lagringsenheter, kommunikationsnätverk, persondatorer, bärbara datorer och kringutrustning).
Programmet för förvaltning av tillgångsinventering omfattar följande:

- 3.1.1 Dokumenterad tilldelning av tillgångsägande till Iron Mountain-personal för att säkerställa lämplig klassificering av information, fastställande av åtkomstbegränsningar och granskning av åtkomstkontroller.
- 3.1.2 Sanitering av tillgångar innan de avyttras i enlighet med NIST 800-88.
- 3.1.3 Krav på ledningens godkännande före borttagning av utrustning eller programvara som inte är tilldelad en specifik person från Iron Mountains lokaler.

3.2 Kontroller. Iron Mountain-kontrollerna inkluderar följande:

- 3.2.1 Driftprocedurer och tekniska kontroller som är utformade för att skydda dokument, datormedia, indata/utdata/säkerhetskopieringsdata och systemdokumentation från obehörigt avslöjande, modifiering och förstörelse.
- 3.2.2 Procedurer för säker kassering av elektroniska eller fysiska medier som innehåller Kundens Personuppgifter.
- 3.2.3 En etablerad process för att spåra alla Kundens fysiska medier från Iron Mountains inledande försvar genom permanent återkallelse eller förstörelse.

4. PERSONALSÄKERHETSÅTGÄRDER

4.1 Sekretess. Iron Mountain ska rimligen kräva att alla Iron Mountain-anställda, inklusive tillfälligt anställda och kontraktsanställda, samtycker till att upprätthålla sekretessen för Kundens Personuppgifter och att följa Iron Mountains interna krav på informationssäkerhet och acceptabel användning.

4.2 Bakgrundsutredningspolicy. Iron Mountain har en policy för bakgrundsutredning och drogtestning (endast USA) som gäller för sina anställda. Iron Mountain kommer att fortsätta att upprätthålla sådana policyer under avtalets löptid. Policykraven omfattar, men är inte begränsade till, drogtestning (endast USA), verifiering av personalidentitet, sökningar i brottsregister, anställningsverifieringar, sökningar i övervakningslistor för myndigheter/terrorister, samt utbildningsverifieringar för vissa anställda och körkorts- och överträdelsehistorik för förarkandidater och befintliga förare. När nedsättande information identifieras vid en bakgrundskontroll utför Iron Mountain en individuell bedömning, i enlighet med tillämpliga arbetslagar och bästa praxis.

4.3 Arbeta med underleverantörer. Iron Mountain ska kräva att alla underleverantörer som utför tjänster enligt Avtalet följer liknande begränsningar som de som anges i detta avsnitt med avseende på all underleverantörspersonal som kommer att utföra tjänster enligt Avtalet som involverar behandling av Kundens Personuppgifter.

4.4 Utbildning i säkerhetsmedvetenhet. Minst en gång om året ska Iron Mountain genomföra allmän utbildning i säkerhetsmedvetenhet och specifik rolltillämplig säkerhetsutbildning för alla Iron Mountain-anställda med tillgång till Kundens Personuppgifter. Iron Mountain bör upprätthålla register som visar namnen på sådana Iron Mountain-anställda som närvarar och datumet för varje säkerhetsmedvetandeutbildning. Iron Mountain ska rutinmässigt granska och uppdatera sitt utbildningsprogram för säkerhetsmedvetenhet.

4.5 Avlägsnande av Iron Mountain-personal. Iron Mountain upprätthåller en disciplinär process som tillämpas på Iron Mountain-anställda som bryter mot säkerhetskraven häri.

4.6 Upphörande av åtkomst vid uppsägning/omplacering. Vid uppsägning eller omplacering till en roll som inte kräver åtkomst till Kundens Personuppgifter ska en Iron Mountain-anställds åtkomst till Kundens Personuppgifter återkallas omedelbart.

1. FYSISK OCH MILJÖMÄSSIG SÄKERHET

5.1 Fysiska säkerhetskontroller. Iron Mountains anläggningar använder fysiska kontroller som rimligen begränsar åtkomsten till Kundens Personuppgifter, inklusive, enligt Iron Mountains bedömning, åtkomstkontrollprotokoll, fysiska barriärer såsom låsta anläggningar och områden, anställdas passerkort, besöksloggar, passerkort för besökare, kortläsare, videoövervakningskameror och larm för intrångsdetektering. Alla besökare måste logga in och eskorteras hela tiden.

5.2 Stödjande verktyg. Iron Mountain ska vidta åtgärder för att skydda sina anläggningar som innehåller Kundens Personuppgifter och system från strömavbrott, telekommunikation, vattenförsörjning, avlopp, uppvärmning, ventilation och luftkonditionering, beroende på vad som är tillämpligt.

5.3 Säkerhet för överföringssystem. Iron Mountain ska vidta åtgärder för att skydda den fysiska säkerheten i sin nätinfrastruktur och sina telekommunikationssystem mot avlyssning och skador på överföringar.

5.4 Utrustning utanför anläggningen. I händelse av att Iron Mountain outsourcar funktioner som kräver användning av utrustning utanför anläggningen till stöd för tjänster ska all utrustning utanför anläggningen som lagrar Kundens Personuppgifter skyddas av säkerhet som motsvarar den som används för utrustning på plats som används för samma ändamål.

5.5 Fysisk tillgång till informationsbehandlingstillgångar. Iron Mountain ska behålla register över Iron Mountain-anställda som är behöriga att ha fysisk åtkomst till Iron Mountain-kontrollerad(-e) datormiljö(-er) som används av Iron Mountain för att tillhandahålla tjänster i ett år och, på Kundens begäran relaterad till en säkerhetsöverträdelse, och med förbehåll för Iron Mountains säkerhetspolicyer, ge Kunden åtkomst till granskningsbara register över sådana Iron Mountain-anställda.

5.6 Fysisk åtkomst begränsad. Iron Mountain ska begränsa fysisk åtkomst till Iron Mountain-kontrollerade anläggningar som Behandlar Kunders Personuppgifter till de Iron Mountain-anställda och behöriga personer som har ett affärsbehov av sådan åtkomst. Iron Mountain ska ha en godkännandeprocess för att godkänna och spåra förfrågningar om fysisk tillgång till sådana anläggningar.

5.7 Reparationer och ändringar. Iron Mountain ska registrera alla säkerhetsrelaterade reparationer och modifieringar av fysiska komponenter, inklusive hårdvara, väggar, dörrar och lås på säkra områden inom anläggningar där Kundens Personuppgifter lagras.

5.8 Registreringar. Upprätthålla ett register över förflyttningar av maskinvara och elektroniska medier och alla ansvariga personer.

6. HANTERING AV KOMMUNIKATIONS- OCH INFORMATIONSBEHANDLING

6.1 Standarder för enhetskonfiguration. Iron Mountain ska skapa, implementera och upprätthålla systemadministrationsprocedurer som uppfyller branschstandarder, inklusive men inte begränsat till systemhärdning, system- och enhetspatchning (operativsystem och applikationer) och korrekt antivirusinstallation och uppdateringar.

6.2 Förändringskontroll för informationsbehandlingssystem. Iron Mountain ska ha en intern formell process för begäran om ändringshantering för system för informationsbehandling och kommunikationsnätverk, och Iron Mountains begäran om ändring ska dokumenteras, testas och godkännas före implementering av ny informationsbehandling eller nätverkskommunikation, systemkorrigeringar eller ändringar av befintliga system.

6.3 Uppdelning av skyldigheter. Iron Mountain ska dela upp arbetsuppgifter och ansvarsområden så att ingen person har ensam möjlighet att ändra informationsbehandlingssystem som får åtkomst till Kundens Personuppgifter.

6.4 Separation av utvecklings- och produktionsmiljöer. Iron Mountains utvecklings-, test- och produktionsmiljöer för informationsbehandlingssystem ska vara logiskt eller fysiskt åtskilda.

6.5 Teknisk arkitekturhantering. Iron Mountain ska upprätta en konfigurationshanteringsprocess för att definiera, hantera och kontrollera de komponenter i informationsbehandlingssystemet som används för att tillhandahålla tjänsterna och den tekniska infrastrukturen för sådana komponenter.

6.6 Intrångsdetektering. Iron Mountain ska kontinuerligt övervaka datorsystem och processer för försök till eller faktiska säkerhetsintrång eller överträdelser och meddela Kunden om obehörig åtkomst till Kundens Personuppgifter.

6.7 Nätverkssäkerhet. Iron Mountain ska se till att följande finns på plats:

6.7.1 När det gäller Iron Mountain-värdmiljö(-er) som används för att tillhandahålla Tjänsterna, larmhändelser för nätverksintrångsdetektering (”IDS”) och intrångsskyddssensorer (”IPS”) som loggas, med dagliga rapporter utfärdade för granskning (gemensamt kallade ”IDS/IPS”).

6.7.2 När det gäller Iron Mountain-värdmiljö(-er) som används för att tillhandahålla Tjänsterna, IDS/IPS som uppdateras minst en gång i veckan men så snart som rimligen möjligt efter att uppdateringarna har mottagits och snabb körning av de senaste hotsignaturerna eller reglerna.
6.7.3 Högriskhamnar på externt riktade system är inte tillgängliga via internet.
6.7.4 Iron Mountains nätverksanslutningar loggas och registreras i loggfiler.
6.7.5 Utplacering av brandvägg(-ar) utformade för att skydda och inspektera all inkommande och utgående nätverkstjänsttrafik mellan definierade nätverkspunkter.
6.7.6 Hårdningspolicyer för att definiera inkommande och utgående nätverksportar eller servicetrafik för alla Iron Mountain-ägda eller -hanterade system som är dokumenterade och godkända inom informationssäkerhetsprogrammet.
6.7.7 Nätverksportar och diagnostiska portar som är ordentligt säkrade, och
6.7.8 policyer, procedurer och tekniska kontroller som är utformade för att förhindra, upptäcka och ta bort skadlig kod eller kända attacker på Iron Mountains informationssystem.

6.8 Krypterade autentiseringsuppgifter. Iron Mountain ska säkerställa att autentiseringsuppgifter som överförs via Iron Mountains nätverksenheter krypteras under transport.

6.9 Säker nätverksadministration. Iron Mountain-nätverk ska hanteras och kontrolleras på ett rimligt sätt för att skydda mot kända hot och för att upprätthålla säkerheten för alla Iron Mountain-hanterade applikationer och data på nätverket eller i transit över nätverket. Tekniska kontroller och säkra kommunikationsprotokoll ska implementeras för att förbjuda obegränsade anslutningar till otillförlitliga nätverk eller offentligt tillgängliga servrar.

6.10 Virusskydd. Iron Mountain ska implementera och upprätthålla ett antivirusprogram, inklusive skydd mot skadlig kod, uppdaterade signaturfiler eller alternativt skydd mot nya hot, patchar och virusdefinitioner, för Iron Mountain-hanterade servrar och arbetsstationer som används för att lagra eller komma åt Kunders Personuppgifter.

6.11 Webbplats – Klientkryptering. Iron Mountain ska säkerställa att Secure Sockets Layering (SSL) är aktiverat på var och en av dess webbplatser och att det innehåller ett giltigt SSL-certifikat som kräver sekretess-, autentiserings- eller behörighetskontroller.

6.12 Säkerhetskopiering av information. Iron Mountain ska skapa lämpliga säkerhetskopior av systemfiler. Dessutom ska Iron Mountain utveckla och upprätthålla haveriberedskapsprocedurer, se avsnittet ”Återhämtning av katastrofer” nedan för mer information.

6.13 Elektronisk information under överföring. Iron Mountain ska använda kryptering med en branschstandardalgoritm med en nyckellängd på minst 128 bitar för att skydda Kundens Personuppgifter som överförs via offentliga nätverk när de kommer från Iron Mountains värdbaserade infrastruktur.

6.14 Kryptografiska kontroller. Iron Mountain ska följa en dokumenterad policy för användning av kryptografiska kontroller. Iron Mountains kryptografiska kontroller ska:
6.14.1 Vara utformad för att på ett rimligt sätt skydda sekretessen och integriteten för Kundens Personuppgifter som behandlas, överförs eller lagras av Iron Mountain i alla delade nätverksmiljöer i enlighet med villkoren i Avtalet.
6.14.2 Tillämpas, i Iron Mountain-värdmiljö(-er) som används för att tillhandahålla tjänster, på Kundens Personuppgifter i transit över eller till ”otillförlitliga” nätverk (dvs. nätverk som Iron Mountain inte lagligen kontrollerar), inklusive de som används för att skicka data till Kundens företagsnätverk från Iron Mountains nätverk, underkastade, i varje enskilt fall, Kundens samarbete i hanteringen av krypteringsnycklar som är nödvändiga för att avkryptera överföringar som mottagits av Kunden, och
6.14.3 Inkludera dokumenterade metoder för hantering av krypteringsnycklar för att stödja säkerheten för kryptografisk teknik.
6.14.4 Inkludera kryptering av alla Kunders Personuppgifter på bärbara datorer eller andra bärbara enheter.

6.15 Loggningskrav. Iron Mountain ska säkerställa följande:
6.15.1 Betydande säkerhets- och systemhändelser loggas och granskas.
6.15.2 Revisionsloggar behålls i minst ett år för system i Iron Mountain-värdmiljö(-er) som används av Iron Mountain för att tillhandahålla tjänster.
6.15.3 Systemgranskningsloggar granskas för avvikelser, och
6.15.4 Logganläggningar och systeminformation är rimligt skyddade mot manipulation och obehörig åtkomst.

6.16 Nätverkstidssynkronisering. Iron Mountain ska synkronisera systemklockorna för alla informationsbehandlingssystem med en gemensam auktoritativ tidskälla.

6.17 Segregation i nätverk. Iron Mountain ska på lämpligt sätt segregera relaterade grupper av informationstjänster, användare och informationssystem i nätverk.

7. ÅTKOMSTKONTROLL

7.1 Åtkomstkontrollpolicy. Iron Mountain upprätthåller åtkomstkontrollpolicyer med avseende på informationsbehandlingstillgångar som Iron Mountain formellt godkänner, publicerar och implementerar.

7.2 Auktorisering av logisk åtkomst. Iron Mountain ska ha en godkännandeprocess för begäran om logisk åtkomst till Kundens Personuppgifter och begäran om åtkomst till Iron Mountain-system som är avsedda för användning i Tjänsterna.

7.3 Åtkomstkontroll och åtkomstgranskning. Iron Mountain ska endast bevilja åtkomst till Kundens Personuppgifter till aktiva Iron Mountain-anställda, inklusive tillfälligt anställda och kontraktsanställda,

och aktiva användarkonton som behöver sådan åtkomst för att utföra sin arbetsfunktion. All privilegierad åtkomst måste granskas och bekräftas för att överensstämma med nuvarande arbetsroll och dokumenteras minst kvartalsvis.

7.4 Kontroll av tredjepartsåtkomst. Innan Iron Mountain beviljar externa parter åtkomst till Iron Mountains informationssystem som har åtkomst till Kundens Personuppgifter ska Iron Mountain säkerställa att lämpliga kontroller finns på plats.

7.5 Kontroll av åtkomst till driftsystem. Iron Mountain ska kontrollera åtkomsten till operativsystem (både programvaru- och maskinvarubaserade operativsystem) genom att kräva en säker inloggningsprocess som unikt identifierar den person som har åtkomst till operativsystemet.

7.6 Mobila datorenheter. Iron Mountain kommer att ha en policy eller procedur på plats som är utformad för att skydda Iron Mountains mobila datorenheter från obehörig åtkomst. Sådana policyer eller procedurer ska behandla fysiskt skydd, åtkomstkontroll och säkerhetskontroller såsom kryptering, virusskydd och säkerhetskopiering av enheten.

7.7 Isolering av Kundsystem. Iron Mountain ska, inom sin värdmiljö(-er) som används för att tillhandahålla Tjänsterna, logiskt avskilja och separera Kundens Personuppgifter från all annan information.

7.8 Konton. Iron Mountain ska göra följande med avseende på konton:

- 7.8.1 Kräva autentisering av identiteten hos varje Iron Mountain-anställd som söker åtkomst till Iron Mountain-system som Behandlar Kundens Personuppgifter och förbjuder användning av delade användarkonton eller användarkonton med generiska inloggningsuppgifter (dvs. ID:n) för att få åtkomst till Kundens Personuppgifter eller system.
- 7.8.2 Kräv att alla användarkonto-ID:n, inklusive sekretessbelagda konton, är direkt knutna till en person (i motsats till en befattning).
- 7.8.3 Om standardadministrationskonton inte är inaktiverade eller borttagna måste tillfälliga lösenord, ID-nummer eller liknande kontroller användas för standardadministrationskontoåtkomst.
- 7.8.4 Kräv att inaktiva konton är låsta eller inaktiverade efter 90 dagars inaktivitet.
- 7.8.5 Förbjud åtkomst till ett konto efter flera misslyckade åtkomstförsök.
- 7.8.6 Kräv unika identifierare och starka lösenord som minst innehåller följande: minst åtta tecken, måste ändras var 90:e dag, och har komplexitetskrav.
- 7.8.7 Förbjuda anställda att dela eller skriva ner lösenord.

7.9 Kontroller för obevakade system. Iron Mountain ska använda en lösenordsskyddad skärmsläckare för alla system som lämnas obevakade och som inte har varit aktiva i 30 minuter.

8. UTVECKLING OCH UNDERHÅLL AV INFORMATIONSSYSTEM

8.1 Systemutvecklingssäkerhet. Iron Mountain ska se till att säkerheten är en del av all utveckling och drift av informationssystem och ska offentliggöra och följa interna säkra kodningsmetoder baserade på säkerhetsstandarder för applikationsutveckling.

8.2 Säkerhetshantering för programvara. Iron Mountains informationssystem (inklusive operativsystem, infrastruktur, affärsapplikationer, tjänster och användarutvecklade applikationer) ska utformas så att de överensstämmer med informationssäkerhetsstandarder.

8.3 Nätverksdiagram. Iron Mountain ska utveckla, dokumentera och upprätthålla fysiska och logiska diagram över nätverksenheter och trafik.

8.4 Sårbarhetsbedömningar av applikationer/etisk hackning. Iron Mountain ska minst en gång per år utföra sårbarhetsbedömningar på applikationer i sin(-a) värdmiljö(-er) som används för att tillhandahålla tjänster som Behandlar Kunders Personuppgifter. Detaljerade resultat är konfidentiell och äganderättsskyddad information om Iron Mountain och kommer inte att tillhandahållas.

8.5 Change Testing och granskning. Iron Mountain ska granska och testa ändringar i applikationer och operativsystem före driftsättning för att säkerställa att det inte finns någon negativ inverkan på Kundens Personuppgifter eller system.

9. HAVERIBEREDSKAP

Iron Mountain ska upprätthålla en plan för haveriberedskap, inklusive replikering av system och elektroniska data som används för att stödja Tjänsterna till ett datacenter för säkerhetskopiering. Replikering av system och elektroniska data omfattar inte Kundens Personuppgifter som fysiskt lagras i en Iron Mountain-anläggning. Iron Mountain kommer att upprätthålla en affärskontinuitetsplan för att återställa kritiska affärsfunktioner. Iron Mountain kommer att utföra haveriberedskapstester minst en gång var tolfte (12) månad.

10. EXTERNA REVISIONER OCH BEDÖMNINGAR

Iron Mountains säkerhetsprotokoll är utformade för att överensstämma med branschstandarder. Iron Mountain kommer att förse Kunden med alla oberoende granskningsrapporter från tredje part som Kunden har beställt (t.ex. PCI, ISO27001, SOC2 osv.) som är relevanta för Tjänsterna i regionen som sådana Tjänster tillhandahålls (”Revisionsrapport”). Iron Mountain kommer att tillhandahålla alla sådana rapporter som beställts med avsikt att vara Kundinriktade, oavsett resultaten av rapporten. Iron Mountain kommer inte att behöva tillhandahålla interna revisionsresultat eller resultat från andra oberoende bedömningar som beställts med avsikt att vara konfidentiella för Iron Mountain. Kunden och dess externa revisorer kommer att få kopior av revisionsrapporten på begäran. Alla revisionsrapporter eller andra resultat som genereras genom de tester eller revisioner som krävs enligt detta avsnitt kommer att betraktas som konfidentiell information om Iron Mountain. Kunden ska ha rätt att tillhandahålla

en kopia av en sådan revisionsrapport till alla tillämpliga Kunder eller tillsynsmyndigheter hos Kunden, med förbehåll för sekretessbestämmelser som är lika restriktiva som de som anges häri. På Kundens begäran ska Iron Mountain skriftligen bekräfta att det inte har skett några ändringar i relevanta policyer, procedurer och interna kontroller sedan slutförandet av en sådan revisionsrapport, inte längre än tre månader från slutet av rapporteringsperioden för revisionsrapporten.

BILAGA 3

Internationella dataöverföringar

1. DEFINITIONER

”**2021 års EU-standardavtalsklausuler**” avser standardavtalsklausulerna för överföring av personuppgifter till tredjeländer enligt GDPR, som antagits av Europeiska kommissionen enligt kommissionens genomförandebeslut (EU) 2021/914, som finns här[3].

”**2022 UK Addendum**” avser mall för tillägg B.1.0 som utfärdats av Storbritanniens Information Commissioner’s Office och som lagts fram för parlamentet i enlighet med s119A i Data Protection Act 2018 den 2 februari 2022, eftersom det kan revideras enligt avsnitt 18 i detta, tillgänglig här[4] .

”**EU-Kundpersonuppgifter**” avser behandling av Kundens Personuppgifter som dataskyddslagar i Europeiska unionen eller i en medlemsstat i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet var tillämpliga på innan de behandlades av Iron Mountain.

”**Skyddat område**” betyder:

i. när det gäller EU:s Kundpersonuppgifter, EU:s medlemsstater och Europeiska ekonomiska samarbetsområdet samt alla länder, territorier, sektorer eller internationella organisationer för vilka ett beslut om adekvat skyddsnivå enligt artikel 45 i GDPR är i kraft,

ii. när det gäller Personuppgifter om Kunder i Storbritannien, Storbritannien och alla länder, territorier, sektorer eller internationella organisationer för vilka ett beslut om adekvat skyddsnivå enligt Storbritanniens bestämmelser om adekvat skyddsnivå gäller,

iii. när det gäller schweiziska Kunders Personuppgifter, alla länder, territorier, sektorer eller internationella organisationer som är erkända som adekvata enligt lagarna i Schweiz,

iv. i händelse av att andra Kundpersonuppgifter överförs från en jurisdiktion som erbjuder liknande skydd som de för Kundpersonuppgifter från EU, Storbritannien eller Schweiz, något land, territorium, sektor eller internationell organisation som erkänns som adekvat enligt lagarna i sådan jurisdiktion.

”**Standardavtalsklausuler”** avser sammantaget EU:s standardavtalsklausuler för 2021 och Storbritanniens tillägg för 2022.

”**Schweiziska Kunders Personuppgifter**” avser behandling av Kunders Personuppgifter för vilka dataskyddslagar i Schweiz var tillämpliga före dess behandling av Iron Mountain.

”**Kundens Personuppgifter i Storbritannien**” avser behandling av Kunders Personuppgifter för vilka dataskyddslagar i Storbritannien var tillämpliga innan de behandlades av Iron Mountain.

2. DIVERSE

2.1 Denna bilaga 3 omfattar följande delar: (i) Del A – Överföringar av Personuppgifter om Kunder inom EU, (ii) Del B – Överföringar av Personuppgifter om Kunder inom Schweiz, (iii) Del C – Överföring av Personuppgifter om Kunder i Storbritannien, som ska gälla enligt vad som är relevant för Iron Mountains överföring av Personuppgifter om Kunder i samband med dess tjänster.

2.2 Standardavtalsklausulerna ska gälla för Iron Mountain och dess dotterbolag som ”Uppgiftsinförare” och för Kunden och dess dotterbolag som ”Uppgiftsutgivare”.

2.3 Undertecknandet och dateringen av Avtalet ska utgöra alla nödvändiga signaturer och datum för Standardavtalsklausulerna.

2.4 För det fall parterna överlåter EU, Personuppgifter om Kunder i Storbritannien eller Schweiz utanför det skyddade området och ett relevant EU-beslut eller annan giltig tillräcklighetsmetod enligt tillämplig Dataskyddslagstiftning som Iron Mountain har förlitat sig på för dataöverföringen anses vara ogiltig, eller någon tillsynsmyndighet kräver att överföringar av Personuppgifter som gjorts i enlighet med ett sådant beslut ska avbrytas, ska Parterna samarbeta och underlätta användningen av en alternativ överföringsmekanism. Parterna är även överens om att lämpliga skyddsåtgärder som vidtas för att underlätta internationella överföringar i denna bilaga 3 inte är exklusiva och att parterna kan fortsätta med ytterligare överföringsmekanismer, såsom EU-USA. Ramverk för datasekretess.

[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

DEL A – ÖVERFÖRINGAR AV EU-KUNDENS PERSONUPPGIFTER

Om och i den utsträckning som Kunden eller dess Dotterbolag överför EU-Kundens Personuppgifter utanför det Skyddade området till Iron Mountain eller dess Dotterbolag i samband med Iron Mountains Tjänster enligt Avtalet ska denna Del A i Bilaga 3 gälla, och Parterna samtycker till följande:

1. **Val av standardavtalsklausuler.** Texten från MODUL TVÅ av EU:s standardavtalsklausuler för 2021 ska gälla där Kunden eller något av dess dotterbolag är personuppgiftsansvarig och Iron Mountain eller något av dess dotterbolag är personuppgiftsbiträde. Texten från MODUL TRE av EU:s standardavtalsklausuler för 2021 ska gälla där Kunden eller något av dess dotterbolag är personuppgiftsbiträde och Iron Mountain eller något av dess dotterbolag är under-Personuppgiftsbiträde. De relevanta bestämmelserna i EU:s standardavtalsklausuler för 2021 införlivas genom hänvisning i detta DPA och är en integrerad del av detta DPA. Inga andra moduler eller klausuler markerade som valfria i EU:s standardavtalsklausuler för 2021 ska gälla. Den information som krävs för ändamålen i bilagorna till EU:s standardavtalsklausuler för 2021 anges i Bilaga 1 – Beskrivning av behandlingen/överföringen, Bilaga 2 – Tekniska och organisatoriska åtgärder och klausul 6.2 i DPA – Lista över under-personuppgiftsbiträden.

2. **Användning av under-personuppgiftsbiträden.** I enlighet med klausul 9 i EU:s standardavtalsklausuler för 2021 ska alternativ 2 (allmänt skriftligt tillstånd) för användning av under-personuppgiftsbiträden för utförandet av tjänsterna gälla. Kunden bekräftar och samtycker till att Iron Mountain kan anlita nya under-personuppgiftsbiträden genom den mekanism som överenskommits i klausul 6 i detta DPA och att tidsperioden för att skicka in förfrågningar om ändringar av under-personuppgiftsbiträden ska vara femton (15) dagar.

3. **Gällande lag och val av forum.** Vid tillämpningen av klausul 17 i EU:s standardavtalsklausuler från 2021 (Gällande lag) ska alternativ 2 som reglerar lag tillämpas, och dessa klausuler ska regleras av lagen i den EU-medlemsstat där Uppgiftsutgivareen är etablerad, i den utsträckning det tillåter tredje parts förmånstagares rättigheter. Vid tillämpning av klausul 18 i EU:s standardavtalsklausuler för 2021 (val av forum och jurisdiktion) ska dessa vara domstolar i den EU-medlemsstat där Uppgiftsutgivareen är etablerad.

4. **Certifiering av radering.** I den mening som avses i klausul 8.5 och 16(d) i EU:s standardavtalsklausuler från 2021 ska ett intyg om radering av Personuppgifter endast tillhandahållas Kunden av Iron Mountain på Kundens skriftliga begäran.

5. **Personuppgiftsincidenter.** Vid tillämpning av klausul 8.6(c) i EU:s standardavtalsklausuler för 2021 ska personuppgiftsincidenter hanteras i enlighet med den mekanism som överenskommits i klausul 7 i DPA.

6. **Revisioner.** Vid tillämpning av klausul 8.9 i EU:s standardavtalsklausuler för 2021 ska revisioner av dessa klausuler utföras i enlighet med den revisionsmekanism som överenskommits i avtalet.

7. **Klagomål.** I den mening som anses i klausul 11 i EU:s standardavtalsklausuler från 2021 ska Iron Mountain informera Kunden om det tar emot ett klagomål från en registrerad med avseende på EU-Kundens Personuppgifter och ska meddela klagomålet till Kunden i enlighet med den mekanism som överenskommits i Avtalet.

8. **Tillsynsmyndighet.** För EU:s standardavtalsklausuler för 2022 ska den relevanta behöriga tillsynsmyndigheten fastställas i enlighet med klausul 13 i EU:s standardavtalsklausuler.

DEL B – ÖVERFÖRING AV SCHWEIZISKA KUNDERS PERSONUPPGIFTER

Om och i den utsträckning Kunden eller dess dotterbolag överför schweiziska Kundpersonuppgifter utanför det skyddade området till Iron Mountain eller dess dotterbolag i samband med Iron Mountains tjänster enligt Avtalet ska denna del B i bilaga 3 gälla och parterna samtycker till följande:

1. **Val av standardavtalsklausuler.** EU:s standardavtalsklausuler 2021 och relevanta bestämmelser under Del A ska gälla där Kunden eller något av dess Dotterbolag är Personuppgiftsansvarig, och Iron Mountain eller något av dess Dotterbolag är Personuppgiftsbiträde, och/eller Kunden eller något av dess Dotterbolag är Personuppgiftsbiträde, och Iron Mountain eller något av dess Dotterbolag är underpersonuppgiftsbiträde, förutom att:

   a. den behöriga tillsynsmyndigheten enligt klausul 13 i EU:s standardavtalsklausuler för 2021 ska vara den schweiziska federala dataskydds- och informationskommissionen,

   b. tillämplig lag för avtalsenliga anspråk enligt klausul 17 i EU:s standardavtalsklausuler för 2021 ska vara schweizisk lag och platsen för jurisdiktion för åtgärder mellan parterna enligt klausul 18 (b) ska vara schweiziska domstolar.

2. Hänvisningar till EU:s GDPR i EU:s standardavtalsklausuler 2021 ska förstås som hänvisningar till FADP.

3. Termen ”medlemsstat” i EU:s standardavtalsklausuler för 2021 ska inte tolkas på ett sådant sätt att den utesluter registrerade i Schweiz från möjligheten att stämma för sina rättigheter på sin hemvist (Schweiz) i enlighet med klausul 18 (c) i EU:s standardavtalsklausuler för 2021.

DEL C – ÖVERFÖRINGAR AV KUNDERS PERSONUPPGIFTER I STORBRITANNIEN

Om och i den utsträckning som Kunden eller dess Dotterbolag överför Personuppgifter från Storbritannien utanför det Skyddade området till Iron Mountain eller dess Dotterbolag i samband med Iron Mountains Tjänster enligt Avtalet ska denna Del C i Bilaga 3 gälla, och Parterna samtycker till följande:

1. **Val av standardavtalsklausuler.** EU:s standardavtalsklausuler för 2021, relevanta bestämmelser under Del A och tillägget för 2022 i Storbritannien ska gälla där Kunden eller något av dess Dotterbolag är Personuppgiftsansvarig och Iron Mountain eller något av dess dotterbolag är Personuppgiftsbiträde och/eller Kunden eller något av dess Dotterbolag är Personuppgiftsbiträde och Iron Mountain eller något av dess Dotterbolag är underpersonuppgiftsbiträde.

2. **Del 1: Tabell 1 - 3 i 2022 års brittiska tillägg:** Information om Parterna – Tabell 1; Valda SCC:er, Moduler och Valda Klausuler; och Bilagainformation, inklusive Bilaga 1A: Förteckning över parter, bilaga 1B: Beskrivning av Överföring och Bilaga 1C: Tekniska och organisatoriska åtgärder för att säkerställa datasäkerheten – tabell 3 ska anses vara slutförda med hänvisning till denna bilaga 3, inklusive del A. Tabell 4 i det brittiska tillägget: Kunden och Iron Mountain bekräftar och samtycker till att det brittiska tillägget kan sägas upp av endera parten.

3. **Del 2:** Obligatoriska klausuler i det brittiska tillägget: Kunden och Iron Mountain bekräftar och samtycker till de obligatoriska klausulerna i det brittiska tillägget.

4. **Tillsynsmyndighet.** UK Information Commissioner’s Office ska fungera som behörig tillsynsmyndighet.

DEL D – ÖVERFÖRING AV ANDRA KUNDERS PERSONUPPGIFTER

Om och i den utsträckning Kunden eller dess dotterbolag överför Kundens Personuppgifter som inte omfattas av DEL A-C till Iron Mountain eller dess dotterbolag i samband med Iron Mountains Tjänster enligt Avtalet, ska Del A i Bilaga 3 gälla i den utsträckning som är relevant och tillämplig enligt tillämplig Dataskyddslagstiftning. I annat fall samtycker parterna, i den utsträckning som eventuella ersättnings- eller ytterligare lämpliga skyddsåtgärder eller överföringsmekanismer enligt Dataskyddslagstiftningen krävs för att överföra Kundens Personuppgifter till ett land som inte tillhandahåller tillräcklig skyddsnivå för Personuppgifter ur Uppgiftsutgivareens perspektiv, till att implementera samma så snart som möjligt och dokumentera sådana krav för implementering i en bilaga till detta DPA.

BILAGA 4

HIPAA – Affärspartneravtal (”BAA”)

Detta BAA kompletterar och ändrar alla nuvarande eller framtida avtal som ingåtts mellan Iron Mountain och dess dotterbolag och Kunden och dess dotterbolag under vilka Iron Mountain eller dess dotterbolag tillhandahåller vissa Tjänster till Kunden eller dess dotterbolag, vilka Tjänster kräver att Affärspartnern använder och/eller avslöjar PHI på uppdrag av den Berörda enheten. Förutom i den utsträckning som ändras i detta BAA ska alla villkor som anges i Avtalet förbli i full kraft och effekt och styra Tjänsterna som tillhandahålls av Iron Mountain till Kunden.

Iron Mountain och Kunden ingår detta BAA för att båda parter ska kunna uppfylla sina respektive skyldigheter när de träder i kraft och blir bindande för parterna enligt regelverket för säkerhet, sekretess och anmälan om överträdelser enligt HIPAA tillsammans med eventuella genomförandebestämmelser, inklusive de som implementeras som en del av Omnibus-regeln (gemensamt kallade ”HIPAA-reglerna”), enligt vilken Kunden och dess dotterbolag är en ”berörd enhet” eller ”Affärspartner” och Iron Mountain och dess dotterbolag är en ”Affärspartner” till Kunden. Vid tillämpningen av detta avtal ska alla hänvisningar nedan till affärspartnern anses vara hänvisningar till Iron Mountain eller dess tillämpliga dotterbolag.

1. **DEFINITIONER**

Termer med versaler som används men inte på annat sätt definieras i detta BAA ska ha samma betydelse som de som tillskrivs dessa termer i HIPAA-regler eller i avtalet, beroende på vad som är tillämpligt.

”**Regel för meddelande om överträdelse**” avser regeln för meddelande om överträdelse för oskyddade skyddade hälsouppgifter i 45 CFR §164 underavsnitt D.

”**Affärspartner**” ska betyda den affärsenhet som identifieras ovan i den utsträckning den tar emot, upprätthåller eller överför skyddad hälsoinformation vid leverans av tjänster till Kunder.

”**HIPAA**” avser Health Insurance Portability and Accountability Act från 1996.

”**HITECH-lagen**” avser tillämpliga bestämmelser i Health Information Technology for Economic and Clinical Health Act, som införlivats i American Recovery and Reinvestment Act från 2009, och inklusive eventuella genomförandebestämmelser.

”**Sekretessregel**” ska betyda standarderna för sekretess för individuellt identifierbar hälsoinformation enligt 45 CFR §160 och §164, underavsnitt A och E.

”**Skyddad hälsoinformation**” eller ”**PHI**” ska ha samma betydelse som termen ”skyddad hälsoinformation” i 45 CFR §160.103 och ska begränsas till den PHI som skapas av Affärspartner på Kundens vägnar eller tas emot från eller på Kundens vägnar i enlighet med Avtalet.

”**Säkerhetsregel**” avser Säkerhetsstandarderna för Skydd av Elektronisk Skyddad Hälsoinformation enligt 45 CFR §160 och §164, underavsnitt A och C.

1. **AFFÄRSPARTNERNS SKYLDIGHETER OCH AKTIVITETER**

1.1. Affärspartner samtycker till att inte använda eller ytterligare avslöja hälsouppgifter på annat sätt än vad som tillåts eller krävs enligt detta BAA eller enligt vad som krävs enligt lag.

1.2. Affärspartner samtycker till att vidta lämpliga skyddsåtgärder, och följa, som tillämpligt, med del C i 45 CFR §164 med avseende på elektroniska hälsouppgifter, för att förhindra användning eller avslöjande av PHI annat än vad som föreskrivs i detta BAA eller Avtalet. Emellertid bekräftar och samtycker Partnerna till att det är Kundens och inte Affärspartnerns ansvar att uppfylla kraven i 45 CFR §164.312 för att implementera krypterings- eller dekrypteringsmekanismer för elektroniska hälsouppgifter som upprätthålls på fysiska medier (t.ex. band) som lagras av Kunden hos Affärspartnern.

1.3. Affärspartner samtycker till att till kunden omedelbart rapportera alla säkerhetsincidenter, överträdelser eller annan användning eller avslöjande av hälsouppgifter som man får kännedom om som inte är tillåtet eller krävs enligt detta BAA eller Avtalet. I händelse av en överträdelse ska sådan anmälan göras i enlighet med och enligt vad som krävs av en affärspartner enligt HIPAA-reglerna, inklusive men inte begränsat till enligt 45 CFR 164.410, men under inga omständigheter mer än tre (3) arbetsdagar efter att affärspartnern har slutfört sin interna utredning och bekräftat en överträdelse som inträffat. Affärspartner kommer att tillhandahålla rimlig hjälp och samarbete i utredningen av sådana överträdelser och ska dokumentera de specifika insättningar som har äventyrats, identiteten på alla obehöriga tredje parter som kan ha fått åtkomst till eller tagit emot hälsouppgifter, om de är kända, och alla åtgärder som har vidtagits av Affärspartner för att mildra effekterna av sådana överträdelser.

1.4. Affärspartner ska, i enlighet med 45 CFR 164.502(e)(1)(ii) och 164.308(b)(2), beroende på vad som är tillämpligt, säkerställa att alla affärspartner som är en underleverantör som skapar, tar emot, upprätthåller eller överför PHI på uppdrag av Affärspartner i syfte att hjälpa till att tillhandahålla Tjänster

enligt Avtalet, samtycker till samma begränsningar, villkor och krav som gäller för Affärspartner med avseende på sådan PHI genom detta BAA.

1.5. Om Affärspartner har vårdnad om PHI i en angiven dokumentuppsättning med avseende på individer, och om Kunden så begär, samtycker Affärspartner till att ge Kunden åtkomst till sådan PHI genom att hämta och leverera sådan PHI i enlighet med villkoren i Avtalet, så att Kunden kan svara en individ för att uppfylla kraven i 45 CFR §164.524.

1.6. Affärspartner samtycker till att om en ändring av PHI i en angiven registeruppsättning i den ansvariges förvar krävs, och om Kunden instruerar Affärspartner att hämta sådan PHI i enlighet med Avtalet, ska Affärspartner utföra sådan tjänst så att Kunden kan göra eventuella ändringar av sådan PHI som kan krävas av antingen Kunden eller en Individ enligt 45 CFR §164.526.

1.7. Affärspartner samtycker till att dokumentera och för Kunden tillgängliggöra den information som krävs för att tillhandahålla en redovisning av avslöjanden av hälsouppgifter, förutsatt att Kunden har försett Affärspartnern med information som är tillräcklig för att göra det möjligt för Affärspartnern att fastställa vilka register eller data som mottas från eller på uppdrag av Kunden av Affärspartnern som innehåller hälsouppgifter. Dokumentationen av avslöjanden ska innehålla sådan information som krävs för att Kunden ska kunna svara på en begäran från en person om redovisning av avslöjanden av hälsouppgifter i enlighet med 45 CFR §164.528 eller andra bestämmelser i HIPAA-reglerna.

1.8. Om inget annat uttryckligen överenskommits i Avtalet ska Affärspartnern omedelbart meddela Kunden om alla förfrågningar från individer om tillgång till eller kunskap eller korrigering av PHI, utan att svara på sådana förfrågningar, och Kunden ska ansvara för att ta emot och svara på sådana individuella förfrågningar.

1.9. I den utsträckning Affärspartnern ska utföra en eller flera av Kundens skyldigheter enligt Underavsnitt E i 45 CFR §164 ska Affärspartnern uppfylla kraven i Underavsnitt E som gäller för Kunden vid utförandet av sådana skyldigheter.

1.10. Affärspartner samtycker till att göra sina interna rutiner, räkenskaper och register tillgängliga för sekreteraren i syfte att fastställa efterlevnad av HIPAA-reglerna.

2. TILLÅTEN ANVÄNDNING OCH AVSLÖJANDE AV AFFÄRSPARTNER

1.1. Affärspartner kan använda eller avslöja hälsouppgifter efter behov för att utföra de tjänster som anges i avtalet.

1.2. Affärspartner kan använda eller avslöja hälsouppgifter enligt vad som krävs enligt lag.

1.3. Affärspartner samtycker till att vidta rimliga åtgärder för att begränsa PHI till det minimum som krävs för att uppnå det avsedda syftet med användningen, avslöjandet eller begäran.

1.4. Affärspartner får inte använda eller avslöja hälsouppgifter på ett sätt som skulle bryta mot underavsnitt E i 45 CFR §164 om detta görs av Kunden.

1.5. Affärspartner kan lämna ut hälsouppgifter för korrekt hantering och administration av Affärspartner eller för att utföra Affärspartnerns juridiska ansvar, förutsatt att avslöjandena krävs enligt lag, eller Affärspartner erhåller rimliga försäkringar från den person till vilken informationen avslöjas att informationen kommer att förbli konfidentiell och användas eller vidare avslöjas endast enligt vad som krävs enligt lag eller för de ändamål för vilka den avslöjades för personen, och personen meddelar Affärspartner om alla fall där denne är medveten om att sekretessen för informationen har brutits.

3. KUNDENS SKYLDIGHETER

3.1. Kunden får inte instruera Affärspartner att agera på ett sätt som inte skulle vara förenligt med HIPAA-reglerna.

3.2. Kunden ska meddela Affärspartner om eventuella begränsningar i sitt meddelande om Kundens integritetspraxis i enlighet med 45 CFR §164.520, i den utsträckning som sådan begränsning kan påverka Affärspartners användning eller avslöjande av hälsouppgifter.

3.3. Kunden ska meddela Affärspartner om eventuella ändringar i eller återkallande av en Individs tillstånd att använda eller avslöja sin PHI, i den utsträckning sådana ändringar kan påverka Affärspartners användning eller avslöjande av PHI.

3.4. Kunden ska skriftligen meddela Affärspartner om eventuella begränsningar av Användning eller Avslöjande av PHI som Kunden har samtyckt till i enlighet med 45 CFR §164.522, i den utsträckning en sådan begränsning kan påverka Affärspartners Användning eller Avslöjande av PHI.

4. AVTALSTID OCH UPPSÄGANDE

4.1. Giltighetstiden för detta BAA ska börja från och med ikraftträdandedatumet och ska upphöra automatiskt vid det senare inträffandet av (i) avtalets upphörande eller (ii) när all PHI som tillhandahålls av Kunden till Affärspartner förstörs eller returneras till Kunden.

4.2. När den andra parten har kännedom om ett väsentligt brott mot BAA, ska den icke-överträdande parten ge den överträdande parten möjlighet att avhjälpa brottet. Om den överträdande parten inte åtgärdar överträdelsen inom trettio (30) dagar, efter att den överträdande parten har mottagit ett skriftligt meddelande från den icke-överträdande parten som anger detaljerna om sådant väsentligt avtalsbrott, ska den icke-överträdande parten ha rätt att säga upp detta BAA och avtalet i enlighet med villkoren i avtalet, eller, om uppsägning inte är möjlig, rapportera problemet till sekreteraren eller någon annan behörig myndighet.

4.3. <u>Effekt av uppsägning:</u>

4.3.1.1. Med undantag för vad som anges i 5.3.2 nedan ska Affärspartner, vid uppsägning av detta BAA av någon anledning, returnera eller förstöra all PHI som mottagits från Kunden i enlighet med Avtalet. Denna bestämmelse ska gälla för hälsouppgifter som innehas av affärspartners underleverantörer eller ombud. Affärspartner får inte behålla några kopior av PHI.

4.3.1.2. I händelse av att Affärspartner fastställer att återlämnande eller förstörande av PHI är ogenomförbart ska Affärspartner meddela Kunden om de villkor som gör återlämnande eller förstöring ogenomförbar. Efter meddelande till Kunden ska Affärspartnern utöka skyddet av detta BAA till sådan PHI och begränsa ytterligare användningar och avslöjanden av sådan PHI till de syften som gör returen eller förstörelsen omöjlig, så länge som Affärspartner upprätthåller sådan PHI i enlighet med villkoren i Avtalet.

5. DIVERSE

5.1. Skadeersättning. Affärspartner samtycker till att gottgöra Kunden för och mot alla böter eller straff som åläggs Kunden till följd av ett verkställighetsförfarande som inletts av Sekreteraren eller någon civilrättslig talan som väckts av en statlig statsåklagare mot Kunden, vilket förfarande eller åtgärd direkt och endast härrör från någon handling eller underlåtenhet av Affärspartner som antingen är en överträdelse av HIPAA-reglerna eller ett väsentligt brott mot detta BAA (”Anspråk”). Affärspartner ska inte vara skyldig att gottgöra Kunden för någon del av sådana böter eller påföljder som uppstår till följd av (i) Kundens brott mot HIPAA-reglerna eller detta BAA, eller (ii) Kundens försumliga eller avsiktliga handlingar eller utelämnanden. Ovanstående ersättningsskyldighet är uttryckligen villkorad av att Kunden beviljar Affärspartner rätten att på Affärspartners eget val och bekostnad, och med eget valt juridiskt ombud, kontrollera eller delta i försvaret av ett sådant Anspråk, dock under förutsättning att i den utsträckning ett sådant Anspråk är en del av ett större förfarande eller åtgärd, ska Affärspartners rätt att kontrollera eller delta begränsas till Anspråket och inte till det större förfarandet eller åtgärden. I händelse av att Affärspartner utövar sin möjlighet att kontrollera försvaret, ska (i) Affärspartner inte reglera något anspråk som kräver att Kunden erkänner något fel utan Kundens föregående skriftliga medgivande, (ii) Kunden ska ha rätt att på egen bekostnad delta i anspråket eller stämningen och (iii) Kunden ska samarbeta med Affärspartnern enligt vad som rimligen kan begäras. Det föregående anger Kundens enda och exklusiva gottgörelse och Affärspartnerns enda ansvar för Kundens förlust, skada, utgift eller ansvar för eventuella Anspråk i samband med detta BAA.

5.2. Förbudsföreläggande. Affärspartner bekräftar att all obehörig användning eller avslöjande av PHI av Affärspartner kan orsaka irreparabel skada för Kunden för vilken Kunden ska ha rätt att, om den så väljer, söka förbudsföreläggande eller annat föreläggande.

5.3. Regulatoriska referenser. En hänvisning i detta BAA till ett avsnitt i HIPAA-reglerna ska innebära att avsnitt i HIPAA, sekretessregeln, säkerhetsregeln, HITECH ACT eller de slutliga Omnibus-reglerna som ändrats och gäller, och för vilka efterlevnad krävs.

5.4. Ändring. Parterna är överens om att i god tro förhandla om alla ändringar av detta BAA som kan krävas från tid till annan enligt vad som är nödvändigt för att Kunden eller Affärspartner ska uppfylla kraven i HIPAA-reglerna. Om parterna inte kan nå en ömsesidig överenskommelse om villkoren för en sådan ändring inom sextio (60) dagar efter mottagandet av en sådan skriftlig begäran från Kunden till Affärspartner, ska endera parten ha rätt att säga upp detta BAA och Avtalet genom att tillhandahålla minst trettio (30) dagars skriftligt varsel till den andra parten.

5.5. Inga tredjepartsförmånstagare. Ingenting uttryckligt eller underförstått i detta BAA är avsett att ge, och inget häri ska ge, någon annan person än Kunden, Affärspartnern och deras respektive efterträdare eller övertagare, några som helst rättigheter, gottgörelser, skyldigheter eller ansvar.

5.6. Oberoende entreprenör. Affärspartner, inklusive dess direktörer, tjänstemän, anställda och ombud, är en oberoende entreprenör och inte ett ombud (enligt definitionen i Federal common law of agency) för Kunden eller en medlem av dess personalstyrka. Utan att begränsa allmängiltigheten i det föregående ska Kunden inte ha någon rätt att kontrollera, styra eller på annat sätt påverka affärspartnerns beteende i samband med utförandet av Tjänsterna, annat än genom upprätthållandet av detta BAA eller Avtalet, eller den ömsesidiga ändringen av detsamma.

5.7. Företräde. Hela avtalet. Tvetydigheter i detta BAA ska lösas för att tillåta parterna att följa HIPAA-reglerna. Detta BAA utgör hela avtalet mellan parterna med avseende på ämnet häri och ska ersätta alla tidigare meddelanden, representationer, avtal och överenskommelser som rör HIPAA-reglerna, inklusive alla tidigare affärspartneravtal mellan parterna.