Databehandlingsaftale

FORMÅL OG FORRANG

Denne Databehandlingsaftale, sammen med dens bilag og eventuelt dokument, til hvilket der udtrykkeligt krydshenvises ("**Databehandlingsaftalen**"), anses for at være en del af tjenesteaftalen mellem Iron Mountain og Kunden ("**Aftalen**"). Vilkårene og betingelserne i Aftalen gælder for og regulerer parternes rettigheder og forpligtelser i henhold til denne Databehandlingsaftale.

Hvis eventuelle vilkår og betingelser indeholdt i denne Databehandlingsaftale er i strid med vilkårene og betingelserne angivet i Aftalen, skal vilkårene og betingelserne angivet i denne Databehandlingsaftale have forrang med hensyn til genstanden for denne Databehandlingsaftale. Denne Databehandlingsaftale erstatter alle tidligere databehandlingsaftaler eller databeskyttelses- eller privatlivsbestemmelser mellem parterne i forbindelse med Tjenesterne, der leveres i henhold til Aftalen.

GENERELLE VILKÅR

1. DEFINITIONER

Medmindre de specifikt er defineret heri, skal alle betegnelser have de samme betydninger, som de er tildelt i Aftalen.

"**Dataansvarlig**" betyder den fysiske eller juridiske person, offentlige myndighed, agentur eller andet organ, som alene eller i fællesskab med andre bestemmer formålene med og midlerne til Behandling af Personoplysninger,

"**Kundens personoplysninger**" betyder Personoplysninger, der tilhører eller indsamles fra Kunden eller dennes tilknyttede selskaber, der Behandles som en del af Tjenesterne,

"**Registreret**" betyder en identificeret eller identificerbar fysisk person,

"Databeskyttelseslovgivning" betyder alle gældende love og forordninger vedrørende Behandlingen af Personoplysninger, der kan eksistere i de relevante retskredse, herunder, men ikke begrænset til, EU's generelle forordning om databeskyttelse (Forordning (EU) 2016/679), den britiske generelle forordning om Databeskyttelse (den generelle forordning om databeskyttelse, der gælder som en del af britisk national lovgivning i medfør af afsnit 3 i Den Europæiske Unions (Udtrædelses-) lov fra 2018 og som ændret ved forordningerne om Databeskyttelse, Privatlivets fred og Elektronisk kommunikation (Ændringer, osv.) (Udtræden af EU) fra 2019 (som ændret)), Databeskyttelsesloven fra 2018, FADP (Den schweiziske Føderale Lov om Databeskyttelse), amerikanske Enkeltstatslovgivninger, LGPD (brasiliansk Generel Databeskyttelseslov), PIPL (Loven om Beskyttelse af Personoplysninger i Folkerepublikken Kina), og eventuel lovgivning og/eller forordning, der implementerer eller foretages i medfør af dem, eller som ændrer, erstatter, genindfører eller konsoliderer enhver af dem, herunder, hvis relevant, vejledningning og adfærdskodekser udstedt af tilsynsmyndigheder,

"**Personoplysninger**" betyder alle oplysninger vedrørende en Registreret,

"**Databehandler**" betyder en fysisk eller juridisk person, offentlig myndighed, agentur eller andet organ, der Behandler Personoplysninger på vegne af den Dataansvarlige,

"**Behandling**" betyder enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som Personoplysninger eller en samling af Personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse,

"**Sikkerhedsbrud**" betyder enhver utilsigtet eller ulovlig skade, tilintetgørelse, tab, ændring eller uautoriseret videregivelse af, eller adgang til, Kundens Personoplysninger, som Iron Mountain, dets personale eller underleverandører Behandler i forbindelse med levering af Tjenesterne,

"**Tjenester**" betyder enhver tjeneste, der leveres af Iron Mountain eller dennes tilknyttede selskaber til Kunden eller dennes tilknyttede selskaber i henhold til Aftalen;

"**Amerikanske Staters Privatlivslove**" betyder alle amerikanske staters privatlivs- og databeskyttelseslove, der gælder for Behandlingen af Personoplysninger i henhold til Aftalen, herunder uden begrænsning, og som ændret eller erstattet fra tid til anden: (1) Californiens Lov om Beskyttelse af Forbrugeres Personoplysninger (California Consumer Privacy Act), som ændret af Californiens Lov om Privatlivsrettigheder (California Privacy Rights Act), og eventuelle gennemførelsesforordninger vedrørende disse (samlet benævnt "**CCPA**") (2) Colorados Privatlivslov (Colorado Privacy Act, "**CPA**"), (3) Virginias Lov om Beskyttelse af Forbrugeres Personoplysninger (Virginia Consumer Data Protection Act, "**CDPA**") (4) Utahs Lov om Beskyttelse af Forbrugeres Personoplysninger (Utah Consumer Privacy Act, "**UCPA**"), og (5) Connecticuts Databeskyttelseslov (Connecticut Data Privacy Act, "**CTDPA**").

2. ANVENDELSESOMRÅDE OG NÆRMERE OPLYSNINGER OM DATABEHANDLING

2.1 Denne Databehandlingsaftale gælder for Kundens Personoplysninger, der Behandles af Iron Mountain som Databehandler i forbindelse med levering af Tjenesterne i medfør af Aftalen på vegne af Kunden.

2.2 Iron Mountain kan indsamle og Behandle Personoplysninger om Kunden og dennes tilknyttede selskabers medarbejdere som Dataansvarlig til legitime forretningsformål, såsom kontraktforvaltning og administration af kundeforhold, og i overensstemmelse med Databeskyttelseslovgivningen og Iron Mountains privatlivserklæring, der er tilgængelig på Iron Mountains websteder og andre gældende privatlivspolitikker. Iron Mountains forpligtelser, der er fastsat i denne Databehandlingsaftale, gælder ikke for behandlingen af sådanne Personoplysninger.

2.3 Genstanden for Behandlingen af Personoplysninger er udførelsen af Tjenesterne. Kunden og Iron Mountains rettigheder og forpligtelser er som angivet i denne Databehandlingsaftale. Bilag 1 til denne Databehandlingsaftale angiver arten og varigheden af, samt formålet med, Behandlingen, de typer af Kundens Personoplysninger, som Iron Mountain Behandler, og kategorierne af Registrerede, hvis Personoplysninger Behandles.

2.4 Når Iron Mountain Behandler Kundens Personoplysninger i forbindelse med levering af Tjenesterne, vil Iron Mountain:

2.4.1 Kun Behandle Kundens Personoplysninger i overensstemmelse med dokumenterede anvisninger fra Kunden. Hvis Iron Mountain er forpligtet til at Behandle Kundens Personoplysninger til eventuelt andet formål ved lov, som Iron Mountain er underlagt, vil Iron Mountain først informere Kunden om dette krav, medmindre en sådan lov forbyder dette af vigtige årsager af offentlig interesse, og

2.4.2 Til enhver tid overholde gældende Databeskyttelseslovgivning og straks underrette Kunden, hvis Iron Mountain mener, at en anvisning vedrørende Behandling af Kundens Personoplysninger, som Kunden har givet, krænker gældende Databeskyttelseslovgivning.

2.5 Kundens anvisninger er bindende for Iron Mountain, medmindre udførelse af anvisningerne kræver levering af en tjeneste i henhold til Aftalen, og Kunden ikke accepterer at betale tjenestegebyrerne for sådanne tjenester.

2.6 Iron Mountain skal sikre, at personale, der skal have adgang til Kundens Personoplysninger, er underlagt en bindende fortrolighedsforpligtelse med hensyn til sådanne Personoplysninger, og skal træffe rimelige foranstaltninger for at sikre pålideligheden og kompetencen af Iron Mountains personale, der har adgang til Kundens Personoplysninger.

3. YDELSE AF KUNDESERVICE

3.1 Iron Mountain skal yde assistance til Kunden, altid under hensyntagen til arten af Behandlingen:

3.1.1 via passende tekniske og organisatoriske foranstaltninger og i det omfang, det er muligt, ved opfyldelse af Kundens forpligtelser til at svare på anmodninger fra Registrerede, der udøver deres rettigheder,

3.1.2 ved sikring af overholdelse af Kundens forpligtelser (såsom sikkerhed af Behandling, underretning om et brud på Persondatasikkerheden til tilsynsmyndigheden, underretning om et brud på Persondatasikkerheden til den Registrerede, konsekvensanalyse vedrørende databeskyttelse og forudgående høring med tilsynsmyndighederne, hvis Behandlingen ville medføre en høj risiko i mangel af foranstaltninger truffet af den Dataansvarlige for at mindske risikoen), under hensyntagen til de oplysninger, der er tilgængelige for Iron Mountain, og

3.1.3 ved at stille alle oplysninger til rådighed for Kunden, som Kunden med rimelighed anmoder om for at give Kunden mulighed for at påvise, at dennes forpligtelser i forbindelse med udvælgelse og udpegelse af Iron Mountain er opfyldt.

4. SIKKERHEDSFORANSTALTNINGER

4.1 Under hensyntagen til sædvanlige driftsmæssige procedurer, omkostningerne ved implementering, samt arten, omfanget, sammenhængen og formålet med Behandling, skal Iron Mountain implementere passende og rimelige tekniske og organisatoriske foranstaltninger, der er beregnet til at beskytte

fortroligheden, integriteten og tilgængeligheden af Kundens Personoplysninger, og for at beskytte Kundens Personoplysninger mod uautoriseret eller ulovlig Behandling og mod utilsigtet tab, tilintetgørelse, skade, ændring, eller videregivelse. Iron Mountains sikkerhedsstandarder er angivet i Bilag 2 til denne Databehandlingsaftale.

4.2 Det er alene Kundens ansvar at vurdere, om disse tekniske og organisatoriske foranstaltninger opfylder Kundens krav.

5. OVERHOLDELSE AF LOVE

Kunden og dennes tilknyttede selskaber skal: (i) Behandle Kundens Personoplysninger i overensstemmelse med Databeskyttelseslovgivningen, (ii) være bemyndiget til at give skriftlige anvisninger til Iron Mountain om Behandlingen af Kundens Personoplysninger i forbindelse med Tjenesterne (herunder på vegne af eventuel tredjepartsenhed, der er en Dataansvarlig for Kundens Personoplysninger), og (iii) til enhver tid bevare kontrollen og myndigheden over Kundens Personoplysninger i forbindelse med Behandlingen.

6. UNDERDATABEHANDLING

6.1 Kunden anerkender og accepterer, at Iron Mountain kan ansætte sit moderselskab, sine tilknyttede selskaber og andre tredjeparts-Underdatabehandlere (herunder tredjeparts-Underdatabehandlere, der ansættes af Iron Mountains tilknyttede selskaber eller moderselskab) med henblik på Behandling af Kundens Personoplysninger i henhold til denne Databehandlingsaftale med forbehold for bestemmelse 6.2 nedenfor.

6.2 En liste over Underdatabehandlere, der er godkendt af Kunden pr. datoen for denne Databehandlingsaftale, er tilgængelig her[1]. Iron Mountain kan til enhver tid erstatte eller udnævne en ny Underdatabehandler, forudsat at Kunden får femten (15) dages forudgående skriftligt varsel, og Kunden ikke gør indsigelse mod sådanne ændringer af påviselige årsager relateret til databeskyttelse inden for den pågældende tidsramme. For at modtage disse e-mailmeddelelser skal Kunden abonnere på og administrere eventuelt eksisterende abonnement på Iron Mountains meddelelsestjeneste via denne webside[2].

6.3 Hvis Kunden ikke abonnerer på denne meddelelsestjeneste, er Iron Mountain ikke erstatningsansvarlig for den manglende meddelelse om Underdatabehandlere, og alle sådanne udnævnelser anses for at være godkendt af Kunden**.** Hvis Kunden gør skriftlig indsigelse af påviselige årsager relateret til databeskyttelse mod udnævnelsen af en erstatnings- eller ny Underdatabehandler inden for det femten (15) dages forudgående skriftlige varsel, skal Iron Mountain gøre rimelige bestræbelser på at stille en ændring i Tjenesterne til rådighed for Kunden eller anbefale en ændring af Kundens konfiguration eller brug af Tjenesterne, i hvert enkelt tilfælde for at undgå Behandlingen af Kundens Personoplysninger af den anfægtede Underdatabehandler, til Kundens overvejelse og godkendelse. Hvis Kunden ikke godkender sådanne ændringer, der foreslås af Iron Mountain inden for femten (15) dage, kan Iron Mountain, ved at give skriftlig meddelelse til Kunden, omgående opsige Tjenesten eller den del af Tjenesten, som ikke kan leveres af Iron Mountain uden brug af den anfægtede Underdatabehandler. En sådan opsigelse skal ikke berøre parternes påløbne rettigheder og forpligtelser, forudsat at ingen opsigelsesgebyrer, udgifter eller anden kompensation skal betales af Iron Mountain eller Iron Mountains tilknyttede selskaber i forbindelse med en sådan opsigelse, og Kunden skal straks tage besiddelse af de aktiver, som Iron Mountain har fået stillet til rådighed som en del af de opsagte Tjenester, med forbehold for vilkårene i Aftalen og på Kundens egen regning.

6.4 Iron Mountain skal sikre, at eventuel kontrakt med Underdatabehandlere, der er omfattet af denne Databehandlingsaftale, indeholder bestemmelser, der i alle væsentlige henseender er de samme som dem i denne Databehandlingsaftale og er som krævet af gældende Databeskyttelseslovgivning. Hvis en Iron Mountain-Underdatabehandler foranlediger, at Iron Mountain overtræder sine forpligtelser i henhold til denne Databehandlingsaftale eller eventuel gældende Databeskyttelseslovgivning, vil Iron Mountain forblive fuldt erstatningsansvarlig over for Kunden for opfyldelsen af Iron Mountains forpligtelser i henhold til disse vilkår.

7. SIKKERHEDSBRUD

7.1 I tilfælde af et formodet Sikkerhedsbrud vil Iron Mountain:

7.1.1 omgående træffe foranstaltninger for at undersøge det formodede Sikkerhedsbrud og for at identificere, forebygge og afbøde virkningerne af det formodede Sikkerhedsbrud og for at afhjælpe Sikkerhedsbruddet,

---

[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=

7.1.2 underrette Kunden uden unødig forsinkelse, når den med rimelighed er sikker på, at et Sikkerhedsbrud har fundet sted, og tilvejebringe en detaljeret beskrivelse af sikkerhedsbruddet for Kunden, herunder oplysninger, der med rimelighed er nødvendige for, at Kunden kan opfylde rapporteringsforpligtelser i henhold til Databeskyttelseslovgivningen.

7.2 Kunden accepterer, at Iron Mountain kan tilvejebringe oplysningerne i henhold til bestemmelse 7.1.2 i faser. I sådanne tilfælde, hvor Iron Mountain ikke har adgang til eller ikke kan tilvejebringe visse oplysninger, der er anført i bestemmelse 7.1.2, for Kunden, vil Iron Mountain informere Kunden herom, og Iron Mountain er ikke erstatningsansvarlig for manglende tilvejebringelse af sådanne oplysninger.

8. REVISIONER

Iron Mountain vil give Kunden og dennes respektive revisorer eller autoriserede agenter, ved at give varsel på mindst ti (10) hverdage til Iron Mountain, tilladelse til at foretage revisioner eller inspektioner i løbet af Aftalens løbetid, forudsat at Iron Mountain ikke er forpligtet til at give eller tillade adgang til oplysninger vedrørende: (i) Iron Mountains andre kunder (ii) nogen af Iron Mountains ikke-offentlige eksterne rapporter, og (iii) eventuelle interne rapporter udarbejdet af Iron Mountains interne revisions- eller compliance-funktion. Formålene med en revision eller inspektion i henhold til denne bestemmelse er begrænset til at bekræfte, at Iron Mountain Behandler Kundens Personoplysninger i overensstemmelse med sine forpligtelser i henhold til denne Databehandlingsaftale. Undtagen hvor et Sikkerhedsbrud har fundet sted, må der ikke udføres mere end én sådan revision i enhver periode på tolv (12) måneder.

9. INTERNATIONALE DATAOVERFØRSLER (BEGRÆNSEDE OVERFØRSLER)

9.1 I det omfang det er relevant, giver Kunden hermed sit samtykke til og godkender internationale overførsler af Kundens Personoplysninger til enheder som angivet i Afsnit 6.2 og i overensstemmelse med Bilag 3 for levering af Tjenesterne, og Kunden og Iron Mountain aftaler:

9.1.1 at overholde gældende Databeskyttelseslovgivning med hensyn til sådanne overførsler,

9.1.2 at de har, under hensyntagen til, uden begrænsning, i) kategorierne af Kundens Personoplysninger, ii) de lande, hvis nationale love muligvis ikke yder et beskyttelsesniveau for Personoplysninger, der kan sammenlignes med dem, der er indeholdt i EU-/britisk lovgivning ("**Tredjeland**"), iii) de relevante tekniske og organisatoriske foranstaltninger, der er angivet i Afsnit 7 og iv) de relevante parter, der deltager i behandlingen af sådanne Personoplysninger, foretaget en vurdering af hensigtsmæssigheden af den relevante overførselsmekanisme, der er vedtaget herunder, hvis påkrævet ved lov, og har fastslået, at en sådan overførselsmekanisme er designet hensigtsmæssigt til at sikre, at Personoplysninger, der overføres i overensstemmelse med denne Databehandlingsaftale, ydes et beskyttelsesniveau i destinationslandet, der i væsentlig grad svarer til det, der garanteres i henhold til Databeskyttelseslovgivningen.

10. ERSTATNINGSANSVAR OG SKADESLØSHOLDELSE

10.1 Uanset eventuelle bestemmelser om det modsatte i Aftalen, i tilfælde af et Sikkerhedsbrud forårsaget direkte af Iron Mountains brud på sine forpligtelser i henhold til denne Databehandlingsaftale, skal Iron Mountain refundere Kunden i det omfang, det er tilladt ved gældende lovgivning for de direkte, verificérbare, nødvendige og med rimelighed afholdte tredjepartsomkostninger for Kunden i (a) undersøgelsen af et sådant Sikkerhedsbrud, (b) udarbejdelse og afsendelse af meddelelser til sådanne Registrerede og tilsynsmyndigheder som kræves af Databeskyttelseslovgivningen, (c) leveringen af kreditovervågningstjenester til sådanne enkeltpersoner, som påkrævet ved lov, i en periode på højst tolv (12) måneder, og (d) betaling af den del af forskriftsmæssige bøder, straffe eller sanktioner pålagt af en tilsynsmyndighed, for hvilke tilsynsmyndigheden angiver, at Iron Mountain er direkte ansvarlig.

10.2 I tilfælde af, at en Registreret fremsætter et krav mod en eller begge parter for påstået krænkelse af Databeskyttelseslovgivningen ("**Registreredes krav**"), hvor dette er tilladt, skal hver part kontrollere sit eget forsvar af ethvert sådant krav (eller dets del af forsvaret) og forblive eneansvarlig for sine egne omkostninger, udgifter og forpligtelser i forbindelse hermed, herunder advokatsalærer eller eventuelle beløb, som en domstol tilkender mod parten eller som følge af et forlig, dog forudsat, at hvor hver part er ansvarlig for en del eller enhver af parterne er ansvarlig for det fulde beløb af de skadeserstatninger, som en registreret har lidt for den samme hændelse eller serie af hændelser, og den Registrerede kun har modtaget fuld kompensation fra én part ("den **Kompenserende part**"), så skal den Kompenserende part være berettiget til at fremsætte krav mod den anden part om tilbagebetaling af den del af kompensationen, der svarer til den skade, som en sådan anden part har forårsaget. Den Kompenserende part kan kun fremsætte sit krav mod den anden part inden for 12 måneder efter hændelsen, i det omfang tilladt ved gældende lov.

10.3 I det maksimale omfang tilladt ved gældende lovgivning, regulerer ansvarsbegrænsningerne og eventuelle udelukkelser af skadeserstatninger, der er angivet i Aftalen, det samlede erstatningsansvar for alle Kundekrav, der opstår som følge af eller i forbindelse med denne Databehandlingsaftale og/eller Aftalen, mod Iron Mountain. Disse ansvarsbegrænsninger og udelukkelser af skadeserstatninger gælder

for alle krav, uanset om de opstår i henhold til kontrakt, for skadevoldende handling eller i henhold til eventuel anden ansvarsteori, og enhver henvisning til Iron Mountains erstatningsansvar betyder Iron Mountain og alle Iron Mountains tilknyttede selskabers samlede erstatningsansvar for krav fra Kunden og alle Kundens tilknyttede selskaber. I det omfang det kræves ved gældende lovgivning, er dette afsnit ikke beregnet til at (i) ændre eller begrænse parternes erstatningsansvar for Registreredes Krav, der fremsættes mod en part, hvor der er solidarisk hæftelse, eller (ii) begrænse en parts ansvar for at betale sanktioner, der er pålagt en sådan part af en tilsynsmyndighed.

10.4 Bestemmelser 10.1 til 10.3 angiver hver parts eneste og eksklusive retsmiddel og hver parts eneansvar for eventuelt tab, skade, udgift eller forpligtelse i forbindelse med denne Databehandlingsaftale

11. ANMODNINGER FRA OFFENTLIGE MYNDIGHEDER

11.1 I det omfang, det er tilladt ved lov og med forbehold for bestemmelse 11.2 til 11.5 nedenfor, accepterer Iron Mountain at underrette Kunden, hvis den:

11.1.1 modtager en juridisk bindende anmodning fra en offentlig myndighed, herunder retslige myndigheder, i henhold til lovgivningen i destinationslandet om videregivelse af Kundens Personoplysninger, der overføres i medfør af Aftalen, eller

11.1.2 bliver opmærksom på offentlige myndigheders direkte adgang til Kundens Personoplysninger, der overføres i medfør af Aftalen i overensstemmelse med lovgivningen i destinationslandet .

11.2 Hvis det er forbudt for Iron Mountain at underrette Kunden i henhold til lovgivningen i destinationslandet, accepterer Iron Mountain at gøre sit bedste for at opnå et afkald på forbuddet med henblik på at kommunikere så mange oplysninger som muligt så hurtigt som muligt.

11.3 Iron Mountain accepterer at gennemgå lovligheden af anmodningen om videregivelse, især om den forbliver inden for de beføjelser, der er tildelt den anmodende offentlige myndighed, og at anfægte anmodningen, hvis den konkluderer, at der er rimelig grund til at antage, at anmodningen er ulovlig i henhold til lovgivningen i destinationslandet. Den skal ikke videregive Kundens anmodede Personoplysninger, før den er forpligtet til at gøre det i henhold til de gældende procedureregler.

11.4 Iron Mountain indvilliger i at tilvejebringe det mindste antal oplysninger, der er tilladt ved besvarelse af en anmodning om videregivelse, baseret på en rimelig fortolkning af anmodningen.

11.5 Iron Mountain accepterer at opbevare oplysningerne i medfør af denne bestemmelse i Aftalens løbetid og gøre dem tilgængelige for den kompetente tilsynsmyndighed efter anmodning herom.

12. DIVERSE

12.1 Med forbehold for arten af de Tjenester, der leveres af Iron Mountain, skal Iron Mountain ved opsigelse/udløb af Aftalen, baseret på Kundens specifikke anvisning og med forbehold for vilkårene i Aftalen, enten slette/tilintetgøre eller returnere alle Kundens Personoplysninger til Kunden eller til en tredjepart udpeget af Kunden. Alle Kundens Personoplysninger, der er indeholdt i Kundens aktiv, som opbevares af Iron Mountain på vegne af Kunden, vil blive returneret til Kunden i overensstemmelse med en aftalt udtrædelses- eller overgangsplan, og med forbehold for aftalte omkostninger, som fastsat i Aftalen eller andet gældende kontraktdokument. I alle andre tilfælde, hvis Aftalen intet angiver om sletning/tilintetgørelse eller returnering af Kundens Personoplysninger, og Kunden undlader at give eventuelle anvisninger vedrørende sletning/tilintetgørelse eller returnering af Kundens Personoplysninger inden for femten (15) dage efter opsigelsen/udløbet af Aftalen, skal Iron Mountain sende en skriftlig meddelelse til Kunden, der anmoder om at modtage specifikke anvisninger inden for 15 (femten) dage om, hvorvidt Kundens Personoplysninger skal slettes/tilintetgørelse eller returneres, og informerer Kunden om alle gældende gebyrer for sikker tilintetgørelse eller andre gebyrer, der skal betales af Kunden. Hvis Kunden undlader at give skriftlige anvisninger inden for en sådan femten (15) dages tidsramme og betale de gældende gebyrer inden for samme periode, bemyndiger Kunden hermed Iron Mountain til yderligere at Behandle, slette, tilintetgøre alle Kundens Personoplysninger efter opsigelse af Aftalen efter Iron Mountains valg og for Kundens regning.

12.2 Uanset Bestemmelse 12.1 misligholder Iron Mountain ikke sine forpligtelser med hensyn til sletning af Kundens Personoplysninger, der opbevares på backup-bånd, så længe sådanne backup-bånd overskrives (og Kundens Personoplysninger dermed slettes) under normal forretningsgang.

12.3 Med undtagelse af Standardkontraktbestemmelserne (som defineret i Bilag 3 til denne Databehandlingsaftale), er denne Databehandlingsaftale og eventuel tvist, krav eller uoverensstemmelse, der opstår som følge af eller i forbindelse med denne Databehandlingsaftale, eller overtrædelsen, opsigelsen eller gyldigheden deraf, underlagt Aftalens lovvalgsbestemmelse, og eventuel tvist, uoverensstemmelse eller krav, der opstår som følge af eller i forbindelse med denne Databehandlingsaftale, vil primært blive løst gennem eventuel defineret tvistbilæggelsesproces, der er indeholdt i Aftalen.

12.4 Hver part kan underrette den anden part skriftligt fra tid til anden om eventuelle ændringer af denne Databehandlingsaftale, som parten med rimelighed anser for nødvendige for at imødekomme kravene i Databeskyttelseslovgivningen eller eventuel afgørelse truffet af en tilsynsmyndighed eller kompetent domstol. Alle sådanne ændringer træder kun i kraft, hvis og i det omfang, de er angivet i en gensidigt

aftalt ændring af denne Databehandlingsaftale, der underskrives af begge parter, medmindre den ene part informerer den anden part om eventuelt nyt lovkrav og sender en sådan ændring, der kun omfatter de nødvendige ændringer, og som kan indgås uden formelt at acceptere den, dvs. ved ikke at gøre indsigelse inden for en bestemt frist, betragtes de som gensidigt aftalte ændringer til denne Databehandlingsaftale.

BILAG 1

Nærmere oplysninger om Behandling og Dataoverførsel (hvis relevant)

A. LISTE OVER PARTER:

Parterne i denne Databehandlingsaftale og rollerne som Dataeksportør og Dataimportør er angivet i Aftalen og Bilag 3 (Internationale dataoverførsler), hvis relevant.

B. BESKRIVELSE AF BEHANDLING/OVERFØRSEL (hvis relevant):

Kategorier af Registrerede, hvis Personoplysninger behandles/overføres:

Afhængigt af arten af Iron Mountains Tjenester og Kundens forretning kan Kunden indsende Personoplysninger, der tilhører forskellige kategorier af Registrerede, til Iron Mountain, hvis omfang bestemmes og kontrolleres af Kunden efter eget skøn. Som sådan, kan kategorier af Registrerede omfatte: tidligere og nuværende medarbejdere, tidligere og nuværende kontrahenter eller konsulenter, kontrahenter eller konsulenter og eksterne udstationerede fra bureauer, jobansøgere og -kandidater, studerende og frivillige, enkeltpersoner identificeret af medarbejdere eller pensionister som begunstigede, ægtefælle, registreret partner, pårørende og nødkontakter, pensionister, tidligere og nuværende direktører og ledere, aktionærer, obligationsindehavere, kontoindehavere, slutbrugere/forbrugere (voksne, børn), patienter (voksne, børn), forbipasserende (overvågningskameraer), og webstedsbrugere.

Kategorier af behandlede/overførte Personoplysninger:

Afhængigt af arten af Iron Mountains Tjenester og Kundens forretning kan Kunden indsende Personoplysninger, der tilhører forskellige kategorier af Personoplysninger, til Iron Mountain, hvis omfang bestemmes og kontrolleres af Kunden efter eget skøn. Som sådan kan kategorier omfatte personoplysninger vedrørende Kunden og/eller Kundens egne kunder, medarbejdere, osv.

Overførte følsomme oplysninger (hvis relevant):

Afhængigt af arten af Iron Mountains tjenester og Kundens forretning kan Kunden indsende følsomme oplysninger til Iron Mountain, hvis omfang bestemmes og kontrolleres af Kunden efter eget skøn.

Hvis relevant, hyppigheden af overførslen (f.eks. hvorvidt oplysningerne overføres på engangs- eller løbende basis):

Overførslen sker løbende.

Behandlingens art:

Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse,

Formål med databehandling/overførsel (hvis relevant) og Viderebehandling:

Levering af tjenester som angivet i Aftalen.

Opbevaring af oplysninger:

Personoplysningerne vil blive opbevaret af Iron Mountain under varigheden af de Tjenester, der tilbydes Kunden, og indtil det tidspunkt, hvor Personoplysningerne returneres eller tilintetgøres som bestemt i overensstemmelse med bestemmelse 12.1 i denne Databehandlingsaftale.

Hvis relevant, for overførsler til (under)Databehandlere, skal der også angives genstand for, art og varighed af Behandlingen:

Under hele Aftalens varighed leverer Underdatabehandlerne blandt andet informationsteknologi- (IT) og konsulenttjenester, herunder global IT-support, hændelsesrapportering og administrationstjenester.

C. KOMPETENT TILSYNSMYNDIGHED

Som angivet i Bilag 3 (Internationale Dataoverførsler), hvis relevant.

BILAG 2

TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER ("SIKKERHEDSFORANSTALTNINGER")

1. INFORMATIONSSIKKERHEDSPROGRAM OG -POLITIK

Iron Mountain skal opretholde et informationssikkerhedsprogram med passende fysiske, tekniske og administrative kontroller, der er beregnet til at opfylde branchestandarderne. Informationssikkerhedsprogrammet skal omfatte:

1.1 Dokumentation, intern udgivelse og kommunikation af Iron Mountains informationssikkerhedspolitikker, -standarder og -procedurer,

1.2. Dokumenteret, klar tildeling af ansvar og myndighed for etablering og opretholdelse af informationssikkerhedsprogrammet,

1.3 Regelmæssig afprøvning af de vigtigste kontroller, systemer og procedurer i informationssikkerhedsprogrammet,

1.4 Administrative, tekniske og driftsmæssige foranstaltninger, der er beregnet til at beskytte alle Kundens Personoplysninger ved hjælp af de praksisser, procedurer og processer, der er beskrevet i dette Sikkerhedsbilag, i det omfang de er relevante og gældende for det format, hvori Kundens Personoplysninger opbevares.

2. RISIKOVURDERING

Iron Mountain skal opretholde et risikovurderingsprogram for informationssikkerhed, der er beregnet til at identificere og med rimelighed vurdere forudsigelige interne og eksterne risici og sårbarheder, der kan påvirke sikkerheden, fortroligheden og/eller integriteten af Kundens Personoplysninger. Iron Mountain skal evaluere og opdatere, hvis nødvendigt, rimeligt og hensigtsmæssigt, effektiviteten af det nuværende informationssikkerhedsprogram til begrænsning af sådanne risici på årsbasis, eller når der sker en væsentlig ændring i risiko eller sårbarheder for Kundens Personoplysninger.

3. ADMINISTRATION AF AKTIVER TIL BEHANDLING AF OPLYSNINGER OG FYSISKE MEDIER

3.1 Forvaltning af Databehandlingsaktiver Iron Mountain opretholder et program til administration af aktivbeholdningen for at administrere de fysiske, tekniske og administrative kontroller vedrørende Iron Mountains aktiver til behandling af oplysninger (såsom computere, servere, lagringsenheder, kommunikationsnetværk, personlige computere, bærbare computere og perifere enheder).
Programmet til administration af aktivbeholdningen omfatter følgende:

- 3.1.1 Dokumenteret tildeling af ejerskab af aktiver til Iron Mountain-personale for at sikre passende klassificering af oplysninger, bestemmelse af adgangsbegrænsninger og gennemgang af adgangskontroller.
- 3.1.2 Sanering af aktiver forud for deres bortskaffelse i overensstemmelse med NIST 800-88.
- 3.1.3 Krav om ledelsesgodkendelse inden fjernelse af udstyr eller software, der ikke er tildelt en bestemt enkeltperson, fra Iron Mountains lokaler.

3.2 Kontroller. Iron Mountains kontroller omfatter følgende:

- 3.2.1 Driftsprocedurer og tekniske kontroller, der er beregnet til at beskytte dokumenter, computermedier, input-/output-/backup-data og systemdokumentation mod uautoriseret videregivelse, ændring og tilintetgørelse.
- 3.2.2 Procedurer for sikker bortskaffelse af elektroniske eller fysiske medier, der indeholder Kundens Personoplysninger.
- 3.2.3 En etableret proces til sporing af alle Kundens fysiske medier fra den indledende opbevaring hos Iron Mountain til og med permanent fjernelse eller tilintetgørelse.

4. SIKKERHEDSFORANSTALTNINGER FOR ARBEJDSSTYRKEN

4.1 Fortrolighed. Iron Mountain skal med rimelighed kræve, at alle Iron Mountain-medarbejdere, herunder vikar- og kontraktansatte, accepterer at opretholde fortroligheden af Kundens Personoplysninger og overholder Iron Mountains interne krav til informationssikkerhed og acceptabel brug.

4.2 Politik for Baggrundsundersøgelser. Iron Mountain har indført en politik for baggrundsundersøgelser og narkotikatest (kun USA) for sine medarbejdere. Iron Mountain vil fortsætte med at opretholde sådanne politikker under Aftalens løbetid. Kravene i politikken omfatter, men er ikke begrænset til, screening for narkotika (kun USA), bekræftelse af personales identitet, søgninger efter straffeattester, bekræftelse af ansættelse, søgninger i regerings-/terrorlister samt bekræftelse af uddannelse for visse medarbejdere, og kørekort- og overtrædelseshistorik for chaufførkandidater og eksisterende chauffører. Når der identificeres belastende oplysninger i et baggrundstjek, foretager Iron Mountain en individualiseret vurdering i overensstemmelse med gældende arbejdslovgivning og bedste praksis.

4.3 Arbejde med Underleverandører. Iron Mountain skal kræve, at enhver underleverandør, der udfører Tjenester i henhold til Aftalen, overholder lignende begrænsninger som dem, der er angivet i dette Afsnit, med hensyn til eventuelt underleverandørpersonale, der skal udføre Tjenester i henhold til Aftalen, der involverer Behandling af Kunders Personoplysninger.

4.4 Træning i Sikkerhedsbevidsthed. Iron Mountain skal mindst en gang om året gennemføre generel træning i sikkerhedsbevidsthed og specifik rollerelevant sikkerhedstræning for alle Iron Mountain-medarbejdere med adgang til Kunders Personoplysninger. Iron Mountain skal føre optegnelser, der viser navnene på sådanne Iron Mountain-medarbejdere, der deltager, og datoen for hver træning i sikkerhedsbevidsthed. Iron Mountain skal rutinemæssigt gennemgå og opdatere sit træningsprogram for sikkerhedsbevidsthed.

4.5 Fjernelse af Iron Mountain-personale. Iron Mountain opretholder en disciplinær proces, der anvendes på Iron Mountain-medarbejdere, der overtræder sikkerhedskravene heri.

4.6 Opsigelse af Adgang ved Opsigelse/Overflytning. Ved opsigelse eller overflytning til en rolle, der ikke kræver adgang til Kunders Personoplysninger, skal en Iron Mountain-medarbejders adgang til Kunders Personoplysninger straks tilbagekaldes.

5. FYSISK OG MILJØMÆSSIG SIKKERHED

5.1 Fysiske Sikkerhedskontroller. Iron Mountains faciliteter bruger fysiske kontroller, der med rimelighed begrænser adgangen til Kunders Personoplysninger, herunder, som Iron Mountain finder passende, adgangskontrolprotokoller, fysiske barrierer såsom låste faciliteter og områder, medarbejderadgangskort, besøgslogfiler, besøgsadgangskort, kortlæsere, videoovervågningskameraer og indbrudsalamer. Alle besøgende skal logge ind og ledsages til enhver tid.

5.2 Understøttende Forsyningstjenester. Iron Mountain skal anvende foranstaltninger, der er beregnet til at beskytte sine faciliteter, der indeholder Kunders Personoplysninger og systemer, mod strømsvigt, samt svigt af telekommunikation, vandforsyning, spildevand, varme, ventilation og aircondition, som relevant.

5.3 Sikkerhed af Transmissionssystemet. Iron Mountain skal anvende foranstaltninger, der er beregnet til at beskytte den fysiske sikkerhed af sin netværksinfrastruktur og telekommunikationssystemer mod opfangelse af transmissioner og skader.

5.4 Eksternt Udstyr. I tilfælde af, at Iron Mountain udliciterer funktioner, der kræver brug af eksternt udstyr til støtte for tjenester, skal eventuelt eksternt udstyr, der opbevarer Kunders Personoplysninger, beskyttes med samme grad af sikkerhed som det, der bruges til internt udstyr, der bruges til samme formål.

5.5 Fysisk Adgang til Databehandlingsaktiver. Iron Mountain skal opbevare optegnelser over Iron Mountain-medarbejdere, der er autoriserede til at have fysisk adgang til Iron Mountain-kontrollerede computermiljø(er), der bruges af Iron Mountain til at levere Tjenester i et år, og, efter Kundens anmodning herom i forbindelse med et Sikkerhedsbrud, og med forbehold for Iron Mountains sikkerhedspolitikker, give adgang til Kunden for at se revisionsbare optegnelser over sådanne Iron Mountain-medarbejdere.

5.6 Fysisk Adgang Begrænset. Iron Mountain skal begrænse fysisk adgang til Iron Mountain-kontrollerede faciliteter, der Behandler Kunders Personoplysninger, til de Iron Mountain-medarbejdere og autoriserede enkeltpersoner, der har et forretningsmæssigt behov for en sådan adgang. Iron Mountain skal have en godkendelsesproces for godkendelse og sporing af anmodninger om fysisk adgang til sådanne faciliteter.

5.7 Reparationer og Ændringer. Iron Mountain skal registrere alle sikkerhedsrelaterede reparationer og ændringer af alle fysiske komponenter, herunder hardware, vægge, døre og låse på sikre områder i faciliteter, hvor Kunders Personoplysninger opbevares.

5.8 Optegnelser. Føre en optegnelse over bevægelser af hardware og elektroniske medier og enhver person, der er ansvarlig herfor.

6. KOMMUNIKATION OG DRIFTSSTYRING AF INFORMATIONSBEHANDLING

6.1 Standarder for Enhedskonfiguration. Iron Mountain skal oprette, implementere og opretholde systemadministrationsprocedurer, der opfylder branchestandarder, herunder, uden begrænsning, systemhærdning, system- og enhedsrettelser (operativsystem og applikationer) og korrekt antivirusinstallation og -opdateringer.

6.2 Ændringskontrol af Informationsbehandlingssystemer. Iron Mountain skal indføre en intern, formel anmodningsproces for ændringsstyring for informationsbehandlings- og kommunikationsnetværkssystemer, og Iron Mountains ændringsanmodninger skal dokumenteres, testes og godkendes forud for implementering af eventuelle nye informationsbehandlings- eller netværkskommunikationsfunktioner, systemrettelser eller ændringer af eksisterende systemer.

6.3 Adskillelse af Pligter. Iron Mountain skal adskille opgaver og ansvarsområder, så ingen person har enekompetence til at ændre informationsbehandlingssystemer, der har adgang til Kunders Personoplysninger.

6.4 Adskillelse af Udviklings- og Produktionsmiljøer. Iron Mountains udviklings-, test- og produktionsmiljøer for informationsbehandlingssystemer skal være logisk eller fysisk adskilt.

6.5 Teknisk Arkitekturstyring. Iron Mountain skal oprette en konfigurationsstyringsproces for at definere, styre og kontrollere de systemkomponenter i informationsbehandling, der anvendes til at levere Tjenesterne og den tekniske infrastruktur for sådanne komponenter.

6.6 Registrering af Indtrængen. Iron Mountain skal løbende overvåge computersystemer og -processer for forsøg på eller faktisk indtrængen eller sikkerhedsovertrædelser, og underrette Kunden om eventuel uautoriseret adgang til Kundens Personoplysninger.

6.7 Netværkssikkerhed. Iron Mountain skal sikre, at følgende er indført:

6.7.1 Med hensyn til Iron Mountain-hostede miljø(er), der bruges til at levere Tjenesterne, vil systemer til påvisning af netværksindtrængen (network intrusion detection system, "IDS") og

sensorer til forebyggelse af indtrængen (intrusion prevention sensors, "IPS") advare om hændelser, der logges, med daglige rapporter udstedt til gennemgang (samlet benævnt "IDS/IPS"),

6.7.2 Med hensyn til Iron Mountain-hostede miljø(er), der bruges til at levere Tjenesterne, skal IDS/IPS opdateres mindst en gang om ugen, men så hurtigt som det med rimelighed er muligt, efter at opdateringerne er modtaget, og med omgående kørsel af de seneste trusselssignaturer eller -regler,

6.7.3 Højrisikoporte på kundeorienterede systemer er ikke tilgængelige fra internettet,

6.7.4 Iron Mountains netværksforbindelser logges og registreres i logfiler,

6.7.5 Installation af firewall(s), der er beregnet til at beskytte og inspicere al indgående og udgående netværkstjenestetrafik mellem definerede netværkspunkter,

6.7.6 Politikker for hærdning med henblik på at definere indgående og udgående netværksporte eller tjenestetrafik for alle Iron Mountain-ejede eller -styrede systemer, der dokumenteres og godkendes inden for informationssikkerhedsprogrammet,

6.7.7 Netværks- og diagnostiske porte, der er beskyttet korrekt, og

6.7.8 Politikker, procedurer og tekniske kontroller, der er beregnet til at forebygge, påvise og fjerne ondsindet kode eller kendte angreb på Iron Mountains informationssystemer.

6.8 Krypterede Autentificeringsoplysninger. Iron Mountain skal sikre, at autentificeringsoplysninger, der sendes via Iron Mountains netværksenheder, krypteres under transit.

6.9 Sikker Netværksadministration. Iron Mountain-netværk skal med rimelighed styres og kontrolleres for at beskytte mod kendte trusler og for at opretholde sikkerheden af alle Iron Mountain-styrede applikationer og data på netværket eller i transit over netværket. Der skal implementeres tekniske kontroller og sikre kommunikationsprotokoller for at forbyde ubegrænsede forbindelser til upålidelige netværk eller offentligt tilgængelige servere.

6.10 Virusbeskyttelse. Iron Mountain skal implementere og opretholde et antivirusstyringsprogram, herunder malwarebeskyttelse, opdaterede signaturfiler eller alternativ beskyttelse mod nye trusler, patches og virusdefinitioner, for Iron Mountain-administrerede servere og arbejdsstationer, der bruges til at huse eller få adgang til Kunders Personoplysninger.

6.11 Websted – Klientkryptering. Iron Mountain skal sikre, at Secure Sockets Layering (SSL) er aktiveret for hvert af sine websteder og indeholder et gyldigt SSL-certifikat, der kræver fortroligheds-, autentificerings- eller godkendelseskontroller.

6.12 Sikkerhedskopiering af Oplysninger. Iron Mountain skal oprette passende sikkerhedskopier af systemfiler. Derudover skal Iron Mountain udarbejde og opretholde en katastrofeberedskabsplan; se afsnittet "Gendannelse efter katastrofer" nedenfor for yderligere oplysninger.

6.13 Elektroniske Oplysninger i Transit. Iron Mountain skal anvende kryptering med en brancheankerkendt algoritme med en nøglelængde på mindst 128 bit for at beskytte Kunders Personoplysninger, der overføres via offentlige netværk, når de stammer fra en infrastruktur, der hostes af Iron Mountain.

6.14 Kryptografiske Kontroller. Iron Mountain skal følge en dokumenteret politik for brug af kryptografiske kontroller. Iron Mountains kryptografiske kontroller skal:

6.14.1 Være designet til med rimelighed at beskytte fortroligheden og integriteten af Kunders Personoplysninger, der behandles, overføres eller opbevares af Iron Mountain i eventuelle delte netværksmiljøer i overensstemmelse med vilkårene i Aftalen,

6.14.2 Anvendes, i Iron Mountain-hostede miljø(er), der bruges til at levere tjenester, på Kunders Personoplysninger under transit på tværs af eller til "upålidelige" netværk (dvs. netværk, som Iron Mountain ikke har juridisk kontrol over), herunder dem, der bruges til at sende data til Kundens virksomhedsnetværk fra Iron Mountains netværk, i hvert tilfælde med forbehold for Kundens samarbejde om administration af krypteringsnøgler, der er nødvendige for at dekryptere transmissioner, der modtages af Kunden, og

6.14.3 Omfatte dokumenterede administrationspraksisser for krypteringsnøgler for at understøtte sikkerheden af kryptografiske teknologier.

6.14.4 Omfatte kryptering af alle Kunders Personoplysninger på bærbare computere eller andre bærbare enheder.

6.15 Logningskrav. Iron Mountain skal sikre følgende:

6.15.1 At væsentlige sikkerheds- og systemhændelser logges og gennemgås,

6.15.2 At revisionslogfiler opbevares i mindst et år for systemer i Iron Mountain-hostede miljø(er), der bruges af Iron Mountain til at levere tjenester,

6.15.3 At systemrevisionslogfiler gennemgås for uregelmæssigheder, og

6.15.4 At log-faciliteter og systemoplysninger beskyttes på rimelig vis mod manipulation og uautoriseret adgang.

6.16 Synkronisering af Netværkstid. Iron Mountain skal synkronisere systemurene i alle informationsbehandlingssystemer ved hjælp af en fælles autoritativ tidskilde.

6.17 Adskillelse på Netværk. Iron Mountain skal på passende vis adskille relaterede grupper af informationstjenester, brugere og informationssystemer på netværk.

7. ADGANGSKONTROL

7.1 Politik for Adgangskontrol. Iron Mountain opretholder politikker for adgangskontrol med hensyn til aktiver til behandling af oplysninger, som Iron Mountain formelt godkender, udgiver og implementerer.

7.2 Godkendelse af Logisk Adgang. Iron Mountain skal indføre en godkendelsesproces for anmodninger om logisk adgang til Kunders Personoplysninger og anmodninger om adgang til Iron Mountain-systemer, der bruges i Tjenesterne.

7.3 Adgangskontrol og Adgangsgennemgang. Iron Mountain giver kun adgang til Kunders Personoplysninger til aktive Iron Mountain-medarbejdere, herunder vikar- og kontraktansatte, og aktive brugerkonti, der har brug for en sådan adgang for at kunne udføre deres jobfunktion. Al privilegeret adgang skal gennemgås og bekræftes for at være i overensstemmelse med den aktuelle jobrolle og skal dokumenteres mindst hvert kvartal.

7.4 Kontrol af Tredjepartsadgang. Inden eksterne parter får adgang til Iron Mountains informationssystemer, som tilgår Kunders Personoplysninger, skal Iron Mountain sikre, at der er indført passende kontroller.

7.5 Adgangskontrol for Operativsystemer. Iron Mountain skal kontrollere adgangen til operativsystemer (både software- og hardwarebaserede operativsystemer) ved at kræve en sikker loginproces, der entydigt identificerer den person, der får adgang til operativsystemet.

7.6 Mobile Databehandlingsenheder. Iron Mountain skal indføre en politik eller procedure, der er beregnet til at beskytte Iron Mountains mobile databehandlingsenheder mod uautoriseret adgang. Sådanne politikker eller procedurer skal omfatte fysisk beskyttelse, adgangskontrol og sikkerhedskontroller såsom kryptering, virusbeskyttelse og sikkerhedskopiering af enheder.

7.7 Isolering af Kundesystemer. Iron Mountain skal inden for sit/sine hostede miljø(er), der bruges til at levere Tjenesterne, logisk adskille Kunders Personoplysninger fra alle andre oplysninger.

7.8 Konti. Iron Mountain skal gøre følgende med hensyn til konti:

- 7.8.1 Kræve godkendelse af identiteten af hver Iron Mountain-medarbejder, der søger adgang til Iron Mountain-systemer, der Behandler Kunders Personoplysninger og forbyde brugen af delte brugerkonti eller brugerkonti med generiske brugeroplysninger (dvs. id'er), til at få adgang til Kunders Personoplysninger eller systemer.
- 7.8.2 Kræve, at alle brugerkonto-id'er, herunder privilegerede konti, knyttes direkte til en person (i modsætning til en stilling).
- 7.8.3 Hvis standardadministrationskonti ikke deaktiveres eller fjernes, skal der kræves brug af midlertidige adgangskoder, id'er eller lignende kontroller til adgang til standardadministrationskonti.
- 7.8.4 Kræve, at inaktive almindelige konti låses eller deaktiveres efter 90 dages inaktivitet.
- 7.8.5 Forbyde adgang til en konto efter flere mislykkede adgangsforsøg.
- 7.8.6 Kræve unikke identifikatorer og stærke adgangskoder, der som minimum omfatter følgende: skal indeholde mindst 8 tegn; skal ændres hver 90. dag; og skal have kompleksitetskrav.
- 7.8.7 Forbyde medarbejdere at dele eller nedskrive adgangskoder.

7.9 Kontroller for Ikke-overvågede systemer. Iron Mountain skal bruge en adgangskodebeskyttet pauseskærm til alle systemer, der efterlades uden opsyn og ikke har været aktive i 30 minutter.

8. INDKØB, UDVIKLING OG VEDLIGEHOLDELSE AF INFORMATIONSSYSTEMER

8.1 Systemudviklingssikkerhed. Iron Mountain skal sikre, at sikkerhed er en del af al udvikling og drift af informationssystemer, og skal udgive og overholde interne sikre kodningsmetoder baseret på sikkerhedsstandarder for applikationsudvikling.

8.2 Styring af Softwaresikkerhed. Iron Mountains informationssystemer (herunder operativsystemer, infrastruktur, forretningsapplikationer, tjenester og brugerudviklede applikationer) skal være designet til at være i overensstemmelse med informationssikkerhedsstandarder.

8.3 Netværksdiagrammer. Iron Mountain skal udvikle, dokumentere og opetholde fysiske og logiske diagrammer over netværksenheder og trafik.

8.4 Vurderinger af Applikationssårbarheder/Etisk Hacking. Iron Mountain skal mindst én gang om året udføre sårbarhedsvurderinger af applikationer i dets hostede miljø(er), der bruges til at levere tjenester, der Behandler Kunders Personoplysninger. Detaljerede resultater er fortrolige og ejendomsretligt beskyttede oplysninger tilhørende Iron Mountain og vil ikke blive tilvejebragt.

8.5 Test og Gennemgang af Ændringer. Iron Mountain skal gennemgå og teste ændringer i applikationer og operativsystemer inden implementering for at sikre, at der ikke er nogen negativ indvirkning på Kunders Personoplysninger eller systemer.

9. IT-KATASTROFEBEREDSKAB

Iron Mountain skal opretholde en katastrofeberedskabsplan, herunder kopiering af systemer og elektroniske data, der bruges til at understøtte Tjenesterne, til et backup-datacenter. Kopiering af systemer og elektroniske data omfatter ikke Kunders Personoplysninger, der fysisk opbevares i en Iron Mountain-facilitet. Iron Mountain vil opretholde en forretningskontinuitetsplan for gendannelse af kritiske forretningsfunktioner. Iron Mountain vil udføre katastrofegendannelsestest mindst én gang hver tolvte (12) måned.

10. EKSTERNE REVISIONER OG VURDERINGER

Iron Mountains sikkerhedsprotokoller er beregnet til at være i overensstemmelse med branchestandarder. Iron Mountain vil tilvejebringe eventuelle uafhængige tredjepartsrevisionsrapporter for Kunden, som Iron Mountain har bestilt (f.eks. PCI, ISO27001, SOC2, osv.), der er relevante for Tjenesterne i den region, hvor sådanne Tjenester leveres ("Revisionsrapport"). Iron Mountain vil tilvejebringe alle sådanne bestilte rapporter med henblik på at være kundeorienteret, uanset resultaterne af rapporten. Iron Mountain vil ikke være forpligtet til at tilvejebringe

interne revisionsresultater fra andre uafhængige vurderinger, der blev bestilt med henblik på at være fortrolige for Iron Mountain. Kunden og dennes eksterne revisorer vil få udleveret kopier af Revisionsrapporten efter anmodning herom. Eventuel Revisionsrapport eller andre resultater, der genereres gennem de test eller revisioner, der kræves i dette afsnit, vil blive betragtet som Iron Mountains Fortrolige Oplysninger. Kunden har ret til at udlevere en kopi af en sådan Revisionsrapport til kundens eventuelle relevante Kunder eller tilsynsmyndigheder med forbehold for fortrolighedsbestemmelser, der er lige så restriktive som dem heri. Iron Mountain skal efter Kundens anmodning herom skriftligt bekræfte, at der ikke har været nogen ændringer i de relevante politikker, procedurer og interne kontroller siden udarbejdelsen af en sådan Revisionsrapport, hvilket ikke må være mere end tre måneder fra afslutningen af rapporteringsperioden for Revisionsrapporten.

BILAG 3

Internationale Dataoverførsler

1. DEFINITIONER

”**EU-standardkontraktbestemmelser** fra 2021” betyder standardkontraktbestemmelserne for overførsel af Personoplysninger til tredjelande i medfør af den Generelle Forordning om Databeskyttelse, vedtaget af Europa-Kommissionen i henhold til Kommissionens Gennemførelsesafgørelse (EU) 2021/914, der er tilgængelig her[3] .

“**Det britiske Tillæg fra 2022**” betyder Skabelontillæg B.1.0 udstedt af Storbritanniens Information Commissioner’s Office og fremlagt for Parlamentet i overensstemmelse med s119A i Databeskyttelsesloven fra 2018 den 2. februar 2022, som den kan revideres i henhold til Afsnit 18 deri, der er tilgængelig her[4] .

“**EU-kunders Personoplysninger**” betyder behandlingen af Kunders Personoplysninger, for hvilke Databeskyttelseslovene i Den Europæiske Union eller i EU-medlemsstater eller Det Europæiske Økonomiske Samarbejdsområde fandt anvendelse forud for Iron Mountains behandling,

“**Beskyttet Område**” betyder:

i. for så vidt angår EU-kunders Personoplysninger, medlemsstaterne i Den Europæiske Union og Det Europæiske Økonomiske Samarbejdsområde og eventuelt land, territorium, sektor eller international organisation, for hvilke der er truffet en tilstrækkelighedafgørelse i henhold til Artikel 45 i den Generelle Forordning om Databeskyttelse,

ii. for så vidt angår britiske Kunders Personoplysninger, Storbritannien og eventuelt land, territorium, sektor eller international organisation, for hvilken en tilstrækkelighedsafgørelse i henhold til Storbritanniens tilstrækkelighedsforordninger er i kraft,

iii. i tilfælde af scweiziske Kunders Personoplysninger, eventuelt land, territorium, sektor eller international organisation, der anerkendes som tilstrækkelig i henhold til lovgivningen i Schweiz,

iv. i tilfælde af eventuelle andre Kunders Personoplysninger, der overføres ud af en retskreds, der tilbyder lignende beskyttelse som for Kunders Personoplysninger i EU, Storbritannien eller Schweiz, eventuelt land, territorium, sektor eller international organisation, der anerkendes som tilstrækkelig i henhold til lovgivningen i en sådan retskreds,

“**Standardkontraktbestemmelser**” betyder samlet EU-standardkontraktbestemmelserne fra 2021 og det britiske Tillæg fra 2022.

"**Schweiziske Kunders Personoplysninger**" betyder Behandlingen af Kunders Personoplysninger, for hvilke Databeskyttelseslove i Schweiz fandt anvendelse forud for Iron Mountains Behandling,

“**Britiske Kunders Personoplysninger**” betyder Behandlingen af Kunders Personoplysninger, for hvilke Databeskyttelseslove i Storbritannien fandt anvendelse forud for Iron Mountains behandling,

2. DIVERSE

2.1 Dette Bilag 3 omfatter følgende Dele: (i) Del A – Overførsel af EU-kunders Personoplysninger, (ii) Del B – Overførsel af schweiziske Kunders Personoplysninger, (iii) Del C – Overførsel af britiske Kunders Personoplysninger, som skal gælde som relevant for Iron Mountains overførsel af Kunders Personoplysninger i forbindelse med dets Tjenester.

2.2 Standardkontraktbestemmelserne gælder for Iron Mountain og dennes tilknyttede selskaber som "dataimportører" og for Kunden og dennes tilknyttede selskaber som "dataeksportører".

2.3 Underskriften på og dateringen af Aftalen udgør alle påkrævede underskrifter og datoer for Standardkontraktbestemmelserne.

2.4 I tilfælde af, at parterne overfører EU-, britiske eller schweiziske Kunders Personoplysninger uden for det Beskyttede område, og en relevant afgørelse fra Europa-Kommissionen eller anden gyldig tilstrækkelighedsmetode i henhold til gældende Databeskyttelseslovgivning, som Iron Mountain har påberåbt sig for dataoverførsel, anses for at være ugyldig, eller hvis en tilsynsmyndighed kræver, at overførsler af Personoplysninger, der foretages i medfør af en sådan afgørelse, suspenderes, skal parterne samarbejde og formidle anvendelsen af en alternativ overførselsmekanisme. Parterne er også enige om, at de passende sikkerhedsforanstaltninger, der anvendes til at formidle internationale overførsler i dette Bilag 3, ikke er eksklusive, og at parterne kan forfølge yderligere overførselsmekanismer, såsom EU-USA-lovgivningsrammerne for Databeskyttelse/Privatlivets fred.

DEL A – OVERFØRSLER AF EU-KUNDERS PERSONOPLYSNINGER

[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

Hvis og i det omfang Kunden eller dennes Tilknyttede selskaber overfører EU-kunders Personoplysninger uden for det Beskyttede Område til Iron Mountain eller dennes Tilknyttede selskaber i forbindelse med Iron Mountains Tjenester i henhold til Aftalen, finder denne Del A i Bilag 3 anvendelse, og Parterne er enige om følgende:

1. **Valg af Standardkontraktbestemmelser.** Teksten fra MODUL TO af EU-standardkontraktbestemmelserne fra 2021 skal gælde, hvor Kunden eller ethvert af dennes Tilknyttede selskaber er en Dataansvarlig, og Iron Mountain eller ethvert af dennes Tilknyttede selskaber er en Databehandler. Teksten fra MODUL TRE af EU-Standardkontraktbestemmelserne fra 2021 skal gælde, hvor Kunden eller ethvert af dennes Tilknyttede selskaber er en Databehandler, og Iron Mountain eller ethvert af dennes Tilknyttede selskaber er en Underdatabehandler. De relevante bestemmelser i EU-standardkontraktbestemmelserne fra 2021 er indarbejdet ved henvisning i denne Databehandlingsaftale og er en integreret del af denne Databehandlingsaftale. Ingen andre moduler eller eventuelle bestemmelser, der er markeret som valgfrie i EU-standardkontraktbestemmelserne fra 2021, finder anvendelse. De oplysninger, der kræves med henblik på Bilagene til EU-standardkontraktbestemmelserne fra 2021, er angivet i Bilag 1 – Beskrivelse af Behandlingen/Overførslen, Bilag 2 – Tekniske og organisatoriske Foranstaltninger, og afsnit 6.2 i Databehandlingsaftalen – Liste over Underdatabehandlere.

2. **Anvendelse af Underdatabehandlere.** Med henblik på bestemmelse 9 i EU-standardkontraktbestemmelserne fra 2021, finder mulighed 2 (Generel Skriftlig Tilladelse) for brug af Underdatabehandlere til udførelsen af Tjenesternes anvendelse. Kunden anerkender og accepterer, at Iron Mountain kan ansætte nye Underdatabehandlere gennem den mekanisme, der er aftalt i bestemmelse 6 i denne Databehandlingsaftale, og at fristen for indsendelse af anmodninger om ændringer til underdatabehandlere skal være femten (15) dage.

3. **Gældende lov og valg af værneting.** Med henblik på bestemmelse 17 i EU-standardkontraktbestemmelserne (Gældende Lov) fra 2021 finder mulighed 2 gældende lov anvendelse, og disse bestemmelser er underlagt lovgivningen i den EU-medlemsstat, hvor dataeksportøren er etableret, i det omfang det giver mulighed for tredjemandsløftet. Med henblik på bestemmelse 18 i EU-standardkontraktbestemmelserne fra 2021 (Valg af værneting) er disse domstolene i den EU-medlemsstat, hvor dataeksportøren er etableret.

4. **Certificering af sletning.** Med henblik på Bestemmelse 8.5 og 16(d) i EU-standardkontraktbestemmelserne fra 2021 skal Iron Mountain kun tilvejebringe en certificering af sletning af Personoplysninger for Kunden efter Kundens skriftlige anmodning herom.

5. **Brud på persondatasikkerheden.** Med henblik på bestemmelse 8.6(c) i EU-standardkontraktbestemmelserne fra 2021 skal brud på persondatasikkerheden håndteres i overensstemmelse med den mekanisme, der er aftalt i bestemmelse 7 i Databehandlingsaftalen.

6. **Revisioner.** Med henblik på bestemmelse 8.9 i EU-standardkontraktbestemmelserne fra 2021 skal revisioner af disse bestemmelser udføres i overensstemmelse med den revisionsmekanisme, der er aftalt i Aftalen.

7. **Klager.** Med henblik på bestemmelse 11 i EU-standardkontraktbestemmelserne fra 2021 skal Iron Mountain informere Kunden, hvis Iron Mountain modtager en klage fra en Registreret med hensyn til EU-kunders Personoplysninger, og skal kommunikere klagen til Kunden i overensstemmelse med den mekanisme, der er aftalt i Aftalen.

8. **Tilsynsmyndighed.** For EU-standardkontraktbestemmelserne fra 2022 fastlægges den relevante kompetente tilsynsmyndighed i overensstemmelse med bestemmelse 13 i EU-standardkontraktbestemmelserne.

DEL B – OVERFØRSEL AF SCHWEIZISKE KUNDERS PERSONOPLYSNINGER

Hvis og i det omfang Kunden eller dennes tilknyttede selskaber overfører schweiziske Kunders Personoplysninger uden for det Beskyttede Område til Iron Mountain eller dennes tilknyttede selskaber i forbindelse med Iron Mountains Tjenester i henhold til Aftalen, skal denne Del B i Bilag 3 finde anvendelse, og parterne er enige om følgende:

1. **Valg af Standardkontraktbestemmelser.** EU-standardkontraktbestemmelserne fra 2021 og relevante bestemmelser i Del A finder anvendelse, hvor Kunden eller ethvert af dennes Tilknyttede selskaber er en Dataansvarlig, og Iron Mountain eller ethvert af dennes Tilknyttede selskaber er en Databehandler, og/eller Kunden eller ethvert af dennes Tilknyttede selskaber er en Databehandler, og Iron Mountain eller ethvert af dennes Tilknyttede selskaber er en Underdatabehandler, med undtagelse af, at:

   a. den kompetente tilsynsmyndighed i henhold til Bestemmelse 13 i EU-standardkontraktbestemmelserne fra 2021 er den schweiziske Føderale Databeskyttelses- og Informationskommission;

b. den gældende lovgivning for kontraktmæssige krav i henhold til bestemmelse 17 i EU-standardkontraktbestemmelserne fra 2021 er schweizisk lovgivning, og værneting for søgsmål mellem parterne i henhold til bestemmelse 18 (b) er de schweiziske Domstole.

2. Henvisninger til EU's Generelle Forordning om Databeskyttelse i EU-standardkontraktbestemmelserne fra 2021 skal fortolkes som henvisninger til FADP.

3. Betegnelsen "medlemsstat" i EU-standardkontraktbestemmelserne fra 2021 skal ikke fortolkes på en sådan måde, at det udelukker Registrerede i Schweiz fra muligheden for at sagsøge for deres rettigheder på deres sædvanlige bopælssted (Schweiz) i overensstemmelse med Bestemmelse 18 (c) i EU-standardkontraktbestemmelserne fra 2021.

DEL C – OVERFØRSEL AF BRITISKE KUNDERS PERSONOPLYSNINGER

Hvis og i det omfang Kunden eller dennes Tilknyttede selskaber overfører britiske Kunders Personoplysninger uden for det Beskyttede Område til Iron Mountain eller dennes Tilknyttede selskaber i forbindelse med Iron Mountains Tjenester i henhold til Aftalen, skal denne Del C i Bilag 3 finde anvendelse, og Parterne er enige om følgende:

1. **Valg af Standardkontraktbestemmelser.** EU-standardkontraktbestemmelserne fra 2021, relevante bestemmelser i Del A, og det britiske Tillæg fra 2022 finder anvendelse, hvor Kunden eller ethvert af dennes Tilknyttede selskaber er en Dataansvarlig, og Iron Mountain eller ethvert af dennes Tilknyttede selskaber er en Databehandler, og/eller Kunden eller ethvert af dennes Tilknyttede selskaber er en Databehandler, og Iron Mountain eller ethvert af dennes Tilknyttede selskaber er en Underdatabehandler.

2. **Del 1: Tabel 1 - 3 i det britiske Tillæg fra 2022:** Oplysninger om Parterne - Tabel 1; Udvalgte SCC'er, Moduler og Udvalgte Bestemmelser, og Bilagsoplysninger, herunder Bilag 1A: Liste over Parter, Bilag 1B: Beskrivelse af Overdragelse og Bilag 1C: Tekniske og organisatoriske foranstaltninger til beskyttelse af datasikkerheden - Tabel 3, betragtes som fuldført med henvisning til dette Bilag 3, herunder Del A. Tabel 4 i det britiske Tillæg: Kunden og Iron Mountain anerkender og accepterer, at det britiske Tillæg kan opsiges af begge Parter.

3. **Del 2:** Obligatoriske Bestemmelser i det britiske Tillæg: Kunden og Iron Mountain anerkender og accepterer de Obligatoriske Bestemmelser i det britiske Tillæg.

4. **Tilsynsmyndighed.** Storbritanniens Information Commissioner's Office fungerer som kompetent tilsynsmyndighed.

DEL D – OVERFØRSLER AF ANDRE KUNDERS PERSONOPLYSNINGER

Hvis og i det omfang Kunden eller dennes tilknyttede selskaber overfører Kunders Personoplysninger, der ikke er omfattet af DEL A-C, til Iron Mountain eller dennes tilknyttede selskaber i forbindelse med Iron Mountains Tjenester i henhold til Aftalen, skal Del A i Bilag 3 finde anvendelse i det omfang, det er relevant og gældende i henhold til den gældende Databeskyttelseslovgivning. Ellers, i det omfang, at eventuelle erstatnings- eller yderligere passende sikkerhedsforanstaltninger eller overførselsmekanismer i henhold til Databeskyttelseslovgivningen er nødvendige for at overføre Kunders Personoplysninger til et land, der ikke yder et tilstrækkeligt beskyttelsesniveau for Personoplysninger ud fra dataeksportørens perspektiv, accepterer parterne at implementere disse så hurtigt som praktisk muligt og dokumentere sådanne krav til implementering i et bilag til denne Databehandlingsaftale.

BILAG 4

HIPAA – Forretningspartneraftale

Denne Forretningspartneraftale supplerer og ændrer alle aktuelle eller fremtidige Aftaler indgået mellem Iron Mountain og dennes tilknyttede selskaber og Kunden og dennes tilknyttede selskaber, i henhold til hvilke Iron Mountain eller dennes tilknyttede selskaber leverer visse Tjenester til Kunden eller dennes tilknyttede selskaber, hvor disse Tjenester kræver, at Forretningspartneren Anvender og/eller Videregiver Beskyttede Helbredsoplysninger på vegne af den Omfattede Enhed. Undtagen i det omfang, det er ændret i denne Forretningspartneraftale, skal alle vilkår og betingelser, der er angivet i Aftalen, forblive i fuld kraft og effekt og regulere de Tjenester, som Iron Mountain leverer til Kunden.

Iron Mountain og Kunden indgår denne Forretningspartneraftale for at begge parter kan opfylde deres respektive forpligtelser, efterhånden som de træder i kraft og er bindende for parterne i henhold til HIPPA-reglerne vedrørende privatlivets fred, sikkerhed og underretning om brud (HIPAA Privacy, Security, and Breach Notification Rules), sammen med eventuelle gennemførelsesforordninger, herunder dem, der implementeres som en del af Omnibus-reglen (samlet benævnt “HIPAA-reglerne”), i henhold til hvilke Kunden og dennes tilknyttede selskaber er en "Omfattet Enhed" eller "Forretningspartner", og Iron Mountain og dennes tilknyttede selskaber er en "Forretningspartner" til Kunden. I forbindelse med denne Aftale skal eventuelle henvisninger til Forretningspartner i det følgende betragtes som henvisninger til Iron Mountain eller dennes relevante tilknyttede selskab.

1. DEFINITIONER

Betegnelser, der anvendes, men som ikke på anden måde er defineret i denne Forretningspartneraftale, skal have samme betydning som er tilskrevet de pågældende betegnelser i HIPAA-reglerne eller i Aftalen, som relevant.

"**Regel for Underretning om Brud**" betyder Reglen for Underretning om Brud for Ubeskyttede Helbredsoplysninger i 45 CFR §164 Underdel D.

“**Forretningspartner**” betyder den ovenfor angivne Forretningspartnerenhed i det omfang, den modtager, opretholder eller overfører Beskyttede helbredsoplysninger ved levering af Tjenester til Kunder.

"**HIPAA**" betyder Health Insurance Portability and Accountability Act fra 1996.

"**HITECH-lov**" betyder de gældende bestemmelser i Health Information Technology for Economic and Clinical Health Act, som er indarbejdet i American Recovery and Reinvestment Act fra 2009, og herunder eventuelle gennemførelsesforordninger.

“**Privatlivsregel**” betyder Privatlivsstandarderne for Individuelt Identificerbare Helbredsoplysninger i 45 CFR §160 og §164, Underdele A og E.

“**Beskyttede Helbredsoplysninger**” skal have samme betydning som betegnelsen “beskyttede helbredsoplysninger” i 45 CFR §160.103 og skal være begrænset til de Beskyttede Helbredsoplysninger, der oprettes af Forretningspartnere på vegne af Kunden eller som modtages fra eller på vegne af Kunden i medfør af Aftalen.

“**Sikkerhedsregel**” betyder Sikkerhedsstandarderne for Beskyttelse af Elektronisk Beskyttede Helbredsoplysninger i 45 CFR §160 og §164, Underdele A og C.

2. FORRETNINGSPARTNERENS FORPLIGTELSER OG AKTIVITETER

2.1. Forretningspartneren indvilliger i ikke at Anvende eller Videregive Beskyttede Helbredsoplysninger på anden måde end som tilladt eller påkrævet af denne Forretningspartneraftale eller som påkrævet ved lov.

2.2. Forretningspartneren accepterer at anvende passende sikkerhedsforanstaltninger, og overholde, som relevant, Underdel C af 45 CFR §164 med hensyn til Elektronisk Beskyttede Helbredsoplysninger, for at forhindre Anvendelse eller Videregivelse af Beskyttede Helbredsoplysninger andet end som fastsat i denne Forretningspartneraftale eller Aftalen; Parterne anerkender og accepterer dog, at det er Kunden og ikke Forretningspartnerens ansvar at overholde kravene i 45 CFR §164.312 til at implementere krypterings- eller dekrypteringsmekanismer for elektronisk Beskyttede Helbredsoplysninger, der opretholdes på fysiske medier (f.eks. bånd), der opbevares af Kunden hos en Forretningspartner.

2.3. Forretningspartneren accepterer omgående at rapportere til Kunden eventuel Sikkerhedshændelse, Brud eller anden Anvendelse eller Videregivelse af Beskyttede Helbredsoplysninger, som den bliver opmærksom på, som ikke er tilladt eller påkrævet i henhold til denne Forretningspartneraftale eller Aftalen. I tilfælde af et Brud skal en sådan underretning ske i overensstemmelse med og som påkrævet af en forretningspartner i henhold til HIPAA-reglerne, herunder uden begrænsning i medfør af 45 CFR 164.410, men under ingen omstændigheder mere end tre (3) hverdage efter, at Forretningspartneren har gennemført sin interne undersøgelse og bekræftet, at et Brud er forekommet. Forretningspartneren vil yde rimelig assistance og samarbejde i undersøgelsen af ethvert sådant Brud og skal dokumentere de specifikke Deponeringer, der er blevet kompromitteret, identiteten af eventuel uautoriseret tredjepart,

der kan have fået adgang til eller modtaget Beskyttede Helbredsoplysninger, hvis kendt, og eventuelle handlinger, der er blevet truffet af Forretningspartnere for at afbøde indvirkningerne af et sådant Brud.

2.4. Forretningspartneren skal i overensstemmelse med 45 CFR 164.502(e)(1)(ii) og 164.308(b)(2), som relevant, sikre, at eventuel Forretningspartner, der er en Underleverandør, der opretter, modtager, vedligeholder eller overfører Beskyttede Helbredsoplysninger på vegne af Forretningspartneren med henblik på at hjælpe med at levere Tjenester i medfør af Aftalen, accepterer de samme begrænsninger, betingelser og krav, der gælder for Forretningspartneren med hensyn til sådanne Beskyttede Helbredsoplysninger gennem denne Forretningspartneraftale.

2.5. Hvis Forretningspartneren er i besiddelse af Beskyttede Helbredsoplysninger i et udpeget sæt optegnelser med hensyn til Enkeltpersoner, og hvis Kunden anmoder herom, accepterer Forretningspartneren at give Kunden adgang til sådanne Beskyttede Helbredsoplysninger ved at hente og tilvejebringe sådanne Beskyttede Helbredsoplysninger i overensstemmelse med vilkårene og betingelserne i Aftalen, så Kunden kan besvare en Person for at opfylde kravene i 45 CFR §164.524.

2.6. Forretningspartneren accepterer, at hvis en ændring af Beskyttede Helbredsoplysninger i et Udpeget Sæt Optegnelser i Forretningspartnerens besiddelse er påkrævet, og hvis Kunden beder Forretningspartneren om at hente sådanne Beskyttede Helbredsoplysninger i overensstemmelse med Aftalen, skal Forretningspartneren udføre en sådan tjeneste, så Kunden kan foretage eventuelle ændringer af sådanne Beskyttede Helbredsoplysninger, som enten Kunden eller en Enkeltperson måtte kræve i medfør af 45 CFR §164.526.

2.7. Forretningspartneren accepterer at dokumentere og stille de oplysninger til rådighed for Kunden, der er nødvendige for at give en redegørelse for Videregivelse af Beskyttede Helbredsoplysninger, forudsat at Kunden har givet Forretningspartneren tilstrækkelige oplysninger til at gøre det muligt for Forretningspartneren at bestemme, hvilke optegnelser eller data modtaget fra eller på vegne af Kunden af Forretningspartneren indeholder Beskyttede Helbredsoplysninger. Dokumentation for Videregivelser skal indeholde sådanne oplysninger, som ville være nødvendige for, at Kunden kan besvare en anmodning fra en Enkeltperson om en redegørelse for Videregivelser af Beskyttede Helbredsoplysninger i overensstemmelse med 45 CFR §164.528 eller andre bestemmelser i HIPAA-reglerne.

2.8. Medmindre andet udtrykkeligt er aftalt i Aftalen, skal Forretningspartneren straks underrette Kunden om eventuelle anmodninger fra Enkeltpersoner om indsigt i eller viden om eller berigtigelse af Beskyttede Helbredsoplysninger, uden at svare på sådanne anmodninger, og Kunden er ansvarlig for at modtage og svare på alle sådanne Individuelle anmodninger.

2.9. I det omfang Forretningspartneren skal opfylde en eller flere af Kundens forpligtelse(r) i henhold til Underdel E af 45 CFR §164, skal Forretningspartneren overholde kravene i Underdel E, der gælder for Kunden under udførelsen af sådan(ne) forpligtelse(r).

2.10. Forretningspartneren accepterer at stille sine interne praksisser, regnskaber og optegnelser til rådighed for Sekretæren med henblik på at fastslå overholdelse af HIPAA-reglerne.

3. TILLADTE ANVENDELSER OG VIDEREGIVELSER AF FORRETNINGSPARTNEREN

3.1. Forretningspartneren kan Anvende eller Videregive Beskyttede Helbredsoplysninger efter behov for at udføre de Tjenester, der er angivet i Aftalen.

3.2. Forretningspartneren kan Anvende eller Videregive Beskyttede Helbredsoplysninger som påkrævet ved lov.

3.3. Forretningspartneren indvilliger i at gøre rimelige bestræbelser på at begrænse Beskyttede Helbredsoplysninger til det mindste antal, der er nødvendigt for at opfylde det tilsigtede formål med Anvendelsen, Videregivelsen eller anmodningen.

3.4. Forretningspartneren må ikke Anvende eller Videregive Beskyttede Helbredsoplysninger på en måde, der ville overtræde Underdel E af 45 CFR §164, hvis dette gøres af Kunden.

3.5. Forretningspartneren kan Videregive Beskyttede Helbredsoplysninger med henblik på korrekt forvaltning af Forretningspartneren eller for at varetage Forretningspartnerens juridiske ansvarsområder, forudsat at Videregivelserne er påkrævet ved lov, eller Forretningspartneren indhenter rimelige forsikringer fra den person, til hvem oplysningerne videregives, om, at oplysningerne vil forblive fortrolige og kun vil blive anvendt eller videregivet som påkrævet ved lov eller til de formål, hvortil de blev videregivet til personen, og personen skal underrette Forretningspartneren om eventuelle tilfælde, hvor denne er bekendt med, at fortroligheden af oplysningerne er blevet kompromitteret.

4. KUNDENS FORPLIGTELSER

4.1. Kunden må ikke bede Forretningspartneren om at handle på en måde, der ikke ville være i overensstemmelse med HIPAA-reglerne.

4.2. Kunden skal underrette Forretningspartneren om eventuel(le) begrænsning(er) i sin meddelelse om Kundens privatlivspraksisser i overensstemmelse med 45 CFR §164.520, i det omfang en sådan begrænsning kan påvirke Forretningspartnerens Anvendelse eller Videregivelse af Beskyttede Helbredsoplysninger.

4.3. Kunden skal underrette Forretningspartneren om eventuelle ændringer i eller tilbagekaldelse af en enkeltpersons tilladelse til at Anvende eller Videregive deres Beskyttede Helbredsoplysninger, i det omfang sådanne ændringer kan påvirke Forretningspartnerens Anvendelse eller Videregivelse af Beskyttede Helbredsoplysninger.

4.4. Kunden skal skriftligt underrette Forretningspartneren om eventuel begrænsning i Anvendelsen eller Videregivelsen af Beskyttede Helbredsoplysninger, som Kunden har accepteret i overensstemmelse med 45 CFR §164.522, i det omfang en sådan begrænsning kan påvirke Forretningspartnerens Anvendelse eller Videregivelse af Beskyttede Helbredsoplysninger.

5. AFTALEPERIODE OG OPSIGELSE

5.1. Aftaleperioden for denne Forretningspartneraftale begynder pr. Ikrafttrædelsesdatoen og ophører automatisk ved den senere forekomst af (i) udløbet af Aftalen, eller (ii) når alle Beskyttede Helbredsoplysninger tilvejebragt af kunden for Forretningspartneren tilintetgøres eller returneres til Kunden.

5.2. Efter en parts kendskab til en væsentlig misligholdelse af Forretningspartneraftalen af den anden part, skal den ikke-misligholdende part give den misligholdende part mulighed for at afhjælpe misligholdelsen. Hvis den misligholdende part ikke afhjælper misligholdelsen inden for tredive (30) dage efter den misligholdende parts modtagelse af en skriftlig meddelelse fra den ikke-misligholdende part, der angiver de nærmere oplysninger om en sådan væsentlig misligholdelse, har den ikke-misligholdende part ret til at opsige denne Forretningspartneraftale og Aftalen i henhold til vilkårene i Aftalen, eller, hvis opsigelse ikke er mulig, skal den ikke-misligholdende part indberette problemet til Sekretæren eller eventuel anden kompetent myndighed.

5.3. Opsigelsens Virkning:

5.3.1.1. Undtagen som angivet i 5.3.2 nedenfor, ved opsigelse af denne Forretningspartneraftale uanset årsag, skal Forretningspartneren returnere eller tilintetgøre alle Beskyttede Helbredsoplysninger modtaget fra Kunden i overensstemmelse med Aftalen. Denne bestemmelse gælder for Beskyttede Helbredsoplysninger, der er i Forretningspartnerens underleverandører eller agenters besiddelse. Forretningspartneren må ikke opbevare kopier af Beskyttede Helbredsoplysninger.

5.3.1.2. I tilfælde af, at Forretningspartneren fastslår, at returnering eller tilintetgørelse af Beskyttede Helbredsoplysninger ikke er muligt, skal Forretningspartneren give Kunden meddelelse om de betingelser, der gør returnering eller tilintetgørelse umulig. Ved meddelelse til Kunden skal Forretningspartneren udvide beskyttelserne i denne Forretningspartneraftale til sådanne Beskyttede Helbredsoplysninger og begrænse yderligere Anvendelser og Videregivelser af sådanne Beskyttede Helbredsoplysninger til de formål, der gør returnering eller tilintetgørelse umulig, så længe Forretningspartneren opretholder sådanne Beskyttede Helbredsoplysninger i medfør af vilkårene i Aftalen.

6. DIVERSE

6.1. Skadesløsholdelse. Forretningspartneren accepterer at skadesløsholde Kunden for og mod eventuelle bøder eller sanktioner, der pålægges Kunden som følge af eventuel håndhævelsesprocedure, der indledes af Sekretæren eller eventuelt civilretligt søgsmål anlagt af en Offentlig Anklager mod Kunden, hvis retssag eller handling direkte eller udelukkende skyldes en handling eller undladelse af Forretningspartneren, som enten er en overtrædelse af HIPAA-reglerne eller et væsentligt brud på denne Forretningspartneraftale ("Krav"). Forretningspartneren er ikke forpligtet til at skadesløsholde Kunden for eventuel del af sådanne bøder eller sanktioner, der skyldes (i) Kundens overtrædelse af HIPAA-reglerne eller denne Forretningspartneraftale, eller (ii) Kundens uagtsomme eller forsætlige handlinger eller undladelser. Ovennævnte skadesløsholdelsesforpligtelse er udtrykkeligt betinget af, at Kunden tildeler Forretningspartneren retten, efter Forretningspartnerens valg og for dennes regning, og efter valg af egen advokat, til at kontrollere eller deltage i forsvaret af ethvert sådant Krav, dog forudsat, at i det omfang et sådant Krav er en del af en større procedure eller retssag, skal Forretningspartnerens ret til at kontrollere eller deltage begrænses til Kravet og ikke til den større procedure eller retssag. I tilfælde af, at Forretningspartneren udøver sin mulighed for at kontrollere forsvaret, skal (i) Forretningspartneren ikke indgå forlig om eventuelt krav, der kræver eventuel indrømmelse af skyld af Kunden uden dennes forudgående skriftlige samtykke, (ii) Kunden have ret til for egen regning at deltage i kravet eller søgsmålet, og (iii) Kunden efter rimelig anmodning herom samarbejde med Forretningspartneren. Ovenstående angiver Kundens eneste og eksklusive retsmiddel og

Forretningspartneres eneste erstatningsansvar for Kundens tab, skade, udgift eller erstatningsansvar for eventuelle Krav i forbindelse med denne Forretningspartneraftale.

6.2. Fogedforbud. Forretningspartneren anerkender, at eventuel uautoriseret Anvendelse eller Videregivelse af Beskyttede Helbredsoplysninger af Forretningspartneren kan forårsage uoprettelig skade for Kunden, for hvilken Kunden er berettiget til, hvis denne vælger det, at søge fogedforbud eller anden rimelig afhjælpning.

6.3. Forskriftsmæssige Henvisninger. En henvisning i denne Forretningspartneraftale til et afsnit i HIPAA-reglerne betyder det pågældende afsnit i HIPAA, Privatlivsreglen, Sikkerhedsreglen, HITECH-loven eller de endelige Omnibus-regler som ændret og i kraft, og for hvilke overholdelse er påkrævet.

6.4. Ændring. Parterne accepterer at forhandle i god tro om eventuelle ændringer til denne Forretningspartneraftale, der kan være påkrævede fra tid til anden som nødvendigt for, at Kunden eller Forretningspartneren kan overholde kravene i HIPAA-reglerne. Hvis parterne ikke kan nå til enighed om vilkårene for en sådan ændring inden for tres (60) dage efter datoen for modtagelse af en sådan skriftlig anmodning fra kunden til Forretningspartneren, skal begge parter have ret til at opsige denne Forretningspartneraftale og Aftalen ved at give mindst tredive (30) dages skriftligt varsel til den anden part.

6.5. Ingen Begunstiget Tredjepart. Intet udtrykt eller underforstået i denne Forretningspartneraftale er beregnet til at overdrage, og intet heri skal overdrage, til nogen anden person end Kunden, Forretningspartneren og deres respektive efterfølgere eller erhververe, eventuelle rettigheder, retsmidler, forpligtelser eller erstatningsansvar overhovedet.

6.6. Uafhængig Kontrahent. Forretningspartneren, herunder dennes direktører, ledere, medarbejdere og agenter, er en uafhængig kontrahent og ikke en agent (som defineret i Føderal sædvaneret) for Kunden eller et medlem af dennes arbejdsstyrke. Uden at begrænse det generelle i det foregående har Kunden ingen ret til at kontrollere, dirigere eller på anden måde påvirke Forretningspartnerens adfærd under udførelsen af tjenesterne, bortset fra gennem håndhævelsen af denne Forretningspartneraftale eller Aftalen, eller den gensidige ændring af disse.

6.7. Præcedens; Hele Aftalen. Enhver tvetydighed i denne Forretningspartneraftale skal løses for at give parterne mulighed for at overholde HIPAA-reglerne. Denne Forretningspartneraftale udgør hele aftalen mellem parterne med hensyn til genstanden herfor og erstatter alle tidligere meddelelser, erklæringer, aftaler og forståelser vedrørende HIPAA-reglerne, herunder alle tidligere forretningspartneraftaler mellem parterne.