Databehandlingstillæg

Opdateret 28. marts 2025

Denne databehandlingsaftale ("databehandlingstillæg") er inkorporeret i og udgør en del af Limes servicebetingelser ("aftale"), som er indgået mellem entiteten Lime og kunden, der er identificeret i aftalen. Formålet med dette databehandlingstillæg er at definere parternes aftale vedrørende behandling af personoplysninger i overensstemmelse med kravene i den gældende databeskyttelseslovgivning. Alle begreber, som ikke er defineret heri, har den betydning, der er angivet i henholdsvis aftalen eller databehandlingstillægget.

I forbindelse med levering af tjenester til kunden i henhold til aftalen kan Lime behandle personoplysninger på vegne af kunden, og parterne er enige om at overholde følgende regler for samtlige personoplysninger. Lime vil i det efterfølgende blive omtalt som "behandler" og kunden som "ansvarlig", alternativt "parten" eller i forening "parterne".

Databehandlingstillægget har forrang i forhold til modstridende eller uforenelige bestemmelser i servicebetingelserne angående behandlingen af personoplysninger.

1 Definitioner

Udover de begreber, der er defineret i databehandlingstillæggets brødtekst, har følgende begreber den betydning, der fremgår nedenfor.

1.1 **Personoplysninger**: Enhver form for information om en identificeret eller identificerbar fysisk person ("den registrerede").

1.2 **Den registrerede:** En identificeret eller identificerbar fysisk person. Ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, navnlig ved henvisning til en identifikator eller til et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.

1.3 **Behandling (af personoplysninger)**: Enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, opbevaring, tilpasning eller ændring, søgning, konsultation, brug, overførsel, formidling eller anden form for overladelse, indsamling eller samkøring, blokering, sletning eller tilintetgørelse.

1.4 **Den ansvarlige**: En fysisk eller juridisk person, en myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der foretages behandling af personoplysninger.

1.5 **Behandler**: En fysisk eller juridisk person, en myndighed, en institution eller et andet organ, der behandler personoplysninger på den ansvarliges vegne.

1.6 **Gældende databeskyttelseslovgivning**: Den generelle forordning om databeskyttelse – dvs. Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF – samt den nationale lovgivning, der gennemfører eller supplerer databeskyttelsesforordningen og gælder for behandlingen af personoplysninger i henhold til denne aftale.

1.7 **Følsomme personoplysninger**: Race eller etnisk oprindelse, politisk, filosofisk eller religiøs overbevisning, medlemskab i fagforening, mistanke om, anklage for eller dom for kriminalitet, helbred, genetiske data, biometriske data til unik identificering af en person, vedkommendes sexliv eller seksuelle orientering samt andre følsomme oplysninger.

1.8 **Tredjeland**: Et land uden for EU/EØS.

2 Behandling af personoplysninger:

2.1 Behandleren skal udelukkende behandle alle personoplysninger i overensstemmelse med dette databehandlingstillæg samt i overensstemmelse med dokumenterede

instruktioner, der udstedes af en ansvarlig, medmindre behandleren i henhold til EU-lovgivningen (herunder den nationale lovgivning i EU's medlemsstater) skal behandle personoplysningerne.

2.2 Den ansvarlige skal udstede skriftlige instruktioner til behandleren om, hvordan behandlingen skal udføres.

2.3 Behandleren skal behandle personoplysningerne i hele den periode, der fremgår af aftalen, og i en begrænset periode derefter (se afsnit 11). **Bilag A** indeholder oplysninger om behandling af personoplysninger, herunder i) kategorier af personoplysninger, ii) kategorier af registrerede, iii) behandlingens karakter og formål, iv) hvor behandlingen sker og v) behandlingens varighed.

2.4 Dette databehandlingstillæg omfatter ikke personoplysninger, der er blevet overført fra tjenesten til tredjepartssoftware (som defineret i aftalen), idet din aftale med den pågældende udbyder af tredjepartssoftwaren træder i kraft i stedet.

3 Behandlerens forpligtelser

3.1 Behandleren behandler kun data i overensstemmelse med dette databehandlingstillæg og instruktionerne. For klarheds skyld kan behandleren behandle personoplysninger, hvis sådan behandling er påkrævet i henhold til relevant lovgivning, der finder anvendelse på behandleren. Behandleren skal informere den ansvarlige om sådanne krav, medmindre behandleren ikke må offentliggøre sådanne oplysninger grundet en vigtig samfundsinteresse. Når behandleren behandler personoplysninger i henhold til dette databehandlingstillæg, skal denne overholde gældende databeskyttelseslovgivning.

3.2 Behandleren skal sikre, at alle fysiske personer, der arbejder under dennes ledelse, og som har adgang til personoplysninger, overholder denne aftale og den ansvarliges instruktioner.

3.3 Behandleren og dennes medarbejdere skal under behandlingen overholde tavshedspligt og fortrolighed, for så vidt angår alle fortrolige oplysninger, de har adgang til i forbindelse med dette databehandlingstillæg. Denne bestemmelse finder også anvendelse efter databehandlingstillæggets udløb.

3.4 Behandleren skal træffe de sikkerhedsforanstaltninger, der er påkrævet i henhold til artikel 32 i databeskyttelsesforordningen.

3.5 Behandleren skal i videst muligt omfang hjælpe den ansvarlige med at opfylde dennes forpligtelser over for de registrerede under hensyntagen til tekniske og organisatoriske foranstaltninger.

3.6 Behandleren skal på den ansvarliges anmodning bistå den ansvarlige med at sikre, at forpligtelserne i henhold til artikel 32-36 i databeskyttelsesforordningen opfyldes, idet der tages højde for behandlingstypen og de for behandleren tilgængelige oplysninger.

3.7 Behandleren skal omgående underrette den ansvarlige, hvis behandleren mener, at den ansvarliges instruktioner er uklare eller på anden måde strider imod den gældende databeskyttelseslovgivning. Behandleren må ikke udføre en sådan instruktion, før de ansvarlige har bekræftet, at instruktionen er lovlig.

4 Den ansvarliges forpligtelser

4.1 Når den ansvarlige anvender tjenesterne, som behandleren stiller til rådighed i overensstemmelse med aftalen, skal den ansvarlige behandle personoplysninger i overensstemmelse med gældende databeskyttelseslovgivning. Den ansvarlige skal sikre, at der til enhver tid er juridisk grundlag for behandlingen og skal formulere korrekte instruktioner, således at behandleren (og dennes underbehandlere) kan opfylde krav og forpligtelser i henhold til dette databehandlingstillæg og – hvis det er relevant –aftalen.

4.2 Den ansvarlige kan behandle og videregive personoplysninger, der omfattes af aftalen, til behandleren (herunder til eventuelle underbehandlere, som behandleren måtte have).

4.3 Den ansvarlige er alene ansvarlig for personoplysningernes nøjagtighed, integritet, indhold, pålidelighed og lovlighed, hvad angår de personoplysninger, der videregives til behandleren. Behandleren påtager sig intet ansvar for konsekvenserne af, at de personoplysninger, denne modtager, viser sig at være urigtige.

4.4 Den ansvarlige har opfyldt sine forpligtelser om at stille obligatoriske oplysninger til rådighed for de registrerede om personoplysninger, overførsel af personoplysninger til behandleren og om behandlerens behandling af personoplysninger i overensstemmelse med gældende databeskyttelseslovgivning.

4.5 Når den ansvarlige anvender de tjenester, der i overensstemmelse med aftalen stilles til rådighed af behandleren, må den ansvarlige ikke videregive følsomme personoplysninger til behandleren, medmindre dette udtrykkeligt er aftalt og specificeret skriftligt mellem parterne.

4.6 Den ansvarlige skal omgående underrette behandleren om ændringer i forhold til den ansvarliges kontaktperson eller øvrige kontaktoplysninger.

5 Sikkerhedsforanstaltninger

Behandleren skal implementere tilstrækkelige organisatoriske og tekniske sikkerhedsforanstaltninger for at beskytte personoplysningerne i henhold til den gældende databeskyttelseslovgivning (herunder artikel 32 i GDPR) med det formål at værne om personoplysningernes fortrolighed, integritet og adgang til personoplysningerne som beskrevet i nærmere detaljer i **Bilag B**. Behandleren skal løbende gennemgå sine organisatoriske og tekniske sikkerhedsforanstaltninger og opdatere dem ved behov i henhold til den gældende databeskyttelseslovgivning.

6 Revision og inspektion

6.1 Behandleren skal give den ansvarlige adgang til alle oplysninger, der kræves for at vise, at de forpligtelser, der fremgår af databeskyttelsesforordningens artikel 28, er opfyldt, og for at muliggøre og bidrage til revisioner, herunder inspektioner, der udføres af den ansvarlige eller en tredjepart, der er udpeget af den ansvarlige.

6.2 Den ansvarlige kan vurdere behandlerens overholdelse af databehandlingstillægget maksimalt en (1) gang om året. Hvis det i henhold til gældende databeskyttelseslovgivning måtte være påkrævet, kan den ansvarlige kræve hyppigere vurderinger.

6.3 Den ansvarlige skal, for at anmode om revision, forelægge en detaljeret revisionsplan til behandleren mindst fire uger forud for den foreslåede revision. Planen skal omfatte revisionens omfang, varighed og startdato. Hvis revisionen udføres af en tredjepart, skal dette generelt ske i henhold til aftale mellem den ansvarlige og behandleren. Hvis behandlingen sker i et miljø med personoplysninger fra andre ansvarlige eller lignende, kan behandleren efter eget skøn af sikkerhedsmæssige årsager beslutte, at revisionen skal udføres af et generelt velanset revisionsselskab, der vælges af behandleren.

6.4 Hvis den anmodede revision allerede er udført og beskrevet i en rapport af en tredjepartsrevisor i overensstemmelse med ISAE 3402, ISO eller lignende i løbet af de seneste 12 måneder, og hvis behandleren bekræfter, at de reviderede kontroller ikke har ændret sig væsentligt, skal den ansvarlige acceptere disse resultater i stedet for at anmode om revision af de kontroller, rapporten omfatter.

6.5 Revisionen skal udføres i løbet af facilitetens normale kontortid og i overensstemmelse med behandlerens politikker og må ikke medføre urimelig afbrydelse af behandlerens drift.

6.6 Den ansvarlige er ansvarlig for alle omkostninger, der opstår i forbindelse med en revision, som den ansvarlige anmoder om og for behandlerens assistance i denne henseende.

6.7 Behandleren skal til enhver tid give tilsynsmyndigheden eller en anden myndighed, der er juridisk berettet dertil, mulighed for at føre tilsyn i overensstemmelse med gældende lovgivning. Behandleren og dennes ansatte skal på anmodning derom samarbejde med tilsynsmyndigheden i dennes udførelse af sine forpligtelser.

7 Støtte til den ansvarlige

7.1 Idet der i videst muligt omfang tages højde for behandlingens art, skal behandleren assistere den ansvarlige med tilstrækkelige tekniske og organisatoriske foranstaltninger, således at den ansvarlige kan opfylde sin forpligtelse om at reagere på anmodninger fra registrerede, der ønsker at udøve deres rettigheder.

7.2 Behandleren skal i det omfang, det er praktisk muligt og lovligt, underrette den ansvarlige om i) anmodninger modtaget fra registrerede om at videregive personoplysninger (med undtagelse af, hvor den ansvarlige har bemyndiget behandleren til at reagere på sådanne anmodninger) og ii) anmodninger fra myndigheder om at videregive personoplysninger (med undtagelse af, hvor den ansvarlige har autoriseret behandleren til at reagere på sådanne anmodninger).

7.3 Grundet en efterforsknings fortrolighed i forbindelse med retshåndhævende myndigheders efterforskning kan behandleren dog være forhindret i at underrette den ansvarlige. Medmindre behandleren er forpligtet i henhold til loven eller på anmodning derom understøttet af en retsafgørelse, ransagningskendelse eller lignende, må behandleren ikke videregive oplysninger om dette databehandlingstillæg til myndighederne, hvad angår personoplysningerne.

7.4 Idet der tages højde for behandlingens art og arten af de oplysninger, der er tilgængelige for behandleren, skal behandleren assistere den ansvarlige med at sikre, at forpligtelserne i henhold til den gældende databeskyttelseslovgivning opfyldes, herunder (såfremt det er relevant) den ansvarliges forpligtelse til i) at træffe tilstrækkelige tekniske og organisatoriske foranstaltninger, ii) anmelde brud på datasikkerheden til tilsynsmyndigheden, iii) underrette registrerede om brud på datasikkerheden, iv) udføre konsekvensanalyser angående databeskyttelsen og v) rådføre sig med tilsynsmyndigheden forud for behandlingen.

7.5 Behandleren skal skriftligt og uden ugrundet ophold underrette den ansvarlige, hvis behandleren bliver bekendt med et brud på datasikkerheden. Behandleren skal give den ansvarlige en beskrivelse af bruddet på datasikkerheden. Hvis behandleren ikke har alle relevante oplysninger angående bruddet på datasikkerheden, når den indledningsvist underretter den ansvarlige om, at der er sket et brud på datasikkerheden, skal behandleren stille sådanne oplysninger til rådighed i videre underretninger.

7.6 Behandleren kan opkræve betaling fra den ansvarlige for udført arbejde og rimelige omkostninger, der opstår i forbindelse med den ansvarliges støtte som beskrevet ovenfor og i overensstemmelse med gældende databeskyttelseslovgivning uagtet opfyldelse af forpligtelserne i henhold til afsnit 7.5 herover (forudsat at bruddet på datasikkerheden ikke kan tilskrives den ansvarlige). Dette omfatter f.eks. arbejde og omkostninger, der opstår som følge af, at registrerede har anmodet om uddrag fra registeret angående behandling af deres personoplysninger, sletning af personoplysninger, overførsel af personoplysninger (portabilitet) eller videregivelse af obligatoriske oplysninger til de registrerede.

8 Brug af underbehandlere

8.1 Som en del af den service, der i overensstemmelse med aftalen leveres af behandleren til den ansvarlige, får behandleren hermed generel skriftlig, forudgående autorisation

til at anvende underbehandlere til behandling af personoplysninger på vegne af den ansvarlige.

8.2 Behandleren skal sikre, at alle underbehandlere er bundet af skriftlige aftaler, som sikrer, at underbehandlere er underlagt forpligtelser angående behandling af personoplysninger, der som minimum svarer til de forpligtelser, der fremgår af dette databehandlingstillæg.

8.3 Hvis en underbehandler ikke opfylder sine forpligtelser i overensstemmelse med gældende databeskyttelseslovgivning, er behandleren fuldt ud ansvarlig i forhold til den ansvarlige for at opfylde underbehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder i henhold til databeskyttelsesforordningen, og især de rettigheder, der er omfattet af databeskyttelsesforordningens artikel 79 og 82, i forhold til den ansvarlige og behandleren, herunder underbehandleren.

8.4 Behandleren skal stille en opdateret og aktuel liste over underbehandlere til rådighed, og disse skal anvendes til at udføre de tjenester, som behandleren yder i henhold til aftalen. Listen skal indeholde oplysninger om underbehandlernes identitet, kontaktpersonen for den underbehandler, hvor personoplysningerne behandles, samt en generel beskrivelse af den type tjeneste, hver underbehandler yder. Listen over underbehandlere findes på Limes websted https://www.lime-technologies.com/subprocessors/. Den ansvarlige godkender ved underskrift af databehandlingstillægget behandlerens brug af underbehandlerne på listen.

8.5 Behandleren skal underrette den ansvarlige om eventuelle planer om at antage en ny underbehandler eller om at udskifte en eksisterende underbehandler. Den ansvarlige kan gøre indsigelse mod sådanne ændringer. Såfremt der ikke inden for ti (10) dage fra modtagelse af meddelelse derom gøres indsigelse, antages det, at den ansvarlige ikke har gjort indsigelser.

8.6 Behandleren kan træffe tilstrækkelige korrigerende foranstaltninger, hvis der gøres indsigelse. Hvis den ansvarlige opdager, at der ikke er truffet korrigerende foranstaltninger, eller at indsigelsen ikke er afhjulpet inden tredive (30) dage, kan parterne opsige databehandlingstillægget, og hvis databehandlingstillægget er nødvendigt for, at behandleren kan opfylde sine forpligtelser i henhold til aftalen, opsige aftalen ved skriftlig meddelelse derom.

9 Overførsel af personoplysninger til tredjelande

9.1 Behandleren og dennes underbehandlere kan overføre personoplysninger til tredjelande i det omfang, det er nødvendigt for dermed at udføre de tjenester, som behandleren yder i overensstemmelse med aftalen, og forudsat at overførslen sker i overensstemmelse med databeskyttelsesforordningens kapitel V.

9.2 Når der anvendes standardkontraktbestemmelser (Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021 om

standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679, eller beslutninger og standardkontraktbestemmelser, der erstatter disse bestemmelser), kan behandleren eller underbehandleren efter eget skøn beslutte, hvilken version og hvilke moduler af standardkontraktbestemmelserne der i det enkelte tilfælde finder anvendelse.

9.3 I overensstemmelse med de krav, der fremgår af gældende databeskyttelseslovgivning og gælder for overførsler baseret på, at der træffes tilstrækkelige sikkerhedsforanstaltninger, skal behandleren i hvert enkelt tilfælde foretage en risikovurdering for at sikre, at lovgivningen i det pågældende tredjeland ikke påvirker effektiviteten af de fornødne garantier negativt, og for at sikre, at effektive retsmidler for registrerede er tilgængelige. Behandleren skal om nødvendigt identificere og gennemføre supplerende foranstaltninger såsom tekniske, organisatoriske eller kontraktlige foranstaltninger for at sikre, at beskyttelsesniveauet i det pågældende tredjeland i væsentlig grad svarer til beskyttelsesniveauet i EU/EØS.

9.4 På den ansvarliges rimelige anmodning derom skal behandleren indberette oplysningerne, som risikovurderingen baseres på. Den ansvarlige kan gøre skriftlig indsigelse mod behandlerens risikovurderinger, hvis disse ændres, efter databehandlingstillægget træder i kraft, og den ansvarlige skønner, at de nye risikovurderinger ikke opfylder kravene for den ansvarliges behandling af personoplysninger i overensstemmelse med gældende databeskyttelseslovgivning. Den ansvarlige kan anmode om, at behandleren træffer tilstrækkelige korrigerende foranstaltninger. Hvis parterne ikke er enige om risikovurderingen og/eller de tilstrækkelige korrigerende foranstaltninger inden for tredive (30) dage, kan parterne opsige databehandlingstillægget, og hvis databehandlingstillægget er nødvendig for, at den ansvarlige opfylder sine forpligtelser i henhold til aftalen, kan aftalen opsiges ved skriftlig meddelelse derom.

9.5 Hvis domstolen, kommissionen eller en anden kompetent EU-institution eller national domstol eller myndighed finder, at overførselsmekanismen, der anvendes til overførsel til et tredjeland, er ugyldig eller ulovlig, skal behandleren sikre, at al behandling af personoplysninger i et tredjeland baseres på en anden (gyldig) overførselsmekanisme.

10 Databehandlingstillæggets varighed

10.1 Dette databehandlingstillæg gælder, så længe behandleren behandler personoplysninger på vegne af den ansvarlige i overensstemmelse med aftalen.

10.2 Databehandlingstillægget ophører automatisk med at gælde, når aftalen opsiges.

11 Foranstaltninger ved databehandlingstillæggets opsigelse

11.1 Afhængigt af hvad den ansvarlige skriftligt instruerer behandleren om, skal behandleren ved opsigelse af dette databehandlingstillæg slette eller returnere alle

personoplysninger, der behandles på vegne af den ansvarlige i overensstemmelse med databehandlingstillægget, samt alle kopier af oplysningerne, medmindre lagring af personoplysningerne er påkrævet i overensstemmelse med gældende databeskyttelseslovgivning.

11.2 Hvis den ansvarlige ikke har givet instruktioner eller reageret på behandlerens anmodning om instruktioner tredive (30) dage efter databehandlingstillæggets opsigelse, skal behandleren returnere alle personoplysninger til den ansvarlige og derefter slette alle personoplysninger.

12 Fortrolighed

Behandleren må ikke under databehandlingstillæggets varighed eller derefter videregive information om behandlingen af personoplysninger i overensstemmelse med dette databehandlingstillæg til en tredjepart eller på anden vis afsløre information, som denne har modtaget som følge af dette databehandlingstillæg. Forpligtelsen om fortrolighed gælder ikke informationer, som behandleren er forpligtet til at videregive til myndighederne. I tillæg til dette afsnit (12) gælder endvidere aftalens forpligtelser om fortrolighed.

13 Ændringer og tilføjelser

13.1 Dette databehandlingstillæg kan ændres som følge af ændringer i lovgivningen, sikkerhedskrav eller øvrige praktiske omstændigheder. I tilfælde af en ændring, der påvirker behandlingen af personoplysninger i overensstemmelse med databehandlingstillægget, skal den anden part modtage meddelelse derom via en e-mail, der sendes til dennes ovenfor anførte kontaktperson. Sådan meddelelse om en ændring anses for at være accepteret af den anden part, forudsat at den anden part ikke har gjort rimelige, skriftlige indsigelser inden for tredive (30) dage fra datoen for meddelelsen.

13.2 Hvis en kompetent domstol, myndighed eller voldgiftsinstans finder, at en bestemmelse i dette databehandlingstillæg ikke kan håndhæves eller er ugyldig, påvirker dette ikke de øvrige bestemmelser. I så henseende skal parterne udskifte den ikke-håndhævelige eller ugyldige bestemmelse med en lovlig bestemmelse, der afspejler den ikke-håndhævelige eller ugyldige bestemmelses formål.

14 Ansvar

14.1 Ved skadeserstatning i forbindelse med behandling, der ifølge en endelig afgørelse eller overenskomst skal betales til den registrerede grundet misligholdelse af en bestemmelse i dette databehandlingstillæg, instruktioner og/eller en gældende bestemmelse i gældende databeskyttelseslovgivning, finder databeskyttelsesforordningens artikel 82 anvendelse.

14.2 Administrative bøder i henhold til databeskyttelsesforordningens artikel 83 eller kapitel 12, paragraf 41 i lov nr. 502 af 23. maj 2018 ("databeskyttelsesloven") med tillægsbestemmelserne til EU's databeskyttelsesforordning skal betales af den part, der er blevet pålagt den administrative bøde.

14.3 De aftalemæssige ansvarsbegrænsninger, der er angivet i aftalen, gælder også for dette databehandlingstillæg, uden at dette dog indskrænker forpligtelserne i henhold til 14.1 og 14.2.

14.4 Hvis en part bliver bekendt med et forhold, der kan påføre den anden part skader, skal parten omgående underrette den anden part om et sådant forhold og aktivt samarbejde med den anden part for at forebygge og minimere en sådan skade.

15 Valg af lov og værneting

15.1 Dette databehandlingstillæg skal fortolkes og finde anvendelse i overensstemmelse med aftalens bestemmelser om valg af lov.

15.2 Enhver tvist, der måtte opstå i forbindelse med dette databehandlingstillæg, skal ultimativt afgøres i overensstemmelse med aftalens bestemmelser om tvistafgørelse.

Bilag A – Instruktioner for behandling af personoplysninger

Kategorier af personoplysninger	Den ansvarlige kan i henhold til aftalen indlæse personoplysninger på tjenesten, som behandleren stiller til rådighed. Indlæsning af personoplysninger i tjenesten er udelukkende op til den ansvarlige og kan f.eks. omfatte følgende kategorier af personoplysninger: - Navn - Telefonnummer - E-mailadresse - Kundehistorik
Kategorier af registrerede	Den ansvarlige kan i henhold til aftalen indlæse personoplysninger på tjenesten, som behandleren stiller til rådighed. Indlæsning af personoplysninger i tjenesten er udelukkende op til den ansvarlige og kan f.eks. omfatte personoplysninger om følgende kategorier af registrerede: - Den ansvarliges ansatte, kunder, leverandører og konsulenter - Den ansvarliges potentielle kunders ansatte
Behandlingens karakter og formål	Behandlingen af personoplysninger for at stille behandlerens tjenester til rådighed i overensstemmelse med aftalen og den ansvarliges instruktioner
Behandlingssted	- Behandleren behandler personoplysningerne i EU/EØS. - Se listen over underbehandlere for oplysninger om underbehandlernes behandling.
Behandlingens varighed	Behandlingen af personoplysninger finder sted i den gyldighedsperiode, der fremgår af aftalen, og i en begrænset periode derefter i henhold til dette databehandlingstillæg. Behandleren skal samarbejde med den ansvarlige for at fastsætte, hvor længe personoplysningerne skal opbevares hos den ansvarlige.

Bilag B – Tekniske sikkerhedsforanstaltninger

Lime implementerer og opretholder følgende sikkerhedstiltag:

Informationssikkerheds-styringssystem (ISMS)	Lime opretholder et ISMS, som er i overensstemmelse med ISO 27001 og omfatter centrale del af Limes drift. Sikkerhedsmæssige politikker og procedurer – inklusive risikostyring, handlingsplan for hændelser, virksomhedskontinuitet og leverandørsikkerhed – gennemgås regelmæssigt og er underlagt intern og ekstern revision.
Organisatorisk sikkerhed og forvaltning	Lime har en sikkerhedsansvarlig og en etableret forvaltningsstruktur for at holde øje med sikkerheden. Medarbejderne skal gennemføre obligatorisk sikkerhedstræning ved ansættelse og derefter årligt.
Adgangsstyring	Adgang til systemer og data gives ud fra princippet om minimering af autorisation og på baggrund af den enkelte rolles behov. Adgangsanmodninger skal godkendes af systemejere, og der foretages regelmæssige granskninger af adgangsrettigheder. Single Sign-On (SSO) og tofaktorgodkendelse (MFA) anvendes i centrale systemer.
Håndtering af adgangskoder	Lime stiller krav om, at adgangskoder skal indeholde mindst otte (8) tegn og har defineret krav om deres kompleksitet. Adgangskoder må ikke genbruges eller opbevares i et læsbart format. Brugeroplysninger må ikke videregives.
Systemovervågning og logføring	Lime fører log over adgang til og aktiviteter i centrale tjenester. Der er konfigureret alarmer og automatiske udløsningsmekanismer, som registrerer afvigelser eller mistænkelig adfærd, hvilket understøtter identificering og analyse af hændelser.
Hændelseshåndtering	Lime har en veldokumenteret og gennemtestet handlingsplan for hændelser. Alle hændelser klassificeres ud fra alvorsgrad og håndteres af de relevante teams. Kunder underrettes uden unødig forsinkelse om den identificerede hændelse, hvis hændelsen påvirker deres data.
Backup, virksomhedskontinuitet og katastrofegendannelse	Lime har virksomhedskontinuitets- og katastrofegendannelsesplaner for alle virksomhedskritiske systemer. Daglige backups opbevares i op til 90 dage (hvilket kan forlænges til maksimalt 365 dage).
Enheds- og slutpunktssikkerhed	Virksomhedens enheder administreres centralt og konfigureres med kryptering, anti-malware-software og firewall. Kun de enheder, der lever op til Limes krav, kan få adgang til Limes tjenester.

Leverandørsikkerhed	Lime vurderer leverandører i forbindelse med onboarding og derefter løbende. Leverandører, som har adgang til Limes data eller systemer, skal opfylde en række definerede krav til sikkerhed og compliance.
Cloudsikkerhed og hosting af data	Lime CRM (SaaS) hostes på Amazon Web Services (AWS), som opretholder brancheførende fysiske og miljømæssige kontrolforanstaltninger og har adskillige sikkerhedscertificeringer. Data krypteres ved overførsel med TLS 1.2/1.3 og med AES-256-kryptering ved opbevaring.
Sikker udviklingspraksis	Lime følger en sikker softwareudviklingslivscyklus (SDLC), som inkluderer risikovurderinger, kodegranskning, sårbarhedsscanning samt adskillelse af udviklings-, test- og produktionsmiljøer. Udviklerne er uddannet i sikker kodningspraksis, herunder OWASP Top 10 awareness.
Penetrationstest	Limes cloudtjenester er underlagt årlige penetrationstests, som udføres af uafhængige tredjeparter.
Logføring og auditspor	Centrale aktiviteter i Limes cloudtjenester og understøttende infrastruktur logføres, herunder adgang til og ændringer af data. Kunder kan anmode om udtræk af logdata med henblik på undersøgelser.
Identitets- og adgangsstyring	Adgang til Limes CRM understøtter Single Sign-On (SSO) via Microsoft Entra ID eller andre OIDC-udbydere samt tofaktorgodkendelse ved konfiguration via eksterne identifikationssystemer.
Produktsikkerhed og patch-administration	Lime opdaterer jævnligt sine cloudtjenester med sikkerhedspatches og forbedringer. Der anvendes automatiske værktøjer til at håndtere afhængigheder og identificere kendte sårbarheder.