Databehandleravtale

Oppdatert 28. mars 2025

Denne databehandleravtalen («DBA») innlemmes i og gjøres til en del av Limes tjenestevilkår («Avtalen»), som inngås av og mellom Lime-enheten og kunden som er identifisert i Avtalen. Formålet med DBA-en er å gjenspeile det partenes avtale sier om behandling av personopplysninger, i tråd med kravene i gjeldende personvernlovgivning. Alle termer som er skrevet med stor forbokstav, men som ikke er definert i denne teksten, skal ha den betydningen som er angitt i Avtalen eller i DBA, etter hva som er relevant.

I forbindelse med levering av Tjenester til Kunden i henhold til Avtalen kan Lime behandle personopplysninger på vegne av Kunden, og partene er enige om å overholde følgende bestemmelser angående alle personopplysninger. Lime skal heretter omtales som «Behandler», «Behandleren», mens kunden skal omtales som «Behandlingsansvarlig», «den Behandlingsansvarlige». Noen steder kan de hver for seg omtales som «part», «parten» eller og samlet som «parter», «partene».

Denne DBA-en har forrang fremfor motstridende eller uforenlige bestemmelser i Tjenestevilkårene om behandling av personopplysninger.

1 Definisjoner 2
2 Behandling av personopplysninger 3
3 Behandlerens forpliktelser 3
4 Behandlingsansvarliges forpliktelser 4
5 Sikkerhetsforanstaltninger 4
6 Revisjoner og inspeksjoner 5
7 Støtte til den Behandlingsansvarlige 5
8 Bruk av underbehandlere 6
9 Overføring av personopplysninger til Tredjestat 7
10 Databehandleravtalens varighet 8
11 Tiltak i forbindelse med opphør av Databehandleravtalen 8
12 Konfidensialitet 9
13 Endringer og tillegg 9
14 Erstatningsansvar 9
15 Valg av lov og verneting 10
Vedlegg A – Instruksjoner for behandling av personopplysninger 11
Vedlegg B – Tekniske sikkerhetstiltak 12

1 Definisjoner

I tillegg til vilkårene som er definert i hovedteksten i DBA-en skal følgende begreper ha den betydningen som er angitt nedenfor.

1.1 **Personopplysninger:** Enhver form for opplysninger knyttet til en identifisert eller identifiserbar person (Den registrerte).

1.2 **Den registrerte:** En identifisert eller identifiserbar enkeltperson. En identifiserbar person er noen som kan identifiseres, enten direkte eller indirekte, særlig ved henvisning til et identifikasjonsnummer eller til en eller flere faktorer som er spesifikke for personens fysiske, fysiologiske, mentale, økonomiske, kulturelle eller sosiale identitet.

1.3 **Behandling (av personopplysninger):** Ethvert tiltak eller enhver serie av tiltak som gjøres i forhold til personopplysninger, uansett om dette skjer automatisk eller ikke, f.eks. innsamling, registrering, organisering, lagring, tilpasning eller endring, søk, konsultasjon, bruk, overføring, formidling eller annen utlevering, sammenstilling eller kombinasjon, blokkering, sletting eller destruering.

1.4 **Behandlingsansvarlig:** En enkeltperson eller juridisk person, myndighet, institusjon eller annet organ som alene eller sammen med andre bestemmer formålene for og hvordan behandlingen av personopplysninger skal foregå.

1.5 **Behandler:** En enkeltperson eller juridisk person, myndighet, institusjon eller annet organ som utfører behandling av personopplysninger på vegne av den Behandlingsansvarlige.

1.6 **Gjeldende personvernlovgivning:** Personvernforordningen (GDPR) – dvs. Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF – og nasjonale lover som gjennomfører eller kommer som tillegg til GDPR, og som gjelder for behandlingen av personopplysninger ifølge denne DBA-en.

1.7 **Sensitive personopplysninger**: Rasemessig eller etnisk opprinnelse, politisk, filosofisk eller religiøs overbevisning, fagforeningsmedlemskap, hvorvidt en person er mistenkt for eller har vært etterforsket eller dømt for en forbrytelse, helseforhold, genetiske opplysninger eller biometriske opplysninger som brukes til å identifisere en person, opplysninger om en persons seksuelle forhold eller seksuelle orientering eller andre sensitive personopplysninger.

1.8 **Tredjestat:** Et land utenfor EU/EØS.

2 Behandling av personopplysninger

2.1 Behandleren skal utføre behandling av personopplysninger kun i henhold til denne DBA-en og i samsvar med dokumenterte instruksjoner fra Behandlingsansvarlige, med mindre Behandleren er forpliktet ifølge EU/EØS-lovgivning (herunder de nasjonale lovene i medlemslandene) til å utføre behandling av personopplysningene.

2.2 Behandlingsansvarlige skal gi Behandleren skriftlige instruksjoner om hvordan behandlingen skal foregå.

2.3 Behandleren skal utføre behandling av personopplysningene i hele avtaleperioden som er angitt i Avtalen, og i en begrenset periode etter dette (se avsnitt 11). **Vedlegg A** inneholder informasjon om behandlingen av personopplysninger inkludert i) kategorier av personopplysninger, ii) kategorier av Registrerte, iii) behandlingens art og formål, iv) behandlingssted og v) behandlingens varighet.

2.4 DBA-en gjelder ikke for personopplysninger som er blitt overført fra Tjenesten til en tredjepartsprogramvare (som definert i Avtalen), ettersom de vil styres av avtalen du har inngått med leverandøren av tredjepartsprogramvaren.

3 Behandlerens forpliktelser

3.1 Behandleren skal utføre behandlingen kun i henhold til DBA-en og instruksjonene. Behandleren kan, for klarhetens skyld, utføre behandling av personopplysninger hvis slik behandling er nødvendig ifølge en aktuell lov som gjelder for Behandleren. Behandleren skal informere Behandlingsansvarlige om slike krav hvis denne ikke er forhindret fra å utlevere slik informasjon på grunn av en viktig offentlig interesse. Ved behandling av personopplysninger i henhold til DBA-en skal Behandleren opptre i samsvar med gjeldende personvernlovgivning.

3.2 Behandleren skal sørge for at alle enkeltpersoner som arbeider under dennes ledelse og som har innsyn i personopplysninger, følger DBA-en og den Behandlingsansvarliges instruksjoner.

3.3 Under behandlingen skal Behandleren og dennes ansatte forplikte seg til konfidensialitet og hemmelighold av personopplysningene de har innsyn i ifølge denne Avtalen. Denne bestemmelsen gjelder også etter at DBA-en opphører.

3.4 Behandleren skal treffe de sikkerhetsforanstaltninger som kreves av artikkel 32 i personvernforordningen.

3.5 I den grad det er mulig skal Behandleren hjelpe Behandlingsansvarlige med å oppfylle dennes forpliktelser overfor de Registrerte ved å iverksette hensiktsmessige tekniske og organisatoriske tiltak.

3.6 På forespørsel fra Behandlingsansvarlige skal Behandleren hjelpe Behandlingsansvarlige med å sikre at forpliktelsene ifølge personvernforordningens

avsnitt 32–36 blir oppfylt, under hensyntagen til hvilken type behandling det gjelder og hvilke opplysninger Behandleren har tilgang til.

3.7 Behandleren skal varsle Behandlingsansvarlige umiddelbart dersom Behandleren anser den Behandlingsansvarliges instruksjoner for å være uklare eller på noen måte i strid med gjeldende personvernlovgivning. Behandleren skal ikke følge en slik instruksjon før Behandlingsansvarlige har bekreftet at instruksjonen er lovlig.

4 Behandlingsansvarliges forpliktelser

4.1 Ved bruk av tjenestene som leveres av Behandleren i henhold til Avtalen, skal den Behandlingsansvarlige utføre behandling av personopplysninger i samsvar med gjeldende personvernlovgivning. Behandlingsansvarlige er ansvarlig for å sikre at det til enhver tid finnes rettslig grunnlag for behandlingen, og for å formulere korrekte instruksjoner slik at Behandleren (og dennes underbehandlere) kan oppfylle sine forpliktelser ifølge denne Avtalen og, dersom det er aktuelt, Avtalen.

4.2 Den Behandlingsansvarlige har rett til å utføre behandling og utlevering av personopplysningene som er dekket av Avtalen til Behandleren (herunder eventuelle underbehandlere).

4.3 Behandlingsansvarlige er fullt ut ansvarlig for at personopplysninger som utleveres til Behandleren, er nøyaktige, fullstendige, uskadet, pålitelige og lovlige. Behandleren er ikke ansvarlig for noen konsekvenser av at personopplysningene denne mottar, viser seg ikke å være korrekte.

4.4 Behandlingsansvarlige har oppfylt sin plikt til å gi de Registrerte påbudt informasjon om behandling av personopplysninger og overføring av personopplysninger til Behandleren og om Behandlerens behandling av personopplysninger i henhold til gjeldende personvernlovgivning.

4.5 Ved bruk av Tjenestene som leveres av Behandleren i henhold til Avtalen, skal Behandlingsansvarlige ikke utlevere noen sensitive personopplysninger til Behandleren med mindre dette er uttrykkelig avtalt og spesifisert skriftlig mellom partene.

4.6 Behandlingsansvarlige skal varsle Behandleren umiddelbart om eventuelle endringer av kontaktperson eller kontaktopplysninger.

5 Sikkerhetsforanstaltninger

5.1 Behandleren skal gjennomføre hensiktsmessige tekniske og organisatoriske tiltak. for å beskytte personopplysningene under gjeldende personvernlovgivning (herunder artikkel 32 i GDPR), nærmere bestemt for å beskytte konfidensialiteten, integriteten og tilgangen til personopplysningene, som videre beskrevet i vedlegg B. Behandleren skal

løpende revidere de tekniske og organisasjonsmessige sikkerhetstiltakene og oppdatere dem der det er nødvendig, i tråd med gjeldende personvernlovgivning.

6 Revisjoner og inspeksjoner

6.1 Behandleren skal gi den Behandlingsansvarlige tilgang til alle opplysninger som er nødvendige for å dokumentere at forpliktelsene som er nedfelt i DBA-en er oppfylt, og for å muliggjøre og bidra til revisjoner, herunder inspeksjoner, gjennomført av Behandlingsansvarlige eller en tredjepart oppnevnt av Behandlingsansvarlige.

6.2 Behandlingsansvarlige kan revidere Behandlerens etterlevelse av DBA maksimalt en (1) gang per år. Hvis det gjeldende personvernlovgivning krever det, kan Behandlingsansvarlige kreve hyppigere gjennomganger.

6.3 For å be om en revisjon skal Behandlingsansvarlige sende en detaljert revisjonsplan til Behandleren minst fire uker før den foreslåtte revisjonen. Planen må inneholde omfang, varighet og foreslått startdato for revisjonen. Hvis revisjonen skal gjøres av en tredjepart, må dette som en generell regel avtales mellom Behandlingsansvarlige og Behandleren. Hvis Behandlingen skjer i et miljø med personopplysninger fra andre Behandlingsansvarlige eller lignende, kan Behandleren, etter eget skjønn, bestemme at revisjonen av hensyn til sikkerheten skal utføres av et generelt høyt ansett revisjonsfirma som velges av Behandleren.

6.4 Hvis den påkrevde revisjonen allerede er gjennomført og beskrevet i en rapport i henhold til ISAE 3402, ISO eller tilsvarende av en kvalifisert tredjepartsrevisor i løpet av de siste 12 månedene, og Behandleren bekrefter at de reviderte kontrollene ikke er vesentlig endret, må den Behandlingsansvarlige akseptere disse resultatene i stedet for å be om en revisjon av kontrollene som er dekket av rapporten.

6.5 Revisjonen skal utføres i bedriftens normale åpningstid i henhold til Behandlerens retningslinjer og skal ikke medføre urimelige forstyrrelser i Behandlerens drift.

6.6 Den Behandlingsansvarlige er ansvarlig for alle kostnader som oppstår i tilknytning til en revisjon som Behandlingsansvarlige ber om, og Behandlerens assistanse i forbindelse med dette.

6.7 Behandleren skal gi tilsynsmyndigheten, eller annen myndighet som er juridisk berettiget til det, mulighet til å utføre tilsyn i henhold til den til enhver tid gjeldende lovgivning. Behandleren og dennes ansatte skal, på forespørsel, samarbeide med tilsynsmyndigheten når den utfører sine forpliktelser.

7 Støtte til den Behandlingsansvarlige

7.1 Under hensyntagen til Behandlingens art og så langt det er mulig, skal Behandleren bistå Behandlingsansvarlige med egnede tekniske og organisatoriske tiltak slik at

Behandlingsansvarlige kan oppfylle sin plikt til å svare på forespørsler når Registrerte utøver sine rettigheter.

7.2 Så langt det er praktisk mulig og lovlig, skal Behandleren varsle Behandlingsansvarlige om i) henvendelser mottatt fra Registrerte om utlevering av personopplysninger, bortsett fra når Behandlingsansvarlige har gitt Behandleren fullmakt til å svare på en slik henvendelse, og ii) henvendelser fra myndigheter om å utlevere personopplysninger, bortsett fra når Behandlingsansvarlige har gitt Behandleren fullmakt til å svare på en slik henvendelse.

7.3 Behandleren kan imidlertid være forhindret fra å varsle Behandlingsansvarlige på grunn av hemmelighold i forbindelse med en etterforskning. Behandleren skal ikke utlevere opplysninger om denne DBA-en til myndighetene i forbindelse med personopplysninger, med mindre denne pålegges å gjøre dette ifølge lov eller forespørselen underbygges av en rettsavgjørelse, ransakingsordre eller tilsvarende.

7.4 Under hensyntagen til arten av Behandlingen og informasjonen som er tilgjengelig for Behandleren, skal Behandleren hjelpe Behandlingsansvarlige med å sørge for at forpliktelsene ifølge gjeldende personvernlovgivning blir oppfylt, herunder (hvis aktuelt) den Behandlingsansvarliges plikt til i) å iverksette hensiktsmessige tekniske og organisatoriske tiltak, ii) rapportere brudd på personopplysningssikkerheten til tilsynsmyndigheten, iii) varsle Registrerte om brudd på personopplysningssikkerheten, iv) gjennomføre konsekvensutredninger knyttet til beskyttelse av opplysninger og v) rådføre seg med tilsynsmyndigheten før behandling.

7.5 Behandleren skal umiddelbart varsle den Behandlingsansvarlige skriftlig dersom Behandleren har blitt klar over et brudd på personopplysningssikkerheten. Behandleren skal gi Behandlingsansvarlige en beskrivelse av bruddet. Dersom Behandleren ikke har all relevant informasjon knyttet til bruddet på personopplysningssikkerheten når den først informerer Behandlingsansvarlige om at dette har funnet sted, kan Behandleren gi denne informasjonen stykkevis.

7.6 Behandleren har rett til å fakturere Behandlingsansvarlige for det utførte arbeidet og rimelige kostnader som har påløpt i forbindelse med Behandlerens støtte som beskrevet ovenfor, og i henhold til gjeldende personvernlovgivning, uten at det går ut over forpliktelsene som følger av avsnitt 7.5 over (forutsatt at den Behandlingsansvarlige ikke kan lastes for bruddet på personopplysningssikkerheten. Dette omfatter f.eks. arbeid og kostnader som følge av at Registrerte har bedt om registerutskrift i forbindelse med behandling av personopplysningene deres, sletting av personopplysninger, overføring av personopplysninger (portabilitet) eller utlevering av påbudt informasjon til Registrerte.

8 Bruk av underbehandlere

8.1 Som et ledd i tjenesteleveransen fra Behandleren til Behandlingsansvarlige ifølge Avtalen, gis Behandleren herved en generell skriftlig forhåndstillatelse til å bruke

underbehandlere til behandling av personopplysninger på vegne av Behandlingsansvarlige.

8.2 Behandleren skal sørge for at alle underbehandlere er bundet av skriftlige avtaler som sikrer at underbehandleren er underlagt forpliktelser knyttet til Behandlingen av personopplysninger som, som minimum, tilsvarer forpliktelsene som er nedfelt i denne DBA-en.

8.3 Dersom underbehandleren ikke oppfyller sine forpliktelser ifølge gjeldende personvernlovgivning, skal Behandleren være fullt ut ansvarlig overfor Behandlingsansvarlige for å oppfylle underbehandlerens forpliktelser.

8.4 Behandleren skal legge frem en oppdatert og aktuell liste over underbehandlere som brukes for å utføre tjenestene som leveres av Behandleren ifølge Hovedavtalen. Listen skal inneholde informasjon om underbehandlernes identitet, kontaktperson hos underbehandleren, hvor personopplysningene blir behandlet og en generell beskrivelse av hvilken type tjeneste hver underbehandler leverer. Listen over underbehandlere er tilgjengelig på Limes nettside https://www.lime-technologies.com/subprocessors/. Ved å signere denne Avtalen godtar Behandlingsansvarlige Behandlerens bruk av de oppførte underbehandlerne.

8.5 Behandleren skal varsle Behandlingsansvarlige om eventuelle planer om å leie inn en ny eller bytte ut en eksisterende underbehandler. Behandlingsansvarlige kan motsette seg slike endringer. Dersom det ikke fremsettes noen protest innen ti (10) dager fra varselet er mottatt, antas det at Behandlingsansvarlige ikke har fremsatt noen protest.

8.6 Behandleren har rett til å iverksette hensiktsmessige korrigerende tiltak i tilfelle av en slik protest. Hvis Behandlingsansvarlige finner at det ikke er iverksatt korrigerende tiltak eller at protesten ikke er utbedret innen tretti (30) dager, har Behandleren rett til å si opp DBA-en og, dersom DBA-en er nødvendig for at Behandleren skal oppfylle sine forpliktelser ifølge Avtalen, si opp Avtalen ved skriftlig varsel.

9 Overføring av personopplysninger til Tredjestat

9.1 Behandleren og dennes underbehandlere kan overføre personopplysninger til en Tredjestat i den grad det er nødvendig for å utføre tjenestene Behandleren leverer ifølge Avtalen, og på betingelse av at overføringen skjer ifølge kapittel 5 i personvernforordningen.

9.2 Ved bruk av standard personvernbestemmelser (Kommisjonsbeslutning (EU) 2021/914 av 4. juni 2021 om standard personvernbestemmelser for overføring av personopplysninger til tredjestater i henhold til Europaparlamentets og Rådets forordning (EU) 2016/679, eller beslutninger og standard personvernbestemmelser som erstatter disse bestemmelsene), har Behandleren eller underbehandleren rett til å avgjøre hvilken versjon og hvilke moduler i de standard personvernbestemmelsene som gjelder i det enkelte tilfelle.

9.3 I henhold til kravene i gjeldende personvernlovgivning for overføring basert på at hensiktsmessige sikkerhetsforanstaltninger er tatt, skal Behandleren gjennomføre en risikovurdering i hvert enkelt tilfelle for å sikre at lovgivningen i den aktuelle Tredjestaten ikke har negativ innflytelse på effektiviteten av de aktuelle sikkerhetstiltakene, og sørge for at det finnes effektive botemidler for de Registrerte. Om nødvendig skal Behandleren identifisere og iverksette ytterligere tiltak, som tekniske, organisatoriske eller kontraktsmessige tiltak, for å sørge for at beskyttelsesnivået i den aktuelle Tredjestaten i hovedsak tilsvarer beskyttelsesnivået i EU/EØS.

9.4 På rimelig forespørsel fra Behandlingsansvarlige skal Behandleren rapportere hvilke opplysninger risikovurderingen er basert på. Behandlingsansvarlige har rett til skriftlig å motsette seg Behandlerens risikovurderinger hvis de endres etter at DBA-en trer i kraft og Behandlingsansvarlige mener at de nye risikovurderingene ikke oppfyller kravene til den Behandlingsansvarliges behandling av personopplysninger i henhold til gjeldende personvernlovgivning. Behandlingsansvarlige har rett til å be om at Behandleren iverksetter hensiktsmessige korrigerende tiltak. Dersom partene ikke blir enige om risikovurderingen og/eller hensiktsmessige korrigerende tiltak innen tretti (30) dager, har partene rett til å si opp DBA-en og, dersom DBA-en er nødvendig for at Behandleren skal oppfylle sine forpliktelser ifølge Avtalen, har denne rett til å si opp Avtalen ved skriftlig varsel.

9.5 Dersom EU-domstolen, EU-kommisjonen eller noen annen kompetent EU-institusjon eller nasjonal domstol eller myndighet finner at overføringsmekanismen som brukes til overføring til en Tredjestat, er ugyldig eller ulovlig, skal Behandleren sørge for at all behandling av personopplysninger i en Tredjestat baseres på en annen (gyldig) overføringsmekanisme.

10 Databehandleravtalens varighet

10.1 Denne DBA-en gjelder så lenge Behandleren utfører behandling av personopplysninger på vegne av Behandlingsansvarlige ifølge Avtalen.

10.2 Denne DBA-en opphører automatisk ved opphør av Avtalen.

11 Tiltak i forbindelse med opphør av Databehandleravtalen

11.1 Ved opphør av denne DBA-en skal Behandleren, avhengig av hvilke skriftlige instruksjoner Behandlingsansvarlige gir til Behandleren, slette eller levere tilbake alle personopplysninger som blir behandlet på vegne av Behandlingsansvarlige ifølge DBA-en, samt alle kopier av opplysningene, med mindre lagring av personopplysningene kreves ifølge gjeldende personvernlovgivning.

11.2 Dersom Behandlingsansvarlige ikke har fremlagt noen instruksjoner eller svart på Behandlerens forespørsel om instruksjoner, kan Behandleren tidligst tretti (30) dager

etter at DBA-en opphører, velge å levere tilbake alle personopplysninger til Behandlingsansvarlige og/eller slette alle personopplysningene.

12 Konfidensialitet

Behandleren skal ikke, verken så lenge DBA-en er gyldig eller senere, utlevere informasjon om behandlingen av personopplysninger ifølge denne DBA-en til en tredjepart eller på annen måte avsløre informasjon som er mottatt som følge av denne DBA-en. Konfidensialitetsplikten gjelder ikke informasjon som Behandleren har plikt til å utlevere til myndighetene. I tillegg til dette avsnittet (12) skal konfidensialitetsforpliktelsene i Avtalen også gjelde.

13 Endringer og tillegg

13.1 Det kan komme endringer i denne DBA-en på grunn av endringer i lovgivning, sikkerhetskrav eller andre praktiske omstendigheter. Dersom en endring påvirker behandlingen av personopplysninger ifølge denne DBA-en, skal den andre parten varsles per e-post sendt til kontaktpersonen som er angitt ovenfor. Et slikt varsel om endring skal anses for å ha blitt akseptert av den andre parten såfremt den andre parten ikke har fremsatt rimelige skriftlige protester innen tretti (30) dager etter varslingsdatoen.

13.2 Dersom en kompetent domstol, myndighet eller voldgiftsnemnd finner at noen bestemmelse i denne DBA-en er ugjennomførbar eller ugyldig, skal dette ikke påvirke de andre bestemmelsene. I denne forbindelse skal partene erstatte den ugjennomførbare eller ugyldige bestemmelsen med en lovlig bestemmelse som gjenspeiler formålet med den ugjennomførbare eller ugyldige bestemmelsen.

14 Erstatningsansvar

14.1 Ved erstatning for skader i forbindelse med behandlingen som, ifølge en endelig avgjørelse eller et forlik, skal betales til den Registrerte på grunn av et brudd på en bestemmelse i denne DBA-en, skal instruksjonene og/eller enhver anvendelig bestemmelse i gjeldende personvernlovgivning, artikkel 82 i personvernforordningen, anvendes.

14.2 Administrasjonsgebyrer ifølge artikkel 83 i personvernforordningen eller kapittel 7, avsnitt 26 av den norske personvernloven av 15. juni 2018 nr. 38 med tilleggsbestemmelser til EUs personvernforordning, skal dekkes av parten som har blitt ilagt et slikt administrasjonsgebyr.

14.3 Uten at det går ut over forpliktelsene under 14.1 og 14.2, skal den avtaleregulerte ansvarsbegrensningen som er angitt i Avtalen også gjelde denne DBA-en.

14.4 Hvis noen av partene blir oppmerksom på noen omstendighet som kan påføre den andre parten skade, skal parten umiddelbart informere den andre parten om

omstendigheten og aktivt samarbeide med den andre parten for å forebygge og minimere skaden.

15 Valg av lov og verneting

15.1 Denne DBA-en skal fortolkes og gjelde i henhold til bestemmelsene om verneting i Avtalen.

15.2 Eventuelle tvister som oppstår i forbindelse med denne DBA-en skal avgjøres endelig i henhold til bestemmelsene om tvisteløsning i Avtalen.

***

Vedlegg A – Instruksjoner for behandling av personopplysninger

Kategorier av personopplysninger	Behandlingsansvarlige kan legge inn personopplysninger i tjenesten som leveres av Databehandleren ifølge Avtalen. personopplysningene som legges inn i tjenesten er helt opp til Behandlingsansvarlige og kan f.eks. bestå av følgende kategorier av personopplysninger: - navn - telefonnummer - e-postadresse - kundehistorikk
Kategorier av Registrerte	Behandlingsansvarlige kan legge inn personopplysninger i tjenesten som leveres av Databehandleren ifølge Avtalen. personopplysningene som legges inn i tjenesten er helt opp til Behandlingsansvarlige og kan f.eks. bestå av personopplysninger som gjelder følgende kategorier av Registrerte: - den Behandlingsansvarliges ansatte, kunder, leverandører og konsulenter. - ansatte hos den Behandlingsansvarliges potensielle kunder.
Behandlingens art og formål	Behandling av personopplysninger for å levere tjenestene som leveres av Databehandleren i henhold til Avtalen og den Behandlingsansvarliges instruksjoner.
Sted for behandlingen	- Databehandleren utfører behandlingen av personopplysninger innenfor EU/EØS. - Se listen over underdatabehandlere for nærmere opplysninger om underdatabehandlernes behandling.
Behandlingens varighet	Behandling av personopplysninger vil finne sted i Avtalens gyldighetstid og i en begrenset periode etter dette ifølge Avtalen. Databehandleren skal samarbeide med Behandlingsansvarlige om å avgjøre hvor lenge personopplysningene skal lagres hos Behandlingsansvarlige.

Vedlegg B – Tekniske sikkerhetstiltak

Lime skal gjennomføre og oppdatere følgende sikkerhetstiltak:

Ledelsessystem for informasjonssikkerhet (ISMS)	Lime bruker et ledelsessystem for informasjonssikkerhet (ISMS) i tråd med ISO 27001 som dekker sentrale deler av selskapets operasjoner. Retningslinjer og prosedyrer for sikkerhet – herunder risikohåndtering, hendelseshåndtering, forretningsmessig kontinuitet og leverandørsikkerhet – revideres jevnlig og er underlagt interne og eksterne revisjoner.
Organisasjonssikkerhet og organisasjonsledelse	Lime har utpekt en sikkerhetsansvarlig og etablert en styringsstruktur som fører tilsyn med sikkerhetsoperasjonene. De ansatte blir pålagt å gjennomføre obligatorisk sikkerhetsopplæring i forbindelse med onboarding og årlig.
Tilgangskontroller	Det gis tilgang til systemer og data basert på prinsippet om færrest mulig rettigheter og kravene som følger av arbeidsrollen. Anmodninger om tilgang må godkjennes av systemeierne, og det må gjennomføres regelmessige revisjoner av tilgangene som blir gitt. Det brukes engangspålogging (SSO) og flerfaktorautentisering (MFA) på tvers av nøkkelsystemene.
Administrasjon av passord	Lime krever at alle passord består av minst åtte (8) tegn og har en viss kompleksitet. Passord må ikke gjenbrukes eller lagres i et lesbart format. Det er forbudt å dele brukeropplysningene sine med andre.
Systemovervåking og loggføring	Lime loggfører tilgangen og systemaktiviteten på tvers av nøkkeltjenester. Det settes opp varsler og automatiske triggere for å påvise avvik eller mistenkelig atferd, noe som letter påvisning og analyse av hendelser.
Håndtering av hendelser	Lime har en dokumentert og utprøvd beredskapsplan for håndtering av hendelser. Alle hendelser blir klassifisert etter alvorsgrad og håndtert av relevante team. Kundene blir informert om hendelser som kan påvirke opplysningene deres, uten unødige forsinkelser.
Sikkerhetskopiering, forretningskontinuitet og gjenoppretting etter katastrofe	Lime bruker planer for forretningskontinuitet og gjenoppretting av kritiske systemer etter katastrofer. Det tas daglig såkalte uforanderlige sikkerhetskopier som lagres i inntil 90 dager. Denne perioden kan forlenges til maksimalt 365 dager.
Enhets- og endepunktsikkerhet	Selskapets enheter administreres sentralt og konfigureres med kryptering, programvare som beskytter mot skadevare og brannmurer. Bare godkjente enheter har tilgang til Limes tjenester.

Leverandørsikkerhet	Lime bistår leverandørene under onboarding og på regelmessig basis. Leverandører som har tilgang til Limes data eller systemer, må oppfylle definerte sikkerhets- og samsvarskrav.
Nettskysikkerhet og vertstjenester	Lime CRM (SaaS) bruker Amazon Web Services (AWS) som vert. AWS bruker bransjeledende fysiske og miljømessige kontrollmekanismer og har flere sikkerhetssertifiseringer. Dataene krypteres med TLS 1.2/1.3 mens de overføres og med AES-256-kryptering når de hviler.
Sikre utviklingspraksiser	Lime følger en sikker livssyklus for programvareutvikling (SDLC) som inkluderer risikovurderinger, gjennomganger av kode, sårbarhetsskanninger og adskillelse av utviklings-, test- og produksjonsmiljøer. Utviklerne får opplæring i sikre kodepraksiser, for eksempel «OWASP Top Ten».
Penetrasjonstester	Limes nettskytjenester gjennomgår årlige penetrasjonstester utført av uavhengige tredjeparter.
Loggføring og revisjonsspor	Nøkkelaktiviteter i Limes nettskytjenester og støttestrukturer blir loggført, herunder tilgangs- og dataendringer. Kundene kan be om utskrifter av loggen for å gjøre undersøkelser.
Identitets- og tilgangsstyring	Autentisering til Lime CRM støtter engangspålogging (SSO) med Microsoft Entra ID eller andre OIDC-leverandører og har støtte for MFA ved konfigurering via eksterne identitetssystemer.
Produktsikkerhet og administrasjon av programfikser	Lime oppdaterer skytjenestene sine regelmessig med programfikser og forbedringer. Det brukes automatiserte verktøy for å håndtere avhengigheter og identifisere kjente sårbarheter.