**Databehandleravtale**

For leveranse av tjenester fra LINK Mobility

|  |  |  |  |
| --- | --- | --- | --- |
| **Kundes kontaktinformasjon** | | **LINK kontaktinformasjon** | |
| Selskap: |  | Selskap: |  |
| Orgnr: |  | Orgnr: |  |
| Kontaktperson: |  | Kontaktperson: |  |
| Stilling: |  | Stilling: |  |
| Addresse: |  | Addresse: |  |
| Telefon: |  | Telefon: |  |
| E-post: |  | E-post: |  |
| E-mail for rapportering av hendelser: |  |  |  |

1. Innledning

Denne Databehandleravtalen (“**DPA**”) er inngått mellom LINK og Kunde, og er sammen med Tjenestebilag og andre bilag del av tjenesteavtale mellom Partene (“**Avtalen**”).

"**Personvernlogvivning**" betyr Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 ("**GDPR**") og Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (Kommunikasjonsverndirektivet), og nasjonal lovgivning om personvern, med de endringer som følger av oppdatert lovgivning på området til enhver tid.

Begreper som definert i GDPR artikkel 4 skal i denne Databehandleravtalen forstås slik de er definert i GDPR.

1. Omfang

Det er enighet mellom Partene om at LINK som del av sin levering av tjenester under Avtalen vil behandle personopplysninger på vegne av Kunden. Kunde utpeker derfor LINK som databehandler. Vilkårene for behandling av personopplysninger fremgår av denne DPA. LINK garanterer at LINK vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Personvernlovgivningen, og vern av den registrertes rettigheter.

Denne DPA dekker behandling av personopplysninger når LINK behandler personopplysninger på vegne av Kunde, som databehandler (GDPR Artikkel 28.3), eller som underdatabehandler (GDPR Artikkel 28.4).

Under denne DPA har Kunde rollen som behandlingsansvarlig, og er fullt ansvarlig overfor en behandlingsansvarlig Kunde behandler personopplysninger på vegne av gjennom bruk av LINKs tjenester. Enhver henvisning til «Behandlingsansvarlig» vil derfor heretter vise til Kunde.

LINK som databehandler, LINKs underdatabehandlere og enhver person som handler for den Behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, skal behandle nevnte opplysninger bare i henhold til Avtalen, eller etter instruks fra den behandlingsansvarlige eller denne DPA, med mindre det kreves i henhold til Personvernlovgivningen.LINK skal omgående underrette Kunde dersom LINK mener at en instruks er i strid med Personvernlovgivningen.

LINKs behandling av personopplysninger er tilgjengelig på <https://linkmobility.com/privacy/> .

1. Behandlingsansvarliges plikter

Behandlingsansvarlig tilsikrer at personopplysninger behandles på en lovlig måte, for spesifikke, uttrykkelig angitte og berettigede formål. Behandlingsansvarlig vil ikke instruere LINK til å behandle flere personopplysninger enn det som er nødvendig for formålene de behandles for (

Behandlingsansvarlig er ansvarlig for å sikre at rettslig vilkår for behandling som definert i Personvernlovgivningen (Jf. GDPR Artikkel 6.1) er på plass på tidspunktet når personopplysninger blir overført til LINK. Dersom grunnlaget er samtykke (Jf. GDPR Artikkel 6.1(a)), garanterer Behandlingsansvarlig for at samtykke er eksplisitt, frivillig, tydelig og informert.

Behandlingsansvarlig garanterer videre at de registrerte som personopplysningene gjelder har mottatt informasjon som krevet i Personvernlovgivningen (ref. GDPR Artikkel 13 og 14) om behandling av personopplysninger.

Instrukser som gjelder behandlingen av personopplysninger, skal primært gis direkte til LINK. I tilfeller der behandlingsansvarlig instruerer en underdatabehandler direkte etter bestemmelsene i avsnitt 10, skal behandlingsansvarlig umiddelbart informere LINK om dette. LINK skal ikke under noen omstendigheter være ansvarlig for behandling som er utført av en underdatabehandler basert på instrukser gitt direkte fra behandlingsansvarlig, og som fører til brudd med denne DPA, Avtalen eller Personvernlovgivningen.

1. Konfidensialitet

LINK sikrer at ansatte, underdatabehandlere og andre personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt.

Behandlingsansvarlig forplikter seg til å behandle dokumentasjon og informasjon mottatt fra LINK konfidensielt, herunder dokumentasjon og informasjon, om LINK eller LINKs underdatabehandleres implementerte tekniske og organisatoriske tiltak eller informasjon som er definert som konfidensiell. Behandlingsansvarlig vil likevel alltid kunne dele slik informasjon med tilsynsmyndighetene dersom dette er nødvendig for å overholde behandlingsansvarliges plikter etter Personvernlovgivningen.

1. Sikkerhet

Sikkerhetskravene som gjelder for LINKs behandling av personopplysninger følger av Sikkerhetsbilaget til denne DPA.

1. Tilgang til Personopplysninger og oppfyllelse av de registrertes rettigheter

Med mindre annet er avtalt eller følger av gjeldende lovgivning, skal Behandlingsansvarlig ha rett til å kreve tilgang til Personopplysninger som behandles av LINK på vegne av Behandlingsansvarlig.

Dersom LINK eller Underleverandør mottar en forespørsel fra en Registrert om behandlingen av Personopplysninger, skal LINK videresende forespørselen til Behandlingsansvarlig, med mindre LINK etter gjeldende lovgivning eller i tråd med Behandlingsansvarliges instrukser selv er berettiget til å håndtere forespørselen.

Idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for LINK, skal LINK bistå Behandlingsansvarlig med å oppfylle Behandlingsansvarliges plikt til å svare på anmodninger som de Registrerte inngir for å utøve sine rettigheter fastsatt i Personvernlovgivningen, herunder retten til (i) innsyn, (ii) korrigering og (iii) sletting, (iv) begrensning eller å motsette seg en behandling, samt (v) til å få utlevert egne Personopplysninger i et strukturert, alminnelig anvendt og maskinleselig format (dataportabilitet). LINK skal kompenseres for slik bistand i tråd med LINKs gjeldende priser, i den grad Behandlingsansvarlig krever bistand som går utover det som kreves i Personvernlovgivningen.

1. Annen bistand til behandlingsansvarlig

Dersom LINK eller en Underleverandør mottar en forespørsel fra relevant tilsynsmyndighet for innsyn i, eller informasjon om, registrerte Personopplysninger eller behandlingsaktiviteter omfattet av denne Databehandleravtalen, skal LINK varsle Behandlingsansvarlig om forespørselen, med mindre LINK etter gjeldende lovgivning eller i tråd med Behandlingsansvarliges instrukser selv er berettiget til å håndtere forespørselen.

Dersom Behandlingsansvarlig er forpliktet til å gjennomføre en vurdering av personvernkonsekvenser og/eller gjennomføre forhåndsdrøftelser med relevant tilsynsmyndighet i forbindelse med behandlingen av Personopplysninger under denne Databehandleravtalen, skal LINK bistå Behandlingsansvarlig, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for LINK. Behandlingsansvarlig skal dekke kostnader påført LINK som følge av slik bistand, i den grad Behandlingsansvarlig krever bistand som går utover det som kreves i Personvernlovgivningen.

1. Melding om brudd på personopplysningssikkerheten

LINK skal underrette Behandlingsansvarlig uten ugrunnet opphold etter å ha fått kjennskap til et brudd på personopplysningssikkerheten. Behandlingsansvarlig er ansvarlig for å melde Sikkerhetsbrudd til relevant tilsynsmyndighet i henhold til GDPR artikkel 33.

Underretningen til Behandlingsansvarlig skal som et minimum beskrive (i) arten av Sikkerhetsbruddet, herunder, når det er mulig, kategoriene av og omtrentlig antall Registrerte og Personopplysninger som er berørt, (ii) de sannsynlige konsekvensene av Sikkerhetsbruddet, (iii) de tiltak som LINK har truffet eller foreslår å treffe for å håndtere Sikkerhetsbruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av Sikkerhetsbruddet.

Dersom Behandlingsansvarlig er forpliktet til å underrette de Registrerte om Sikkerhetsbrudd, skal LINK bistå Behandlingsansvarlig, idet det tas hensyn til behandlingens art og i den grad det er mulig. Behandlingsansvarlig skal dekke kostnadene knyttet til slik kommunikasjon med de Registrerte.

1. Overføring til tredjeland

Overføring av Personopplysninger til land utenfor EU eller EØS, inkludert ved deling av eller tilgang til opplysninger, vil kun skje ved dokumentert instruks fra Behandlingsansvarlig.

For overføring til underdatabehandlere er dokumentert instruks beskrevet i punkt 10 nedenfor, og krever bruk av EUs standardvilkår ( eget bilag til denne Databehandleravtalen, modul tre – overføring fra LINK som databehandler til en underdatabehandler i et tredjeland.)

Kunde forstår og aksepterer at overføring til operatører i tredjeland som er nødvendig for levering av meldinger til mottakere av meldinger som befinner seg i slike land ikke er dekket av kravene beskrevet her.

1. Bruk av underdatabehandlere

Behandlingsansvarlig godkjenner at LINK kan engasjere en underleverandør, her referert til som underdatabehandler, for å bistå i å yte tjenesten og behandle personopplysninger, såfremt LINK sikrer at forpliktelser som er fastsatt i denne databehandleravtalen og i Personvernlovgivningen pålegges underdatabehandler gjennom en skriftlig avtale; og at enhver underdatabehandler gir tilstrekkelige garantier for at det blir gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Personvernlovgivningen og Databehandleravtalen, samt gir Behandlingsansvarlig og relevant tilsynsmyndighet den tilgang og informasjon som er nødvendig for å verifisere slike garantier.

LINK skal være fullt ut ansvarlig overfor Behandlingsansvarlig for at underdatabehandler oppfyller sine forpliktelser.

Underdatabehandlere som benyttes er listet i bilag: Omfang. LINK kan oppdatere listen for å vise tillegg eller erstatning av underdatabehandler ved å varsle Kunde senest 3 måneder før den dag underdatabehandler skal påbegynne behandlingen av Personopplysninger. Enhver innvending mot slike endringer må fremsetter til LINK innen 3 uker fra varsel mottas. Dersom Behandlingsansvarlig motsetter seg endringen eller utskiftningen av en Underleverandør, kan LINK terminere Avtalen og Databehandleravtalen med 1 måneds varsel.

Ved å inngå denne Databehandleravtalen, gir Behandlingsansvarlig fullmakt til LINK til å inngå EUs standardvilkår på vegne av Behandlingsansvarlig, eller til å sikre annet rettslig grunnlag for Overføring til et Tredjeland for underdatabehandler som er godkjent i henhold til ovennevnte prosedyre. Dersom Kunde ikke selv er Behandlingsansvarlig, vil Kunde sikre at Behandlingsansvarlig har gitt tilsvarende fullmakt. LINK skal på forespørsel gi Behandlingsansvarlig en kopi av slike EU standardvilkår eller en beskrivelse av annet rettslig grunnlag for Overføringen.

LINK skal yte rimelig bistand og dokumentasjon til bruk i den Behandlingsansvarliges selvstendige risikovurdering av bruken av Underleverandører eller Overføringen av Personopplysninger til et Tredjeland.

1. Revisjon

På forespørsel skal LINK gi Kunde tilgang til dokumentasjon av tekniske og organisatoriske tiltak som er implementert for å sikre tilstrekkelig sikkerhetsnivå, og annen informasjon som er nødvendig for å synliggjøre LINKs overholdelse av denne DPA og Personvernlovgivningen.

Den behandlingsansvarlige og relevante Tilsynsmyndigheter under Personvernlovgivningen har rett til å utføre revisjoner, herunder revisjon i Databehandlers lokaler og vurdering av personopplysninger som behandles, systemer og utstyr som benyttes, implementerte tekniske og organisatoriske tiltak som sikkerhetsretningslinjer og tilsvarende, og underdatabehandlere.

Behandlingsansvarlig vil ikke gis tilgang til informasjon som gjelder andre kunder av LINK, eller informasjon som er dekket av konfidensialitetsforpliktelser.

Behandlingsansvarlig kan gjennomføre revisjon én (1) gang per år, med minst to ukers varsel. Dersom Behandlingsansvarlig utpeker en ekstern revisor for å utføre revisjon, skal ekstern revisor gis konfidensialitetsplikt. Behandlingsansvarlig skal bære alle kostnader knyttet til revisjon initiert av Behandlingsansvarlig, eller som påløper ved Behandlingsansvarliges revisjon, herunder kompensasjon til LINK i den grad Behandlingsansvarlig krever bistand som går utover det som kreves i Personvernlovgivningen. LINK vil likevel bære kostnadene dersom revisjon viser manglende overholdelse av DPA eller Personvernlovgivningen.

1. Varighet og oppsigelse

DPA løper så lenge LINK behandler personopplysninger på vegne av Behandlingsansvarlig.

Dersom LINK misligholder DPA eller ikke overholder Personvernlovgivningen, kan Behandlingsansvarlig (i) instruere LINK til å avslutte videre behandling av personopplysninger med umiddelbar virkning, og/eller (ii) si opp DPA med umiddelbar virkning.

1. Ved opphør

LINK vil ved oppsigelse av DPA slette alle personopplysninger, med mindre annet følger av gjeldende rett. Kunde vil ha tilgang til personopplysninger frem til opphør, slik at eventuelle behov for kopier av personopplysninger vil kunne gjøres av Kunde frem til opphør.

LINK vil på forespørsel bekrefte til Kunde at sletting er gjennomført i henhold til DPA.

1. Mislighold og ansvarsbegrensning

Manglende overholdelse av en Parts plikter i henhold til DPA utgjør mislighold av Avtalen, og Parten skal uten ugrunnet opphold utbedre misligholdet.

Den misligholdende Parten skal oppdatere den annen part om tiltak som er iverksatt for å rette den manglende overholdelsen.

Begge Parter er fullt ut ansvarlig for sine underleverandørers handlinger og unnlatelser som om det var Parten selv som utførte handlingen eller unnlatelsen. LINK er ikke ansvarlig for Operatørers handlinger og unnlatelser.

Den Misligholdende Parten skal erstatte den skadelidte Parts økonomiske tap som følge av misligholdet, innenfor de begrensninger som er angitt i punkt 13.5.

Ingen av partene er ansvarlige overfor den annen part for mislighold som har årsak i den annen parts systemer, handlinger, uaktsomhet eller unnlatelser, eller av generelle internett- eller strømbrudd eller andre feil utenfor partens rimelige kontroll.

Ansvarsbegrensningene som gjelder I tjenesteavtalen mellom partene omfatter ansvar i denne DPA.

1. Varsler og endringer

Alle varsler i forbindelse med denne DPA skal være skriftlig (herunder e-post) og skal anses å være behørig levert eller mottatt når det er levert direkte, per post eller e-post til den andre Partens adresse som angitt på forsiden.

Ved endringer I Personvernlovgivningen, herunder dom eller uttalelse fra kompetent myndighet eller annen autoritativ kilde, som medfører en endret tolkning av Personvernlovgivningen, eller dersom det gjøres endringer i leveransen av Tjenesten som krever endringer i Databehandleravtalen, skal partene samarbeide for å oppdatere Databehandleravtalen tilsvarende.

Endringer i DPA blir kun gjeldende dersom de er skriftlige og signert av begge parter.

1. Lovvalg og verneting

Tjenesteavtalens vilkår for lovvalg, tvisteløsning og verneting gjelder dersom lokasjon er innenfor EØS. I andre tilfeller vil denne DPA styres av norsk rett, og verneting er Oslo tingrett.

.

\*\*\*

[Sted, dato]

|  |  |  |
| --- | --- | --- |
| **[Kunde]** |  | **LINK** |
| [Click and type name] |  | [Click and type name] |
| [Click and type title] |  | [Click and type title] |

Bilag: Sikkerhet

**Krav til informasjonssikkerhet**

LINK, som i henhold til Databehandleravtalen behandler Personopplysninger på vegne av Behandlingsansvarlig, skal gjennomføre egnede tekniske og organisatoriske tiltak som er fastsatt i Personvernlovgivningen og/eller tiltak pålagt av relevant tilsynsmyndighet i henhold til Personvernlovgivningen for å oppnå et egnet sikkerhetsnivå.

LINK skal vurdere egnet sikkerhetsnivå og ta hensyn til risikoene forbundet med behandlingen, herunder risiko for utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering eller tilgang til Personopplysninger som er overført, lagret eller på annen måte behandlet.

All overføring av Personopplysninger mellom Databehandler og Behandlingsansvarlig eller mellom Databehandler og en tredjepart skal gjøres ved bruk av tilstrekkelige sikkerhetstiltak, eller som avtalt mellom partene.

Dette Bilaget inneholder en generell beskrivelse av de tekniske og organisatoriske tiltak som skal iverksettes av LINK for å sikre et tilstrekkelig nivå av sikkerhet for Personopplysninger.

I den grad LINK har tilgang til slik informasjon, skal LINK gjøre generelle beskrivelser av underdatabehandleres tekniske og organisatoriske tiltak tilgjengelige for Behandlingsansvarlig, for å sikre et tilstrekkelig nivå av sikkerhet.

**Tekniske og organisatoriske tiltak**

*Fysisk tilgangsstyring*

LINK skal iverksette forholdsmessige tiltak for å hindre uautorisert fysisk tilgang til Databehandlers eiendom og lokaler hvor det oppbevares eller behandles Personopplysninger. Tiltakene skal inkludere:

* Prosedyrer og/eller fysiske systemer for tilgangskontroll, herunder vakthold
* Automatisk dørlåsing eller andre tiltak for elektroniske tilgangskontroll
* Alarmsystem, videoovervåkning eller lignende tiltak
* Loggføring av besøkende i lokalet
* ID, nøkkel eller andre krav for adgang til lokalene

*Tilgangsstyring for systemer*

LINK skal iverksette forholdsmessige tiltak for å hindre uautorisert tilgang til systemer hvor det oppbevares Personopplysninger. Tiltakene skal inkludere:

* Prosedyrer for passordbeskyttelse (herunder f.eks. krav til lengde og bruk av spesialtegn, regelmessig endring av passord etc.)
* Tilgang til systemer kreve godkjenning fra HR eller IT-administratorer
* Gjestebrukere og anonyme brukere nektes adgang til systemer
* Sentral administrasjon av systemtilgang
* Rutiner for manuell låsing av PC når man forlater arbeidsstasjon, og automatisk låsing etter maksimalt 5 minutter
* Restriksjoner på bruk av utskiftbare medier, som f.eks. minnepinner, CD/DVD eller flyttbare harddisker, samt krav til kryptering

*Tilgangsstyring for Personopplysninger*

LINK skal iverksette forholdsmessige tiltak for å hindre uautoriserte brukere tilgang til Personopplysninger som ligger det utenfor deres autorisasjon å behandle, for å hindre uautorisert tilgang, fjerning, modifikasjon eller utlevering av Personopplysninger. Tiltakene skal inkludere:

* Differensierte tilgangsrettigheter definert basert på arbeidsoppgaver
* Automatisk loggføring av brukertilgang i IT-systemer

*Kontroll over oppføring, endring etc. av Personopplysninger*

LINK skal iverksette forholdsmessige tiltak for å kontrollere og stadfeste hvorvidt og av hvem Personopplysninger har blitt ført inn i systemet, modifisert eller fjernet. Tiltakene skal inkludere:

* Differensierte tilgangsrettigheter definert basert på arbeidsoppgaver
* Automatisk loggføring av brukertilgang i IT-systemer, og regelmessig gjennomgang av sikkerhetslogger for å avdekke og følge opp potensielle sikkerhetshendelser
* Sikre at det er mulig å verifisere og stadfeste til hvilke tredjeparter Personopplysninger kan ha, eller har blitt, utlevert ved bruk av elektronisk kommunikasjonsutstyr
* Sikre at det er mulig å verifisere og stadfeste hvilke Personopplysninger som har blitt oppført i systemet, endret eller slettet, samt når og av hvem

*Kontroll over utlevering av personopplysninger*

LINK skal iverksette forholdsmessige tiltak for å hindre uautorisert tilgang, modifisering eller fjerning av Personopplysninger ved overføring. Tiltakene skal inkludere:

* Bruk av "state of the art" kryptering på all elektronisk overføring av Personopplysninger
* Kryptering ved bruk av VPN eller HTTPS for fjerntilgang, transport og kommunikasjon av Personopplysninger
* Lage revisjonsspor for all utlevering av Personopplysninger

*Tilgjengelighetskontroll*

LINK skal iverksette forholdsmessige tiltak for å sikre at Personopplysninger er beskyttet mot tilfeldig ødeleggelse eller tap. Tiltakene skal inkludere:

* Hyppig backup av Personopplysninger
* Fjernlagring
* Bruk av virusbeskyttelse/brannvegg
* Overvåkning av systemer for å avdekke virus etc.
* Sikre at funksjonsfeil/maskinfeil ikke kan medføre at lagrede Personopplysninger ødelegges
* Sikre at installerte systemer kan gjenopprettes i tilfelle av forstyrrelser
* Avbruddsfri strømtilførsel
* Prosedyrer for å sikre virksomhetskontinuitet (Business Continuity)

*Kontroll med at personopplysninger holdes atskilt*

LINK skal iverksette forholdsmessige tiltak for å sikre at Personopplysninger som er samlet inn for ulike formål, også behandles atskilt. Tiltakene skal inkludere:

* Differensierte tilgangsrettigheter definert basert på arbeidsoppgaver
* Atskilte IT-systemer

*Kontroll over underdatabehandler*

I tilfeller når underdatabehandler benyttes skal LINK iverksette forholdsmessige tiltak for å sikre at Personopplysningene behandles i tråd med den Behandlingsansvarliges instruksjoner. Tiltakene skal inkludere:

* Entydig og klar ordlyd i avtaler og andre skriftlige instruksjoner
* Overvåkning av kontraktsutførelse

*Opplæring og informasjon*

LINK skal iverksette tiltak for å sikre at alle ansatte er klar over rutiner for sikkerhet og konfidensialitet, gjennom:

* Entydig og klar regulering i arbeidsavtaler på konfidensialitet, sikkerhet og krav til etterlevelse av interne rutiner
* Interne rutiner og kursing i krav til behandling av Personopplysninger for å skape bevissthet blant ansatte

Bilag: Omfang

**Behandlingens omfang**

Denne databehandleravtalen omhandler LINKs behandling av Personopplysninger på vegne av Behandlingsansvarlig som del av LINKs leveranse av meldingstjenester til Behandlingsansvarlig. Meldingstjenestene inkluderer Behandlingsansvarliges tilgang til LINKs løsning for meldinger til mottakere valgt av Behandlingsansvarlig for formål og hyppighet som er valgt av Behandlingsansvarlig i dennes bruk av tjenestene. Avtalen gir nærmere informasjon om de spesifikke meldingstjenestene som gis til Behandlingsansvarlig under Avtalen. Ytterligere informasjon, om aktuelt: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Kategorier av registrerte**

Kategoriene av registrerte som behandles under denne databehandleravtalen defineres av Behandlingsansvarlig. Behandlingen kan omfatte behandling av Personopplysninger om Behandlingsansvarliges sluttbrukere (mottakere og/eller avsendere av meldinger, avhengig av den Behandlingsansvarliges bruk av tjenestene under Avtalen). Ytterligere informasjon, om aktuelt: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Typen personopplysninger**

Behandlingen omfatter følgende kategorier av Personopplysninger, avhengig av den Behandlingsansvarliges konkrete bruk av Tjenesten:

* Alminnelige Personopplysninger, herunder navn, kontaktopplysninger slik som e-postadresse, telefonnummer etc.
* Lokasjonsdata, herunder GPS- og Wifi-lokasjonsdata, samt lokasjonsdata hentet fra LINKs nettverk. (som ikke er trafikkdata)
* Trafikkdata, herunder Personopplysninger som behandles i relasjon til formidling av kommunikasjon på et elektronisk kommunikasjonsnettverk eller fakturering av slike tjenester.
* Opplysninger relatert til innholdet i kommunikasjon, slik som e-post, telefonsvar, SMS/MMS, nettleserdata etc.

Spesielle kategorier av Personopplysninger, herunder opplysninger som avslører rasemessig eller etnisk opprinnelse, politisk oppfatning, religiøs- eller filosofisk overbevisning, fagforeningsmedlemskap og helseopplysninger, vil bli behandlet under denne avtale dersom Kunde benytter tjenestene til å behandle slike personopplysninger

**Gjenstand for behandlingen**

Behandlingens gjenstand er den levering av tjenester fra LINK til Kunde som følger av hovedavtalen, og som krever behandling av personopplysninger. Personopplysninger vil bli behandlet som beskrevet i Avtalen. Ytterligere informasjon, om aktuelt: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Behandlingens varighet**

Behandlingens varighet er den samme som Avtalens varighet. LINK sletter personopplysninger når det ikke lenger er nødvendig å behandle dem for å levere tjenestene under hovedavtalen.

**Behandlingens art**

Personopplysninger behandles ved at Kunde legger personopplysninger inn på LINKs plattform, enten direkte gjennom egen tilgang til plattformen, eller gjennom oversendelse av personopplysninger til LINK ansatt for innlegging på Kundes område. Personopplysningene vil videre bli behandlet for at meldinger skal kunne bli formidlet og mottakerregister korrekt som definert av Kunde, før prosessen med å sende meldinger initieres. Ytterligere informasjon, om aktuelt: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Behandlingens formål**

Formålet med å engasjere LINK for å behandle personopplysninger på vegne av Kunde er Kundes behov for kommunikasjon med sluttbrukere definert av Kunde.

**Underdatabehandlere**

Underdatabehandlere som er godkjent under denne databehandleravtalen er beskrevet i [LINK Mobility sub-processors list - LINK Mobility International](https://linkmobility.com/list/). Denne Databehandleravtalen er å anse som en instruksjon fra Kunde om å overføre Personopplysninger til de beskrevne underdatabehandlere.

**Standard contractual clauses (SCC) Appendix**

***(As per COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021***

***on standard contractual clauses for the transfer of personal data to third countries pursuant to***

***Regulation (EU) 2016/679 of the European Parliament and of the Council)***

**between**

**LINK, and its affiliates established within EEA**

hereinafter “data exporter”

**and**

**The Customer (MODULE FOUR) or the respective Sub-processor in Third Country (MODULE THREE)**

hereinafter “data importer”

The SCC text is found at: [Publications Office (europa.eu)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN)

**The Data exporter and Data importer enter into SCC with the following modules:**

* **MODULE ONE: Transfer controller to controller: No**
* **MODULE TWO: Transfer controller to processor: No**
* **MODULE THREE: Transfer processor to processor: \_Yes (in case of a sub-processor in Third Country) / No (in case of Customer in Third Country)**
* **MODULE FOUR: Transfer processor to controller: \_Yes (in case of Customer in Third Country) / No (in case of a sub-processor in Third Country)**

**Specifications required for each applicable module follow below:**

**Specifications relevant to MODULE THREE: Transfer processor to processor**

**Clause 7 – The Parties agree that this clause shall be included:**

Docking clause (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A. (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A. (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**Clause 9– The Parties agree that Option 2 part of the clause shall apply to them:**

[OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 3 months in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).]

**Clause 11– The Parties agree that this optional part of the clause shall not be included:**

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

**Clause 17 – The Parties agree that Option 1 part of the clause shall apply to them:**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the state in which the data exporter is established.]

* When the data exporter is based in Switzerland the Parties agree these Clauses shall be governed by the law of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

**Clause 18:**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the state in which the data exporter is established.

* When the data exporter is based in Switzerland the Parties agree that any dispute arising from these Clauses shall be resolved by the courts of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

The Parties agree that the term ’member state’ must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

**Specifications relevant to MODULE FOUR: Transfer processor to controller**

**Clause 7 – The Parties agree that this clause shall be included:**

Docking clause (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A. (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A. (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**Clause 11 – The Parties agree that this optional part of the clause shall not be included:**

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

**Clause 17:**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the state in which the data exporter is established.

* When the data exporter is based in Switzerland the Parties agree these Clauses shall be governed by the law of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

**Clause 18:**

Any dispute arising from these Clauses shall be resolved by the courts of the state in which the data exporter is established.

* When the data exporter is based in Switzerland the Parties agree that any dispute arising from these Clauses shall be resolved by the courts of:
  + Switzerland (when the data transfer is exclusively subject to the FADP)
  + Norway (when the data transfer is subject to both the FADP and the GDPR)

**ANNEX I**

**A. LIST OF PARTIES**

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: [LINK Mobility xx] and its affiliates as listed in the “Subsidiary companies” section on LINK Mobility sub-processors list - LINK Mobility International (https://linkmobility.com/list/)..

Address: [address of LINK Mobility xx] and its affiliates’ addresses as listed in the “Subsidiary companies” section on LINK Mobility sub-processors list - LINK Mobility International (https://linkmobility.com/list/).

Contact person’s name, position and contact details:

* Jan Wieczorkiewicz, DPO
* +48601690816
* jan.wieczorkiewicz@linkmobility.com

Activities relevant to the data transferred under these Clauses: provision/use of communication services towards recipients

Signature and date: . . . . . . . . . . [signature by person(s) who is/are authorized to sign for all entities listed]

Role (controller/processor): processor(s).

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

**Specifications relevant to MODULE THREE: Transfer processor to processor**

1. Name: [name of Sub-processor in Third Country]

Address: : [address of Sub-processor in Third Country].

Contact person’s name, position and contact details: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Activities relevant to the data transferred under these Clauses: provision/use of communication services towards recipients

Signature and date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Role (controller/processor): controller

**Specifications relevant to MODULE FOUR: Transfer processor to controller**

2. Name: [name of Customer]

Address: : [address of Customer]

Contact person’s name, position and contact details: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Activities relevant to the data transferred under these Clauses: provision/use of communication services towards recipients

Signature and date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Role (controller/processor): processor

**B. DESCRIPTION OF TRANSFER**

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

* Regarding MODULE THREE:
  + The categories defined by data exporter’s Customer. The processing involves processing of personal data related to end-users of data exporter’s Customer (recipients and/or senders of messages depending on the data exporter’s Customer use of the services under the applicable service agreement).
* Regarding MODULE FOUR:
  + The categories defined by data importer/controller. The processing involves processing of personal data related to data importer’s/controller's end-users (recipients and/or senders of messages depending on the importer’s/controller's use of the services under the applicable service agreement).

Categories of personal data transferred

The personal data transferred concern the following categories of data:

* Basic Personal Data, such as name, contact details such as email, phone number etc.
* Location data, such as GPS, Wi-Fi location data and location data derived from data exporter's network (that is not traffic data as defined below).
* Traffic data: personal data processed in relation to the conveyance of communication on an electronic communications network or billing thereof.
* Data related to content of communication, such as e-mails, voice mails, SMS/MMS, browsing data etc.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

* If applicable to the specific service - special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

* continuous basis

Nature of the processing

* Regarding MODULE THREE:
  + Personal data will be processed by data exporter’s Customer entering the data into data exporter’s or data importer’s platform, either through its access to said platform, or by providing data to data exporter’s or data importer’s employees in order for them to enter data to the data exporter’s Customer’s area of the platform. The processing includes deriving statistical data related to the provision of the services – such as delivery statuses and other information prescribed under the service contract between data exporter and data exporter’s Customer. The data will further be processed in order for messages to be set up as required by data exporter’s Customer, and the list of recipients to be correct, before the process for sending the defined messages to the defined recipients is initiated.
* Regarding MODULE FOUR:
  + Personal data will be processed as a result of entering the data by data importer or data importer’s client into data exporter’s platform, either through its access to said platform, or by providing data to data exporter’s employees in order for them to enter data to the data importer or data importer’s client’s area of the platform. The processing includes deriving statistical data related to the provision of the services – such as delivery statuses and other information prescribed under the service contract between data exporter and data importer. The data will further be processed in order for messages to be set up as required by data importer or data importer’s client, and the list of recipients to be correct, before the process for sending the defined messages to the defined recipients is initiated.

Purpose(s) of the data transfer and further processing

* Regarding MODULE THREE:
  + Fulfillment of data exporter’s Customert’s requirements for communication towards recipients.
* Regarding MODULE FOUR:
  + Fulfillment of data importer or data importer’s client’s requirements for communication towards recipients.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

* The processing will continue for the duration of data importer’s contract with data exporter. Personal Data shall be retained for as long as it is necessary to fulfil the purposes for processing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

* As described respectively above.

**C. COMPETENT SUPERVISORY AUTHORITY**

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

* The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 is the one competent in the state in which the data exporter is established
* When the data exporter is based in Switzerland the parties establish a parallel supervision:
  + The Federal Data Protection and Information Commissioner (FDPIC), insofar as the data transfer is governed by the FADP
  + The Norwegian Data Protection Authority, insofar as the data transfer is governed by the GDPR