

Databehandleravtale for NLF-medlemmer

I henhold til Europa-parlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 (heretter GDPR) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale

mellom

Medlem / kunde av NLF:

.....
som behandlingsansvarlig

og

Norges Lastebileier-Forbund

som databehandler

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til GDPR om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

Avtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Avtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med behandlingsansvarlig sin bruk av egne sider på lastebil.no, heretter kalt *Min Side*.

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av *Min Side*.

2. Instruksjer

Databehandler skal følge de skriftlige instruksjer for forvaltning av personopplysninger i *Min Side* som behandlingsansvarlig har bestemt skal gjelde.

Databehandler forplikter seg til å overholde alle plikter i henhold til GDPR som gjelder ved bruk av *Min Side* til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instruksjer fra behandlingsansvarlig som er i strid med bestemmelsene i GDPR.

3. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å levere og administrere *Min Side*.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av *Min Side* uten at dette på forhånd er godkjent av behandlingsansvarlig. Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av *Min Side*:

På bedriften sitt område på lastebil.no kan en bedrift velge å registrere ansatte, ansattes pårørende, arbeidskontrakter og annen dokumentasjon med personlige opplysninger.

Slik informasjon er i utgangspunktet tilgjengelig for:

- Den ansatte
- De personer i bedriften som av bedriften er gitt innsyn i personopplysninger ("personalansvar")

Som et minimum lagres navn, epost, mobil og adresse. Bedriften kan velge om det lagres fødselsdato, sertifikater, avtaler med mere. Bedriften kan også bruke sin side på lastebil.no til å sende informasjon fra bedriften til sine ansatte – via epost, NLF sin WebApp eller sms.

5. Eierskap og behandlingsansvar

Behandlingsansvarlig er ansvarlig for data som lagres og behandles ved bruk av databehandler sine tjenester, og har eierskap til disse dataene.

Behandlingsansvarlig forutsettes å ha hjemmel til å behandle disse dataene gjennom ansettelsesavtale eller lignende, i henhold til gjeldende lover og forskrifter.

Det er behandlingsansvarlig som i første hånd er ansvarlig for å sikre disse opplysningene mot innsyn, mens databehandler forestår den tekniske sikkerheten.

6. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretagelse av den registrertes rettigheter, jf. GDPR, kapittel III, Artikkel 13 til 23.

Den registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

7. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivarettatt.

Databehandler skal dokumentere opplæringen av egne ansatte i informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

8. Taushetsplikt

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Taushetsplikten omfatter ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere eller administrere *Min Side*.

9. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til GDPR, Artikkel 5 nr.1 bokstav f og Artikkel 32-36. Databehandler plikter å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i denne avtalen.

Ansatte hos behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

10. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ubegrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

Varslet til behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet.

11. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører til *Min Side* som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med levering og administrasjon av *Min Side*.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen. Databehandler plikter å forelegge avtalene for behandlingsansvarlig etter forespørsel.

Databehandler skal kontrollere at underleverandører til *Min Side* overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for økonomiske tap som påføres behandlings- ansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører til *Min Side*.

12. Overføring til land utenfor EU/EØS

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig vil ikke bli overført til land utenfor EU/EØS (tredjeland).

13. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten i *Min Side*.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene. Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene.

Databehandler skal bistå behandlingsansvarlig dersom bruk av *Min Side* medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før *Min Side* tas i bruk, jf. GDPR, Artikkel 35 og 36. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernforebyggende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

14. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av *Min Side*. Databehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig.

Kostnad for sletting bæres av Databehandler.

Backup-kopier som er tatt som en del av systemets drift vil kunne ligge lagret i inntil to uker før de automatisk slettes.

Behandlingsansvarlig har selv mulighet på *Min Side* til å ta ut informasjon for tilbakelevering av personopplysninger, for hver person som er registrert av Behandlingsansvarlig. Etter behandlingsansvarliges ønske vil databehandler kunne bistå med dette, eventuell kostnad for dette bæres av Behandlingsansvarlig.

15. Mislighold

Ved mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 13 ovenfor.

16. Avtalens varighet

Denne avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig.

17. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til databehandlers adresse.

18. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.

Denne avtale er i to – 2 – eksemplarer, hvorav partene har hvert sitt.

.....
Sted og dato

På vegne av behandlingsansvarlig

På vegne av databehandler

.....
(underskrift)

.....
(underskrift)