FORSVARET
Forsvarets logistikkorganisasjon

2023034158 – TSA for Fly-drivstoff

Bilag 13
Informasjonssikkerhet og personopplysningsvern

1 Informasjonssikkerhet og personopplysningsvern

1.1 Informasjonssikkerhet

Leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav til informasjonssikkerhet i forbindelse med gjennomføring av tjenesten. Dette innebærer at Leverandøren skal iverksette forholdsmessige tiltak for å sikre konfidensialitet av Oppdragsgivers data samt tiltak for å sikre at data ikke kommer på avveie. Videre skal Leverandøren iverksette forholdsmessige tiltak mot utilsiktet endring og sletting av data samt mot angrep av virus og annen skadevoldende programvare.

Dersom Oppdragsgiver har nærmere krav til hvorledes informasjonssikkerheten skal ivaretas fra Leverandørens side, skal Oppdragsgiver angi dette i Bilag 2 som svar til Bilag 1 (Kravspesifikasjon).

Leverandøren plikter å holde Oppdragsgivers data atskilt fra eventuelle tredjeparters data for å redusere faren for beskadigelse av data og/eller innsyn i data. Med atskilt forstås at nødvendige tekniske tiltak som sikrer data mot uønsket endring og innsyn, er iverksatt og opprettholdt. Som uønsket endring og innsyn anses også tilgang fra ansatte hos Leverandøren eller andre som ikke har behov for informasjonen i sitt arbeid for Oppdragsgiver.

Dersom Oppdragsgiver har nærmere krav til hvorledes Leverandøren skal ivareta kravet til atskillelse av data, skal Oppdragsgiver angi dette i Bilag 1 (Kravspesifikasjon).

Leverandøren skal påse at leverandører av tredjepartsleveranser foretar tilstrekkelig og nødvendig sikring av Oppdragsgivers data.

Dersom Oppdragsgiver har nærmere krav til hvorledes Leverandøren skal påse at leverandør(er) av tredjepartsleveranser foretar tilstrekkelig og nødvendig sikring av Oppdragsgivers data, skal Oppdragsgiver angi dette i Bilag 1 (Kravspesifikasjon).

1.2 Krav til sikkerhet i informasjonssystemer

For å redusere risikoen for digitale hendelser skal Leverandøren etablere hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak for å forebygge, avdekke og redusere konsekvensene av digitale hendelser. Tiltakene skal samlet sørge for et forsvarlig sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå skal det blant annet ses hen til den teknologiske utviklingen, sikkerheten i Leverandørens systemer/utstyr/anlegg, Leverandørens kapasitet/beredskap ved hendelseshåndtering samt Leverandørens tiltak for overvåkning, revisjon og testing av nettverk og informasjonssystemer. *(For veiledning se NSMs grunnprinsipper for IKT-sikkerhet på* www.nsm.no*).*

Dersom Leverandørens informasjonssystemer er skjermingsverdige etter sikkerhetsloven kapittel 6, skal de sikres etter og i medhold av bestemmelsene i denne loven.

1.3 Varsling av cyberhendelser

Leverandøren skal uten ugrunnet opphold varsle om cyberhendelser i Leverandørens nettverk, informasjonssystemer eller sikkerhetsløsninger som har eller kan ha en vesentlig betydning for

(i) Leverandørens leveranser til Forsvaret,

(ii) behandling av informasjon om Forsvaret, eller
(iii) den generelle sikkerheten i Leverandørens nettverk eller informasjonssystemer.

Varslingen skal skje til Cyberforsvarets cybersikkerhetssenter (MILCERT), med kopi til NSM Nasjonalt cybersikkerhetssenter (NCSC), i den form som følger av eget skjema utlevert i forbindelse med oppstartsmøte.

Leverandøren skal påse at tilsvarende bestemmelser inkluderes i avtaler med Leverandørens underleverandører som direkte og for en vesentlig del medvirker til gjennomføring av Leverandørens kontraktsforpliktelser, eller som har tilgang til sensitiv informasjon om Forsvaret gjennom sitt oppdrag for Leverandøren.

1.4 Personopplysningsvern

Dersom Leverandøren ved utførelsen av tjenesten skal behandle personopplysninger, skal Leverandøren i besvarelsen til Bilag 1 Kravspesifikasjon beskrive hvordan tilfredsstillende behandling i tråd med personopplysningsregelverket skal oppnås og gjennomføres. Dette omfatter blant annet krav til innebygget personvern. Dette gjelder uavhengig av om Oppdragsgiver har stilt krav om dette i Bilag 1.

Leverandøren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av personopplysninger. Dersom Oppdragsgiver har nærmere krav knyttet til Leverandørens informasjonssikkerhetstiltak, skal Oppdragsgiver angi dette i Bilag 6.

Leverandøren skal dokumentere at informasjonssystemene og sikkerhetstiltakene er tilfredsstillende. Dokumentasjonen skal på forespørsel være tilgjengelig for Oppdragsgiver og dennes revisorer, samt for Datatilsynet og Personvernnemnda. Dersom Oppdragsgiver har nærmere dokumentasjonskrav knyttet til informasjonssystemet og sikkerhetstiltakene, skal Oppdragsgiver angi dette i Vedlegg F. Dersom Oppdragsgiver ber om informasjon for å gjennomføre vurdering av personvernkonsekvenser («Data Protection Impact Assessments»), skal Leverandøren bistå med å fremskaffe slik informasjon.

Leverandøren kan ikke overlate personopplysninger til andre for lagring, bearbeidelse eller sletting uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra Oppdragsgiver. Dersom det er innhentet særlig eller generell skriftlig tillatelse, skal Leverandøren underrette Oppdragsgiver om eventuelle planer om å benytte andre databehandlere eller utskiftning av databehandlere, og dermed gi Oppdragsgiver muligheten til å motsette seg slike endringer. Underleverandører som er godkjent av Oppdragsgiver skal fremgå av Bilag 6 (Administrative bestemmelser).

Personopplysninger skal ikke overføres til land utenfor EØS-området uten overføringsgrunnlag og dokumentasjon som påviser at vilkårene for å benytte overføringsgrunnlaget er oppfylt. Leverandøren skal i et slikt tilfelle dokumentere dette i Bilag 2 som svar til Bilag 1 (Kravspesifikasjon).

Dersom oppdraget går ut på å behandle personopplysninger på vegne av Oppdragsgiver, plikter Oppdragsgiver og Leverandøren å inngå en databehandleravtale i samsvar med personopplysningslovgivningen, se Bilag 1 (Kravspesifikasjon). Databehandleravtale må være inngått før behandlingen av personopplysninger påbegynnes.

Partenes erstatningsansvar for skade som rammer den registrerte eller andre fysiske personer og som skyldes overtredelse av personvernforordningen (forordning 2016/679), personopplysningsloven med forskrifter eller annet regelverk som gjennomfører personvernforordningen, følger bestemmelsene i personvernforordningen artikkel 82. Erstatningsbegrensningen i punkt 10 kommer ikke til anvendelse for ansvar som følger av personvernforordningen artikkel 82.

Partene er hver for seg ansvarlige for overtredelsesgebyr ilagt i henhold til personvernforordningens art. 83.