Personvernpolicy

Innhold

1. INTRODUKSJON

1.1 Formål

Denne Personvernpolicyen gjelder for Forsvarets forum og fungerer som en manual for vår behandling av personopplysninger i samsvar med EUs personvernforordning (**GDPR**) og gjeldende nasjonal personvernlovgivning.

Begrepene brukt i dette dokumentet skal ha samme betydning som i GDPR.

Denne Personvernpolicyen består av to deler:

- **Del 1 - Styrende del:** Intern organisering av personvern i virksomheten og våre grunnleggende personvernprinsipper
- **Del 2 - Gjennomførende del:** Rutiner for implementering av personvern i vår virksomhet

1.2 Versjoner

Dato	Versjon	Ansvarlig
1. august 2024	1.0	Paal Ravnaas

2. DEL 1 - STYRENDE DEL

2.1 Oversikt over Forsvarets forums behandling av personopplysninger

Vi behandler personopplysninger som behandlingsansvarlig for abonnenter på vårt magasin, mottakere av vårt nyhetsbrev, kontaktpersoner hos våre leverandører, bedriftskunder og samarbeidspartnere, besøkende på vår nettside og våre sosiale medier, besøkende til våre lokaler, samt jobbsøkere og våre medarbeidere (ansatte i Forsvaret som jobber hos oss).

2.2 Fordeling av roller og ansvar i virksomheten

Forsvarets forum er ansvarlig for å sikre at denne Personvernpolicyen er implementert i virksomheten og at de ansatte er kjent med innholdet i den.

Redaktøren har det operative ansvaret for at denne Personvernpolicyen etterleves for behandling av personopplysninger knyttet til HR (tidligere og nåværende ansatte, samt jobbsøkere).

Personvernansvarlig har det operative ansvaret for at denne Personvernpolicyen etterleves for behandling av personopplysninger knyttet til alt annet enn HR.

Redaktøren har det operative ansvaret for IT-sikkerhet.

Ovennevnte personer skal møtes minst en gang i kvartalet for å diskutere virksomhetens personvern og etterlevelse av denne Personvernpolicyen.

2.3 Personvernombud

Forsvarets forum har ikke utpekt et eget personvernombud. Vi er på nåværende tidspunkt ikke forpliktet til å utpeke et personvernombud etter GDPR artikkel 37. Vi støtter oss på Forsvarets

personvernombud og personvernombudet i Forsvarets fellestjenester. Rutinen vil være å møtes ved revisjoner og endringer.

2.4 Revisjon

Vi vil gjennomgå vår etterlevelse av denne Personvernpolicyen minst én gang i året. Blant annet vil vi da påse at følgende gjennomgås og om nødvendig oppdateres:

- Vår protokoll over behandlingsaktiviteter
- Våre personvernerklæringer
- Vår cookieerklæring
- Våre databehandleravtaler
- Våre risikovurderinger

Den eller de i Forsvarets forum som er tillagt det operative ansvaret (se pkt. 2.2 ovenfor), skal årlig avgi en rapport til Forsvarets fellestjenester (FFT) om etterlevelse av denne Personvernpolicyen. Dessuten skal FFT omgående orienteres om forhold som i vesentlig grad bryter med denne Personvernpolicyen.

2.5 Prinsipper for behandling av personopplysninger

Vi vil behandle personopplysninger i samsvar med personvernprinsippene i GDPR artikkel 5, herunder følgende:

Prinsipp	Definisjon	Eksempler på hvordan vi overholder prinsippene
Dataminimering	Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.	1. Vi vil ikke samle inn personopplysninger som vi ikke har behov for. 2. Vi vil begrense bruken av personopplysninger i dokumenter som vi produserer.
Riktighet	Personopplysninger skal være korrekte og om nødvendig oppdaterte.	1. Vi vil kontrollere innsamlede opplysninger hvis vi har grunn til å tro at opplysningene er uriktige. 2. Vi vil korrigere lagrede personopplysninger hvis vi har grunn til å tro at opplysningene er utdaterte.
Lagringsbe-grensning	Personopplysninger skal ikke lagres i lengre perioder enn det som er nødvendig for formålene de behandles for.	1. Vi vil etablere bestemte lagringstider. 2. Vi vil slette og anonymisere personopplysninger når lagringstiden er utløpt.
Integritet og konfidensialitet	Personopplysninger skal beskyttes mot uautorisert og ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade.	1. Vi vil iverksette tekniske og organisatoriske tiltak som gir egnet sikkerhet for personopplysningene. 2. Vi vil benytte systemer tilpasset den tekniske utviklingen og sørge for at leverandørene vi benytter også har et tilfredsstillende sikkerhetsnivå.

Prinsipp	Definisjon	Eksempler på hvordan vi overholder prinsippene
Ansvar	Enhver behandlingsansvarlig er ansvarlig for og skal kunne påvise overholdelse av personvernlovgivningen.	1. Vi vil dokumentere våre retningslinjer og rutiner for personvern. 2. Vi vil kontrollere overholdelse av våre retningslinjer og rutiner.

3. DEL 2 - GJENNOMFØRENDE DEL

3.1 Protokoll over behandlingsaktiviteter (GDPR art. 30)

Vi skal føre en "Protokoll over behandlingsaktiviteter". Protokollene vil revideres årlig og oppdateres når virksomheten gjennomgår endringer.

Behandlingsprotokollen skal som et minimum inneholde informasjon om: (i) den behandlingsansvarlige, (ii) formålet med behandlingen, (iii) en beskrivelse av de registrerte og kategoriene av personopplysninger, (iv) kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, (v) dersom personopplysninger blir overført til en tredjestat utenfor EØS eller en internasjonal organisasjon; en beskrivelse av denne tredjestaten eller den internasjonale organisasjonen og dokumentasjon på nødvendige garantier, (vi) de planlagte tidsfristene for lagring og sletting av personopplysningene, og (vii) en generell beskrivelse av personopplysningssikkerheten.

3.2 Behandlingsgrunnlag

3.2.1 Generelt

Vi kan bare behandle personopplysninger i den utstrekning vi har et behandlingsgrunnlag. De behandlingsgrunnlagene vi baserer oss på er angitt i vår "Protokoll over behandlingsaktiviteter".

I pkt. 3.2.2 og 3.2.3 nedenfor følger en generell oversikt over vår tilnærming til behandlingsgrunnlag.

3.2.2 "Alminnelige" personopplysninger (GDPR art. 6)

Vi vil som regel basere oss på ett av følgende behandlingsgrunnlag:

- *Avtale* – Behandlingen er nødvendig for å inngå eller oppfylle en avtale med den registrerte. Eksempel: For å håndtere en abonnementsavtale .
- *Lovkrav* – Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse. Eksempel: Innsamling og lagring av opplysninger for bokføringsformål.
- *Berettiget interesse* – Behandlingen er nødvendig for å oppnå en berettiget interesse som overstiger den registrertes rett til personvern. Eksempel: Bruk av personopplysninger for å følge opp virksomhetskunder og leverandører.
- *Samtykke* – Den registrerte har gitt sitt frivillige, spesifikke, informerte og dokumenterte samtykke til behandlingen. Eksempel: For markedsføringsformål (se pkt. 3.5 nedenfor).

3.2.3 Særlige kategorier av personopplysninger (GDPR art. 9 og 10)

Ved behandling av særlige kategorier av personopplysninger vil vi utvise særlig forsiktighet. Særlige kategorier av personopplysninger er opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person,

helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, samt opplysninger om straffedommer og lovovertredelser.

Vi vil kun behandle slike særlige kategorier av personopplysninger dersom det er påkrevd for å utføre visse bestemte behandlingsaktiviteter, og vil i så tilfelle typisk basere oss på ett av følgende behandlingsgrunnlag (i tillegg til de alminnelige behandlingsgrunnlagene i GDPR art. 6):

- *Arbeidsrettslige forpliktelser* – Behandlingen er nødvendig for å kunne oppfylle forpliktelser og utøve særlige rettigheter på området arbeidsrett.

3.3 Formålsbegrensning

Vi kan bare behandle personopplysninger for spesifikke, uttrykkelige, angitte og legitime formål. Formålene med vår behandling fremgår av vår "Protokoll over behandlingsaktiviteter".

Vi skal sørge for at personopplysningene ikke behandles på en måte som er uforenlig med det opprinnelige formålet som opplysningene ble samlet inn for. Basert på en konkret vurdering fra sak til sak vil følgende formål typisk ikke være uforenlig med det opprinnelige formålet: bokføring, revisjon, etterforskning, tvisteløsning, analyser og rapportering, innovasjon og forretningsutvikling, samt virksomhetsoverdragelser.

3.4 Lagring og sletting av personopplysninger (GDPR art. 5)

Vi kan bare lagre personopplysninger så lenge det er nødvendig. De planlagte lagringstidene for de ulike kategoriene av personopplysninger vil fremgå av vår "Protokoll over behandlingsaktiviteter" og vår "Rutine for lagring og sletting". Her vil vi også gi en kort begrunnelse for de angitte lagringstidene.

Vi vil kunne ta i bruk følgende slettemetoder: Automatisk sletting, manuell sletting eller anonymisering. Hvis vi velger manuell sletting, vil vi sørge for at den blir utført på årlig basis.

Vi vil sørge for at databehandlere som lagrer personopplysninger på våre vegne overholder de lagringstidene som vi har etablert. Vi kan videre kreve at hver databehandler sletter eller tilbakeleverer personopplysninger til oss etter at tjenestene som behandlingen knytter seg til er levert.

3.5 Markedsføring (GDPR art. 6 og art. 21, markedsføringsloven § 15)

Vår markedsføringskommunikasjon, herunder utsendelse av nyhetsbrev og arrangementsinvitasjoner, må være i overensstemmelse med GDPR og relevant markedsføringslovgivning.

Vi vil ikke sende markedsføringskommunikasjon pr. e-post eller SMS med mindre:

- vi har mottakers samtykke, eller
- vi har et eksisterende/løpende kundeforhold (som gir oss muligheten til å basere vår behandling av personopplysninger på berettiget interesse fremfor den registrertes samtykke).

Vi vil alltid gi mottaker anledning til å melde seg av vår markedsføringskommunikasjon (opt-out/unsubscribe).

Vi utfører for øyeblikket ikke profilering (vurdering av visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons interesser etc.) for markedsføringsformål. Dersom vi planlegger å gjøre det, vil vi først vurdere om lovgivningen krever at vi innhenter samtykker for dette.

3.6 Bruk av cookies (GDPR art. 6 og ekomloven § 2-7(b)

Vi benytter cookies på nettsidene våre forsvaretsforum.no. For å overholde gjeldende regelverk har vi publisert en cookieerklæring på nettsiden(e). Vi vil innhente samtykke til bruk av cookies fra de besøkende i den grad dette er påkrevd, og ellers respektere deres nettleserinnstillinger. *Nødvendige cookies* vil vi imidlertid benytte uavhengig av de besøkendes innstillinger.

3.7 Informasjon og åpenhet (GDPR art. 12 – 14)

Vi skal behandle personopplysninger på en åpen og transparent måte. Vi vil på et klart og enkelt språk gi de registrerte informasjon om hvem vi behandler personopplysninger om, hvem vi er, hvorfor vi behandler deres personopplysninger og hvordan behandlingen utføres.

Forsvaret har en "Personvernerklæring" for ansatte, som alle ansatte i Forsvaret har tilgang til.

Vi har også publisert en "Personvernerklæring (ekstern)" på våre nettsider forsvaretsforum.no med informasjon til personer utenfor vår egen virksomhet som vi behandler personopplysninger om.

3.8 De registrertes rettigheter (GDPR art. 12 og art. 15 – 23)

Vi skal respektere de registrertes rettigheter etter GDPR. Dersom vi mottar en forespørsel fra en registrert om å utøve sine personvernrettigheter, skal denne forespørselen håndteres i samsvar med vår "Rutine for håndtering av forespørsler fra de registrerte".

3.9 Innebygd personvern og personvern som standardinnstilling (GDPR art. 25)

Innebygd personvern – På tidspunktet når vi bestemmer hvilke systemer, verktøy og virkemidler vi skal bruke for vår behandling av personopplysninger, og på tidspunktet for selve behandlingen, vil vi iverksette egnede tiltak med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger (se pkt. 2.5 over). Hvis vi ber andre tjenesteleverandører om å utføre systemutvikling eller tilpasning av våre verktøy, skal vi kreve at også disse sørger for å ta tilstrekkelig hensyn til personvernet.

Personvern som standardinnstilling – Vi skal sørge for at innstillingene i våre systemer, verktøy og virkemidler er forhåndsinnstilt på en personvernvennlig måte. Blant annet skal vi etterstrebe standardinnstillinger som innebærer at opplysningene som samles inn begrenses til "need to have", at tilgangen begrenses til "need to know", og at opplysningene slettes så snart vi ikke har behov for dem.

3.10 Databehandleravtaler (GDPR art. 28)

3.10.1 Når vi opptrer som behandlingsansvarlig

Før vi engasjerer en databehandler (en tredjepart som behandler personopplysninger på vegne av oss), vil vi gjøre to ting:

Først vil vi gjøre en vurdering av om databehandleren gir oss tilstrekkelig trygghet for at den vil behandle personopplysningene i samsvar med kravene etter GDPR. Dette kan blant annet gjøres i form av en risikovurdering basert på leverandørens sikkerhetsdokumentasjon.

Så vil vi inngå en databehandleravtale ("**DPA**") med databehandleren. DPAen vil kunne utgjøre et vedlegg til en annen avtale som er inngått mellom oss og databehandleren. Vi kan benytte databehandlerens DPA-mal forutsatt at denne oppfyller alle krav etter GDPR art. 28(3).

3.10.2 Når vi opptrer som databehandler

Hvis vi behandler personopplysninger på vegne av andre, uten å bestemme formålet med behandlingen og hvilke midler som skal benyttes, opptrer vi som databehandler.

Om vi opptrer som databehandler, skal vi sørge for å inngå en DPA med den behandlingsansvarlige. I så fall vil vi unngå å bruke personopplysningene for våre egne formål, samt sørge for at slike opplysninger ikke er lagret sammen med andre opplysninger vi behandler.

3.11 Internasjonal overføring av personopplysninger (GDPR kap. V)

Overføring av personopplysninger til land utenfor EØS (med unntak av noen land, opplistet her), er i utgangspunktet forbudt etter GDPR. "Overføring" innebærer både at virksomheter utenfor EØS lagrer våre personopplysninger, og at virksomheter utenfor EØS remotely får tilgang til våre personopplysninger (selv om de er lagret innenfor EØS).

Vi overfører per i dag ikke personopplysninger til land utenfor EØS. Hvis vi likevel i framtiden skal overføre personopplysninger til land utenfor EØS, vil vi sørge for at det foreligger nødvendige garantier i henhold til GDPR, for eksempel at vi inngår EUs standardklausuler (Standard Contractual Clauses, SCCs) med virksomheten utenfor EØS. Vi vil også vurdere om tiltakene som er innført sikrer et beskyttelsesnivå for personopplysningene som er tilnærmet likt som i EØS.

3.12 Personopplysningssikkerhet (GDPR art. 32)

Vi skal sørge for at vi behandler personopplysninger på en sikker måte, blant annet ved hjelp av følgende tiltak:

Sikkerhetskrav	Definisjon	Hvordan vi oppfyller sikkerhetskravet
Konfidensialitet	Beskyttelse mot uautorisert tilgang og utlevering av personopplysninger.	1. Våre ansatte og samarbeidspartnere vil være underlagt tilfredsstillende konfidensialitetsforpliktelser. 2. Våre systemer vil være kryptert og underlagt tilfredsstillende tilgangskontroll. 3. Våre avtaler med IT-leverandører vil inneholde forpliktelser om personopplysningssikkerhet. 4. Våre fysiske fasiliteter vil være tilstrekkelig beskyttet mot uautorisert tilgang.
Integritet	Beskyttelse mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.	1. Våre systemer vil være kryptert og underlagt tilfredsstillende tilgangskontroll. 2. Viktige dokumenter vil ha versjonskontroll (revisjonskontroll).
Tilgjengelighet	Personopplysningene er tilgjengelige for autoriserte ved behov.	1. Våre avtaler med sentrale IT-leverandører vil ha tilfredsstillende SLAer. 2. Våre viktigste systemer vil være tilgjengelige ved bruk av fjerntilgang (VPN eller liknende).
Robusthet	Behandlingssystemene og -tjenestenes evne til å gjenopprette normaltilstand.	1. Våre avtaler med sentrale IT-leverandører vil ha tilfredsstillende SLAer.

Sikkerhetskrav	Definisjon	Hvordan vi oppfyller sikkerhetskravet
		2. Vi vil ha sikkerhetskopi (backup) av våre personopplysninger.

Vi vil dokumentere våre sikkerhetstiltak, for eksempel ved å gjennomføre risikovurderinger. Dokumentasjonen skal vedlikeholdes, for eksempel ved å foreta oppdateringer dersom vi gjør vesentlige endringer i våre IT-systemer eller fasiliteter.

3.13 Brudd på personopplysningssikkerheten (GDPR art. 33 og art. 34)

Vi vil potensielt kunne oppleve et brudd på personopplysningssikkerheten (sikkerhetsbrudd). Ethvert sikkerhetsbrudd skal håndteres i samsvar med vår "Rutine for håndtering av sikkerhetsbrudd".

3.14 Vurdering av personvernkonsekvenser (GDPR art. 35)

Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for de registrertes rettigheter og friheter, vil vi før behandlingen foreta en vurdering av hvilke personvernkonsekvenser den planlagte behandlingen vil ha (DPIA).

En DPIA må i det minste inneholde (i) en systematisk beskrivelse av den planlagte behandlingsaktiviteten, (ii) en vurdering av nødvendighet og forholdsmessighet, (iii) en vurdering av risiko for de registrertes rettigheter og friheter, og (iv) en beskrivelse av nødvendige tiltak for å sikre balansen mellom personverninteresser og virksomhetens interesser. Vi vil følge Datatilsynets veileder for vurdering av personvernkonsekvenser.

3.15 Opplæring

Vi vil sørge for at våre ansatte som er involvert i behandlingen av personopplysninger har fått den opplæringen som er nødvendig for å sikre en effektiv gjennomføring av denne Personvernpolicyen.