

# MINDSHIFTS FORPLIKTELSE TIL PERSONVERN OG DATASIKKERHET

Versjon 1.0 – dato 09.september 2022

## INTRODUKSJON

Mindshift håndterer gjennom sine prosjekter og gjennom utvikling og salg av produktet /unlock personopplysninger. Å sørge for at vi følger gjeldende personvernregler er derfor høyt prioritert hos oss.

Personopplysningsloven som trådte i kraft 20. juli 2018 i Norge, er den sentrale loven på området. Personopplysningsloven § 1 gjør EUs generelle personvernforordning (kalt «GDPR») til norsk lov.

GDPR oppstiller blant annet generelle regler om lovlig behandlingsgrunnlag, informasjon til de registrerte og andre krav som må følges dersom data som består av personopplysninger skal lagres eller deles med andre. Kort fortalt er personopplysninger alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Typiske personopplysninger er navn, adresse, telefonnummer, e-post, fødselsnummer og dynamiske IP-adresser.

I dette dokumentet beskriver vi seks overordnede prinsipper/tiltak Mindshift har gjort for å overholde GDPR, og noen av de viktigste inkluderer, men er ikke begrenset til, følgende:

### 1. SAMTYKKE

Mindshift utfører gjennom produktet /unlock profilering av ansatte eller jobbkandidater for våre kunder. Når Mindshift utfører profilering anser vi det som svært viktig at brukerne informeres om dette, og samtykker til det. Det betyr at hver sluttbruker selv må gi et samtykke som oppfyller de krav GDPR stiller til samtykke. Uten samtykke foretar vi ikke en profilering.

Personopplysningsloven fastslår at personopplysninger bare skal samles inn for bestemte formål. Derfor har vi i Mindshift strenge krav til samtykketekstene vi bruker, slik at formålet med innsamlingen av personopplysninger er klart og tydelig formulert. Brukeren skal enkelt forstå for *hvilke formål* personopplysningene de oppgir kan brukes til.

Mindshift sørger for at det er tydelig for brukerne hvilken instans som har ansvar for hva eller hvilke deler av behandlingen slik at brukeren skal kunne ivareta eget personvern (som er et krav etter personopplysningsloven). Dette gjør vi ved å informere om *hvor* opplysningene er lagret og delt. Videre vil alltid samtykketeksten informere sluttbrukeren om hvem, utenom Mindshift som leverandør, som får tilgang til resultatene av profileringen. Dette kan eksempelvis dreie seg om en leder til en ansatt som blir profilert.

### 2. RUTINER FOR LAGRING AV DATA

Mindshift har gode rutiner for pseudonymisering og anonymisering av opplysningene som behandles i /unlock. Personopplysninger innhentes, lagres og behandles kun i den grad det er nødvendig for å oppnå formålet. Innsamlede data som ikke lenger er nødvendige for det angitte formålet slettes eller anonymiseres. Mindshift vil etter beste evne også oppfylle kvalitetskravet etter personopplysningsloven, som innebærer at personopplysninger må være relevante, korrekte og fullstendige ut fra formålene de skal benyttes til.

### 3. ÅPENHET

Mindshift er åpne om hvordan vi behandler personopplysningene som Mindshift samler inn og behandler i /unlock. Den enkelte kunde/bruker gis også mulighet til å få utlevert alle data Mindshift besitter om vedkommende i et brukervennlig format.

For å sikre personvernet ved utveksling og deling av personopplysninger med andre private eller offentlige virksomheter, må ansvarsforholdene være tydelige.

Dette har Mindshift løst ved å utforme klare og tydelige samtykketekster som brukere alltid vil måtte forholde seg til før de oppgir personopplysninger.

Videre har vi på tilgjengeliggjort en personvernerklæring og /unlock brukervilkår på våre nettsider. Disse lenkes det til i samtykketeksten slik at bruker enkelt kan lese disse før produktet tas i bruk. I tillegg har Mindshift sin egen side om personvern på sine nettsider. Her er også sjekklister fra vår personvernkonsekvensvurdering (DPIA) tilgjengelige..

#### **4. INNEBYGD PERSONVERN**

Mindshift følger prinsippet om innebygd personvern, som er et sentralt prinsipp i GDPR. Prinsippet medfører krav om hvordan løsninger som behandler personopplysninger skal utvikles («privacy by design»). Det skal tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Dette skal sørge for at informasjonssystemene oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter.

Rent praktisk betyr dette at Mindshift stiller krav til sine leverandører om at de sørger for at løsning/system de leverer oppfyller kravene til innebygd personvern. I tillegg kartlegger vi personvernmessige muligheter og begrensninger før leveranser/tjenester utvikles ytterligere, slik at systemene kan bygges opp på en slik måte at personvernkravene kan etterleves på en systematisk måte.

I tillegg innebærer prinsippet om innebygd personvern et krav til hvordan standard innstillinger skal være når sluttbruker tar system eller løsning i bruk («privacy by default»). Den mest personvernvennlige innstillingen skal være aktiv når sluttbruker tar system eller løsning i bruk. For /unlock innebærer dette at samtykkeinnhenting er det første brukeren besvarer. Brukeren må aktivt velge å gi eller ikke gi samtykke for å ta i bruk produktet. Dersom samtykke ikke blir gitt vil produktet avsluttes automatisk.

#### **5. INTERNKONTROLL**

I forbindelse med utviklingen av produktet /unlock tok Mindshift i juni 2022 initiativ til å utføre en [Personvernkonsekvensvurdering](#) (DPIA) slik datatilsynet anbefaler. I den forbindelse har alle tredjepartsleverandører blitt risikovurdert. Mindshift har fått juridisk bistand fra Bing Hodneland advokatselskap DA i dette arbeidet.

Mindshift har utnevnt et personvernombud (Sarah Fjeld Oueslati). Dette er en intern ressurs som har god kjennskap til personvern og fungerer som en rådgiver for ledelsen i personvernspørsmål. Mindshift har også en egen epostadresse der personvernombud kan kontaktes ([personvern@mindshift.no](mailto:personvern@mindshift.no)).

Mindshift har etablert internkontrollrutiner i tråd med [datatilsynets anbefaling](#). Dette innebærer blant annet at Mindshift protokollfører alle nye behandlinger av personopplysninger, har en streng tilgangsstyring etter behov til systemer der personopplysninger blir samlet inn, behandlet, lagret og delt, samt at vi gjennomfører en årlig personvernkonsekvensvurdering.

#### **6. RISIKOREDUSERENDE TILTAK VED BRUK AV TREDJEPARTSLEVERANDØRER**

Mindshift har basert sine datalagringsløsninger på Microsoft sine skytjenester basert i Europa og overfører derfor ikke data utenfor EU/EØS. Men Mindshift sin tjeneste /unlock baserer seg på bruk av tredjepartsleverandører som overfører data til USA. Derfor har Mindshift har iverksatt tiltak for grenseoverskridende dataoverføringer hos tredjepartsleverandører (Typeform og Mailchimp). Mindshift sikrer at EUs standard kontraktsklausuler er på plass, og gjennomfører hensiktsmessige tekniske og organisatoriske tiltak for beskyttelse av personopplysningene.