DATABEHANDLERAVTALE FOR UNLOCK

med behandlingsinstruks, sikkerhetstiltak, underdatabehandlere og regler for sletting og anonymisering

Dokumentstatus	Versjon	Dato
Gjeldende	1.0	19. august 2026

Denne databehandleravtalen ("Databehandleravtalen") er inngått mellom Mindshift AS (databehandler) og Kunden.

Databehandleravtalen er Vedlegg B til Kundeavtale for unlock ("Hovedavtalen") og utgjør en integrert del av Hovedavtalen. Ved motstrid mellom Hovedavtalen og Databehandleravtalen om behandling av personopplysninger, går Databehandleravtalen foran.

1. Formål og anvendelsesområde

1.1 Databehandleravtalen regulerer Mindshifts behandling av personopplysninger på vegne av Kunden ved levering av /unlock, en standardisert tjeneste for teamkartlegging og aggregert teaminnsikt. Tjenesten kan også omfatte individuelle refleksjonsprofiler når denne funksjonen er gjort tilgjengelig. Individuelle refleksjonsprofiler skal bare være tilgjengelige for den registrerte selv og skal ikke gjøres tilgjengelige for Kunden, ledere eller andre brukere.

1.2 Kunden er behandlingsansvarlig for behandlingen av personopplysninger om personer som Kunden inviterer til eller administrerer gjennom unlock. Mindshift er databehandler for behandlingen som utføres for å levere Tjenesten til Kunden.

1.3 Mindshift kan være selvstendig behandlingsansvarlig for særskilte og avgrensede behandlinger som Mindshift fastsetter formål og vesentlige midler for, eksempelvis egne kunde- og avtalekontakter, dokumentasjon av avtaleaksept, lovpålagt regnskapsføring og enkelte opplysninger til sikkerhets- og misbruksforebygging. Slike behandlinger omfattes ikke av denne Databehandleravtalen og skal beskrives i Personvernerklæring for Mindshift AS.

1.4 Videre bruk av data som er dokumentert og irreversibelt anonymisert, faller utenfor personvernforordningen. Kravene til fremstilling og kontroll av slike data følger av punkt 14 og Vedlegg 4.

2. Definisjoner

Begreper som «personopplysninger», «behandling», «behandlingsansvarlig», «databehandler», «underdatabehandler», «personvernbrudd» og «den registrerte» skal forstås slik de er definert i personvernforordningen (GDPR). Med «Tjenesten» menes /unlock, herunder de moduler, funksjoner og tjenester som Mindshift til enhver tid gjør tilgjengelige for Kunden i henhold til avtalen.

3. Roller og ansvar

3.1 Kunden bestemmer om Tjenesten skal benyttes, det konkrete organisatoriske formålet, hvilke team og personer som inviteres, samt hvordan aggregerte teamrapporter benyttes internt.

3.2 Kunden skal:

- sikre et gyldig behandlingsgrunnlag og oppfylle informasjonsplikten overfor de registrerte
- vurdere nødvendighet, forholdsmessighet og eventuelle arbeidsrettslige informasjons- og drøftingsplikter
- bare invitere personer og behandle data som er nødvendige for det oppgitte formålet
- sikre at administratorer og ledere har riktig tilgang og bruker rapporter i samsvar med Hovedavtalen
- ikke forsøke å identifisere individuelle svar eller kreve utlevert individuelle svar eller profiler
- ikke bruke Tjenesten til kontroll, prestasjonsvurdering, måling av effektivitet eller ferdigheter, personalsaker, rangering, helse-, arbeidsevne- eller egnethetsvurdering
- behandle henvendelser fra registrerte og gi Mindshift nødvendige dokumenterte instrukser.

3.3 Mindshift skal bare behandle personopplysninger etter dokumenterte instrukser fra Kunden, med mindre behandling kreves etter unionsretten eller norsk rett. I så fall skal Mindshift informere Kunden før behandlingen, med mindre loven forbyr dette av hensyn til viktige samfunnsinteresser.

3.4 Mindshift skal straks informere Kunden dersom en instruks etter Mindshifts vurdering er i strid med GDPR eller annet relevant personvernregelverk. Mindshift kan stanse den berørte behandlingen til instruksen er bekreftet, endret eller trukket tilbake.

3.5 Kunden instruerer Mindshift til å håndheve frivillig deltakelse som en bindende produktregel. Når en invitert person kontakter support@mindshift.no og velger å ikke delta, kan Mindshift registrere henvendelsen, bistå Kunden med å følge opp henvendelsen og gjennomføre nødvendige tiltak etter Kundens dokumenterte instruks. Kunden skal ikke presse eller sanksjonere personen som velger å ikke delta i kartleggingen.

4. Dokumenterte instrukser og produktgrenser

4.1 Hovedavtalen, denne Databehandleravtalen med Vedlegg 1–4, Kundens valg av team og deltakere og Kundens bruk av Tjenestens standardfunksjoner utgjør Kundens dokumenterte instrukser.

4.2 Databehandleren skal behandle personopplysninger gjennom Tjenestens standardfunksjoner slik disse følger av Hovedavtalen.

5. Taushetsplikt og personell

5.1 Mindshift skal sikre at personer som gis tilgang til personopplysninger, er autorisert, bundet av taushetsplikt og bare behandler opplysningene etter instruks.

5.2 Tilgang skal begrenses etter tjenstlig behov. Autoriserte Mindshift-administratorer kan ha stående teknisk autorisasjon, men tilgang til konkrete kundedata skal bare benyttes når det er nødvendig for support, feilretting, sikkerhetshendelser, rettighetskrav eller datakvalitetskontroll som ikke med rimelighet kan utføres med testdata. Administrativ tilgang skal logges.

6. Informasjonssikkerhet

6.1 Mindshift skal gjennomføre egnede tekniske og organisatoriske tiltak etter GDPR artikkel 32, under hensyn til behandlingens art, omfang, formål, kontekst og risiko for de registrertes rettigheter og friheter.

6.2 Bekreftede og planlagte tiltak fremgår av Vedlegg 2. Mindshift kan endre sikkerhetstiltak dersom det samlede sikkerhetsnivået opprettholdes eller forbedres.

6.3 Kunden er ansvarlig for sikker forvaltning av egne brukere, roller, enheter og innloggingsopplysninger. Tilgang er personlig og skal ikke deles.

7. Underdatabehandlere

7.1 Kunden gir generell skriftlig godkjenning til bruk av de direkte underdatabehandlerne i Vedlegg 3. Videre underdatabehandlere i leverandørkjeden dokumenteres og følges opp som angitt i Vedlegg 3.

7.2 Mindshift skal inngå skriftlig avtale med hver underdatabehandler som pålegger minst de samme relevante personvernforpliktelsene som denne Databehandleravtalen. Mindshift er fullt ansvarlig overfor Kunden for underdatabehandlerens oppfyllelse.

7.3 Mindshift skal varsle Kunden skriftlig om planlagte endringer i direkte underdatabehandlere før endringen trer i kraft og gi Kunden rimelig tid til å motsette seg endringen på saklig personvern- eller sikkerhetsgrunnlag. Partene skal søke en rimelig løsning. Dersom dette ikke lykkes, kan Kunden avslutte den berørte tjenesten.

8. Overføringer utenfor EØS

8.1 Mindshift skal ikke overføre eller gjøre personopplysninger tilgjengelige utenfor EØS uten dokumentert instruks og gyldig overføringsgrunnlag etter GDPR kapittel V.

8.2 Vedlegg 3 skal for hver direkte underdatabehandler angi behandlings- og tilgangssted og, der behandling innebærer overføring av personopplysninger utenfor EØS, relevant overføringsgrunnlag etter GDPR kapittel V. Opplysningene kan fremgå direkte av Vedlegg 3 eller av gjeldende leverandørdokumentasjon som det henvises til der.

8.3 Overføringer utenfor EØS skal bare skje på grunnlag av Kundens dokumenterte instrukser og i samsvar med GDPR kapittel V.

9. Registrertes rettigheter

9.1 Kunden har ansvar for å vurdere og besvare krav om innsyn, retting, sletting, begrensning, dataportabilitet og protest som gjelder kartleggingen.

9.2 Mindshift skal, så langt det er mulig og uten ugrunnet opphold, bistå Kunden gjennom egnede tekniske og organisatoriske tiltak. Dersom Mindshift mottar et krav direkte, skal kravet videresendes til Kunden, med mindre Mindshift behandler kravet i egenskap av selvstendig behandlingsansvarlig.

9.3 Bistanden skal ivareta løftene om konfidensialitet. Kundeadministratorer og ledere skal ikke få tilgang til individuelle svar eller profiler gjennom ordinær rettighetshåndtering.

9.4 Valg om ikke å delta etter punkt 3.5 er en avtalt produktregel og behandlingsinstruks, ikke en avgjørelse om hvorvidt vilkårene for en bestemt registrertrettighet er oppfylt. Andre rettighetskrav behandles etter punkt 9.1–9.3.

10. Bistand med etterlevelse

Mindshift skal, under hensyn til behandlingens art og informasjonen Mindshift har tilgjengelig, bistå Kunden med risikovurderinger, sikkerhet etter artikkel 32, melding og informasjon om personvernbrudd etter artikkel 33–34, vurdering av personvernkonsekvenser etter artikkel 35 og eventuell forhåndsdrøfting etter artikkel 36.

11. Personvernbrudd

11.1 Ved personvernbrudd som berører Kundens personopplysninger skal Mindshift varsle Kunden uten ugrunnet opphold og så snart det er praktisk mulig.

11.2 Varslet skal, så langt informasjonen foreligger, beskrive hendelsens art, berørte kategorier og omtrentlig antall registrerte og dataposter, sannsynlige konsekvenser, iverksatte eller foreslåtte tiltak og kontaktpunkt for oppfølging. Informasjonen kan gis trinnvis.

11.3 Mindshift skal dokumentere hendelsen, begrense skade, bevare relevant bevis og bistå Kunden med lovpålagt varsling. Varsling innebærer ikke erkjennelse av ansvar.

12. Dokumentasjon og revisjon

12.1 Mindshift skal gjøre tilgjengelig informasjon som er nødvendig for å påvise etterlevelse av GDPR artikkel 28 og denne Databehandleravtalen.

12.2 Kunden kan én gang per tolvmåned, og ellers ved dokumentert vesentlig risiko, personvernbrudd eller pålegg fra tilsynsmyndighet, gjennomføre eller la en uavhengig revisor gjennomføre en forholdsmessig kontroll. Kontroll skal varsles minst 30 dager i forkant når forholdene tillater det, gjennomføres uten unødig driftsforstyrrelse og være underlagt konfidensialitet.

12.3 Dokumentkontroll og tilgjengelige revisjonsrapporter skal normalt benyttes før stedlig kontroll.

13. Varighet, opphør, eksport og sletting

13.1 Databehandleravtalen gjelder så lenge Mindshift behandler personopplysninger på vegne av Kunden.

13.2 Kunden velger ved inngåelsen sletting som avslutningsalternativ etter GDPR artikkel 28 nr. 3 bokstav g. Før opphør kan Kunden eksportere aggregerte teamrapporter og andre opplysninger Kunden allerede har tilgang til gjennom Tjenesten. Individuelle svar, individuelle profiler og rådata utleveres ikke til Kunden.

13.3 En avviklingsperiode på 12 måneder etter opphør inngår i Tjenesten. I perioden skal opplysningene bare behandles for sikker avvikling, mulig gjenåpning etter Kundens dokumenterte instruks, eksport av tillatte data, rettighetskrav, tvisteløsning og sletting. Kunden kan kreve tidligere sletting.

13.4 Ved utløpet av avviklingsperioden skal Mindshift slette Kundens personopplysninger og eksisterende kopier, med mindre videre lagring er pålagt ved lov. Sletting fra sikkerhetskopier skjer etter Vedlegg 4.

14. Anonymisering og bruk av anonymiserte opplysninger

14.1 Kunden instruerer Mindshift til å kunne fremstille statistiske datasett ved irreversibel anonymisering som del av Tjenesten. Anonymiseringen skal gjennomføres og dokumenteres etter Vedlegg 4 før data brukes til Mindshifts egne formål.

14.2 Mindshift kan etter dokumentert anonymisering beholde og bruke data til statistikk, produktutvikling, metodeutvikling og overordnede benchmarkanalyser. Mindshift skal ikke bruke identifiserbare eller pseudonymiserte kartleggingssvar til slike egne formål.

14.3 Anonyme datasett skal ikke inneholde identifikatorer eller kombinasjoner som med rimelige midler kan knyttes til en person, et lite team eller en kunde. Mindshift skal ikke forsøke å reidentifisere personer eller kunder.

14.4 Dersom anonymiseringskravene ikke er oppfylt, skal datasettet fortsatt behandles som personopplysninger under denne Databehandleravtalen og skal ikke brukes til Mindshifts egne utviklings- eller benchmarkformål.

15. Ansvar, lovvalg og prioritet

15.1 Partenes ansvar følger GDPR og Hovedavtalen. Ingen bestemmelse begrenser ansvar eller rettigheter som ikke lovlig kan begrenses.

15.2 Avtalen er underlagt norsk rett. Tvister behandles etter Hovedavtalens tvisteløsningsbestemmelser.

15.3 Ved motstrid gjelder i denne rekkefølgen: ufravikelig personvernregelverk, eventuelle gjeldende standard personvernbestemmelser for overføring, denne Databehandleravtalen med vedlegg og deretter Hovedavtalen.

16. Elektronisk inngåelse

16.1 Databehandleravtalen er et vedlegg til Kundeavtale for /unlock og utgjør en integrert del av Avtalen.

16.2 Databehandleravtalen blir bindende når Kunden aksepterer Kundeavtale for /unlock.

16.3 Vesentlige endringer skal varsles. Endringer som innebærer nye formål, datakategorier, overføringer eller vesentlig redusert sikkerhet krever ny vurdering og, når nødvendig, ny aksept eller instruks.

Vedlegg 1 – Behandlingsbeskrivelse og instruks

Dette vedlegget oppfyller kravene i artikkel 28 nr. 3 og Datatilsynets anbefaling om at instruksen skal dokumenteres.

1. Formål

Databehandleren skal behandle personopplysninger utelukkende for å levere /unlock til Kunden i samsvar med Kundeavtale for /unlock og Kundens dokumenterte instrukser.

Behandlingen omfatter levering, drift, vedlikehold, support og videreutvikling av Tjenesten.

2. Behandlingens art

Behandlingen omfatter blant annet:

- innsamling
- registrering
- organisering
- lagring
- strukturering
- sammenstilling
- analyse
- tilgjengeliggjøring
- sletting

i den utstrekning dette er nødvendig for å levere Tjenesten.

3. Formål med behandlingen

Behandlingen skjer for å muliggjøre teamkartlegging, beregning av resultater, aggregerte teamrapporter og øvrige funksjoner som inngår i Tjenesten. Når funksjonen for individuelle refleksjonsprofiler er aktivert, kan beregnede individuelle resultater gjøres tilgjengelige for den registrerte selv. Slike profiler skal ikke gjøres tilgjengelige for Kunden eller andre brukere.

4. Registrerte

- ansatte
- innleide
- konsulenter
- andre personer Kunden inviterer til å bruke Tjenesten

5. Kategorier personopplysninger

- navn
- e-postadresse
- organisasjonstilknytning
- teamtilhørighet
- rolle
- kartleggingssvar
- pseudonyme interne identifikatorer for bruker og team
- beregnede scorer/resultater
- systemgenererte metadata
- tekniske logger

6. Særlige kategorier

Tjenesten er ikke utviklet for behandling av særlige kategorier personopplysninger etter GDPR artikkel 9.

Kunden skal ikke registrere slike opplysninger gjennom Tjenesten.

7. Kundens instrukser

Databehandleren skal kun behandle personopplysninger:

- etter dokumenterte instrukser fra Kunden
- for å oppfylle lovpålagte plikter
- når dette følger av Kundeavtale for /unlock og denne avtalen.

Vedlegg 2 – Tekniske og organisatoriske tiltak

Databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er passende ut fra risikoen, jf. GDPR artikkel 32.

Tiltakene omfatter blant annet:

- tilgangsstyring
- autentisering
- autorisasjon
- kryptering ved overføring
- beskyttelse av lagrede personopplysninger
- logging av relevante sikkerhetshendelser
- sikkerhetskopiering
- gjenoppretting etter hendelser
- testing og evaluering av sikkerhetstiltak

- opplæring av personell med tilgang til personopplysninger
- håndtering av personvern- og sikkerhetshendelser

Databehandleren kan endre de tekniske løsningene når dette opprettholder eller forbedrer sikkerhetsnivået.

Vedlegg 3 – Underdatabehandlere og overføringer

Vedlegget beskriver Mindshifts direkte underdatabehandlere og behandlingskjeder slik de er dokumentert per 13. august 2026.

A. Direkte underdatabehandlere og behandlingskjede

Leverandør	Oppgave og data	Behandlings-/tilgangssted og overføring
Appfarm AS	Applikasjonsplattform for brukere, organisasjon, team, roller, kartleggingsstatus, beregnede scorer, teamresultater og rapporter. Appfarm mottar beregnede resultater med pseudonyme interne identifikatorer for bruker og team og kobler resultatene til riktig bruker internt. Rå Typeform-svar inngår ikke i den ordinære resultatflyten tilbake til Appfarm.	Sentral plattformbehandling skjer i EU/EØS, herunder Belgia. Appfarm benytter også integrerte underdatabehandlere som kan behandle data i andre land, herunder USA. Gjeldende behandlingssteder og overføringsgrunnlag følger Appfarms til enhver tid gjeldende Data Processors-liste.
Typeform SL	Gjennomføring av kartlegging. Behandler pseudonyme interne identifikatorer for bruker og team, rå kartleggingssvar, Typeform response-ID, tidspunkt og relevante tekniske metadata. Typeform opplyser at respondentens IP-adresse ikke lagres som del av responsdata; IP-adressen brukes til å generere Network ID.	Kartleggings-/responsdata omfattes av Typeforms EU-hostingoppsett. Eventuelle videre underdatabehandlere, behandlingssteder og eventuelle overføringer utenfor EØS følger Typeforms gjeldende DPA og underdatabehandlerliste.
Webhuset AS	Hosting av Mindshifts Windows-baserte integrasjons- og beregningsserver samt sikkerhetskopiering av servermiljøet. Serveren mottar rå Typeform-data og pseudonyme interne identifikatorer for bruker og team, bearbeider data, beregner scorer/teamresultater og sender beregnede resultater med med de samme pseudonyme identifikatorene til Appfarm via API. Serveren har ikke navn/e-post eller koblingen mellom de pseudonymiserte id'ene og identifiserbar bruker.	Norge. Webhuset opplyser at hosting-/cloud-tjenester leveres fra norske datasentre i Oslo og Bergen. Ingen direkte tredjelandsoverføring er dokumentert for selve Cloud Server-leveransen. Relevante videre underleverandører fremgår av Bilag 2 til Webhusets DPA.
Microsoft Ireland Operations Limited / Microsoft 365	Behandling av /unlock-relaterte support- og personvernhenvendelser mottatt via support@mindshift.no. Opplysninger kan omfatte navn, e-postadresse, virksomhets-/teamtilhørighet og innhold i henvendelsen. Kartleggingssvar og beregnede scorer skal ikke sendes via supportkanalen med mindre det er nødvendig for å håndtere en konkret henvendelse.	Behandling skjer gjennom Microsoft 365. Gjeldende behandlingssteder, underdatabehandlere og eventuelle internasjonale overføringer følger Microsofts Products and Services Data Protection Addendum og tilhørende Microsoft-dokumentasjon.
Mailchimp / The Rocket Science Group LLC	Direkte underdatabehandler for Mindshift for tjeneste- og kartleggingsrelaterte e-postutsendelser. Aktuelle data kan omfatte e-postadresse, eventuelt navn, lenke til tjenesten/kartleggingen og leverings-/utsendelsesmetadata. Rå kartleggingssvar og beregnede scorer overføres ikke til Mailchimp.	USA og andre behandlingssteder som fremgår av Mailchimps gjeldende underdatabehandlerliste. Mailchimps DPA angir EU–US Data Privacy Framework som relevant overføringsgrunnlag og SCC-er der dette er nødvendig.

B. Videre underdatabehandlere og dokumentasjonskilder

Mindshift skal holde oppdatert informasjon om identiteten til videre underdatabehandlere og den behandlingen de utfører tilgjengelig for Kunden. Endringer i underdatabehandlerkjeden håndteres etter reglene om underdatabehandlere i punkt 7.

Vedlegg 4 – Sletting og anonymisering

1. Opphør

Ved opphør av avtalen skal personopplysninger slettes eller returneres til Kunden i samsvar med GDPR artikkel 28 nr. 3 bokstav g, med mindre lagring følger av lov.

2. Anonymisering

Mindshift kan anonymisere personopplysninger slik at de ikke lenger kan knyttes til en identifisert eller identifiserbar fysisk person.

Anonymiserte opplysninger omfattes ikke av denne avtalen etter at anonymiseringen er gjennomført.

Databehandleren skal anvende dokumenterte metoder for anonymisering som er egnet til å redusere risikoen for reidentifisering.

3. Bruk av anonyme data

Når personopplysninger er anonymisert slik at de ikke lenger kan knyttes til en identifisert eller identifiserbar fysisk person, kan Mindshift bruke de anonymiserte opplysningene til statistikk, analyse, forskning, kvalitetsforbedring, utvikling og videreutvikling av Tjenesten.