BUILDEX

# Databehandleravtale

Behandling av personopplysninger etter GDPR artikkel 28

| | |
|---|---|
| Versjon | 1.0 |
| Gjeldende fra | 20. april 2026 |
| Databehandler | Buildex AS (under stiftelse), org.nr. [tildeles] |
| Dokument-ID | BX-DPA-v1.0 |
| Rettsgrunnlag | Personvernforordningen (GDPR) art. 28, personopplysningsloven |
| Språk | Norsk (bokmål) |

## 1. Bakgrunn og formål

Denne databehandleravtalen ("avtalen") er inngått mellom Buildex AS (under stiftelse), org.nr. [tildeles] ("Buildex" / "databehandleren") og den kunden som har inngått avtale om abonnement på Buildex-plattformen ("kunden" / "behandlingsansvarlig").

Avtalen regulerer Buildex sin behandling av personopplysninger på vegne av kunden i forbindelse med leveransen av Buildex-plattformen ("tjenesten"), og oppfyller kravene til databehandleravtale i EUs personvernforordning (forordning 2016/679, "GDPR") artikkel 28.

Avtalen kommer til anvendelse uavhengig av hvilken abonnementsform kunden har valgt, og utgjør en integrert del av avtaleforholdet mellom partene sammen med Buildex sine salgsvilkår og kundens bestilling.

## 2. Definisjoner

Begreper som "personopplysninger", "behandling", "behandlingsansvarlig", "databehandler", "registrert", "underdatabehandler" og "tilsynsmyndighet" skal forstås i samsvar med definisjonene i GDPR. Med "tjenesten" menes Buildex sin skybaserte plattform som beskrevet i kundens bestilling.

## 3. Partenes roller

Kunden er behandlingsansvarlig for de personopplysninger som behandles i tjenesten. Buildex er databehandler og behandler personopplysninger på vegne av kunden, utelukkende i samsvar med denne avtalen og kundens dokumenterte instrukser.

Kunden er ansvarlig for å påse at det foreligger tilstrekkelig rettsgrunnlag for behandlingen og for å informere de registrerte i samsvar med GDPR artikkel 13 og 14.

## 4. Behandlingens karakter, formål og varighet

Behandlingens karakter, formål, varighet, kategorier av registrerte og kategorier av personopplysninger er nærmere beskrevet i Vedlegg A til denne avtalen.

Buildex skal kun behandle personopplysninger i det omfang og for de formål som er nødvendig for å levere tjenesten i henhold til avtalen, eller som følger av skriftlige instrukser fra kunden.

## 5. Kundens instrukser

Buildex skal behandle personopplysninger kun etter dokumenterte instrukser fra kunden, med mindre annet følger av EU- eller medlemsstatsrett som Buildex er underlagt. I slike tilfeller skal Buildex informere kunden om rettskravet før behandlingen, med mindre slik underretning er forbudt etter nevnte rett.

Salgsvilkårene, bestillingen og denne avtalen med tilhørende vedlegg utgjør kundens opprinnelige instruks til Buildex. Ytterligere eller endrede instrukser gis skriftlig (inkludert per e-post).

Dersom Buildex mener at en instruks fra kunden er i strid med GDPR eller annen personvernlovgivning, skal Buildex uten ugrunnet opphold informere kunden om dette.

## 6. Taushetsplikt og opplæring

Buildex skal sikre at personer som er autorisert til å behandle kundens personopplysninger har forpliktet seg til taushetsplikt eller er underlagt lovbestemt taushetsplikt, og at slike personer har tilstrekkelig kunnskap om personvern og informasjonssikkerhet.

Tilgang til kundens personopplysninger skal begrenses til personer med tjenstlig behov.

## 7. Informasjonssikkerhet

Buildex skal iverksette egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er tilpasset risikoen, jf. GDPR artikkel 32. Tiltakene omfatter blant annet tilgangskontroll, pseudonymisering der det er relevant, kryptering av data under overføring, logging, regelmessige sikkerhetskopier, samt rutiner for gjenoppretting ved hendelser.

En oversikt over Buildex sine tekniske og organisatoriske sikkerhetstiltak fremgår av Vedlegg C. Tiltakene kan videreutvikles og endres i takt med teknologisk utvikling og endret risikobilde, forutsatt at sikkerhetsnivået opprettholdes eller forbedres.

## 8. Underdatabehandlere

### 8.1 Generelt samtykke

Kunden gir ved inngåelsen av denne avtalen et generelt samtykke til at Buildex benytter underdatabehandlere. Gjeldende underdatabehandlere på avtaletidspunktet fremgår av Vedlegg B.

### 8.2 Krav til underdatabehandlere

Buildex skal påse at alle underdatabehandlere er underlagt en skriftlig avtale som pålegger dem forpliktelser tilsvarende dem som følger av denne avtalen, herunder kravene i GDPR artikkel 28 nr. 3 og 4. Buildex er overfor kunden ansvarlig for at underdatabehandlere oppfyller sine forpliktelser.

### 8.3 Varsling om endringer

Buildex skal varsle kunden skriftlig minst 30 dager før Buildex tar i bruk en ny underdatabehandler, eller bytter ut en eksisterende underdatabehandler. Kunden kan innen varslingsperiodens utløp protestere skriftlig mot endringen på saklig personverngrunnlag. Ved protest kan partene søke å finne en omforent løsning; dersom slik løsning ikke oppnås, har kunden rett til å si opp avtalen med virkning fra tidspunktet endringen trer i kraft, og uten kostnader for gjenstående periode.

## 9. Overføring av personopplysninger utenfor EØS

Kundens personopplysninger lagres som hovedregel innenfor EØS. Enkelte underdatabehandlere, særlig for tilleggsfunksjoner som AI-assistanse og feillogging, kan innebære overføring av personopplysninger til tredjeland utenfor EØS. Slik overføring skjer kun når det foreligger et gyldig overføringsgrunnlag etter GDPR kapittel V, herunder beslutninger om tilstrekkelig beskyttelsesnivå eller EUs standardkontraktklausuler (SCCs) med eventuelle supplerende tiltak.

Vedlegg B angir for hver underdatabehandler behandlingsland og gjeldende overføringsgrunnlag.

## 10. Bistand til behandlingsansvarlig

### 10.1 Registrertes rettigheter

Buildex skal, i den grad det er mulig og hensyntatt behandlingens art, bistå kunden med egnede tekniske og organisatoriske tiltak for å oppfylle kundens plikt til å svare på anmodninger fra registrerte om å utøve sine rettigheter etter GDPR kapittel III (innsyn, retting, sletting, begrensning, dataportabilitet og innsigelse).

### 10.2 Henvendelser direkte til Buildex

Dersom en registrert, en tilsynsmyndighet eller annen tredjepart retter en henvendelse om kundens personopplysninger direkte til Buildex, skal Buildex uten ugrunnet opphold videresende henvendelsen til kunden og ikke besvare denne uten kundens forhåndsgodkjennelse, med mindre Buildex er pålagt dette ved lov.

### 10.3 Øvrig bistand

Buildex skal videre bistå kunden med å sikre etterlevelse av pliktene etter GDPR artikkel 32–36, herunder ved gjennomføring av vurderinger av personvernkonsekvenser (DPIA) og eventuelle forhåndsdrøftelser med tilsynsmyndigheten. Buildex kan kreve rimelig vederlag etter medgått tid for bistand som går utover det som følger av Buildex sin standard produktstøtte.

## 11. Varsling om brudd på personopplysningssikkerheten

Buildex skal varsle kunden uten ugrunnet opphold, og senest innen 72 timer, etter å ha blitt kjent med et brudd på personopplysningssikkerheten som berører kundens personopplysninger. Varselet skal så langt mulig inneholde:

- En beskrivelse av bruddet, herunder kategoriene og det omtrentlige antall registrerte og personopplysninger som berøres.
- Sannsynlige konsekvenser av bruddet.
- Tiltak som er iverksatt eller foreslås for å håndtere bruddet og begrense eventuelle skadevirkninger.
- Kontaktinformasjon for ytterligere oppfølging.

Informasjon som ikke er tilgjengelig på varslingstidspunktet, gis fortløpende så snart den foreligger. Kunden er ansvarlig for eventuell varsling til tilsynsmyndighet og til de registrerte etter GDPR artikkel 33 og 34.

## 12. Sletting og retur ved opphør

Ved opphør av avtaleforholdet, uavhengig av opphørsgrunn, skal Buildex etter kundens valg enten slette eller tilbakelevere alle personopplysninger som er behandlet på vegne av kunden, og slette eksisterende kopier, med mindre lagring er pålagt ved EU- eller medlemsstatsrett.

Kundens rett til eksport av egne data og Buildex sine rutiner for sletting og håndtering av sikkerhetskopier fremgår av salgsvilkårene og Vedlegg C til denne avtalen.

## 13. Revisjon og kontroll

Buildex skal stille til rådighet for kunden all informasjon som er nødvendig for å påvise at forpliktelsene i denne avtalen og GDPR artikkel 28 overholdes, og gjøre det mulig for kunden eller en revisor utpekt av kunden å gjennomføre revisjon, herunder inspeksjon.

Revisjon gjennomføres i utgangspunktet ved at Buildex fremlegger oppdatert dokumentasjon av sikkerhetstiltak, herunder relevante tredjepartsrapporter, sertifiseringer eller egenrapportering. Stedlig inspeksjon kan avtales ved saklig begrunnet behov, skal varsles skriftlig med minst 30 dagers frist, og gjennomføres i normal arbeidstid på en måte som ikke unødig forstyrrer Buildex sin drift. Kostnader knyttet til stedlig inspeksjon, herunder Buildex sitt tidsbruk, dekkes av kunden, med mindre inspeksjonen avdekker vesentlig mislighold fra Buildex sin side.

## 14. Ansvar

Partenes ansvar etter denne avtalen reguleres av ansvarsbegrensningene i salgsvilkårene, med mindre annet følger av ufravikelig lov. Ansvarsfordeling mellom behandlingsansvarlig og databehandler etter GDPR artikkel 82 berøres ikke.

## 15. Varighet

Avtalen gjelder så lenge Buildex behandler personopplysninger på vegne av kunden. Bestemmelsene om sletting, retur, taushetsplikt og revisjon gjelder også etter avtalens opphør i den utstrekning det er nødvendig.

## 16. Endringer i avtalen

Buildex kan endre denne avtalen med 30 dagers skriftlig varsel, herunder for å reflektere endringer i personvernlovgivning, tilsynspraksis, sikkerhetsstandarder eller tjenestens tekniske oppsett. Vesentlige endringer til kundens ugunst gir kunden rett til å si opp avtalen med virkning fra endringens ikrafttredelse.

Endringer i listen over underdatabehandlere (Vedlegg B) følger prosedyren i punkt 8.3. Oppdatering

av Vedlegg A (behandlingens gjenstand) og Vedlegg C (sikkerhetstiltak) kan gjøres av Buildex når det er nødvendig som følge av endringer i tjenesten, forutsatt at beskyttelsesnivået opprettholdes eller forbedres.

## 17. Forrang, lovvalg og verneting

Ved eventuell motstrid mellom denne avtalen og Buildex sine salgsvilkår, gjelder denne avtalen for spørsmål om behandling av personopplysninger.

Avtalen reguleres av norsk rett. Tvister som måtte oppstå mellom partene skal søkes løst gjennom forhandlinger. Dersom forhandlinger ikke fører frem, er Asker og Bærum tingrett avtalt verneting i første instans.

## Vedlegg A – Behandlingens gjenstand

### A.1 Formålet med behandlingen

Buildex behandler personopplysninger på vegne av kunden for å levere Buildex-plattformen, herunder funksjoner for prosjektstyring, dokumenthåndtering, HMS/KS, tegnings- og BIM-forvaltning, fremdriftsplanlegging, byggeplassverktøy, stoffkartotek og tilhørende brukeradministrasjon og support.

### A.2 Behandlingens art

Behandlingen omfatter innsamling, registrering, lagring, organisering, gjenfinning, visning, tilgjengeliggjøring mellom autoriserte brukere, utsending av systemgenererte e-poster og dokumenter til brukere og kontaktpersoner, sikkerhetskopiering og sletting av personopplysninger som kunden eller kundens brukere registrerer i tjenesten.

### A.3 Varighet

Behandlingen pågår så lenge kunden har et aktivt abonnement, samt i den perioden som er nødvendig for å sluttføre dataeksport og sletting etter avtalens opphør i tråd med salgsvilkårene.

### A.4 Kategorier av registrerte

- Kundens ansatte og innleide som er gitt tilgang til tjenesten.
- Ansatte hos underentreprenører og andre samarbeidspartnere som er gitt tilgang til kundens prosjekter.
- Kontaktpersoner hos byggherrer, leverandører og andre tredjeparter som er registrert i kundens prosjekter.
- Besøkende på byggeplass registrert via PSI/adgangskontroll.

### A.5 Kategorier av personopplysninger

- Kontakt- og identitetsopplysninger: navn, stilling, arbeidsgiver, telefonnummer, e-postadresse.
- Brukerkontoopplysninger: brukernavn, rolle, tilganger, aktivitetslogg, innloggingstidspunkter.
- Prosjektrelaterte opplysninger: kommentarer, aksjonspunkter, oppgaver, møtereferat og lignende som kan inneholde personopplysninger.
- HMS-relaterte opplysninger: registreringer av uønskede hendelser, avvik, observasjoner, vernerunder og sjekklister, som kan inneholde opplysninger om involverte personer.

- Adgangskontroll: tidspunkter for inn- og utregistrering på byggeplass, gjennomført PSI.

### A.6 Særlige kategorier

Tjenesten er ikke utformet for behandling av særlige kategorier av personopplysninger etter GDPR artikkel 9 eller opplysninger om straffbare forhold etter artikkel 10. Kunden er ansvarlig for å sikre at slike opplysninger ikke registreres i tjenesten, med mindre dette er uttrykkelig avtalt skriftlig med Buildex og det er etablert nødvendige tilleggstiltak.

Dersom kundens bruk av tjenesten medfører at helseopplysninger knyttet til HMS-hendelser (skader, nestenulykker og lignende) registreres, behandles disse under samme tekniske og organisatoriske sikkerhetstiltak som øvrige personopplysninger, jf. Vedlegg C. Kunden forplikter seg til å begrense slik registrering til det som er strengt nødvendig for HMS-dokumentasjon.

## Vedlegg B – Underdatabehandlere

Buildex benytter følgende underdatabehandlere i leveransen av tjenesten:

| Underdatabehandler | Land | Formål med behandlingen | Overføringsgrunnlag |
|---|---|---|---|
| ServeTheWorld AS | Norge | Hosting, drift og lagring (servere i Oslo) | EØS |
| Anthropic PBC | USA | AI-assistanse (f.eks. stoffkartotek-søk og risikovurdering) | SCCs + supplerende tiltak |
| Resend, Inc. | Tyskland | Utsending av transaksjons-e-post (systemgenererte e-poster som brukerinvitasjoner, møtereferat, | EØS |

Buildex-plattformen kjører på fullt self-hosted infrastruktur i Norge. Databaser (Supabase open source) og filhåndtering (Nextcloud) driftes av Buildex på servere hos ServeTheWorld AS i Oslo. Supabase Inc. og Nextcloud GmbH er derfor ikke underdatabehandlere i denne avtalen. Feilovervåkning og analyse skjer på self-hosted programvare på samme infrastruktur.

Endringer i listen over underdatabehandlere varsles i samsvar med punkt 8.3 i hoveddelen av avtalen.

## Vedlegg C – Tekniske og organisatoriske sikkerhetstiltak

Buildex har iverksatt følgende kategorier av tekniske og organisatoriske tiltak for å ivareta sikkerheten for kundens personopplysninger, jf. GDPR artikkel 32:

### C.1 Organisatoriske tiltak

- Interne retningslinjer og rutiner for informasjonssikkerhet og personvern.
- Taushetspliktserklæringer for personell med tilgang til kundens data.
- Løpende opplæring i personvern og informasjonssikkerhet.

- Rutiner for å behandle henvendelser fra registrerte og tilsynsmyndigheter.
- Avtalefestede krav til underdatabehandlere.

### C.2 Tilgangskontroll

- Tilgang til kundens data er begrenset til personell med tjenstlig behov (minimumsprinsippet).
- Rollebasert tilgangsstyring i tjenesten (RLS-policies på databasenivå).
- Personlige brukerkontoer og sterke passordkrav.
- Logging av tilgang og endringer i kundens data.

### C.3 Kryptering og beskyttelse av data

- Kryptering av data under overføring (TLS/HTTPS).
- Beskyttelse av servere bak brannmur og herdet oppsett.
- Tekniske tiltak mot vanlige angrepsvektorer, herunder SQL-injection, XSS og uautorisert API-tilgang.

### C.4 Driftssikkerhet

- Overvåkning av drift og tilgjengelighet.
- Regelmessige, krypterte sikkerhetskopier.
- Beredskaps- og gjenopprettingsrutiner for hendelser og sikkerhetsbrudd.
- Patch- og oppdateringsrutiner for plattformens komponenter.

### C.5 Lokasjon og digital suverenitet

- Kundens produksjonsdata lagres innenfor EØS, med primær lagring i Norge.
- Infrastruktur og filhåndtering driftes av Buildex på norsk jord, hos en norsk leverandør.

### C.6 Sletting

- Data slettes fra produksjonssystemer innen 30 dager etter avtalens opphør, forutsatt at kunden ikke har bedt om eksport innen denne fristen.
- Sikkerhetskopier slettes permanent senest 90 dager etter opphør.