PRACTICLE

Standard databehandleraftale (DPA)

for anvendelse af Practicle

Version	1.1
Gældende fra	16. september 2026
Sprog	Dansk
Genereret	31. oktober 2026

Denne standard-databehandleraftale (i det følgende benævnt ”Aftalen”) regulerer den behandling af personoplysninger, der foretages i forbindelse med levering og anvendelse af softwareløsningen Practicle.

Parterne:

Kunden (som defineret i Hovedaftalen, licensordren eller den elektroniske kontooprettelse) (i det følgende benævnt ”Dataansvarlig”)

Practicle

Snerlehaven 1, 2630 Tåstrup, Danmark

CVR-nr.: 27353606

E-mail: support@practicle.dk

(i det følgende benævnt ”Databehandler”)

Hver for sig benævnt en ”Part” og samlet ”Parterne”.

1. Formål, genstand og aftalegrundlag

1.1. Aftalen fastlægger de rettigheder og forpligtelser, der påhviler Parterne ved Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige i medfør af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (GDPR), navnlig artikel 28.

1.2. Aftalen understøtter desuden den Dataansvarliges forpligtelser til forsyningskædesikkerhed i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 (NIS2-direktivet).

1.3. Nærværende Aftale udgør et integreret bilag til parternes aftalegrundlag vedrørende levering og brug af Practicle (”Hovedaftalen”). I tilfælde af uoverensstemmelser mellem bestemmelserne i Hovedaftalen og denne Aftale vedrørende behandling og beskyttelse af personoplysninger har denne Aftale forrang.

2. Anvendelsesområde efter driftsmodel (SaaS vs. On-Premises)

2.1. SaaS / Cloud-leverance: Ved Practicle som SaaS/cloud-løsning er Databehandleren driftsansvarlig for hostinginfrastrukturen. Databehandleren fungerer i denne model som databehandler for alle personoplysninger, som den Dataansvarlige eller dennes brugere indlæser, opretter eller genererer i applikationen.

2.2. On-Premises særinstallation: Ved betalt særinstallation installeres og driftes platformen i den Dataansvarliges eget infrastrukturmiljø. Databehandleren har ingen standardadgang til data og fungerer ikke som databehandler i den daglige drift. Nærværende Aftale finder i denne driftsmodel udelukkende anvendelse, såfremt den Dataansvarlige udtrykkeligt anmoder Databehandleren om teknisk bistand, support eller fejlretning, som medfører adgang til personoplysninger.

3. Dataejerskab og instruks

3.1. Ejerskab: Alle data, herunder personoplysninger, som kunden opretter eller uploader i Practicle, tilhører udelukkende den Dataansvarlige.

3.2. Dokumenteret instruks: Databehandleren må udelukkende behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre andet kræves i henhold til EU-ret eller medlemsstaternes nationale ret. Hovedaftalen, denne DPA, systemets konfigurationsvalg samt den Dataansvarliges løbende brug af platformen udgør den samlede instruks.

3.3. Tilsidesættelse af instrukser: Databehandleren underretter straks den Dataansvarlige, hvis en instruks efter Databehandlerens vurdering er i strid med GDPR eller anden databeskyttelsesretlig lovgivning.

4. Fortrolighed og adgangsbegrænsning

4.1. Tavshedspligt: Databehandleren sikrer, at alle personer, der autoriseres til at tilgå personoplysninger, har påtaget sig en skriftlig tavshedspligt eller er underlagt en lovbestemt tavshedspligt.

4.2. Need-to-know: Databehandlerens medarbejdere tilgår udelukkende kundedata, når det er strengt nødvendigt for at yde teknisk support, fejlfinde eller levere aftalt bistand. Enhver

administrativ adgang logges.

5. Behandlingssikkerhed og NIS2-forsyningskædesikkerhed

5.1. Tekniske og organisatoriske foranstaltninger: Databehandleren implementerer og vedligeholder passende tekniske og organisatoriske foranstaltninger jf. GDPR art. 32 for at sikre et sikkerhedsniveau svarende til risiciene. Foranstaltningerne er specificeret i Bilag B.

5.2. NIS2-efterlevelse (Supply Chain Risk Management): For at understøtte den Dataansvarliges lovpligtige styring af cybersikkerhedsrisici i forsyningskæden garanterer Databehandleren:

- Anvendelse af ISO 27001-certificeret hostinginfrastruktur inden for EU (Tyskland).
- Løbende systemhærdning, firewallbeskyttelse, sårbarhedsstyring og validering af server-side API-input mod injektions- og webangreb.
- Robust adgangskontrol med understøttelse af Keycloak SSO, LDAP, 2FA samt beskyttelse mod brute force og credential stuffing via rate limiting.
- Systemunderstøttelse i Practicle til håndtering af frameworks, kontroller og periodiske audits (vha Practicle Compliance).

6. Anvendelse af underdatabehandlere

6.1. Generel forhåndsgodkendelse: Den Dataansvarlige giver generel forhåndsgodkendelse til, at Databehandleren gør brug af underdatabehandlere til opfyldelse af leverancen. Godkendte underdatabehandlere fremgår af Bilag C.

6.2. Varsling om ændringer: Databehandleren varsler den Dataansvarlige med minimum 30 dages skriftligt varsel (via e-mail eller meddelelse i platformen) forud for tilføjelse eller udskiftning af en underdatabehandler. Den Dataansvarlige har ret til at gøre begrundet, saglig indsigelse inden for varslingsfristen.

6.3. Forpligtelser for underdatabehandlere: Databehandleren pålægger underdatabehandlere de samme databeskyttelses- og sikkerhedskrav, som Databehandleren er underlagt i medfør af denne Aftale.

6.4. Tredjelandsoverførsler: Databehandling og lagring finder sted inden for EU/EØS. Eventuel overførsel til tredjelande må kun ske under overholdelse af GDPR kapitel V.

7. Sikkerhedshændelser og brud på persondatasikkerheden

7.1. Varslingspligt: Databehandleren underretter den Dataansvarlige uden unødig forsinkelse og senest inden for 24 timer, efter at Databehandleren er blevet bekendt med et konstateret eller formodet brud på persondatasikkerheden.

7.2. Indhold af varsling: Underretningen skal som minimum oplyse om hændelsens karakter, de berørte datakategorier, omtrentligt antal berørte personer, sandsynlige konsekvenser og iværksatte/foreslåede afbødende foranstaltninger.

7.3. Hændelseshåndtering: Parterne samarbejder loyalt med henblik på at mitigere sikkerhedshændelser og tilvejebringe nødvendig dokumentation til brug for tilsynsmyndigheder eller berørte parter.

8. Bistand til den Dataansvarlige

8.1. De registreredes rettigheder: Platformen stiller funktionalitet til rådighed, så den Dataansvarlige selvstændigt kan opfylde anmodninger om indsigt, berigtigelse, begrænsning, indsigelse, eksport og sletning.

8.2. Direkte anmodninger om datasletning: Såfremt registrerede retter henvendelse direkte til Databehandleren, henvises vedkommende til den Dataansvarliges administrator jf. Practicles datasletningspolitik.

8.3. DPIA og tilsyn: Databehandleren bistår den Dataansvarlige i fornødent og rimeligt omfang med oplysninger til brug for konsekvensanalyser vedrørende databeskyttelse (DPIA) og eventuelle forudgående høringer hos tilsynsmyndigheder, jf. GDPR art. 35 og 36. Bistanden er begrænset til udlevering af oplysninger og teknisk dokumentation, som Databehandleren har i forvejen og som er nødvendige for analysen. Såfremt bistanden kræver særskilt tidsforbrug eller tilpasning fra Databehandlerens side, afregnes dette efter medgået tid til Databehandlerens til enhver tid gældende timesats, medmindre andet er udtrykkeligt aftalt.

9. Revision, dokumentation og audit

9.1. Dokumentation: Databehandleren stiller al nødvendig dokumentation for overholdelse af GDPR art. 28 og denne Aftale til rådighed for den Dataansvarlige.

9.2. Tilsyn og audit: Den Dataansvarlige eller en uafhængig revisor bemyndiget af denne har ret til at gennemføre inspektioner af behandlingssikkerheden med et forudgående varsel på minimum 14 arbejdsdage i normal arbejdstid. Tilsyn må ikke forstyrre driften eller give adgang til andre kunders data. Den Dataansvarlige afholder alle omkostninger forbundet hermed, og bistand fra Databehandleren, der overstiger udlevering af eksisterende standarddokumentation, afregnes efter medgået tid.

10. Ophør, eksport og datasletning

10.1. Løbende dataeksport og snapshots: Den Dataansvarlige har til enhver tid under aftaleperioden adgang til via administrationsmodulet at trække en komplet eksport eller tage et snapshot af hele sin database.

10.2. Sletning ved aftaleophør: Ved ophør af Hovedaftalen for SaaS-leverancen sletter Databehandleren alle kundens personoplysninger og eksisterende datakopier senest 30 dage efter aftalens udløb, medmindre EU-ret eller national ret foreskriver fortsat opbevaring. Tekniske backups overskrives automatisk i henhold til den faste rotationscyklus (maksimalt 30 dage).

Bilag A: Instruktion for behandling af personoplysninger

A.1. Formål og behandlingsaktiviteter

Formålet med behandlingen er at stille ITSM- og ledelsesplatformen Practicle til rådighed som SaaS, og ved særskilt aftale som support til en On-Premises særinstallation. Behandlingen omfatter opbevaring, registrering, strukturering, fremsøgning, visning, sagsstyring (servicedesk/support), konfigurationsstyring (CMDB), opgavestyring, dokumentationsarkivering, password management samt styring af compliance-krav (f.eks. NIS2-frameworks).

A.2. Kategorier af registrerede

- Den Dataansvarliges medarbejdere, administratorer, konsulenter og IT-brugere.
- Den Dataansvarliges slutbrugere, kunder, leverandører eller eksterne samarbejdspartnere, der henvender sig via support eller registreres i systemets moduler.

A.3. Kategorier af personoplysninger

Almindelige personoplysninger:

- Identifikations- og stamdata: Navn, brugernavn, virksomhedsnavn, stillingsbetegnelse, afdeling.
- Kontaktoplysninger: E-mailadresser, telefonnumre, adresse.
- System- og netværksdata: IP-adresser, browser- og enhedsinformation, login-historik, brugerroller, handlings- og audit-logs.
- Sags- og procesdata: Indhold i supporttickets, interne notater, projektdata, CMDB-relationer og brugeruploadede dokumenter.
- Krypterede adgangsoplysninger: Adgangskoder og API-nøgler ved brug af password management-modulet.

Særlige kategorier af personoplysninger (følsomme data):

Practicle er som udgangspunkt ikke tiltænkt behandling eller opbevaring af særlige kategorier af personoplysninger som omhandlet i GDPR artikel 9. Den Dataansvarlige bør derfor ikke anvende platformen til sådanne oplysninger, medmindre dette er særskilt aftalt. Dette ændrer ikke Databehandlerens lovbestemte forpligtelser efter GDPR, herunder artikel 28 og 32, og denne Aftale. Databehandleren er fortsat underlagt disse forpligtelser for den behandling, Databehandleren faktisk foretager, også hvis den Dataansvarlige indlæser sådanne oplysninger i platformen.

A.4. Behandlingens varighed

Behandlingen pågår, så længe Hovedaftalen er i kraft.

Bilag B: Tekniske og organisatoriske sikkerhedsforanstaltninger

Infrastruktur og hosting (Hetzner, Nürnberg, Tyskland):

- Serverinfrastrukturen er placeret i ISO/IEC 27001-certificerede datacentre i Nürnberg, Tyskland.
- Fysisk sikkerhed omfatter 24/7-overvågning, adgangskontrolsystemer, redundant strømforsyning (UPS/dieselgeneratorer) og klimastyring.

Arkitektur og logisk dataadskillelse:

- Multi-tenant arkitektur med PostgreSQL som primær database.
- Logisk dataadskillelse, der sikrer, at hver kundes data er isoleret.
- Parameteriserede forespørgsler og server-side validering for at forhindre SQL-injections og data-leakage.
- Sikre web-headere implementeret (herunder CSP – Content Security Policy og HSTS – HTTP Strict Transport Security).

Adgangsstyring, identitetsstyring og autentificering:

- Understøttelse af Keycloak SSO-integration til Single Sign-On, multifaktor-godkendelse og enterprise identity governance.
- Mulighed for lokal to-faktor-godkendelse (2FA) samt Active Directory / LDAP-integration.
- Granulær, rollebaseret adgangskontrol (RBAC) helt ned på modul- og feltniveau.
- Adgangskoder sikres med stærk hashing og salting.
- Automatisk session timeout og CSRF-beskyttelse.

- Rate limiting på netværks- og applikationsniveau (IP-blokering, filbaseret burst-sikring og automatisk låsning af konti ved gentagne mislykkede loginforsøg).

Netværkssikkerhed, hærdning og overvågning:

- Netværksfirewall, der udelukkende tillader trafik på nødvendige porte og filtrerer scanninger samt brute force-forsøg.
- Systemhærdning med kun strengt nødvendige services eksponeret og løbende udrulning af OS- og sikkerhedsopdateringer.
- Egenudviklet monitoreringsmotor, der overvåger serverbelastning, latency, API-fejl og databasesundhed med automatisk driftsnotifikation ved afvigelser.
- Fuld audit-logning af alle centrale ændringer, administrative handlinger og loginforløb med tidsstempler for sporbarhed.

Kryptering:

- In transit: Al datatransit mellem klient og server krypteres via TLS/HTTPS.
- At rest: Databaser, backups og passwords i password management-modulet lagres stærkt krypteret.

Backup, gendannelse og kundestyret kontrol:

- Automatiske timebaserede backups med 3 dages historik.
- Automatiske daglige backups med 30 dages historik.
- Backups overvåges aktivt for gennemførsel og valideres for integritet med alarm til driftsteamet ved fejl.
- Kunder har selv adgang til at generere snapshots forud for ændringer/opgraderinger og genskabe via et guidet restore-flow.

Bilag C: Godkendte underdatabehandlere

Underdatabehandler	Hetzner Online GmbH
CVR / Reg. nr.	DE 812873730
Ydelse / Leverance	Hosting af serverinfrastruktur, PostgreSQL-database, firewalls og backup-storage
Datacenterplacering	Nürnberg, Tyskland
Retsgrundlag / Overførsel	Inden for EU/EØS (ISO 27001-certificeret)

Ved On-Premises særinstallationer, hvor kunden selv drifter softwaren, gøres der ikke brug af underdatabehandlere til hosting af kundens produktionsdata.

Bilag D: Systemkontakter og hændelseshåndtering

- Kundeservice & teknisk support: support@practicle.dk
- Henvendelser vedrørende datasletning & rettigheder: support@practicle.dk (jf. Practicles datasletningspolitik)
- Rapportering af sikkerhedsbrud (GDPR art. 33 / NIS2-notifikation):
  - E-mail: security@practicle.dk / support@practicle.dk
  - Varslingsfrist ved konstateret brud: Uden unødig forsinkelse og senest inden for 24 timer.