Bilaga: behandling, säkerhet och leverantörer

Tillhör Plasks personuppgiftsbiträdesavtal. Version: 1.14.

1. Beskrivning av behandlingen

Del	Beskrivning
Föremål	Drift av Plask för planering och uppföljning av simundervisning.
Varaktighet	Under Huvudavtalets löptid och därefter endast under ordinarie radering och backupgallring.
Art	Insamling, registrering, strukturering, lagring, visning, ändring, export, delning enligt kundens val, support, säkerhetskopiering och radering.
Ändamål	Grupper, lektioner, närvaro, elevresultat, aktuell progress, anteckningar, uppföljning, behörighet, säkerhet, support och återställning.
Registrerade	Elever, gruppkontakter och Kundens användare. Elever kan vara barn.
Personuppgifter	Namn, frivillig skolklass, elevnivå, grupptillhörighet, närvaro, lektionsresultat, progress, anteckningar, uppföljningsstatus, kontaktuppgifter, användaridentitet och behörighet samt begränsade tekniska och revisionsuppgifter.
Särskilda kategorier	Tjänsten är inte avsedd för hälsouppgifter eller andra särskilda kategorier enligt artikel 9 GDPR. Kunden instrueras att inte lägga in sådana uppgifter.
Frekvens	Löpande när Kunden använder tjänsten.
Radering	Aktiv data raderas på Kundens instruktion. Isolerade säkerhetskopior gallras automatiskt enligt Plasks dokumenterade backup-rutin.

2. Gallring och radering

Denna gallringsrutin utgör en del av Kundens dokumenterade instruktion enligt personuppgiftsbiträdesavtalet. Kunden bestämmer hur länge verksamhetsuppgifter behöver bevaras och kan när som helst lämna en dokumenterad instruktion om radering eller återlämning.

Uppgifter	Hur länge uppgifterna sparas	Gallringsåtgärd
Elevuppgifter, gruppmedlemskap, närvaro, lektionsresultat, progress och anteckningar	Så länge Kunden använder Plask och uppgifterna behövs för Kundens verksamhet.	Raderas i det aktiva systemet efter Kundens dokumenterade instruktion eller genom tjänstens funktion för permanent elevradering.
Arkiverade grupper och lektionshistorik	Så länge Kunden behöver historiken eller till dess att Kunden begär radering.	Arkiverade grupper kan raderas permanent. Vid permanent elevradering tas eleven även bort ur arkiverade gruppkopior.
Gruppkontakter	Så länge Kunden behöver kontaktpersonen i Plask.	Raderas på Kundens instruktion eller senast när Kundens organisation raderas.
Delade progressrapporter	Länken är giltig i tre dagar och kan återkallas tidigare.	Åtkomsten upphör när länken går ut. Länkposten tas bort när Kunden återkallar eller ersätter länken eller när organisationen raderas.
Revisionsloggar	Under avtalstiden och så länge loggarna behövs för säkerhet, incidentutredning och ansvarsskyldighet.	Elevens identitet anonymiseras vid permanent elevradering. Kundens revisionsloggar raderas när Kundens organisation raderas.
Kundens användare och organisationsbehörigheter	Så länge användaren ska ha tillgång till Kundens organisation.	Medlemskap och behörighet tas bort på Kundens instruktion eller när organisationen raderas. Ett användarkonto som används i en annan organisation kan finnas kvar.
Säkerhetskopior	Under säkerhetskopiornas ordinarie, dokumenterade livscykel.	Gallras automatiskt. Raderade uppgifter återförs inte till normal drift annat än vid nödvändig återställning och omfattas då fortsatt av raderingsinstruktionen.
Uppgifter hos underbiträden	Endast så länge respektive tjänst behövs för att leverera och skydda Plask.	Gallras enligt behandlingstiderna i respektive underbiträdes personuppgiftsbiträdesavtal när behandlingen upphör. Redan levererade mejl hos mottagaren ligger utanför Plasks kontroll.
Samtliga kunduppgifter när avtalet upphör	Till dess att Kunden valt återlämning eller radering.	Aktiv data återlämnas eller raderas enligt personuppgiftsbiträdesavtalets punkt 10. Kvarvarande säkerhetskopior försvinner genom ordinarie backupgallring.

Plask kontrollerar gallringsrutinen minst en gång per år och när en funktion, ett underbiträde eller en lagringslösning förändras. Genomförda raderingar på Kundens instruktion dokumenteras utan att de raderade personuppgifterna sparas som bevis.

3. Tekniska och organisatoriska huvudåtgärder

- Inbjudningsbaserad, extern inloggning utan Plask-lösenord.

- Organisationsmedlemskap och roller avgränsar åtkomst mellan kunder och behörighetsnivåer.
- Krypterad överföring över HTTPS/TLS.
- Delningslänkar använder kryptografiskt slumpade tokens, verifieras mot ett hashvärde, gäller i tre dagar och kan återkallas. Råa länkar och tokens ska inte förekomma i revisionsmetadata, felloggar eller felövervakning.
- Revisionslogg för viktiga administrativa ändringar utan att lagra råa delnings-, sessions- eller OAuth-tokenvärden.
- Felövervakning filtrerar känsliga fältnamn och tokeniserade länkar. Text, formulärfält och media maskeras i sessionsåtergivning.
- Privata säkerhetskopior med skriv-/raderingsskydd och automatisk gallring enligt Plasks dokumenterade backup-rutin.
- Permanent elevradering omfattar relaterad progress, lektionsdata, anteckningar, arkiverade gruppkopior och cachade operationer; elevnamn i revisionshistorik anonymiseras.
- Begränsad administrativ åtkomst, sekretess, loggning, säker konfigurationshantering och rutin för incidenter och återställning.
- Löpande uppdatering av beroenden och rimliga kontroller av tjänstens tillgänglighet och databasanslutning.

4. Underbiträden för kunddata

Underbiträdeslistan ska kontrolleras när en leverantör eller tjänst förändras. Leverantörernas egna aktuella underbiträden och exakta behandlingsplatser framgår av deras avtals- och underbiträdesinformation.

Den publika, aktuella versionen finns på https://app.plask.nu/subprocessors.

Leverantör	Tjänst och uppgifter	Huvudsaklig konfiguration / överföringsstöd
Render Services, Inc.	Applikationsdrift, PostgreSQL-databas och schemalagda driftjobb. Kan behandla alla kunduppgifter som lagras i tjänsten.	Primär drift och databas i Frankfurt, Tyskland. Leverantörens DPA och vid behov standardavtalsklausuler.
Cloudflare, Inc.	Privat R2-lagring av krypterade databasbackuper.	EU-jurisdiktion för lagringen; global leverantör. Leverantörens DPA och vid behov standardavtalsklausuler.
Plus Five Five, Inc. (Resend)	Transaktionsmejl, exempelvis inbjudningar och utskick av progressrapportlänk. Behandlar mottagaradress, meddelandeinnehåll och leveransmetadata.	Leverantörens DPA och vid behov standardavtalsklausuler. Elevnamn och anteckningstext skickas inte i dagliga sammanfattningar.
Functional Software, Inc. d/b/a Sentry	Felövervakning och begränsad sessionsåtergivning. Kan behandla tekniska identifierare och filtrerad diagnostik; kunddata kan förekomma oavsiktligt i felkontext.	Text, inmatningar och media maskeras och känsliga fält filtreras i Plask. Leverantörens DPA och vid behov standardavtalsklausuler.

Leverantörernas avtalsunderlag:

- Render – Data Processing Addendum
- Cloudflare – Data Processing Addendum
- Resend – juridiska dokument

- Sentry – Data Processing Addendum

5. Övrig extern behandling

Microsoft används för användarnas inloggning. Microsoft behandlar då användarens kontouppgifter enligt de villkor som gäller för Microsoft-kontot och inloggningstjänsten. Microsoft får normalt inte elev-, närvaro-, progress- eller anteckningsdata genom inloggningen och anges därför inte ovan som underbiträde för själva elevdatat.

DNS- och certifikattjänster kan behandla vanliga nätverksuppgifter men får inte databasinnehåll eller säkerhetskopior genom sin normala funktion.

6. Ändringar

Plask informerar Kundens registrerade avtals- eller dataskyddskontakt minst 30 dagar före ett planerat nytt eller utbytt underbiträde. Kunden ska hålla sin kontaktadress aktuell och kan invända enligt Biträdesavtalet.