

Konsekvensbedömning av dataskydd

För kommunal skolverksamhet som använder Prakto

Förifyllt utkast enligt GDPR artikel 35 – avsett att spara veckor av juristarbete för kommunala dataskyddsombud. Strukturen följer IMY:s mall för konsekvensbedömning.

DOKUMENTINFORMATION

Version	1.0	Tillhandahållare	Prakto
Datum	13 juni 2026	Org.nr	559489–8917
Status	Utkast	DPO	dpo@prakto.se
Referens	IMY:s DPIA-mall	Trust Center	prakto.se/sakerhet

Utkastet ersätter inte Er konsekvensbedömning. Det är Ert ansvar som personuppgiftsansvarig att granska, anpassa, slutföra och godkänna bedömningen.

Om detta dokument. Detta är ett *förifyllt utkast* till konsekvensbedomning enligt GDPR art. 35 som OptiTech Sverige AB tillhandahåller *kostnadsfritt* till kommunala skolhuvudmän som använder eller utvärderar Prakto. Det är avsett att spara veckor av juristarbete genom att förifylla de delar som gäller själva tjänsten (Prakto), så att Ert dataskyddsombud (DSO) kan koncentrera sig på de organisations- och konfigurationsspecifika delarna.

Ansvar. Utkastet ersätter inte Er konsekvensbedomning. Det är Ert ansvar som personuppgiftsansvarig att granska, anpassa, slutföra och godkänna bedomningen. Avsnitt markerade med en **gul ruta** kräver Er aktiva ifyllnad.

Referenser. Strukturen följer IMY:s mall för konsekvensbedomning (imy.se). Underliggande tekniska och organisatoriska säkerhetsåtgärder beskrivs i Praktos Trust Center (prakto.se/sakerhet) samt i Praktos CSA STAR CAIQ self-assessment.

Innehåll

1 Inledning och syfte med bedomningen	4
1.1 Vad är Prakto?	4
1.2 Varför krävs en konsekvensbedomning?	4
1.3 Avgränsning	4
2 Beskrivning av behandlingen	4
2.1 Ändamål	4
2.2 Kategorier av registrerade	5
2.3 Kategorier av personuppgifter	5
2.4 Behandlingens omfattning och varaktighet	6
2.5 Mottagare och tredje ländersexport	6
3 Bedomning av nödvandighet och proportionalitet	6
3.1 Rättslig grund	6
3.2 Dataminimering	7
3.3 Lagringsperiodernas längd	7
3.4 Information till de registrerade	8
4 Riskbedomning	8
4.1 Riskmatris (standardkonfiguration)	8
4.2 Risker för barn (under 18 år)	8
5 Åtgärder för att hantera riskerna	9
5.1 Tekniska åtgärder	9
5.2 Organisatoriska åtgärder	9
5.3 Registrerades rättigheter	9

6	Förblirande risk efter åtgärder	10
6.1	Förhandssamråd med IMY	10
7	Godkännande och versionshantering	10

1 Inledning och syfte med bedomningen

1.1 Vad är Prakto?

Prakto är en svensk EdTech-plattform som koordinerar arbetsplatsförlagt lärande mellan elever, skolor och värdföretag. Tjänsten täcker hela livscykeln: matchning av elev mot praktikplats, ansökan, avtalshantering, handledning, löpande dagbok och tidrapportering, bedömning och slutintyg. Tjänsten omfattar fyra juridiskt distinkta placeringstyper: **LIA** (yrkeshögskola), **APL** (gymnasium), **VFU** (universitet) och **PRAO** (grundskola).

1.2 Varför krävs en konsekvensbedomning?

Enligt GDPR art. 35 ska personuppgiftsansvariga genomföra en konsekvensbedomning när en behandling sannolikt leder till hög risk för registrerades rättigheter och friheter. För kommunal skolverksamhet talar följande omständigheter för att DPIA är nödvändig:

- Behandling av personuppgifter om **barn** (under 18 år) i grundskolan och gymnasiet — IMY identifierar barns uppgifter som hög-risk-kategori.
- Storskalig behandling av personuppgifter (kommun med många elever).
- Överföring av uppgifter till tredje part (värdföretag, handledare).
- Användning av AI-funktioner (matchningsförslag, CV-analys).
- Geolokalisering vid matchning (närhetsberäkning hem-praktikplats).

1.3 Avgränsning

Detta utkast behandlar Praktos *standardkonfiguration*. Följande tillval kan påverka bedomningen och måste utvärderas separat:

- Aktivering av AI-funktioner (matchningsförslag, CV-analys, AI-chatt).
- Aktivering av SSO med externa identitetsleverantörer (Google Workspace, Microsoft Entra).
- Användning av Inngest-cron-jobb för påminnelser via e-post.
- Aktivering av community-funktioner (eleven publicerar inlägg).

2 Beskrivning av behandlingen

2.1 Ändamål

1. Administrera arbetsplatsförlagt lärande (LIA/APL/VFU/PRAO) för eleverna på respektive skola.
2. Matcha elever mot lämpliga praktikplatser baserat på program, intressen, geografi och företagets kompetenskrav.
3. Möjliggöra kommunikation mellan elev, lärare/kontaktperson, handledare och skoladministration.
4. Dokumentera löparande arbete (dagbok, tidrapport, mål, möten) under praktikperioden.
5. Producera bedömning, intyg och betygsunderlag enligt kursplan.
6. Lagra avtal mellan skola, elev och företag inklusive elektronisk signatur.

2.2 Kategorier av registrerade

KATEGORI	ANMÄRKNING
Elever	Inkl. barn under 18 år på grundskola och gymnasium.
Vårdnadshavare	Endast där samtycke krävs för specifik behandling (t.ex. publicering av bild).
Handledare	Anställda hos värd företag.
Lärare och kontakt-personer	Anställda hos skolhuvudmannen.
Skoladministratörer	Anställda hos skolhuvudmannen.
Företagsanvändare	Anställda hos värd företag som hanterar annonser och ansökningar.

2.3 Kategorier av personuppgifter

Förifyllt baserat på fakta i Praktos collections (`src/lib/appwrite-collections.ts`).

DATAKATEGORI	EXEMPEL PÅ UPPGIFTER	LAGLIGT STÖD
Identifikationsdata	Namn, e-postadress, användar-id, klass/program.	Avtal med skolhuvudman; uppgift av allmänt intresse.
Kontaktdata	Telefonnummer, hemadress (frivilligt).	Avtal; samtycke för frivilligt.
Akademisk data	Programtillhörighet, kursresultat, närvaro, mentor, framstegsbedomning.	Uppgift av allmänt intresse (skollagen).
LIA/APL/VFU/PRAO Dagboksanteckningar, tidrapporter, data	målbeskrivningar, mötesprotokoll, handledaromdoming.	Avtal; uppgift av allmänt intresse.
Praktikplats-relaterad data	Vilket företag, vilken handledare, period, status (söker/godkänd/pågående/avslutad).	Avtal med skolhuvudman.
Avtals- och signatur-data	Praktikavtal, signaturer (BankID-attribut: namn, personnummer-hash, IP, tidsstämpel), revisionshistorik.	Avtal; intresseavvägning för bevisvärde.
Kommunikationsdata	Meddelanden mellan elev/lärare/handledare, närvarobekräftelser, påminnelser.	Avtal.
Bedomning och intyg	Slutbetyg, slutintyg, recension.	Uppgift av allmänt intresse (skollagen, arkivlagen).
Tekniska loggar	IP-adress (trunkerad), user-agent, audit-logg över känsliga åtgärder.	Intresseavvägning (säkerhet).

DATAKATEGORI	EXEMPEL PÅ UPPGIFTER	LAGLIGT STÖD
Tillval: AI-data	Förfrågningar och svar från AI-funktioner. Fritext maskeras innan den sänds till underbiträde.	Intresseavvägning; opt-out per skola.

Inga känsliga personuppgifter enligt GDPR art. 9 behandlas i standardkonfigurationen. Skolan ansvarar för att inte ladda upp sådana uppgifter i fritextfält.

2.4 Behandlingens omfattning och varaktighet

[KUND FYLLER I] Ange uppskattat antal registrerade per kategori under en trearsperiod:

- Antal elever: _____
- Antal lärare/kontaktpersoner: _____
- Antal värd företag och handledare: _____
- Antal praktikperioder per år: _____

2.5 Mottagare och tredje ländersexport

Mottagare av personuppgifter består av kommunens egna användare samt OptiTech Sverige AB och dess underbiträden, vilka listas separat i dokumentet *Prakto - Subprocessors*. Sammanfattning:

UNDERBITRÄDE	SYFTE	BEHANDLADE UPPGIFTER	LOKALISERING
Appwrite	Hosting (BaaS)	Alla Kunddata	EU
Resend	Transaktions-e-post	E-postadress, meddelande-innehåll	EU
Inngest	Cron och bakgrundsjobb	Användar-id, tidsstämplar	EU
NVIDIA NIM	AI-inferens (tillval)	Maskerad fritext	EU
OpenAI	AI-tjänster (tillval)	Maskerad fritext	EU/USA (SCC)
Sentry	Felrapportering	Tekniska metadata, scrubbade	EU
Upstash Redis	Rate-limiting	Tunna nycklar (användar-id, IP)	EU

Fullständig och uppdaterad lista publiceras på prakto.se/sakerhet/underbitraden.

3

Bedomning av nödvandighet och proportionalitet

3.1 Rättslig grund

1. **Avtal** (art. 6.1.b) för behandling som är nödvändig för att fullgöra avtalet mellan skolhuvudman och elev (administration av praktik).

2. **Uppgift av allmänt intresse** (art. 6.1.e) för behandling som är nödvändig för skolhuvudmannens uppdrag enligt skollagen och liknande författningar.
3. **Rättslig förpliktelse** (art. 6.1.c) för bevarande enligt arkivlagen (slutbetyg, slutintyg).
4. **Samtycke** (art. 6.1.a) för frivillig behandling som inte täcks ovan (t.ex. publicering av bild i community-funktion, frivilliga uppgifter i CV).

3.2 Dataminimering

Prakto tillämpar dataminimering på följande sätt:

- Eleven ser endast egna uppgifter; handledaren ser endast uppgifter om de elever de handleder.
- Kommunal multi-tenancy säkerställs med kolumn-baserad isolering (`school_id` på varje dokument).
- AI-funktioner får endast maskerad fritext, inte rå personuppgifter (se `src/lib/ai/redact.ts`).
- Audit-loggar innehåller aldrig lösenord, personnummer eller andra känliga uppgifter (automatisk scrubbing).

3.3 Lagringsperiodernas längd

Standardgallringspolicy som tilldelas *varje skola* och som kan justeras av skolans dataskyddsombud:

RESURS	LAGRINGSTID	MOTIVERING
Kontaktuppgifter elev	1 år efter avslut	GDPR storage limitation.
Ansökningar (fritext)	2 år	Anonymiseras därefter.
Dagbok (<code>lia_journal</code>)	6 mn efter avslut	Personlig reflektion, ej bevarandepliktig.
Tidrapport (<code>lia_time</code>)	5 år aggregerat	Detalj anonymiseras efter 6 mn.
Slutbedoming (<code>evaluations</code>)	Bevaras	Arkivlagen 3 § p. 1.
Slutintyg (<code>certificates</code>)	Bevaras	Bevisvärde för eleven.
AI-chatt (<code>ai_chats</code>)	30 dagar	Känslig fritext gallras snabbt.
Audit-logg för signatur (<code>signing_audit_log</code>)	Minst 10 år	Bevisvärde av elektronisk signatur.
Kommunikationstrad	2 år efter sista meddelande	Anonymiseras därefter.

[KUND FYLLER I] Eventuella avvikelser från standardpolicy som er kommun beslutat — t.ex. längre bevarande av tidrapporter för löneunderlag, eller kortare bevarande av kommunikation:

3.4 Information till de registrerade

Prakto tillhandahåller standardmallar för informationstext till elev, vårdnadshavare och handledare. Skolan ansvarar för att anpassa och publicera dessa enligt GDPR art. 13–14.

4

Riskbedoming

4.1 Riskmatris (standardkonfiguration)

Skala: Laag Medel Hog

RISK	SANNOLIKHET		KONSEKVENS	MOTIVERING
Obehörig åtkomst till elev-data (extern angripare)	Låg	Hög		Brandvägg, kryptering i transit/vila, auditloggning, MFA, rate-limit.
Obehörig åtkomst inom kommunen (t.ex. fel lärare)	Låg	Medel		Roll-baserad åtkomstkontroll och <code>school_id</code> -skoping i varje databas-fråga.
Datalek via handledar-portal (token-länk)	Låg	Medel		Token hashas i databas, TTL 90 dagar, rate-limit per IP, audit-logg per användning.
Felaktig matchning (AI-modell)	Medel	Låg		AI är beslutsstöd — aldrig automatiserade beslut om enskild. Människa godkänner.
Förlust av tillgänglighet	Låg	Medel		Daglig backup, RPO 24 timmar, RTO 8 timmar.
Överföring till tredje land via AI-leverantör (tillval)	Låg	Medel		SCC art. 46; maskering innan över-saning; zero data retention där till-gaangligt.
Bristande gallring (data lever för länge)	Medel	Medel		Schemalagd gallringsautomatik enligt avsnitt 3.3.

4.2 Risker för barn (under 18 år)

Eftersom Prakto behandlar uppgifter om elever i grundskolan och gymnasiet krävs särskild aktsamhet:

- Inga marknadsföringsfunktioner mot barn.
- AI-funktioner är opt-in per skola och kan stängas av för specifika åldersgrupper.
- Vårdnadshavarsamtycke krävs för behandling som inte stoder sig på avtal eller uppgift av allmänt intresse.
- Inga uppgifter delas med tredje part för analys eller annonsering.

[KUND FYLLER I] Beskriv kommunens rutin för att inhämta och dokumentera vårdnadshavarsamtycke vid behov:

5 Åtgärder för att hantera riskerna

Förifyllt baserat på kontroller som Prakto har implementerat. Tekniska detaljer finns i Prakto's CSA STAR CAIQ self-assessment.

5.1 Tekniska åtgärder

- **Kryptering i transit:** TLS 1.2+ på alla endpoints. HSTS.
- **Kryptering i vila:** AES-256 i databas och objektsstorage.
- **Stark autentisering:** BankID, SSO (SAML/OIDC) eller användarnamn+lösenord med tvåfaktor-stöd. Lösenord lagras endast som bcrypt-hash.
- **Token-säkerhet:** HMAC-signerade tokens med constant-time-jämförelse (`crypto.timingSafeEqual`). Magic-länkar för handledare hashas (sha256) i databas — klartext lagras aldrig.
- **Rate-limiting:** Per användare och per IP på alla känsliga endpoints. Distribuerad via Upstash Redis.
- **Magic-byte-validering** av uppladdade filer (`lib/file-magic.ts`) för att förhindra MIME-spoofing.
- **Audit-logg:** Alla känsliga åtgärder skrivs till `audit_logs` med actor, IP, user-agent, tidsstämpel. PII auto-scrubbas.
- **Multi-tenancy:** Kolumn-baserad isolering. Varje databasfråga måste filtrera på `school_id/companyId`. Centraliserad i `lib/auth-helpers.ts`.
- **PII-maskering till AI:** Personuppgifter redigeras innan AI-anrop (`src/lib/ai/redact.ts`).

5.2 Organisatoriska åtgärder

- Personal som har åtkomst till produktionsdata är få och dokumenterade.
- Background-check på all personal.
- DPA undertecknad med kund (separat dokument *Prakto - DPA*).
- Underbiträdeslistan är publik och versionerad.
- Incident response-plan (mnål: notifiering inom 72 timmar enligt art. 33).
- årlig granskning av Trust Center och CSA STAR CAIQ.

5.3 Registrerades rättigheter

Prakto ger kommunen tekniska verktyg för att fullgora art. 15–22:

- **Tillgång (art. 15):** Eleven kan ladda ner all egen data från kontoinställningar.
- **Rättelse (art. 16):** Eleven kan redigera egna uppgifter i profilen.

- **Radering (art. 17):** Kommunen kan utöka standardgallringpolicy med ad-hoc-radering per dokument.
- **Begränsning (art. 18):** Konto kan markeras som “legal hold” — då stannar all gallring.
- **Dataportabilitet (art. 20):** Export i JSON-format för överföring till annan skola/system.

6 Förblirande risk efter åtgärder

[KUND FYLLER I] Efter att Era egna organisations- och tekniska åtgärder har lagts till de som Prakto bedriver, bedöm om förblirande risk är acceptabel. Ange:

Förblirande risk: _____

Acceptabel? (Ja/Nej): _____

Motivering: _____

6.1 Förhandssamråd med IMY

Förhandssamråd med IMY enligt art. 36 krävs om DPIA visar hög residual risk. För Prakto's standardkonfiguration *bedöms inte* förhandssamråd vara nödvändigt, men:

- Aktivering av AI-funktioner för barn under 13 år kan motivera samråd.
- Användning av föreslagen geolokalisering i kombination med profilbyggande kan motivera samråd.

7 Godkännande och versionshantering

[KUND FYLLER I]

Personuppgiftsansvarig _____

Dataskyddsombud (DSO) _____

Datum för genomgång _____

Nästa planerade omprov-
ning _____

Underskrift _____

Versionshantering. Detta utkast följer Praktos huvudversion. När Prakto gör väsentliga ändringar i datakategorier, mottagare, lagringstider eller åtgärder publiceras ett nytt utkast med ändringslogg på prakto.se/sakerhet/dpia. Vi rekommenderar att Er DSO återkommer till bedoningen vid varje ny version av detta utkast.

Senast uppdaterat: 13 juni 2026. För frågor: dpo@prakto.se.