SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

Europe Cyber-Safe

Pass för AI-användning — redogörelse för självutvärdering

Organisation	Exempelbyrån Kreativ AB (15 anställda)	**Referens**	SAMPLE-0002
Genomförd den	2026-10-30	**Genomförd av**	director@example.com
Frågeuppsättning	v1.1-EU-sv (EU, sv) · `54f0865e8dc28525`		

> **Självutvärdering genomförd av organisationen. Svaren har inte granskats av Europe Cyber-Safe eller någon annan. Denna rapport är inte juridisk rådgivning.**

Rapporten beskriver läget endast per det datum då självutvärderingen slutfördes.

Klassning per område

Varje område klassas utifrån de svar som lämnats: rött om något svar utlöser rött, annars gult om något svar är gult eller obesvarat, annars grönt. Inget samlat resultat tas fram.

Område	Klassning
D1 AI-inventering	RÖD
D2 Dataskydd	RÖD
D3 Styrning och policy	RÖD
D4 Mänsklig kontroll	GUL
D5 Leverantörsuppföljning	GUL
D6 Hantering av AI-incidenter	GUL

Åtgärder

Röda områden först, därefter de snabbaste först.

#	Område	Åtgärd	Insats
1	D1	Utse en ansvarig för förteckningen och ange det i AI-policyn.	en timme
2	D1	Lägg in en kvartalsvis avstämning av förteckningen i den ansvariga personens kalender.	en timme
3	D2	Lägg till ett avsnitt om AI-användning i integritetspolicyn med ändamål och kategorier av leverantörer; publicera det och informera personalen.	en timme
4	D2	Dela ut listan över vad som inte får föras in till all personal och sätt upp den där verktygen används.	en timme

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

5	D2	Dokumentera för varje verktyg var uppgifterna finns och vilken överföringsmekanism som används, utifrån leverantörens dokumentation; där uppgifter lämnar EES, bekräfta mekanismen (ett beslut om adekvat skyddsnivå, eller EU:s standardavtalsklausuler med en bedömning av överföringen).	en timme
6	D2	Ta för varje verktyg reda på raderingsfunktionen eller det avtalsmässiga åtagandet om radering; sluta använda verktyg där inget av dem finns och personuppgifter berörs.	en timme
7	D3	Utse en beslutsansvarig för AI och skriv ned de tre frågor hen ställer innan ett verktyg godkänns (vilka uppgifter, vilka villkor, vem som kontrollerar resultatet).	en timme
8	D1	Gör klart AI-inventeringen med hjälp av mallen; fråga varje teamledare vilka verktyg de och deras team använder, inklusive webbläsartillägg och mobilappar.	en dag
9	D1	Sluta omedelbart att föra in personuppgifter i verktyg med konsumentvillkor eller okända villkor. Flytta antingen användningen till en företagsnivå med personuppgiftsbiträdesavtal, eller upphör med användningen.	en dag
10	D1	Gå igenom AI-inställningarna i varje större produkt (mötestranskribering, sammanfattning, autokomplettering) och för in dem i förteckningen; bestäm vilka som ska stängas av.	en dag
11	D2	Använd mallen för förbedömning av DPIA för varje verktyg som berör personuppgifter; genomför en fullständig konsekvensbedömning (DPIA) där förbedömningen visar att det behövs.	en dag
12	D3	Anta mallen för AI-policy (två sidor), låt ägaren skriva under den, dela ut den till all personal och notera vem som har tagit del av den.	en dag
13	D3	Håll ett entimmespass om AI-medvetenhet för all personal (med mallpresentationen) och spara närvarolistan.	en dag
14	D3	Gå igenom de fem viktigaste kundavtalen och er yrkesorganisations vägledning om AI med avseende på sekretess- och AI-klausuler; dokumentera resultatet.	en dag
15	D4	Informera personalen om AI:s typiska fel med hjälp av den ensidiga vägledningen; ta med ett verkligt exempel från er egen bransch.	en timme
16	D4	Kom överens om en enkel konvention (en sidfot, ett fält, en mapp) för att märka AI-stödda resultat som har betydelse.	en timme
17	D5	Läs varje leverantörs beskrivning av hur data används; slå på möjligheten att avböja eller byt till en nivå där träning är undantagen; dokumentera resultatet i förteckningen.	en timme
18	D5	Samla in underlag från säkerhetssidan eller förtroendecentret (trust center) för varje leverantör och förvara det tillsammans med förteckningen.	en timme
19	D5	Utse vem som tar emot leverantörsmeddelanden; skriv en avslutsanteckning på ett stycke per kritiskt verktyg (hur man exporterar, hur man avslutar).	en timme
20	D6	Lägg till AI-incidenter i den befintliga rutinen för incidenter eller klagomål, med tre exempel och en namngiven kontaktperson.	en timme

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

21	D6	Utse den som beslutar vid personuppgiftsincidenter och ha er dataskyddsmyndighets anmälningsformulär för personuppgiftsincidenter och en mall för incidentlogg nära till hands (art. 33 i GDPR kräver att varje incident dokumenteras).	en timme
22	D6	Aktivera aktivitetsloggning i verktyg med företagsnivå; där det inte finns, för en enkel gemensam logg över användning som rör personuppgifter eller konfidentiella uppgifter.	en timme
23	D4	Inför ett kontrollsteg med en namngiven person för alla AI-resultat som når kunder eller påverkar register; gör det till en del av det ordinarie godkännandet.	en dag
24	D5	Skaffa företagsvillkoren eller personuppgiftsbiträdesavtalet för varje leverantör; där sådant saknas, sluta skicka personuppgifter till den leverantören.	en dag
25	D5	Flytta AI-verktygen till företagsadministrerade konton med MFA; lägg till dem i checklistan för personal som slutar.	en dag
26	D6	Testa exporten en gång för varje kritiskt verktyg och dokumentera hur åtkomsten stängs av; förvara viktiga uppgifter utanför verktyget.	en dag
27	D4	Dokumentera kontrollsteget, den rättsliga grunden och de kontroller av partiskhet som görs; avgör om användningen omfattas av bilaga III till AI-förordningen och planera för de skyldigheter för tillhandahållare som gäller från och med den 2 december 2027.	en vecka

Lämnade svar

D1 AI-inventering — RÖD

ID	Fråga	Svar	Nivå
D1-1	Har ni förtecknat alla AI-verktyg som används i verksamheten, inklusive gratiskonton som personalen använder på egna enheter eller med egna inloggningar?	Ingen förteckning	röd
D1-2	Tar något verktyg i förteckningen emot personuppgifter om kunder, patienter, klienter eller anställda?	Ja - i minst ett verktyg med konsumentvillkor, eller där villkoren är okända	röd
D1-3	Finns det en namngiven person som ansvarar för att hålla förteckningen aktuell och för att godkänna nya verktyg?	Nej	gul
D1-4	Ingår AI-funktioner som är inbyggda i produkter ni redan använder (e-post, CRM, ekonomisystem, webbläsare, mötesverktyg, telefoner) i förteckningen?	Osäker	gul
D1-5	När stämdes förteckningen senast av mot vad personalen faktiskt använder?	Aldrig, eller ingen förteckning	röd

D2 Dataskydd — RÖD

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

ID	Fråga	Svar	Nivå
D2-1	Framgår det av er integritetspolicy att AI-verktyg används, för vilka ändamål och med vilka leverantörer, så att kunder och personal får veta det?	Nej	röd
D2-2	Har ni, för verktyg som behandlar personuppgifter, genomfört en konsekvensbedömning avseende dataskydd (DPIA) eller en dokumenterad förbedömning som kom fram till att en sådan inte behövs?	Nej	röd
D2-3	Har personalen en skriftlig lista över vad som aldrig får föras in i ett AI-verktyg (till exempel patientuppgifter, kortnummer, kunduppgifter som identifierar klienter, lösenord)?	Muntligt besked, inget skriftligt	gul
D2-4	Vet ni var varje leverantör lagrar och behandlar era uppgifter, och om de lämnar Europeiska ekonomiska samarbetsområdet (EES)?	För vissa verktyg	gul
D2-5	Kan ni radera, eller låta leverantören radera, uppgifter som finns i varje AI-verktyg när ni slutar använda det eller när en person begär det?	Osäker	gul

D3 Styrning och policy — RÖD

ID	Fråga	Svar	Nivå
D3-1	Finns det en skriftlig AI-policy som personalen har tagit del av och som anger vad som är tillåtet och inte?	Utkast finns men har inte delats ut	gul
D3-2	Vem beslutar om ett nytt AI-verktyg eller en ny AI-funktion får användas i verksamheten?	Ledningen, informellt	gul
D3-3	Anger policyn förbjudna användningsområden - till exempel att fatta beslut om personer utan mänsklig kontroll, eller att ta fram innehåll som framställs som skrivet av en människa när det skulle vara vilseledande?	Ja	grön
D3-4	Har all personal som använder AI-verktyg fått medvetandeutbildning under de senaste 12 månaderna om gränser för vad som får föras in, typiska fel och policyn?	En del av personalen	gul
D3-5	Begränsar era kund- eller klientavtal, yrkesregler eller tillsynsmyndighet hur ni får använda AI med deras information, och följer ni det?	Begränsningar finns och vi är osäkra på om vi följer dem	röd

D4 Mänsklig kontroll — GUL

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

ID	Fråga	Svar	Nivå
D4-1	Kontrolleras AI-resultat av en kompetent person innan det går till en kund, in i ett register eller in i ett beslut om en person?	Oftast	gul
D4-2	Känner den personal som använder AI-verktyg till vilka slags misstag verktygen gör - påhittade fakta och källhänvisningar, inaktuell information, felaktigheter som framförs med säkerhet, partiskhet?	En del av personalen	gul
D4-3	Kan ni i efterhand se vilka dokument, e-postmeddelanden eller registerposter som har tagits fram med hjälp av AI?	Ibland	gul
D4-4	Är en namngiven person ansvarig för ett AI-stött beslut på exakt samma sätt som för ett beslut som fattats av en människa?	Ja	grön
D4-5	Använder ni AI för rekrytering, kredit, prissättning, behörighet, prestationsbedömning eller andra beslut om enskilda personer?	Ja, med meningsfull mänsklig kontroll och en dokumenterad grund	gul

D5 Leverantörsuppföljning — GUL

ID	Fråga	Svar	Nivå
D5-1	Har ni för varje AI-leverantör som behandlar era uppgifter ett avtal eller villkor som innehåller ett personuppgiftsbiträdesavtal?	För vissa	gul
D5-2	Vet ni om varje leverantör använder era indata för att träna eller förbättra sina modeller, och har ni avböjt det där det är möjligt?	Okänt	gul
D5-3	Har ni sett några oberoende belägg för säkerheten från varje leverantör (till exempel ISO/IEC 27001-certifikat, SOC 2-rapport, ett nationellt grundskyddsramverk, sammanfattning av penetrationstest)?	Nej	gul
D5-4	Styrs åtkomsten till varje AI-verktyg med företagskonton, flerfaktorsautentisering och borttagning när personal slutar?	Delvis	gul
D5-5	Om en leverantör ändrade sina villkor, drabbades av ett säkerhetsintrång eller lade ned, skulle ni få veta det, och har ni ett sätt att snabbt sluta använda den?	Nej	gul

D6 Hantering av AI-incidenter — GUL

ID	Fråga	Svar	Nivå

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

D6-1	Vet personalen vad som räknas som en AI-incident (till exempel personuppgifter som klistrats in i ett verktyg, ett skadligt eller felaktigt resultat som någon agerat på, ett meddelande om säkerhetsintrång från en leverantör) och hur den ska rapporteras?	Informellt	gul
D6-2	Skulle ni klara anmälan inom 72 timmar till er dataskyddsmyndighet enligt dataskyddsförordningen (GDPR) om personuppgifter röjdes via ett AI-verktyg?	Osäker	gul
D6-3	Har ni haft en AI-incident, eller genomfört en skrivbordsövning för en, under de senaste 12 månaderna?	Ja	grön
D6-4	Sparar ni tillräckligt med uppgifter (vem som använde vilket verktyg, när och till vad) för att i efterhand kunna utreda en AI-incident?	Delvis	gul
D6-5	Skulle ni kunna sluta använda ett visst AI-verktyg inom en arbetsdag om det kompromitterades, utan att förlora viktiga verksamhetsuppgifter?	Delvis	gul

Vägledning som hänvisas till

- AI-förordningen (förordning (EU) 2024/1689) art. 26 (skyldigheter för tillhandahållare av AI-system med hög risk) och bilaga III; för användning enligt bilaga III gäller dessa från och med den 2 dec. 2027 enligt förordning (EU) 2026/1744
- AI-förordningen (förordning (EU) 2024/1689) art. 4 (AI-kunnighet), tillämplig sedan den 2 feb. 2025 och ändrad genom förordning (EU) 2026/1744: leverantörer och tillhandahållare ska vidta åtgärder för att stödja AI-kunnigheten hos personal och andra som använder AI-system för deras räkning
- AI-förordningen (förordning (EU) 2024/1689) art. 50 (transparens: att informera personer om att de interagerar med ett AI-system; att upplysa om AI-genererat eller manipulerat innehåll), tillämplig sedan den 2 aug. 2026
- ISO/IEC 27001:2022; nationella grundskyddsramverk (till exempel BSI IT-Grundschutz, CyberFundamentals); flerfaktorsautentisering och rutiner för behörigheter när personal börjar och slutar
- Europeiska kommissionen, AI literacy - Questions and Answers (2025)
- Europeiska dataskyddsstyrelsen (EDPB), yttrande 28/2024 om vissa dataskyddsaspekter av behandling av personuppgifter i samband med AI-modeller (dec. 2024); er nationella dataskyddsmyndighets vägledning om AI (till exempel Integritetsskyddsmyndigheten (IMY))
- Nationell arbetsrätt och regler om medbestämmande och arbetstagarrepresentation när det gäller övervakning och AI vid rekrytering och arbetsledning; AI-förordningen (förordning (EU) 2024/1689) bilaga III punkt 4 (användning inom anställning är hög risk)
- ENISA, Multilayer Framework for Good Cybersecurity Practices for AI (2023); NCSC/CISA och partnermyndigheter, Guidelines for secure AI system development (nov. 2023)
- EU:s likabehandlingsdirektiv (2000/43/EG, 2000/78/EG, 2006/54/EG) och nationell diskrimineringslagstiftning (direkt och indirekt diskriminering)
- Dataskyddsförordningen (GDPR) art. 22 (automatiserat individuellt beslutsfattande); artikel 29-gruppens riktlinjer om automatiserat beslutsfattande och profilering (WP251 rev.01)
- Dataskyddsförordningen (GDPR) art. 33-34 (anmälan till tillsynsmyndigheten inom 72 timmar när det finns en risk för enskilda; dokumentation av varje personuppgiftsincident); EDPB:s riktlinjer 9/2022 om anmälan av personuppgiftsincidenter

SYNTETISKT EXEMPEL — INTE EN KUNDBEDÖMNING

- Dataskyddsförordningen (GDPR) art. 35 (konsekvensbedömning avseende dataskydd); artikel 29-gruppens riktlinjer om konsekvensbedömning (WP248 rev.01, som EDPB har ställt sig bakom); er nationella myndighets förteckning över behandlingar som kräver en konsekvensbedömning (DPIA)
- Dataskyddsförordningen (GDPR) kapitel V (art. 44-49): beslut om adekvat skyddsnivå; standardavtalsklausuler (kommissionens beslut 2021/914); EDPB:s rekommendationer 01/2020 om kompletterande åtgärder
- Dataskyddsförordningen (GDPR) art. 12-14 (information som ska lämnas till enskilda)
- ENISA:s vägledning om incidenthantering; ert nationella CSIRT:s vägledning om rapportering; rapportering enligt NIS 2 art. 23 (i Sverige genomfört genom cybersäkerhetslagen; för verksamhetsutövare som omfattas)
- ISO/IEC 42001:2023, ledningssystem för AI (roller, konsekvensbedömning, livscykel, leverantörer)
- ISO/IEC 27001:2022 bilaga A 8.15 (loggning) och 8.16 (övervakningsaktiviteter)
- NIST AI Risk Management Framework 1.0 (Govern, Map, Measure, Manage) och dess Generative AI Profile (NIST AI 600-1)
- OWASP Top 10 for LLM Applications 2025 (promptinjektion, röjande av känslig information, leveranskedja)
- ENISA:s vägledning om säkerhet i leveranskedjan för IKT; NIS 2-direktivet art. 21(2)(d) säkerhet i leveranskedjan (i Sverige genomfört genom cybersäkerhetslagen; för verksamhetsutövare som omfattas)

Hänvisningarna till vägledning är offentliga källor som anges för enkelhetens skull; kontrollera den aktuella versionen innan ni förlitar er på dem. Denna redogörelse är inte juridisk rådgivning och är inte ett certifikat.