

1. Syfte

Denna policy beskriver hur CSM NDT Certification AB (CSM) arbetar med informationshantering, dataskydd, sekretess och spårbarhet i samband med utbildning, examination, certifiering och omcertifiering inom oförstörande provning och närliggande verksamhet.

Vårt mål är att kunder, kandidater, certifikatsinnehavare, lärare, examinatorer och övriga intressenter ska känna förtroende för att information hanteras säkert, korrekt och med respekt för både personlig integritet och certifieringsprocessens integritet.

2. Våra grundprinciper

CSM behandlar information enligt följande principer:

Princip	Vad det betyder hos CSM
Laglighet och tydlighet	Personuppgifter och annan information hanteras för tydliga ändamål och med tillämplig rättslig grund.
Minimering	Vi behandlar endast de uppgifter som behövs för ändamålet.
Korrekthet	Uppgifter ska vara så korrekta och uppdaterade som möjligt.
Sekretess	Examineringsmaterial, resultat, personuppgifter och annan känslig information skyddas mot obehörig åtkomst och spridning.
Spårbarhet	Underlag som ligger till grund för examination, certifiering och omcertifiering ska kunna följas upp i efterhand.
Opertiskhet	Informationshantering ska stödja en rättvis, oberoende och opartisk certifieringsprocess.
Säkerhet	Information skyddas genom tekniska, organisatoriska och administrativa åtgärder.

3. Vilken information vi kan hantera

Beroende på relation och ärende kan CSM hantera exempelvis namn, kontaktuppgifter, arbetsgivare eller beställare, identitetsuppgifter, anmälningar, kurs- och examinationsuppgifter, resultat, synintyg, uppgifter om utbildning och erfarenhet, certifikat, giltighetstider, omcertifieringsunderlag, faktureringsuppgifter samt relevant kommunikation.

CSM hanterar även examineringsprov, facit, bedömningsunderlag, praktisk examineringsdata, avvikelser, incidenter och annan dokumentation som behövs för att genomföra, följa upp och kvalitetssäkra examination och certifiering.

4. Varför vi hanterar information

CSM hanterar information för att kunna administrera utbildningar, ta emot anmälningar och ansökningar, genomföra examinationer, fatta och dokumentera certifieringsbeslut, utfärda certifikat, hantera omcertifiering, uppfylla krav enligt standarder och ackreditering,

kommunicera med kunder och kandidater, fakturera, arkivera och hantera uppföljning, avvikelser och klagomål.

När behandling av personuppgifter krävs sker den med en rättslig grund, exempelvis avtal, rättslig förpliktelse, berättigat intresse eller samtycke när detta är relevant och lämpligt.

5. Personuppgifter och rättslig grund

CSM är personuppgiftsansvarig för den behandling av personuppgifter som sker inom ramen för CSM:s egen verksamhet, om inte annat framgår av särskilt avtal eller särskild information.

Personuppgifter behandlas endast när det finns ett tydligt ändamål och en tillämplig rättslig grund. Uppgifter som krävs för examination, certifiering, omcertifiering, spårbarhet, bokföring, avtal eller ackrediteringskrav hanteras normalt utan att separat samtycke krävs. Samtycke används framför allt när behandlingen är frivillig och inte nödvändig för certifieringsverksamheten, till exempel viss marknadskommunikation.

6. Sekretess och skydd av examineringsmaterial

Examineringsprov, facit, bedömningsunderlag, kandidatresultat och praktisk examineringsdata är sekretessbelagd information. Sådant material hanteras endast av behöriga personer och skyddas mot obehörig åtkomst, spridning, ändring och förlust.

Alla som genom anställning, uppdrag eller annat åtagande får tillgång till sekretessbelagd information hos CSM ska omfattas av sekretessförbindelse eller motsvarande avtalsvillkor. Sekretessen gäller även efter avslutat uppdrag.

7. Åtkomst och informationssäkerhet

CSM arbetar enligt principen minsta möjliga åtkomst. Det innebär att en person endast ska ha tillgång till den information som behövs för personens roll eller uppdrag.

Information lagras i CSM:s godkända system och lagringsplatser. Privata molntjänster, privata e-postlådor, obehöriga lokala kopior och USB-minnen ska inte användas för CSM:s information om de inte uttryckligen är godkända för ändamålet.

CSM använder organisatoriska och tekniska skyddsåtgärder, exempelvis behörighetsstyrning, personlig inloggning, sekretesskrav, backup, styrda lagringsplatser, leverantörsavtal och incidenthantering.

8. Utlämnande av uppgifter

CSM lämnar endast ut uppgifter när det finns stöd för det och mottagaren har rätt att ta del av informationen.

Uppgifter kan, beroende på situation, lämnas till kandidaten eller certifikatsinnehavaren, arbetsgivare eller beställare när detta är nödvändigt och förenligt med informationen till kandidaten, behörig myndighet eller ackrediteringsorgan, IT-leverantör eller annat personuppgiftsbiträde enligt avtal, eller annan mottagare när det krävs enligt lag, avtal eller uttryckligt godkännande.

CSM är särskilt försiktigt vid utlämnande av personnummer, resultat, certifikat, kandidatunderlag och annan integritetskänslig eller sekretessbelagd information.

9. Bevarande och gallring

Uppgifter och dokumentation bevaras så länge det behövs för de ändamål de samlades in för och så länge CSM behöver uppgifterna för att uppfylla krav enligt lag, avtal, standard, ackreditering eller CSM:s egna rutiner.

Uppgifter kopplade till certifiering kan behöva bevaras under lång tid för att säkerställa spårbarhet, kunna styrka certifiering och hantera omcertifiering. När uppgifter inte längre behövs ska de gallras eller anonymiseras enligt CSM:s rutiner och tillämpliga krav.

10. Incidenter och avvikelser

CSM hanterar incidenter och avvikelser som kan påverka informationssäkerhet, personuppgifter, sekretess, spårbarhet, opartiskhet eller förtroendet för examination och certifiering.

Exempel på incidenter är felaktigt skickad e-post, obehörig åtkomst, förlorad handling, skadad examineringsdata eller misstänkt dataintrång. Incidenter utreds, dokumenteras och åtgärdas. Personuppgiftsincidenter bedöms särskilt och anmäls till Integritetsskyddsmyndigheten (IMY) när sådan skyldighet föreligger.

11. Dina rättigheter

Den som är registrerad hos CSM har rättigheter enligt GDPR. Det kan bland annat innebära rätt att få information, begära tillgång till sina personuppgifter, begära rättelse, begära radering när förutsättningar finns, begära begränsning av behandling, invända mot viss behandling och lämna klagomål till IMY.

Vissa uppgifter kan CSM behöva fortsätta behandla även om en registrerad person begär radering, exempelvis om uppgifterna behövs för att uppfylla lagkrav, ackrediteringskrav, standardkrav, avtal, bokföring eller för att kunna styrka en certifiering.

12. Kontakt

Frågor om denna policy, personuppgifter, informationssäkerhet eller utlämnande av uppgifter kan skickas till CSM via ordinarie kontaktvägar.

För att skydda den registrerades integritet kan CSM behöva kontrollera identitet innan uppgifter lämnas ut eller en begäran hanteras.