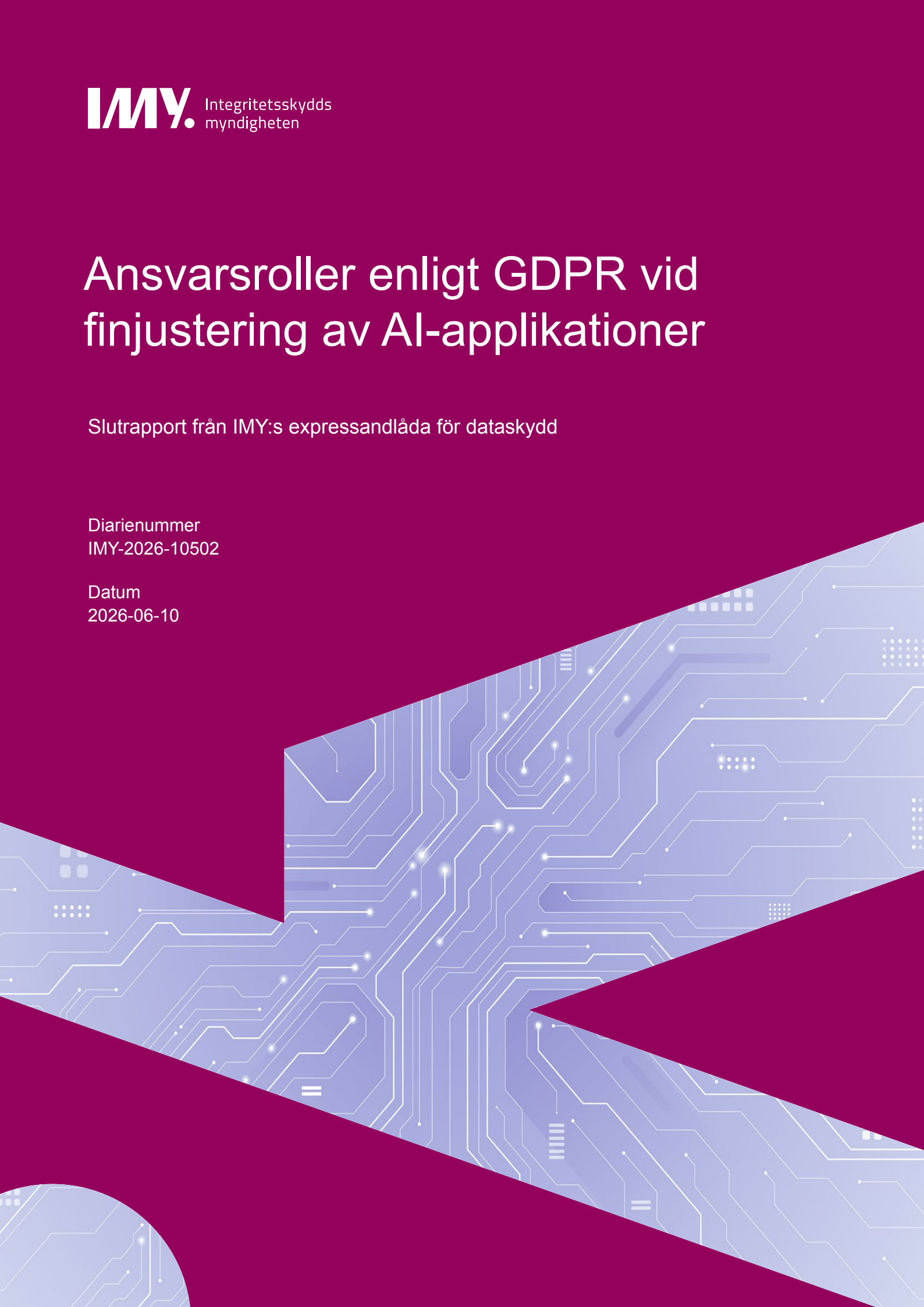
IMY. Integritetsskydds myndigheten

Ansvarsroller enligt GDPR vid finjustering av AI-applikationer

Slutrapport från IMY:s expressandlåda för dataskydd

Diarienummer
IMY-2026-10502

Datum
2026-06-10



Om expressandlådan

Under våren 2026 har IMY provat ett nytt koncept – IMY:s expressandlåda för dataskydd. Det är en kostnadsfri vägledning till privat och offentlig sektor, med fokus på små och medelstora verksamheter, som vill hantera personuppgifter på ett integritetsvänligt sätt. Den här rapporten är ett resultat av vårens pilotprojekt.

Pilotprojektet har pågått under tre månader och deltagaren Eggsplain har fått muntlig vägledning av IMY:s experter inom juridik, AI och informations- och cybersäkerhet. Syftet har varit att reda ut vilka dataskyddsfrågor som varit aktuella i projektet och att ge vägledning i dessa frågor. Expressandlådan är avsedd att fungera som en avskalad version av IMY:s innovationssandlåda för dataskydd.

För att fler ska kunna ta del av vägledningen har resultatet sammanfattats i en rapport. På så sätt bidrar expressandlådan till svensk innovation och konkurrenskraft.

Innehållsförteckning

1. Sammanfattning 4
1.1. Slutsatser 4
2. Projektet 5
2.1. Bakgrund 5
2.2. Projektets mål 5
2.3. Ansvarsroller enligt GDPR 6
2.3.1 Personuppgiftsansvarig 6
2.3.2 Gemensamt personuppgiftsansvar 7
2.3.3 Personuppgiftsbiträde 7
2.4. Tekniken 8
3. Leverantörens roll enligt GDPR 11
3.1. Installation och implementation av hårdvara 11
3.2. Användning och tillhandahållande av AI-applikationer 11
3.3. Service, uppdatering och konsulttjänster 14
4. Övriga reflektioner 15

Postadress:
Box 8114
104 20 Stockholm
Webbplats:
www.imy.se
E-post:
imy@imy.se
Telefon:
08-657 61 00

1. Sammanfattning

Eggsplain är ett svenskt teknikföretag som tillhandahåller AI-relaterad infrastruktur och AI-tjänster. Inom ramen för projektet har IMY analyserat vilken roll, enligt den allmänna dataskyddsförordningen (GDPR)[1], en leverantör kan ha när AI-applikationer tillhandahålls, anpassas eller vidareutvecklas.

Analysen fokuserar särskilt på situationer där en leverantör använder en förtränad AI-modell och finjusterar den, antingen som ett led i den egna produktutvecklingen, för en specifik kunds räkning eller inom ramen för ett gemensamt utvecklingsarbete med kunden.

1.1. Slutsatser

En leverantörs roll enligt GDPR beror på vad leverantören faktiskt gör med personuppgifter. Det räcker inte med att titta på vilken typ av tjänst leverantören tillhandahåller, exempelvis AI-teknik, infrastruktur eller support. Avgörande är i stället om leverantören behandlar personuppgifter och, i så fall, varför behandlingen sker och vem som bestämmer över den.

IMY har inom ramen för projektet särskilt analyserat följande.

Leverantörens installation och implementation av hårdvara.

En leverantör får normalt ingen roll enligt GDPR enbart genom att sälja, hyra ut, leverera eller installera hårdvara. Om leverantören däremot exempelvis migrerar kundens databaser, användarkonton eller loggar till en ny servermiljö kan leverantören behandla personuppgifter för kundens räkning. Då kan leverantören vara personuppgiftsbiträde.

Leverantörens tillhandahållande och finjustering av AI-applikationer.

Vid finjustering av AI-modeller är det framför allt viktigt att bedöma för vems syfte personuppgifterna behandlas. Om leverantören finjusterar modellen på eget initiativ, som ett led i sin produktutveckling, talar det för att leverantören är personuppgiftsansvarig för den behandlingen. Om leverantören i stället finjusterar på uppdrag av en specifik kund, enligt kundens instruktioner och för kundens syften, talar det för att kunden är personuppgiftsansvarig och leverantören är personuppgiftsbiträde. Om leverantören och kunden gemensamt bestämmer varför och hur personuppgifter ska behandlas, kan i stället gemensamt personuppgiftsansvar aktualiseras.

Leverantörens löpande tjänster som service, uppdatering och konsulttjänster.

Vid löpande tjänster kan leverantörens roll variera beroende på vilken behandlingsaktivitet som utförs. Leverantören kan vara personuppgiftsansvarig när personuppgifter behandlas för leverantörens egna ändamål, personuppgiftsbiträde när behandling sker för kundens räkning, eller sakna roll enligt GDPR i en viss aktivitet om leverantören inte behandlar personuppgifter eller endast tillhandahåller en konsult som i sitt arbete bedöms utgöra en del av kundens organisation.

---

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). ”GDPR” är en förkortning av det engelska namnet ”General Data Protection Regulation”.

2. Projektet

2.1. Bakgrund

Sverige har höga ambitioner på AI-området. I Sveriges AI-strategi anges att Sverige ska vara bland de tio främsta AI-nationerna i världen och att AI ska användas för att driva samhällsnytta, hållbar utveckling, konkurrenskraft och innovation.[2] Även AI-kommissionens färdplan för Sverige pekar på att rättslig osäkerhet riskerar att hämma utveckling och användning av AI och framhåller behovet av vägledning för aktörer som vill utveckla och använda AI på ett rättssäkert sätt.[3]

Mot denna bakgrund finns ett behov av vägledning för aktörer som utvecklar och tillhandahåller AI-relaterad infrastruktur och tjänster. I sådana miljöer kan data hanteras i flera led och flera aktörer kan vara involverade i olika behandlingsaktiviteter. När personuppgifter behandlas behöver aktörerna identifiera vilka aktiviteter som innebär behandling av personuppgifter och vilken faktisk funktion respektive aktör har i relation till dessa behandlingar. Vid behandling av personuppgifter är det av grundläggande betydelse att fastställa vilken roll de involverade aktörerna har enligt GDPR. Rollfördelningen avgör vilka skyldigheter som aktualiseras, vem som ansvarar för att uppfylla regelverkets krav och hur ansvar kan regleras mellan aktörerna. Tydlighet i dessa frågor är viktig för ansvarsfördelningen mellan aktörerna och aktörernas möjlighet att redan vid utformning, tillhandahållande eller mottagande av en tjänst identifiera vilka dataskyddsrättsliga skyldigheter som kan aktualiseras. Det är även viktigt för de registrerades möjligheter att utöva sina rättigheter, samt för samhället att skapa förutsebara rättsliga förutsättningar för innovation.

Eggsplain är ett svenskt teknikföretag som tillhandahåller digital infrastruktur och digitala tjänster.[4] Företaget erbjuder bland annat hårdvara, tillgång till utvalda datacenter, en plattformstjänst för att styra och kontrollera var användningen sker samt en app-butik där kunder kan ladda ner AI-applikationer. I en sådan modell aktualiseras frågor om rollfördelning enligt GDPR i flera led av värdekedjan.

2.2. Projektets mål

Målet med projektet är att vägleda leverantörer som tillhandahåller AI-applikationer och relaterad teknik. Projektet syftar särskilt till att klargöra under vilka förutsättningar leverantören kan anses vara personuppgiftsansvarig, gemensamt personuppgiftsansvarig eller personuppgiftsbiträde, samt om det i vissa moment inte aktualiseras någon roll för leverantören enligt GDPR.

Följande tre delar av Eggsplains tjänstecykel har identifierats som särskilt relevanta att analysera utifrån detta:

- Installation och implementation av hårdvaran
- Tillhandahållande och finjustering av AI-applikationer
- Löpande tjänster som tillhandahålls

Projektet är avgränsat till att ge vägledning avseende de ansvarsroller som följer av GDPR. Andra rättsliga frågor som kan aktualiseras vid utveckling, tillhandahållande

[2] *Sveriges AI-strategi*, publicerad 20 februari 2026, uppdaterad 26 februari 2026, hämtad 31 maj 2026, https://www.regeringen.se/regeringens-politik/sveriges-ai-strategi/.
[3] SOU 2025:12. *AI-kommissionens Färdplan för Sverige*.
[4] https://www.eggsplain.com/.

och användning av liknande produkter och tjänster behandlas inte inom ramen för projektet. Bedömningarna i rapporten sker mot bakgrund av nuvarande rättsläge och kan komma att ändras om det tillkommer ny lagstiftning, domstolspraxis eller vägledning från Europeiska dataskyddsstyrelsen (EDPB).[5]

2.3. Ansvarsroller enligt GDPR

GDPR skiljer mellan personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden. Ansvar och roller fördelas beroende på vilken faktisk funktion eller inflytande en aktör har i samband med att personuppgifter behandlas. Bedömningen vilar således inte i första hand på hur parterna själva benämner sin relation, utan på omständigheterna och vilken aktör som styr förutsättningarna för den aktuella personuppgiftsbehandlingen.[6] Det är heller inte tillräckligt att en aktör tillhandahåller en viss tjänst, teknisk miljö eller infrastruktur. Inte heller faktisk åtkomst till personuppgifter är ensamt avgörande.[7]

Avgörande är i stället att identifiera om personuppgiftsbehandling sker, vilken aktör som bestämmer ändamålen och de väsentliga medlen för behandlingen, om flera aktörer gemensamt utövar sådant bestämmande inflytande, eller om en aktör endast behandlar personuppgifter för någon annans räkning.

En och samma aktör kan ha olika roller enligt GDPR i förhållande till olika personuppgiftsbehandlingar. Bedömningen måste därför göras separat för varje behandling.[8] Det kan också förekomma aktiviteter inom samma förlopp som inte innebär behandling av personuppgifter. I sådana fall aktualiseras inte någon roll enligt GDPR för den aktuella aktiviteten.

2.3.1 Personuppgiftsansvarig

Enligt artikel 4.7 GDPR är personuppgiftsansvarig den som, ensam eller tillsammans med andra, bestämmer ändamålen och medlen för behandlingen av personuppgifter. Med ändamål avses varför behandlingen sker, det vill säga syftet med behandlingen. Med medel avses hur behandlingen ska genomföras för att ändamålet ska uppnås.[9]

Bedömningen av vem som är personuppgiftsansvarig utgår från vem som har ett faktiskt och reellt inflytande över behandlingen. Det innebär att bedömningen ska göras utifrån omständigheterna i det enskilda fallet och vem som beslutar vissa nyckelelement, framför allt behandlingens ändamål och väsentliga medel.[10]

Med väsentliga medel avses grundläggande beslut som är nära kopplade till ändamålet och som har betydelse för behandlingens omfattning och konsekvenser. Det kan exempelvis handla om vilka kategorier av personuppgifter som används, vilka registrerade som omfattas och hur länge uppgifterna lagras. Den som bestämmer sådana frågor har normalt ett inflytande som talar för personuppgiftsansvar. Icke-väsentliga medel avser däremot mer praktiska aspekter av implementeringen, såsom valet av viss hårdvara eller programvara samt vissa säkerhetsåtgärder.[11]

---

[5] Läs mer om EDPB på IMY:s webbplats (https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/).
[6] EDPB:s riktlinjer 07/2020, s. 10, p. 12.
[7] EDPB:s riktlinjer 07/2020, s. 19, p. 45.
[8] EDPB:s riktlinjer 07/2020, s. 13, p. 26.
[9] EDPB:s riktlinjer 07/2020, s. 15, p. 35.
[10] EDPB:s riktlinjer 07/2020, s. 12–13, p. 20–21 och 25.
[11] EDPB:s riktlinjer 07/2020, s. 16, p. 40.

Den personuppgiftsansvarige bär huvudansvaret för att behandlingen sker i enlighet med GDPR. Det omfattar bland annat krav på att behandlingen är laglig och har rättslig grund, att information tillhandahålls de registrerade, att personuppgifterna skyddas med tillräcklig säkerhet, att de registrerades rättigheter hanteras samt att efterlevnaden dokumenteras.

2.3.2 Gemensamt personuppgiftsansvar

Gemensamt personuppgiftsansvar föreligger enligt artikel 26.1 GDPR när två eller flera aktörer gemensamt fastställer ändamålen och medlen för en behandling. Det krävs alltså ett gemensamt inflytande över behandlingen, men inte nödvändigtvis att aktörerna påverkar alla delar av behandlingen i samma omfattning.

Att två aktörer har ett gemensamt ekonomiskt intresse, använder samma tekniska infrastruktur eller på annat sätt samverkar är normalt inte tillräckligt för att gemensamt personuppgiftsansvar ska uppstå.[12] Det krävs att aktörerna tillsammans har bestämmande inflytande över varför och hur personuppgifter behandlas. Gemensamt personuppgiftsansvar kan exempelvis aktualiseras när flera aktörer inom ramen för ett gemensamt utvecklings- eller forskningsprojekt tillsammans bestämmer vilka personuppgifter som ska användas, för vilket ändamål och hur behandlingen ska genomföras.[13]

När gemensamt personuppgiftsansvar föreligger ska aktörerna på ett transparent sätt fastställa sitt respektive ansvar för att uppfylla skyldigheterna enligt GDPR.

2.3.3 Personuppgiftsbiträde

Enligt artikel 4.8 GDPR är ett personuppgiftsbiträde den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Rollen förutsätter att biträdet är en separat juridisk enhet i förhållande till den personuppgiftsansvarige, att behandlingen sker för den personuppgiftsansvariges intresse och inom ramen för den personuppgiftsansvariges ändamål och instruktioner.[14]

Det som kännetecknar ett personuppgiftsbiträde är alltså att aktören inte själv bestämmer ändamålen eller de väsentliga medlen för behandlingen. Biträdet utför i stället en behandling på uppdrag av den personuppgiftsansvarige. Ett typiskt exempel är en leverantör som anlitas för att tillhandahålla en teknisk tjänst åt en kund där personuppgifter lagras, överförs, bearbetas eller på annat sätt hanteras för kundens räkning.

Att ett biträde har ett visst utrymme att bestämma praktiska frågor innebär inte att biträdet blir personuppgiftsansvarigt. Ett biträde kan exempelvis behöva välja verktyg, arbetsmetod eller tekniska säkerhetsåtgärder för att kunna utföra uppdraget. Sådana beslut behöver dock fattas inom ramen för den personuppgiftsansvariges ändamål, instruktioner och beslut om de väsentliga medlen för behandlingen.[15]

Personuppgiftsbiträdesrollen innebär särskilda skyldigheter. Biträdet får endast behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige och ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder. Biträdet ska också bistå den personuppgiftsansvarige i vissa

---

[12] EDPB:s riktlinjer 07/2020, s. 22–24, p. 60, 62 och 68.
[13] EDPB:s riktlinjer 07/2020, s. 24, se exemplet med ”Forskningsprojekt av institut”.
[14] EDPB:s riktlinjer 07/2020, s. 27–28, p. 73 och 76 ff.
[15] EDPB:s riktlinjer 07/2020, s. 16, p. 40.

skyldigheter, exempelvis vid hantering av registrerades rättigheter, säkerhetsincidenter och konsekvensbedömningar när det är relevant.[16]

Den personuppgiftsansvarige har samtidigt en skyldighet att endast anlita personuppgiftsbiträden som ger tillräckliga garantier för att behandlingen uppfyller kraven i GDPR och skyddar de registrerades rättigheter.[17] Relationen mellan den personuppgiftsansvarige och biträdet ska regleras genom ett avtal, vanligen kallat personuppgiftsbiträdesavtal.[18]

2.4. Tekniken

En leverantör av AI-teknik, AI-produkter eller AI-tjänster kan utforma sin leverans på olika sätt. En AI-applikation kan till exempel tillhandahållas som en lokalt installerad lösning, genom kundens egen eller leasade infrastruktur, via ett datacenter, genom en molntjänst eller som en SaaS-tjänst[19] där leverantören ansvarar för en större del av den tekniska miljön. Gemensamt för dessa modeller är att AI-applikationen behöver köras i en teknisk miljö där hårdvara, mjukvara, beräkningskapacitet och applikationer samverkar.

På en grundläggande nivå krävs infrastruktur som gör det möjligt att lagra, bearbeta och överföra data samt köra de applikationer och modeller som tjänsten bygger på. Infrastrukturen kan bestå av fysisk hårdvara, virtuella resurser eller molnbaserade tjänster. Det kan exempelvis vara servrar som kunden köper eller leasar, resurser i ett datacenter, publika eller privata molntjänster eller den underliggande miljön som en SaaS-leverantör använder för att tillhandahålla tjänsten.

Ovanpå infrastrukturen etableras en digital driftsmiljö. Den kan exempelvis omfatta operativsystem, behörighetsstyrning, nätverkskonfiguration, lagring, säkerhetsfunktioner och andra komponenter som krävs för att tjänsten ska kunna användas. I vissa lösningar används även en orkestrator eller motsvarande mjukvarukomponent för att hantera installation, distribution, skalning och styrning av applikationer i miljön. Sådana komponenter är inte unika för AI-tjänster, men valet av teknisk lösning kan påverka vilka personuppgiftsbehandlingar som uppkommer och vilka aktörer som får åtkomst till uppgifter. Därmed kan sådana komponenter få betydelse för den dataskyddsrättsliga bedömningen.

Vid utveckling och tillhandahållande av AI-produkter och AI-tjänster kan man göra en övergripande skillnad mellan aktörer som utvecklar och tränar AI-modeller från grunden och aktörer som bygger tjänster ovanpå redan förtränade modeller. En förtränad modell är redan tränad för en viss uppgift och kan användas i befintligt skick, integreras i en applikation eller anpassas ytterligare. En aktör som bygger en AI-tjänst på en förtränad modell kan därför behöva anpassa modellen för den aktuella tjänsten.

En vanlig form av anpassning är finjustering. Finjustering innebär, i förenklad form, att en redan tränad modell tränas vidare på ett mer avgränsat eller specialiserat datamaterial. Syftet kan vara att modellen ska prestera bättre inom ett visst användningsområde, hantera en viss typ av information eller anpassas till en viss verksamhets behov. Finjustering kan ske som ett led i leverantörens egen produktutveckling, exempelvis för att tillhandahålla en förbättrad eller specialiserad AI-

[16] Se artikel 28.3 GDPR.
[17] Se artikel 28.1 GDPR.
[18] Se artikel 28.3 GDPR.
[19] Eng: *Software as a Service* (programvara som tjänst).

applikation till flera kunder. Den kan också ske för en specifik kunds räkning, där kundens data används för att anpassa modellen till kundens särskilda behov.

Hur finjusteringen går till beror bland annat på valet av grundmodell, vilket resultat som ska uppnås och vilken typ av data som används. Dessa faktorer kan i sin tur påverka vilka krav som ställs på den tekniska miljön. Processen kan förenklat beskrivas genom följande moment.

Först behöver relevanta data samlas in, väljas ut och struktureras. Data kan exempelvis komma från interna system, öppna datakällor eller andra externa datakällor. Det är viktigt att säkerställa att aktuella data är representativa för att uppnå ett bra resultat. För att uppnå detta krävs ofta förbehandling innan data kan användas. En del av denna förbehandling kan vara att överflödiga eller irrelevanta data tas bort, felaktigheter korrigeras, saknade värden hanteras och materialet konverteras till ett format som modellen kan använda. I detta steg behöver det också bedömas om datamaterialet innehåller personuppgifter och om dessa i så fall kan användas för finjusteringen.

Därefter kan data behöva märkas upp. Uppmärkning innebär att man skapar förväntade svar för de data som matas in i modellen. Det kan innebära att leverantören eller utvecklaren behöver skapa kategorier, summeringar eller annan information som modellen kan använda för att lära sig relevanta mönster eller som senare kan användas för att validera och testa modellens resultat. Uppmärkning kan göras manuellt, semi-automatiskt eller automatiskt, beroende på datamaterialets struktur, ändamålet med finjusteringen och tillgängliga resurser. Uppmärkta data kan användas som träningsdata, valideringsdata eller testdata.

Finjustering kräver också en teknisk miljö där träningen kan genomföras. Det innefattar bland annat tillgång till beräkningskapacitet, exempelvis CPU:er och GPU:er[20], samt nödvändig mjukvara och verktyg för att genomföra träningen. Den tekniska miljön kan finnas hos leverantören, hos kunden eller hos en extern infrastruktur- eller molnleverantör. Det är också viktigt att säkerställa att data hanteras på ett säkert sätt, exempelvis genom kryptering, säkra anslutningar och andra lämpliga säkerhetsåtgärder.

När modellen, datamaterialet och den tekniska miljön är på plats kan finjustering av AI-modellen påbörjas. Denna process går betydligt snabbare än att träna från grunden, eftersom modellen kan återanvända redan inlärda mönster för den nya specifika uppgiften. Träningsprocessen innebär både övervakning av olika mätvärden under själva träningen och efterföljande validering. Syftet är att undvika överanpassning samt att säkerställa att modellen inte lär sig oönskade mönster, som bias, eller återger data från träningssetet på ett olämpligt sätt.

Vid finjustering kan även modellens utdata eller mellanliggande resultat behöva beaktas. En modell som tränas vidare kan i vissa fall generera information som har samband med det datamaterial som används vid finjusteringen. Det kan inte heller uteslutas att en modell i vissa situationer återger uppgifter från data som använts vid den ursprungliga träningen av grundmodellen. Detta bör beaktas när modeller

[20] Eng. *Central Processing Unit* och *Graphics Processing Unit*.

används som kan ha tränats på personuppgifter, eftersom det kan påverka den dataskyddsrättsliga bedömningen.[21]

Slutligen behöver den finjusterade modellen testas och utvärderas. Det är ett separat steg med data som modellen varken har sett i tränings- eller valideringssteget. Detta görs för att säkerställa att tidigare resultat är tillförlitliga. Det kan handla om att mäta modellens noggrannhet, precision, robusthet, förekomst av snedvridningar eller andra avvikelser. Beroende på användningsområde kan det även behöva analyseras om modellen fungerar tillräckligt väl för den miljö där den ska användas och om resultatet är begripligt för de personer som ska använda eller granska det.

[21] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17 december 2024, p. 31–34.

3. Leverantörens roll enligt GDPR

3.1. Installation och implementation av hårdvara

Eggsplain tillhandahåller hårdvara och serverinfrastruktur till kunden. Tillhandahållandet kan ske genom att kunden köper eller leasar en fysisk server, genom användning av utvalda datacenter eller genom en hybridlösning där flera tekniska leveransmodeller kombineras.

En roll enligt GDPR aktualiseras normalt inte enbart genom att en leverantör säljer, hyr ut, levererar eller installerar hårdvara eller annan serverinfrastruktur, eftersom sådana aktiviteter normalt sett inte aktualiserar någon personuppgiftsbehandling. För att en sådan roll ska aktualiseras krävs att leverantören antingen själv bestämmer över en behandling av personuppgifter eller behandlar personuppgifter för kundens räkning.

En biträdesroll kan exempelvis bli aktuell om leverantören, i samband med implementationen, migrerar kundens befintliga databaser, användarkonton eller loggar till den nya servermiljön. I ett sådant fall behandlar leverantören personuppgifter för kundens räkning, även om behandlingen är begränsad till själva införandet.[22]

3.2. Användning och tillhandahållande av AI-applikationer

Eggsplain tillhandahåller förinstallerade AI-applikationer genom en egenutvecklad app-butik som placeras i den servermiljö som kunden har valt. Eggsplain utvecklar inte AI-modeller från grunden, utan tillhandahåller AI-applikationer som bygger på tredjepartsmodeller eller andra tredjepartsprodukter. Vissa av dessa kan tillhandahållas utan ytterligare anpassning, medan andra kan ha finjusterats innan de görs tillgängliga för kunden.

För att bedöma vilket ansvar som följer av leverantörens roll enligt den ansvars- och rollfördelning som följer av GDPR krävs till att börja med en analys av vilka aktiviteter leverantören utför i samband med tillhandahållandet av applikationerna.[23] Det behöver särskilt bedömas om åtgärderna innebär behandling av personuppgifter och, i så fall, om behandlingen sker för leverantörens egna ändamål, för kundens räkning eller inom ramen för ett gemensamt bestämmande. I det följande behandlas fyra scenarier som illustrerar leverantörens roll:

- Scenario 1: Leverantören tillhandahåller tredjepartsapplikationer utan finjustering.
- Scenario 2: Leverantören tillhandahåller tredjepartsapplikationer och finjusterar dem på eget initiativ för en bredare kundkrets.
- Scenario 3: Leverantören tillhandahåller tredjepartsapplikationer och finjusterar dem på uppdrag av en specifik kund.
- Scenario 4: Leverantören och kunden vidareutvecklar gemensamt en AI-applikation.

[22] Jfr EDPB:s riktlinjer 07/2020, s. 17, se exemplet med ”Hostingtjänster”.
[23] EDPB:s riktlinjer 07/2020, s. 10, p. 12 och s. 13, p. 26.

Scenario 1: Leverantören tillhandahåller tredjepartsapplikationer utan finjustering.

I det första scenariot tillhandahåller leverantören tredjepartsapplikationer utan att själv finjustera eller på annat sätt anpassa den AI-modell som applikationen bygger på. Leverantörens funktion är i detta fall begränsad till att göra applikationen tillgänglig för kunden, exempelvis genom en app-butik, plattform eller annan distributionslösning, utan att leverantören får åtkomst till kundens övriga system.

När leverantörens roll är begränsad till sådan förmedling eller distribution aktualiseras normalt ingen roll enligt GDPR för leverantören i förhållande till den personuppgiftsbehandling som kan ske när kunden använder applikationen. Det förutsätter att leverantören inte får tillgång till eller på annat sätt behandlar personuppgifter vid kundens användning av applikationen, och inte heller bestämmer ändamål eller väsentliga medel för kundens behandling.[24]

Detta utesluter inte att leverantören kan vara personuppgiftsansvarig för andra, separata behandlingar som sker i samband med att applikationen tillhandahålls. Det kan exempelvis vara behandling av användar- eller kontaktuppgifter för kontoadministration, behörighetsstyrning, licenshantering eller fakturering. Sådana behandlingar sker typiskt sett för leverantörens egna administrativa eller kommersiella ändamål och bedöms separat från den behandling som kan ske när kunden installerar eller använder AI-applikationen.

Scenario 2: Leverantören tillhandahåller tredjepartsapplikationer och finjusterar dem på eget initiativ för en bredare kundkrets.

I det andra scenariot väljer och anpassar leverantören AI-applikationerna i syfte att tillhandahålla dem som en standardiserad produkt eller till en bredare kundkrets. Detta innefattar olika aktiviteter, exempelvis val av AI-modeller, anpassning av AI-applikationernas funktionalitet samt finjustering av valda AI-modeller.

Om personuppgifter behandlas i samband med sådan finjustering talar det normalt för att leverantören är personuppgiftsansvarig för den behandlingen eftersom detta sker för ändamål och med väsentliga medel som leverantören själv bestämmer över. Leverantören avgör exempelvis att modellen ska finjusteras, vilket datamaterial som ska användas, hur modellen ska anpassas och att resultatet ska tillhandahållas som en del av leverantörens produkt eller tjänst.

Detta gäller när leverantören finjusterar en modell på eget initiativ, oberoende av uppdrag från en specifik kund eller bestämmande inflytande från någon annan aktör. Behandlingen sker då som ett led i leverantörens egen produktutveckling och för leverantörens egna ändamål.

Scenario 3: **Leverantören tillhandahåller tredjepartsapplikationer och finjusterar dem på uppdrag av en specifik kund.**

I det tredje scenariot finjusterar leverantören AI-applikationen för en specifik kund. Kunden väljer att använda AI-applikationen och ger leverantören i uppdrag att finjustera modellen enligt kundens instruktioner och behov. Finjusteringen genomförs

[24] Se artikel 2.1 samt artikel 4.1–4.2 GDPR.

av leverantören med leverantörens expertis, men utifrån de ändamål och förutsättningar som kunden ytterst bestämmer.

Kunden anger exempelvis syftet för finjusteringen, väljer ut eller tillhandahåller relevanta träningsdata, anger vad modellen ska optimeras eller valideras mot och bestämmer ramarna för träning och testning av den finjusterade AI-applikationen. Leverantören kan samtidigt ha ett visst utrymme att bestämma praktiska eller tekniska frågor kring hur uppdraget genomförs, exempelvis val av verktyg, arbetsmetod eller vissa tekniska inställningar. En sådan möjlighet ändrar normalt inte leverantörens roll, så länge leverantören behandlar personuppgifter för kundens räkning och inom ramen för kundens instruktioner.

Om personuppgifter behandlas inom ramen för sådan kundspecifik finjustering och under de förutsättningar som redogjorts för, talar det normalt för att kunden är personuppgiftsansvarig och att leverantören är personuppgiftsbiträde. Kunden är den som bestämmer, och har intresse av, ändamålet med finjusteringen, de väsentliga medlen samt omfattningen av personuppgiftsbehandlingen, medan leverantören utför behandlingen som ett led i uppdraget.

Scenario 4: Leverantören och kunden vidareutvecklar gemensamt en AI-applikation.

I det fjärde scenariot vidareutvecklar leverantören och kunden gemensamt en AI-applikation. Det kan exempelvis ske genom ett samarbetsprojekt där parterna tillsammans beslutar att en tredjepartsapplikation ska finjusteras för ett visst användningsområde och gemensamt fastställer ändamål och väsentliga medel för den personuppgiftsbehandling som sker inom ramen för vidareutvecklingen. Det kan också ske efter att en applikation först har finjusterats för en specifik kund, men där parterna därefter gemensamt beslutar att använda resultatet för fortsatt vidareutveckling.

Om personuppgifter behandlas inom ramen för ett sådant gemensamt utvecklingsarbete, och både leverantören och kunden har inflytande över varför behandlingen ska ske och de väsentliga medlen för behandlingen, talar det för att parterna är gemensamt personuppgiftsansvariga. Det kan exempelvis vara fallet om parterna tillsammans bestämmer vilka kategorier av personuppgifter som ska användas, för vilket syfte, hur modellen ska finjusteras eller testas och hur resultatet ska användas.

Det är viktigt att skilja mellan olika behandlingsaktiviteter. En ursprunglig finjustering för en specifik kund kan fortfarande utgöra en behandling där kunden är personuppgiftsansvarig och leverantören personuppgiftsbiträde. Om parterna därefter gemensamt beslutar om fortsatt behandling för vidareutveckling eller tillhandahållande av AI-applikationen behöver den behandlingen bedömas separat.[25] Enbart ett samarbete eller ett gemensamt kommersiellt intresse är inte tillräckligt för gemensamt personuppgiftsansvar; det krävs att parterna gemensamt bestämmer ändamål och väsentliga medel för den aktuella behandlingen.

Om efterföljande användning

När en AI-applikation har gjorts tillgänglig för kunden behöver den efterföljande användningen bedömas separat från den finjustering eller vidareutveckling som

[25] EDPB:s riktlinjer 07/2020, s. 22, p. 57.

beskrivits ovan. Vid användning kan AI-applikationen exempelvis kopplas till kundens tekniska miljö, datakällor och andra kompletterande system. Slutanvändare hos kunden kan dessutom förse AI-applikationen med personuppgifter genom användarpromptar, bilder eller annan input, och AI-applikationen kan i sin tur generera svar som innehåller personuppgifter.

Kunden är som utgångspunkt personuppgiftsansvarig för den behandling som sker genom användningen av applikationen i den egna verksamheten. Detta eftersom kunden är den som bestämmer för vilka syften applikationen ska användas, vilka uppgifter eller datakällor som ska användas och hur resultatet ska hanteras.

Leverantörens roll beror på om och hur leverantören behandlar personuppgifter i samband med den efterföljande användningen. Om leverantören exempelvis driftar, underhåller eller tillhandahåller den tekniska miljö där personuppgifter behandlas, kan leverantören vara personuppgiftsbiträde för dessa behandlingsaktiviteter. Om leverantören däremot inte behandlar personuppgifter i samband med kundens användning av applikationen aktualiseras normalt ingen roll enligt GDPR i den delen.

3.3. Service, uppdatering och konsulttjänster

När kunden har valt infrastrukturalternativ och Eggsplains mjukvarulösning har driftsatts hos kunden kan Eggsplain tillhandahålla vissa löpande tjänster. Det kan exempelvis vara teknisk support vid fel, uppdateringar av Eggsplains produkter eller, i begränsade fall, konsulttjänster där Eggsplain bistår kunden med expertis.

Sådana tjänster kan innebära att en leverantör analyserar kundens behov, hanterar kundärenden eller tillhandahåller stöd på plats eller i kundens tekniska miljö. Alla support- eller konsulttjänster innebär inte att leverantören får en roll enligt GDPR. Det avgörande är om leverantören faktiskt behandlar personuppgifter och, i så fall, om behandlingen sker för leverantörens egna ändamål eller för kundens räkning alternativt om en behandling som utförs av en konsult från leverantören får anses ske som en del av kundens organisation. Nedan illustreras några olika exempel.

Exempel 1: Leverantören analyserar kundärenden för att utveckla sin egen kundtjänst

Första exemplet avser en situation där en leverantör har rättsliga förutsättningar att analysera uppgifterna i en samling kundärenden och tillhörande ärendehistorik i syfte att utveckla den egna kundtjänsten. Detta kan innebära att leverantören behandlar personuppgifter såsom kontaktuppgifter, användarnamn, organisationsuppgifter, ärendenummer eller annan information som kunden har lämnat i ärendena. Även om uppgifterna ursprungligen har lämnats inom ramen för ett enskilt kundärende innebär denna situation att det är leverantören som bestämmer att och hur uppgifterna ska användas för analys och utveckling av den egna verksamheten. Leverantören bestämmer därmed ändamålet med behandlingen, vilket underlag som ska analyseras och hur analysen ska genomföras. Leverantören är därför normalt personuppgiftsansvarig för behandlingen i fråga.

Exempel 2: Leverantören hanterar supportärenden för kundens räkning

Ett företag anlitar en leverantör för att hantera supportärenden gentemot företagets kunder, vilket innebär att leverantören får åtkomst till företagets kunddatabaser och behandlar personuppgifter inom ramen för supporten. Leverantören får endast behandla personuppgifterna för att utföra den upphandlade supporttjänsten, inom

ramen för de instruktioner som företaget har lämnat. [26] Det är företaget som bestämmer ändamålet med supporten, vilka kunduppgifter som får behandlas och ramarna för hur supporten ska tillhandahållas i övrigt. Leverantören behandlar därmed personuppgifter för företagets räkning och är normalt personuppgiftsbiträde till företaget. Relationen ska regleras genom ett personuppgiftsbiträdesavtal.

Detta kan jämföras med en mer avgränsad supportåtgärd där en leverantör anlitas för att exempelvis åtgärda ett programvarufel. Om uppdraget inte innebär att leverantören behandlar personuppgifter för kundens räkning i samband med uppdragets utförande, och eventuell åtkomst till personuppgifter endast är tillfällig och underordnad felsökningen, aktualiseras inte nödvändigtvis någon biträdesroll. Bedömningen behöver dock göras utifrån vad leverantören faktiskt gör i det enskilda uppdraget.[27]

Exempel 3: Leverantör tillhandahåller en resurskonsult

En myndighet anlitar en IT-leverantör för att tillhandahålla en resurskonsult för löpande stöd och support i myndighetens ärendehanteringssystem. Resurskonsulten arbetar på plats hos myndigheten eller i en miljö som myndigheten kontrollerar och utför arbetet under myndighetens ledning och kontroll. I arbetet kan resurskonsulten komma att hantera personuppgifter som finns i ärendehanteringssystemet, men behandlingen sker som en del av myndighetens verksamhet.

I en sådan situation där en konsult utför uppdrag direkt under den anlitande myndighetens befogenhet är myndigheten normalt personuppgiftsansvarig för den behandling som konsulten utför i myndighetens system. IT-leverantören får inte nödvändigtvis en roll enligt GDPR enbart genom att tillhandahålla personal till en myndighet, om resurskonsulten i det aktuella arbetet agerar som en del av myndighetens organisation och inte som en del av en självständig tjänst som IT-leverantören tillhandahåller. Detta förutsätter att IT-leverantören inte själv har tillgång till personuppgifterna, inte behandlar dem genom egna system eller tjänster och inte bestämmer ändamål eller väsentliga medel för behandlingen.[28]

4. Övriga reflektioner

Rollfördelningen avgör vilka skyldigheter en aktör har enligt GDPR. Det kan exempelvis handla om att säkerställa rättslig grund, vidta säkerhetsåtgärder, informera registrerade, hantera registrerades rättigheter och ingå personuppgiftsbiträdesavtal.

Detta behöver skiljas från det ansvar som kan följa av den kommersiella relationen mellan parterna eller andra regelverk. Om en leverantör har åtagit sig att tillhandahålla en tjänst eller teknisk lösning med viss funktion eller säkerhetsnivå, och den inte fungerar som avtalat, kan det aktualisera frågor om avtalsbrott, ansvar för att åtgärda fel eller skadestånd. Sådana frågor avgörs normalt inte enbart utifrån GDPR, även om dataskyddsregelverket kan ha betydelse för hur parterna utformar sina krav och åtaganden.

Det är därför viktigt att parterna skiljer mellan skyldigheter enligt GDPR och ansvar som följer av avtal eller andra regler än GDPR.

---

[26] EDPB:s riktlinjer 07/2020, s. 30, se exemplet med ”Callcenter”. Jfr även exemplet med ”Allmän it-support”.
[27] EDPB:s riktlinjer 07/2020, s. 30, se exemplet med ”It-konsult åtgärdar ett programvarufel”.
[28] EDPB:s riktlinjer 07/2020, s. 28, p. 78. Se Öhman, *Dataskyddsförordningen (GDPR) m.m.* (11 sep. 2025, Version 3A, Juno), kommentaren till artikel 29.

IMY. Integritetsskydds myndigheten

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY) arbetar för att skydda dina personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer.

Vi är Sveriges dataskyddsmyndighet. Det är vi som kontrollerar att företag och myndigheter följer dataskyddsförordningen GDPR. Vi vägleder dem som behandlar personuppgifter, för att göra det lättare att göra rätt och för att främja innovation där rättigheter och effektivitet står i balans. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Genom vårt arbete bidrar vi till ett tryggare digitalt Sverige, där människor har tillit till att deras personuppgifter hanteras som de ska och samhällets motståndskraft är stark.

Kontakta Integritetsskyddsmyndigheten

E-post: imy@imy.se
Webb: www.imy.se
Tel: 08-657 61 00
Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm