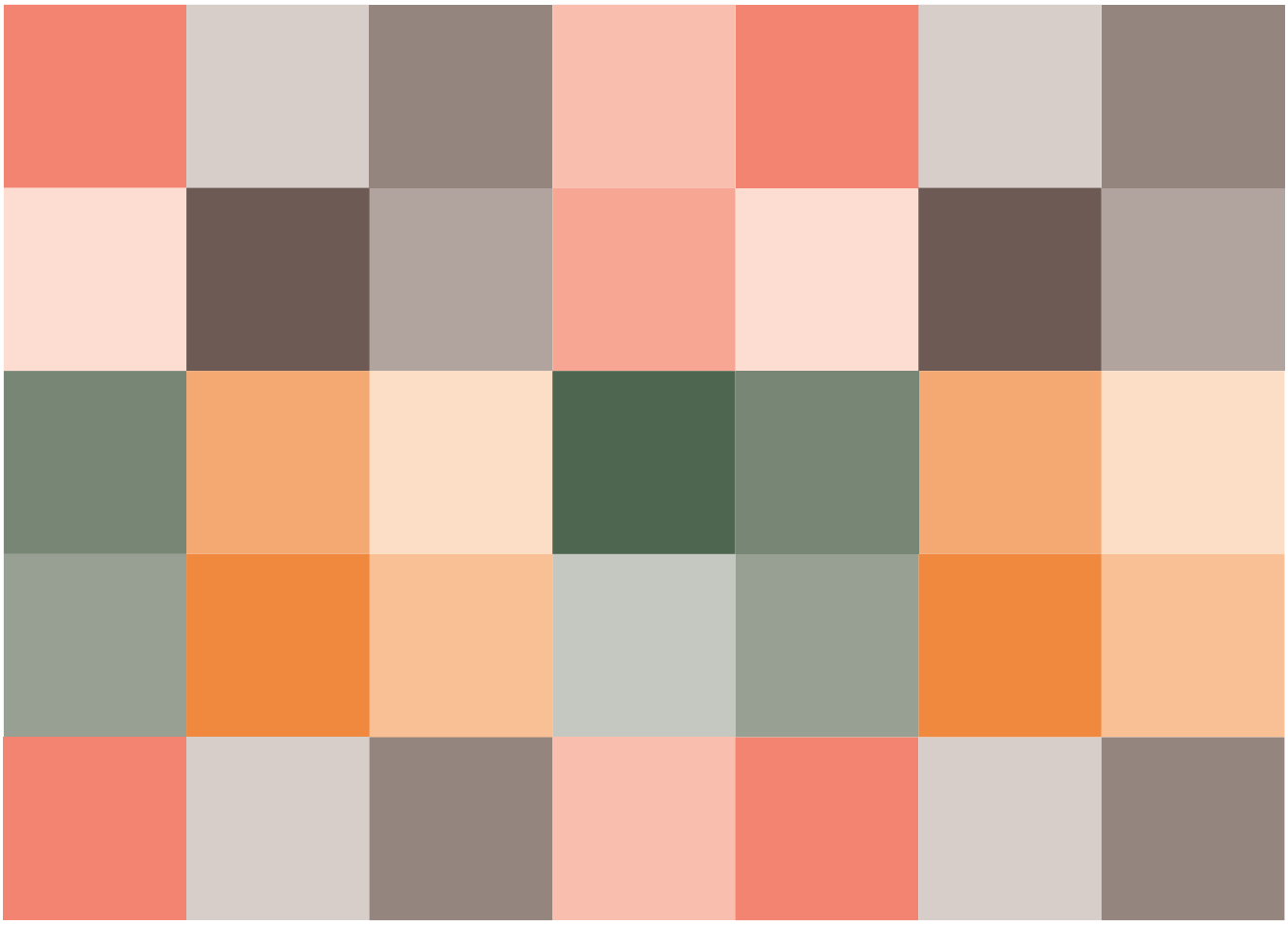

Rättsliga förutsättningar för att dela data

Bilaga till Slutredovisning av uppdrag till Myndigheten för digital förvaltning att föreslå en samverkansstruktur för utveckling av tjänster för data och artificiell intelligens

Diarienummer: Fi2026/00137

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Datum: 2026-05-29

Denna bilaga behandlar rättsliga och säkerhetsmässiga förutsättningar för att dela och använda skyddade data inom offentlig förvaltning, särskilt i situationer där data görs tillgängliga i säkra behandlingsmiljöer utan att överföras till användaren. Fokus ligger på datamängder som innehåller personuppgifter, sekretessreglerade uppgifter eller annan information med särskilt skyddsvärde. Regelverket syftar både till att skydda känslig information och ändamålsenlig användning och delning av data, där krav och eventuella skyddsåtgärder anpassas efter informationens skyddsvärde.

Skydd av personuppgifter och sekretess

Många datamängder inom den offentliga förvaltningen innehåller personuppgifter, ibland även känsliga personuppgifter. Dessa uppgifter måste behandlas i enlighet med reglerna i dataskyddsförordningen[1], anslutande nationell reglering och eventuella registerförfattningar. Grundläggande principer för hur personuppgifter får behandlas finns i artikel 5.1 dataskyddsförordningen. Bland annat måste det finnas en rättslig grund för behandlingen – exempelvis att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Personuppgifter får dessutom bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (den så kallade finalitetsprincipen). Känsliga personuppgifter, såsom uppgifter om hälsa, får inte behandlas alls enligt dataskyddsförordningen. Sådan personuppgiftsbehandling behöver i stället ha stöd i annan unionsrätt eller nationell rätt, såsom patientdatalagen (2008:355).

Vissa kategorier av offentliga förvaltningsdata omfattas dessutom av reglerna om sekretess i offentlighets- och sekretesslagen (2009:400). En uppgift som är belagd med sekretess får inte röjas och inte heller utnyttjas utanför den verksamhet som sekretessen gäller inom. Sekretess kan till exempel gälla för en uppgift om en enskild lider skada eller men av att uppgiften röjs. Ett annat exempel på när sekretess kan gälla är om Sveriges säkerhet äventyras av ett röjande. Huruvida sekretess gäller för en uppgift avgörs från fall till fall, och i förhållande till den som begär

[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.

tillgång till uppgiften. En uppgift kan till exempel vara sekretessbelagd i förhållande till en begärande aktör, men inte i förhållande till en annan.

Datadelning inom den offentliga förvaltningen

Enligt 6 kap. 5 § offentlighets- och sekretesslagen har aktörer inom den offentliga förvaltningen en skyldighet att på begäran lämna en uppgift till en annan aktör inom förvaltningen, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Att uppgiften inte är sekretessbelagd innebär att något av följande gäller: uppgiften är inte sekretessreglerad, den omfattas av undantag från sekretess eller den får lämnas ut efter en sekretessprövning eller enligt en sekretessbrytande bestämmelse.

När en aktör inom den offentliga förvaltningen lämnar ut en uppgift som innehåller personuppgifter till en annan aktör inom förvaltningen, innebär utlämnandet en personuppgiftsbehandling som behöver ske i enlighet med dataskyddsregleringen. När en sådan uppgift lämnas enligt 6 kap. 5 § offentlighets- och sekretesslagen behöver det dock inte göras någon ytterligare kontroll av förenligheten med finalitetsprincipen, utöver prövningen av om uppgiften är sekretessbelagd.[2] Om en uppgift som innehåller personuppgifter kan lämnas ut enligt bestämmelsen, sker utlämnandet alltså i enlighet med finalitetsprincipen. Utlämnandet behöver dock också vara förenligt med de andra grundläggande principerna för behandling av personuppgifter, såsom att uppgiftslämnandet ska omfattas av lämpliga säkerhetsåtgärder och att fler uppgifter än nödvändigt inte delas.

Möjligheten att begära uppgifter enligt 6 kap. 5 § offentlighets- och sekretesslagen, läst i ljuset av dataskyddsregleringen, kan alltså sägas utgöra ramen för den offentliga förvaltningens möjligheter att dela data inom förvaltningen.

Datadelning med allmänheten

Rätten att ta del av allmänna handlingar

Skyldigheten att lämna uppgifter enligt 6 kap. 5 § offentlighets- och sekretesslagen gäller inte i förhållande till någon utanför den offentliga

[2] HFD 2021 ref. 10.

förvaltningen – i stället har allmänheten enligt andra kapitlet tryckfrihetsförordningen rätt att ta del av allmänna handlingar. Denna rätt begränsas dock på ett viktigt sätt genom det så kallade utskriftsundantaget i 2 kap. 16 § första stycket tryckfrihetsförordningen. Undantaget anger att den som ska lämna ut en allmän handling inte är skyldig att i större utsträckning än vad som följer av lag lämna ut en upptagning för automatiserad behandling i annan form än utskrift. En begäran om allmän handling leder alltså inte nödvändigtvis till datadelning, det vill säga delning av information i digitalt format, även om handlingen finns digitalt tillgänglig. Om den som lämnar ut handlingen väljer att tillämpa utskriftsundantaget kan det i stället bli fråga om delning av information på en utskrift, det vill säga i *analogt* format.

Tillgängliggörande av data för vidareutnyttjande

Vid sidan av utlämnande av allmänna handlingar kan den offentliga förvaltningen dela data med allmänheten enligt reglerna om tillgängliggörande av data för vidareutnyttjande. Dessa regler finns i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data (öppna datalagen). Reglerna syftar till att möjliggöra vidareutnyttjande av data som inte omfattas av särskilda skyddsbehov, som utgångspunkt för användning för valfria ändamål. Öppna datalagen genomför EU:s öppna data-direktiv[3], som bygger på tanken att data hos den offentliga förvaltningen som inte har ett särskilt skyddsvärde bör göras tillgängliga för vidareutnyttjande.[4]

Innan data publiceras enligt reglerna om vidareutnyttjande behöver det göras rättsliga och säkerhetsmässiga bedömningar. Krav på informationssäkerhet och skydd av personuppgifter måste kunna upprätthållas, både före och efter det att datamängden har gjorts tillgänglig. Tillgängliggörandet får inte heller vara i strid med offentlighets- och sekretesslagen (2009:400). Sist, men inte minst, måste tillgängliggörandet ske under förutsättning att det inte innebär risker för Sveriges säkerhet. Dessa bedömningar kan vara komplexa:

- Om datamängden innehåller personuppgifter behöver den som delar data dels se till att tillgängliggörandet i sig är förenligt med dataskyddsregleringen, dels ta hänsyn till att datamängden senare kan komma att användas på ett sätt som innebär risker för

[3] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (omarbetning).
[4] Jfr. skäl 23 till öppna data-direktivet.

enskildas personliga integritet.[5] Detta gäller även i de fall personuppgifter i datamängden har tagits bort. I sådana fall kan den som delar data behöva ta hänsyn till att en kombination av datamängder kan leda till att de avidentifierade personerna identifieras på nytt.[6]

- Den som tillgängliggör data behöver ta hänsyn till att tillgängliggörandet kan innebära informationssäkerhetsrisker, bland annat i form av risker för konfidentialitet hos informationen. Data som delas kan sammanställas med andra data som finns tillgängliggjorda och på så vis skapa nya informationsmängder som har ett högre skyddsvärde än den initiala datamängden eller datamängderna var för sig.[7] Detta gäller även om datamängderna var och för sig inte omfattas av sekretess.

Utgångspunkten i öppna datalagen är att data ska göras tillgängliga utan begränsningar i hur den får bearbetas. I vissa fall kan dock användningen förenas med särskilda villkor, exempelvis genom utfärdande av en licens. Villkor får bara ställas om det är motiverat av ett allmänintresse och om de är objektiva, proportionerliga och icke-diskriminerande. Villkor får inte heller begränsa konkurrensen eller i onödan inskränka möjligheterna att vidareutnyttja data. Villkoren kan bland annat ta fasta på skydd av personuppgifter eller garantier för att det informationsbärande innehållet inte kommer att ändras.[8] Att göra data tillgängliga under villkor kan alltså vara ett sätt att minska integritets- och informationssäkerhetsriskerna kopplade till tillgängliggörandet.

Användning av data enligt kapitel II dataförvaltningsförordningen

I kapitel II i dataförvaltningsförordningen[9] finns regler om hur vissa kategorier av skyddade data hos den offentliga sektorn kan användas för forskning och innovation, trots att datamängderna innehåller känsliga uppgifter. Det rör sig om data som inte kan delas fritt på grund av att den innehåller personuppgifter, uppgifter som skyddas av statistiksekretess,

[5] Prop. 2021/22:225, s. 37 och 81.
[6] Skäl 15 till EU:s dataförvaltningsförordning.
[7] Prop. 2021/22:225, s. 36 f.
[8] Skäl 44 till öppna data-direktivet och prop. 2021/22:225, s. 44.
[9] Europaparlementets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

företagshemligheter eller uppgifter som skyddas av tredje parts immateriella rättigheter. Sådana data kan användas under de villkor som fastställs i förordningen. Villkor kan vara att datamängden först ska pseudonymiseras, anonymiseras eller behandlas på något annat sätt för att skydda de känsliga uppgifterna i den. Ett villkor kan också vara att datamängden bara får användas i en säker behandlingsmiljö som tillhandahålls eller kontrolleras av datainnehavaren. Dessutom behöver den som använder datamängden åta sig vissa juridiska skyldigheter, såsom konfidentiell behandling av känsliga uppgifter som kan finnas kvar i datamängden trots att den har bearbetats.

Syftet med reglerna i kapitel II i dataförvaltningsförordningen är att ge EU:s medlemsländer en gemensam rättslig ram för hur de utvalda kategorierna av skyddade data kan användas för forskning och innovation, utan att skyddet för uppgifterna åsidosätts. Reglerna innebär däremot inga skyldigheter att tillåta användning av skyddade data. De är snarare tänkta att stimulera att den offentliga förvaltningens data görs tillgängliga för vidareanvändning – även i de fall datamängden är skyddad.[10] Reglerna syftar därmed till att möjliggöra ökad användning av även skyddade data genom strukturer som kombinerar tillgång till data med bibehållet skydd för känslig information.

Sekundäranvändning av hälsodata enligt EHDS-förordningen

Förordningen om det europeiska hälsodataområdet[11] (EHDS-förordningen) trädde i kraft i mars 2025 och kommer att börja tillämpas i mars 2029. Förordningen innehåller dels regler om enskildas möjlighet att få tillgång till, kontrollera och dela sina e-hälsodata (så kallad primäranvändning), dels regler om återanvändning av hälsodata för forskning, innovation, beslutsfattande och regleringsverksamhet (så kallad sekundäranvändning).

Enligt förordningen kommer hälsodatainnehavare vara skyldiga att göra hälsodata tillgängliga för sekundäranvändning när ett så kallat datatillstånd har utfärdats för den som begär tillgång till datamängden. Tillgången kommer bara få ges i säkra behandlingsmiljöer som är föremål för tekniska och organisatoriska åtgärder samt krav på säkerhet och

[10] Jfr. skäl 6 i förordningen.
[11] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.

interoperabilitet. Hälsodatainnehavare inom den offentliga förvaltningen kommer alltså att vara skyldiga att göra hälsodata tillgängliga i sådana säkra behandlingsmiljöer som avses i förordningen. Vilka förmågor en säker behandlingsmiljö behöver ha enligt EHDS-förordningen och hur ett system med sådana miljöer ska implementeras i Sveriges utreds för närvarande av Statistiska centralbyrån.[12]

[12] Se Statistiska centralbyråns delrapport, *SCB – Uppdrag till Statistiska centralbyrån att utreda förutsättningar för att tillhandahålla säkra behandlingsmiljöer enligt EHDS, S2025/00975 (delvis).*