SVENSKT NÄRINGSLIV

Data Act, Data Governance Act och Open Data Directive – vad innebär de nya reglerna?

JANUARI 2024

Den nya datarätten

EU-kommissionen har sedan år 2020 velat öka och förenkla användandet av data inom hela EU. Därför har EU tagit fram flera nya regelverk som bestämmer hur företags och myndigheters data ska och får användas i olika sammanhang.

Data Act[1], Data Governance Act[2] och Open Data Directive[3] är alla delar av EU:s övergripande strategi för att skapa en gemensam datamarknad. Dessa lagstiftningar kompletterar varandra, och har det gemensamma målet att öka tillgången till och användningen av data.

Data Act tar sikte på data som skapas genom användningen av uppkopplade produkter (även kallat sakernas internet, på engelska Internet of Things eller IOT) och tjänster som hör ihop med de uppkopplade produkterna. Data Governance Act ska dels öka tillgången till data som myndigheter har, dels skapa förutsättningar för en dataförmedlingsmarknad. Open Data Directive handlar mer om medlemsstaternas skyldighet att göra det möjligt för företag och privatpersoner att använda data som myndigheter och andra offentliga aktörer har.

Vad är ”Data Act”?

Data Act, eller dataförordningen på svenska, ska göra det lättare att använda data som skapas vid användning av uppkopplade produkter och förenkla delning av data rent generellt. Data Act gör det också lättare att byta leverantörer av databehandlingstjänster.

Data Act ställer krav på tillverkare och tjänsteleverantörer att låta användare, oavsett om de är företag eller privatpersoner, få tillgång till och återanvända data som skapas genom användningen av uppkopplade produkter eller tjänster som hör ihop med de uppkopplade produkterna. Den gör det möjligt för användarna att dela dessa data med andra, till exempel andra tjänsteleverantörer. Tanken är också att användare enklare ska kunna byta mellan olika tjänster genom att ta med sig ”sin data” till den nya tjänsten, att olagliga dataöverföringar ska hindras och att gemensamma standarder för dataformat ska skapas (så att datan kan användas på flera områden).

Den bakomliggande idén är att fördela värdet av och nyttan med data mellan aktörerna i dataekonomin på ett bättre och mer rättvist sätt genom att främja tillgången och användning av data. På så sätt hoppas EU kunna stimulera innovation inom produkter och tjänster. Det finns dock inget databas- eller katalogskydd för data som skapas genom uppkopplade produkter som omfattas av Data Act. Databas- eller katalogskyddet är en form av upphovsrätt som ger den som gjort en ”betydande investering” för att samla in, verifiera och strukturera data exklusiva rättigheter att kontrollera användningen av databasen eller katalogen. Denna rätt existerar alltså inte för data som hämtats från uppkopplade produkter.

Data Act kommer att ha en betydande påverkan på företag, särskilt de som är leverantörer av uppkopplade produkter och tjänster som hör ihop med sådana produkter. Företag kommer att behöva anpassa sina verksamheter för att uppfylla de nya kraven och skyldigheterna som införs genom Data Act.

---

1 Europaparlamentets och rådets förordning om harmoniserade regler för skälig åtkomst till och användning av data.
2 Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
3 Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

Tidslinje Data Act

- 27 juni 2023. EU-institutionerna når en politisk överenskommelse om Data Act.
- 9 november 2023. Parlamentet godkänner Data Act vid första behandlingen.
- 27 november 2023. Rådet godkänner parlamentets ståndpunkt.
- Q1 2024. Data Act träder i kraft. Kapitel IV om oskäliga villkor gäller endast för kontrakt ingångna efter ikraftträdandet.
- Q3 2025. 20 månader efter ikraftträdandet börjar Data Act tillämpas.
- Q3 2026. 32 månader efter ikraftträdandet börjar reglerna om tillgängliggörande av data för kunder i artikel 3(1) tillämpas.
- Q3 2027. 44 månader efter ikraftträdandet börjar reglerna om oskäliga villkor i Kapitel IV gälla för avtal ingångna innan tillämpningsdatumet förutsatt att de har ingåtts på obestämd tid eller löper ut minst 10 år efter att Data Act trätt i kraft.

Vidareutnyttjande av offentliga data

EU har genom Data Governance Act och Open Data Directive tagit tydliga steg för att offentliga myndigheter ska ge tillgång till data som de har samlat in. Målet är att data ska kunna användas kommersiellt i andra sammanhang. Tanken är att data som har tagits fram eller samlats in på det offentligas bekostnad bör gynna samhället i stort. EU-reglerna på området kompletteras av svensk rätt, framförallt lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.

Öppna data

Med öppna data avses data som är fritt tillgängliga för alla att använda, återanvända och delas fritt för valfritt ändamål. Det förutsätter i regel att data är i ett maskinläsbart och gärna öppet format.

Syftet med Open Data Directive

Med Open Data Directive vill EU ta bort hinder för återanvändande av data som offentlig sektor samlat in. Direktivet ska alltså öka möjligheten att använda öppna data. Direktivet har genomförts i Sverige genom lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.

Syftet med Data Governance Act

Data Governance Act ska öka tillgången till och användningen av data genom att skapa förtroende för datadelning, etablera en marknad för neutrala dataförmedlare och verka för datadelning.

I lagstiftningen ställs krav på framförallt myndigheter, som bl.a. måste ge andra tillgång till data, och förbjuds att ingå exklusiva avtal om tillgång till data[4]. När myndigheterna ger andra tillgång till data får de bara ställa icke-diskriminerande, transparenta, proportionerliga och motiverade villkor på vidareutnyttjandet. Eventuella avgifter för vidareutnyttjandet ska också vara rimliga – och för vissa data, till exempel forskningsdata, är det till och med gratis enligt de svenska kompletterande reglerna. En myndighet har fyra veckor på sig att handlägga en begäran om tillgängliggörande av data.

Det här betyder inte att all data som myndigheter sitter på görs tillgängliga. Reglerna gäller bland annat inte sådan data som är skyddad av upphovsrätt eller känsliga uppgifter som på något sätt kan äventyra Sveriges säkerhet. Offentlighets- och sekretesslagen (2009:400) (OSL) kan fortfarande förhindra utlämnanden. Myndigheterna behöver också säkerställa att mottagaren inte kommer att använda uppgifterna i strid med gällande dataskyddslagstiftning (GDPR).

Checklista: Skyldigheter för de som återanvänder offentliga data

- ☐ Se över villkoren som myndigheten ställer, och följ dem.
- ☐ Säkerställ att det finns en laglig grund enligt GDPR för behandling av eventuella personuppgifter i datan.
- ☐ Behandlas data utanför EU/EES (s.k. tredjeländer) ska myndigheten underrättas och ytterligare skyddsåtgärder sättas på plats.
- ☐ Vidta tekniska och operativa åtgärder för att förhindra återidentifiering av anonymiserade personuppgifter.

Underrätta myndigheten som lämnat ut data om alla incidenter som leder till att anonymiserade personuppgifter blir återidentifierade.

Vilken verksamhet regleras av Data Act?

Data Act reglerar datahantering i vid bemärkelse, med fokus på hur olika aktörer kan ta och låta andra ta del av data. Data Act är tillämplig på följande aktörer:

- tillverkare/leverantörer av uppkopplade produkter och tillhörande tjänster,
- användare av uppkopplade produkter och tillhörande tjänster,
- ”datahållare” som har rätt att nyttja och dela data som till exempel skapats av en uppkopplad tjänst,
- ”datamottagare” som inom ramen för sin professionella verksamhet tar emot data från en datahållare,
- offentliga myndigheter och organ, inklusive EU:s institutioner, som begär tillgång till data som datahållare förfogar över,
- leverantörer av databehandlingstjänster som tillhandahåller sina tjänster inom EU, och
- deltagare i datautrymmen[5] och leverantörer av applikationer som använder smarta kontrakt.

Dataförmedlingstjänster i Data Governance Act

En ’dataförmedlingstjänst’ är en tjänst som med tekniska eller rättsliga medel gör det möjligt att dela data mellan fysiska personer eller datahållare och dataanvändare. Dataförmedlingstjänster är bara till för att dela data, och en leverantör av sådana tjänster får inte använda plattformen för andra ändamål. Tjänsten kan däremot kompletteras med ytterligare tjänster för att underlätta utbytet av data, exempelvis i form av tillfällig lagring, förädling, konvertering, anonymisering och pseudonymisering. Dataförmedlingstjänsterna ska anmäla sig till de nationella tillsynsmyndigheterna i EU och registreras i nationella register – enligt det senaste förslaget ska Post- och telestyrelsen (PTS) utses till behörig myndighet. EU-kommissionen kommer sedan att sammanställa en lista över samtliga dataförmedlingstjänster i EU.

4 Vissa tjänster av allmänt intresse är undantagna det här förbudet.
5 EU-kommissionen vill skapa datautrymmen eller ’data spaces’ för att dela data inom och mellan olika sektorer. Dessa existerar inte ännu.

Checklista: Data Act – Skyldigheter för produkttillverkare, tjänstetillhandahållare och andra datahållare[6]

- [ ] Se till att den uppkopplade produkten och tjänsten är utformad så att data (inklusive relevant metadata), är direkt tillgänglig för användaren på ett enkelt, säkert och kostnadsfritt sätt i ett heltäckande, strukturerat, allmänt använt och maskinläsbart format.
- [ ] Innan ett avtal träffas om en uppkopplad produkt, lämna åtminstone följande information till användaren:
    - Vilken typ, format och uppskattad mängd data som den uppkopplade produkten kan skapa.
    - Om produkten kan skapa data kontinuerligt och i realtid.
    - Om produkten kan lagra data lokalt eller på en server samt hur länge data ska lagras.
    - Hur användaren kan få åtkomst till, hämta eller radera datan, hur det går till tekniskt och vilka villkor som gäller.
- [ ] Innan ett avtal träffas om en tjänst som hör ihop med en uppkopplad produkt, lämna åtminstone följande information till användaren:
    - Vilken typ, uppskattad mängd och hur ofta den data som datahållaren tar emot och villkoren för användarens åtkomst till eller hämtning av data, inklusive hur och hur länge datahållaren lagrar datan.
    - Om datahållaren tänker använda datan själv och vilka ändamål datan ska användas för, och om någon annan part ska få använda datan för ändamål som användaren gått med på.
    - Datahållarens och andra eventuella databehandlingsparters identitet (företagsnamn och geografisk adress).
    - Hur man kan ta kontakt och kommunicera med datahållaren.
    - Hur användaren kan begära att data delas eller avsluta datadelningen med andra.
    - Användarens rätt att lämna in ett klagomål.
    - Om datahållaren har identifierat företagshemligheter[7] i datan och identiteten på innehavaren av företagshemligheten.
    - Avtalstiden samt villkoren för att säga upp avtalet.
- [ ] Registrera inte användarens begäran om tillgång till data för andra ändamål än att tillgodose tillgången.
- [ ] Kartlägg vad i den data som skapas som är företagshemligheter och låt inga obehöriga ta del av dem.
- [ ] Teckna sekretessavtal och se till att systemets användare inte har mer tillgång till data än nödvändigt för att förhindra dataintrång och obehörig åtkomst.

6 De generella skyldigheterna finns i kapitel II.
7 Företagshemligheter är information om affärsförhållanden som inte är allmänt känd eller lättillgänglig, som innehavaren har vidtagit rimliga åtgärder för att hemlighålla, och vars röjande skulle medföra skada i konkurrenshänseende för innehavaren.

Data Act och GDPR

Data som genereras i samband med användningen av en uppkopplad produkt eller en tjänst som hör ihop med produkten kan i många fall också vara personuppgifter. Data Act ändrar inte några av skyldigheterna eller rättigheterna som anges i GDPR, och skapar inga nya rättigheter eller nya rättsliga grunder för behandling av personuppgifter. Snarare är Data Act ett ytterligare lager av reglering som bland annat innebär att information som måste ges enligt GDPR behöver kompletteras med de krav på transparens som följer av Data Act.

För att data ska kunna delas mellan olika aktörer på det sätt som Data Act förutser innebär det alltså att datadelningen behöver vara förenlig med GDPR. Bland annat betyder det att det måste finnas en *rättslig grund* för att dela personuppgifter med tredjeparter. I praktiken kan det ofta vara motiverat att endast dela anonymiserade uppgifter, som alltså faller utanför GDPR:s tillämpningsområde. För att en uppgift ska ses som anonym behöver man säkerställa att mottagaren av anonyma data inte rimligen kan identifiera personer med hjälp av tänkbara hjälpmedel (så som andra databaser eller offentligt tillgängliga uppgifter). Att uppgifter som namn, personnummer, adress och telefonnummer behöver raderas är uppenbart, men även kombinationer av väldigt allmän information kan vara så pass unika att det är möjligt att identifiera en person. Vill man dela anonyma data behöver man alltså tänka på följande:

- Hur unika är uppgifterna för vissa personer?
- Går det att kombinera uppgifterna med en annan databas för att återidentifiera individer?
- Vilka resurser har mottagaren till sitt förfogande, i form av tid, pengar och arbetskraft?

Data Act är också inspirerad av GDPR och ger icke-personuppgifter – det vill säga alla uppgifter som inte är personuppgifter enligt GDPR – ett visst skydd. Det innebär bland annat att datahållare inte kan använda uppgifterna på sätt som försämrar användarens kommersiella sits. Datahållaren får till exempel inte använda uppgifterna för att dra slutsatser om användarens ekonomiska situation, dennes tillgångar eller produktionsmetoder. Datahållaren kan inte heller dela uppgifterna med någon annan förutom om det är ett led i fullgörandet av avtalet med användaren. Den här tredje parten får då inte heller dela uppgifterna vidare eller nyttja datan för andra ändamål än de uttryckligen överenskomna. Den här typen av reglering är väldigt lik hur underleverantörer, eller så kallade personuppgiftsbiträden, får behandla uppgifter enligt GDPR.

Överföringar utanför EU

GDPR ställer krav på skyddsåtgärder när personuppgifter överförs till tredjeland, det vill säga utanför EU/EES. Data Act inför också krav på att skydda icke-personuppgifter från tredjeländers statliga myndigheter. Problem kan uppstå då databehandlingstjänster behöver följa utländsk lag som ger sådana myndigheter möjlighet att kräva tillgång till data som databehandlingstjänsterna förfogar över.

Data Act ställer krav på att databehandlingstjänster endast får lämna ut icke-personuppgifter till myndigheter i tredjeland om vissa villkor är uppfyllda – framförallt får utlämnandet inte ske i strid med nationell eller EU-rätt. Dessutom behöver databehandlingstjänsterna informera kunden om att det finns en sådan begäran, förutom om den görs i ett brottsbekämpande syfte.

Företag som köper in databehandlingstjänster från aktörer som är underställda utländsk lag behöver med andra ord säkerställa att tjänsternas avtalsvillkor är förenliga med kraven i Data Act.

Användarens rättigheter

Rätt till ”egna” data

Kapitel II i Data Act reglerar vilka rättigheter användare har i samband med nyttjandet av en tjänst som hör ihop med en uppkopplad produkt. Användarna har rätt att få tillgång till data som skapats i samband med användningen, och datahållaren ska säkerställa:

- en lätt och säker tillgång till data utan extra avgifter,
- att data är i ett strukturerat, fullständigt och allmänt använt och maskinläsbart format,
- att data är direkt tillgängliga i realtid, förutsatt att det är tekniskt möjligt, och
- att användaren kan dela data med andra aktörer utan dröjsmål.

Reglerna kompletterar de som gäller under GDPR, det vill säga rätten till tillgång och portabilitet. Skillnaden är att kraven i Data Act också gäller för juridiska personer och inte endast fysiska personer (’registrerade’ enligt GDPR). Rätten till dataportabilitet är inte heller begränsad till sådana personuppgifter som samlats in med stöd av avtal med den fysiska personen eller den fysiska personens samtycke.

Rimliga villkor[8]

Data Act ställer tydliga krav på skäliga villkor mellan företag i samband med åtkomst till och användning av data. Reglerna kompletterar de svenska reglerna och svensk marknadspraxis. Följande anses som oskäliga avtalsvillkor om de införs ensidigt av den ena avtalsparten:

a. uteslutet eller begränsat ansvar för uppsåtliga handlingar eller grov vårdslöshet.
b. uteslutning av tillgängliga rättsmedel vid avtalsbrott.
c. ensamrätt att avgöra om levererade data är förenliga med avtalet.

Följande ensidiga ”*take it or leave it*”-avtalsvillkor antas i regel också vara oskäliga, även om det inte är lika kategoriskt:

- En olämplig begränsning av tillgängliga påföljder eller skadeståndsansvar vid avtalsbrott, eller ett utvidgande av skadeståndsansvaret.
- Tillgång till företagshemligheter eller andra skyddade uppgifter i strid med den andra partens berättigade intressen.
- Att ensidigt hindra part från att använda, samla in, få åtkomst till, kontrollera eller i övrigt nyttja data på ett adekvat sätt.
- Oskäligt långa eller orimligt korta uppsägningstider.
- Att hindra part från att erhålla en kopia av data som tillhandahållits eller skapats inom ramen för avtalet.
- Rätt till väsentliga prisändringar eller andra väsentliga avtalsvillkor kopplade till data som ska delas och utan möjlighet att säga upp avtalet på grund av ändringen.

Rätt och lätt att byta tjänster[9]

Användare ska inte vara ”låsta” till vissa leverantörer av databehandlingstjänster som i praktiken är samma sak som molntjänster. För att förhindra inlåsningseffekter har EU infört nya krav på att det ska vara lätt att byta databehandlingstjänster och även att utbyta och använda data i fler system, så kallad *interoperabilitet*.

8 Kraven på rimliga villkor finns framförallt i kapitel IV.
9 Kraven på byte av tjänster och interoperabilitet finns i kapitel VI och VIII.

För att det ska vara lättare att byta databehandlingstjänster anger Data Act att leverantörer ska undanröja kommersiella, tekniska, avtalsmässiga och organisatoriska hinder som förhindrar användarna från att:

- säga upp avtal inom 30 dagar,
- ingå avtal med nya leverantörer inom samma område,
- flytta data och digitala tillgångar till en annan leverantör,
- uppnå en likvärdig funktionsnivå hos en annan leverantör, och
- avskilja leverans av infrastruktur från övriga databehandlingstjänster, det vill säga att det ska gå att köpa datorresurser som servrar, nät eller virtuella resurser utan att köpa programvara och applikationer av samma leverantör.

Kraven får ses som relativt långtgående, och tre år efter Data Acts ikraftträdande får leverantörer inte heller ta betalt för att assistera med bytet av en tjänst till en annan leverantör.

Portabilitet och interoperabilitet

Portabilitet innebär att data kan laddas ner eller flyttas från en tjänst till en annan. Portabilitet är dels en något begränsad rättighet enligt GDPR, dels även en förutsättning för att kunna byta databehandlingstjänster.

Interoperabilitet innebär att två eller fler system eller applikationer kan utbyta och använda data för att utföra sina funktioner i realtid, det vill säga att olika system kan kommunicera med varandra. Det betyder att tjänster som tillhandahålls av olika leverantörer kan fungera ihop.

Dessa skyldigheter är sammanlänkade med kraven på interoperabilitet som förutsätter att databehandlingstjänster ska kunna samverka och utbyta data med andra externa system. Nya EU-standarder om interoperabilitet kommer att publiceras och dataförmedlingstjänster kommer att förväntas vara kompatibla med dessa. De tekniska detaljerna som styr hur dataförmedlingstjänster förväntas göra det lätt för sina användare att byta tjänster och koppla ihop olika tjänster återges med andra ord i detalj först senare.

Konsekvenser av regelbrott[10]

Vem granskar att reglerna följs?

Det är upp till medlemsstaterna att bestämma vilken eller vilka myndigheter som kommer att ansvara för att övervaka tillämpningen och genomförandet av Data Act. Det är inte klarlagt vilken som blir den behöriga myndigheten, men det finns goda skäl att anta att PTS i alla fall kommer att få ett visst ansvar. Om uppgifterna i fråga också är person-uppgifter kommer Integritetsskyddsmyndigheten (IMY) att vara ansvarig för tillsyn även under Data Act.

Sanktioner och andra straff

Även sanktionerna har mycket gemensamt med GDPR och utgår med beaktande av bland annat överträdelsens art, tidigare överträdelser, ekonomisk nytta och förmildrande omständigheter.

För överträdelser kopplade till skyldigheter och rättigheter i förhållande till datadelning (kapitel II), villkor för datadelning (kapitel III) och skyldigheter att göra data tillgängliga för myndigheter (kapitel V) är dataskydds-myndigheterna behöriga att utfärda sanktioner enligt GDPR. Maxbeloppet är 20 miljoner euro eller 4 procent av företagets globala omsättning.

Straffen för övriga överträdelser av Data Act kommer att regleras nationellt.

10 Se kapitel IX.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

Foto: Unsplash