Dataskyddsförordningen – det digitala årtiondets drottning

Hajo Michael Holtz och Jonas Ledendal

1. Inledning

En stark och sammanhängande ram för dataskyddet inom unionen är en förutsättning för att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden inom EU, se skäl 7 i EU:s allmänna dataskyddsförordning (General Data Protection Regulation, GDPR).[1] Dataskyddsförordningen skapar rättslig säkerhet och öppenhet för ekonomiska aktörer genom att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och genom att undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden, se skäl 13 GDPR. Dataskyddsförordningen ingår i EU:s digitala strategi som syftar till att skapa fri rörlighet för innovativa digitala tjänster och produkter inom EU.[2] En del i denna strategi är att skapa förutsättningarna för den europeiska dataekonomin och en inre marknad för data, där data ska kunna röra sig fritt mellan medlemsstater, sektorer och organisationer.[3] Med ”data” avses såväl personuppgifter som icke-personuppgifter, exempelvis aggregerade data eller industridata. Stora datamängder (Big Data), molntjänster (Cloud Services) och sakernas internet (Internet of Things) är avgörande för EU:s konkurrenskraft och data ses ofta som en katalysator för ekonomisk tillväxt, innovation och digitalisering i alla sektorer av ekonomin, särskilt för små och medelstora företag (och uppstartsföretag) och för samhället i stort.[4]

Dataskyddsförordningen har tillämpats sedan den 25 maj 2018 och kan anses vara en milstolpe i både EU-rättens utveckling och i skapan-

[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).
[2] Se Europeiska kommissionen, En strategi för en inre digital marknad i Europa, COM(2015) 192 final, 2015-05-06.
[3] Jfr Europeiska kommissionen, En EU-strategi för data, COM(2020) 66 final, 2020-02-19, s. 12 ff.
[4] Europeiska kommissionen, En strategi för en inre digital marknad i Europa, COM(2015) 192 final, 2015-05-06, s. 14.

det av en digital inre marknad. Dataskyddsförordningen måste därför ses i ett sammanhang med andra rättsakter som är en del i förverkligandet av denna strategi, bland annat regler avseende ansvaret för leverantörer av förmedlingstjänster (Digital Services Act, DSA)[5], regler avseende centrala plattformstjänster (Digital Markets Act, DMA)[6] samt regler avseende en ram för dataförmedlingstjänster och dataaltruism (Data Governance Act, DGA)[7]. Utöver dessa redan antagna rättsakter kan ytterligare lagförslag nämnas som ingår i EU:s digitala strategi och som har beröringar med behandling av personuppgifter i den digitala miljön. Hit hör framförallt regler för att främja och stödja delning av data genom att klargöra vem som kan skapa värde från data och under vilka villkor (förslaget till Data Act) och regler avseende utsläppande på marknaden och vissa tillämpningar av system för artificiell intelligens (förslaget till AI Act). I det här bidraget ges en överblick över hur dataskyddsförordningen förhåller sig till några av de redan antagna rättsakterna inom den digitala inre marknaden, nämligen DMA, DSA och DGA, eller närmare bestämt, hur dessa nya rättsakter förhåller sig till dataskyddsförordningen i egenskap av befintligt regelverk. Andra rättsakter inklusive de föreslagna som ännu inte är antagna analyseras däremot inte närmare i det här bidraget.[8]

2. Data Governance Act

Först ut bland rättsakterna är Data Governance Act (DGA) som antogs den 30 maj 2022. Dess syfte är att förbättra villkoren för datadelning på den inre marknaden genom att skapa en harmoniserad ram för utbyte av data och föreskriva vissa grundläggande krav på dataförvaltning, med särskilt fokus på att underlätta samarbetet mellan medlemsstaterna, se skäl 3 DGA. Konkret innehåller DGA bestämmelser om vidareutnyttjande av skyddade data från den offentliga sektorn, tillhandahållande av dataförmedlingstjänster och dataaltruism. När data som innefattar personuppgifter delas enligt dessa bestämmelser uppkommer frågan om hur dessa förhåller sig till dataskyddsförordningen. När frågan gäller vidareutnyttjande av data från den offentliga förvaltningen behöver

[5] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).
[6] Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader).
[7] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[8] Författarna har anledning att i ett annat sammanhang återkomma i ämnet.

dataskyddsförordningen inte bara avgränsas från DGA, utan även från direktivet om öppna data och vidareutnyttjande av information från den offentliga sektorn (det s.k. öppna data-direktivet).[9]

2.1 Det generella förhållandet

Data Governance Act ska inte påverka tillämpningen av unionsrättsliga och nationella bestämmelser om skydd av personuppgifter, se artikel 1.3 DGA. Vidareutnyttjandet ska alltså, oberoende av DGA, överensstämma med de krav som ställs upp i dataskyddsförordningen. Om förordningen står i strid med unionens dataskyddsrätt eller nationella bestämmelser som antagits i enlighet med unionsrätten ska bestämmelserna om skydd av personuppgifter ha företräde. Det framgår också uttryckligen att förordningen inte skapar någon rättslig grund för behandlingen och heller inte påverkar några av de skyldigheter eller rättigheter som bland annat föreskrivs i EU:s dataskyddsförordning. DGA ska heller inte påverka hur de myndigheter som ska bedriva tillsyn på dataskyddsrättens område utövar sina befogenheter. Om andra myndigheter fungerar som behöriga myndigheter enligt DGA ska denna verksamhet bedrives på ett sätt som inte påverkar dataskyddsmyndigheternas behörighet och befogenhet enligt EU:s dataskyddsförordning, se skäl 4 DGA. Detsamma torde gälla enligt artikel 1.4 i öppna data-direktivet.[10] Artikel 1.4 anger förvisso inte uttryckligen att dataskyddsbestämmelserna ska ges företräde, men detta följer av dess tillämpning inte ska påverka dessa bestämmelser. Skäl 52 i direktivet anger dessutom att ”vidareutnyttjande av personuppgifter endast är tillåtet om principen om ändamålsbegränsning enligt artikel 5.1 b artikel 6 i förordning (EU) 2016/679 efterlevs”. I båda rättsakterna pekar lagstiftaren på att anonymisering utgör ett lämpligt sätt att sammanjämka rätten till skydd av personuppgifter med intresset att dela och vidareutnyttja data.[11]

2.2 Vidareutnyttjande av data från den offentliga förvaltningen

Delning av data från den offentliga sektorn regleras på unionsnivå numera i huvudsak genom två rättsakter. Bestämmelser om vidareutnyttjande av handlingar som innehas av myndigheter och vissa offentliga företag finns

[9] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (omarbetning).
[10] Se även artikel 1.4 i direktiv 2003/98 (det ursprungliga PSI-direktivet) som ersatts av öppna data-direktivet och vilket angav att detta ”inte på något sätt” skulle påverka skyddet av personuppgifter.
[11] Se bl.a. skäl 52 i öppna data-direktivet och skäl 7 DGA.

sedan den 20 juni 2019 i öppna data-direktivet. I svensk nationell rätt har direktivet införlivats genom lagen (2022:818) om den offentliga sektorns tillgängliggörande av data (öppna data-lagen), som trädde i kraft den 1 augusti 2022. Dessa bestämmelser kompletteras numera av DGA som är direkt tillämplig i alla medlemsstater sedan den 24 september 2023. När det gäller vidareutnyttjande av data från offentlig förvaltning är rättsakternas tillämpningsområden ömsesidigt uteslutande, dvs. bestämmelserna i Data Governance Act tillämpas endast när ett vidareutnyttjande inte omfattas av öppna data-direktivet, se artikel 3.1 d DGA.[12]

Öppna data-direktivet är i princip tillämpligt på vidareutnyttjande av alla handlingar som innehas av offentliga myndigheter och vissa offentliga företag som inte omfattas av de undantag som anges i direktivet, se artikel 1 i direktiv 2019/1024. Direktivet innehåller även bestämmelser om särskilda villkor för vidareutnyttjande av vissa forskningsdata, se artikel 10 i direktiv 2019/1024. Undantag görs enligt artikel 1.2 h för handlingar som med hänsyn till skyddet av personuppgifter antingen är helt undantagna från tillgång eller vars tillgång är begränsad genom sådana bestämmelser. Detsamma gäller handlingar som innehåller personuppgifter vilkas vidareutnyttjande är oförenligt med enskilda individers rätt till skydd av personuppgifter, privatliv och integritet, särskilt såsom dessa grundläggande rättigheter konkretiserats genom unionsrättsliga och nationella bestämmelser på dataskyddsrättens område. DGA ska som framgår av artikel 3.1 d motsatsvis tillämpas på vidareutnyttjande av personuppgifter som faller utanför direktivets tillämpningsområde. När en handling undantas genom artikel 1.2 h i direktivet ska denna alltså i stället omfattas av bestämmelserna om vidareutnyttjande av skyddade data i DGA.

En första förutsättning för att öppna data-direktivet över huvud taget ska bli tillämpligt är att de ifrågavarande personuppgifterna kan göras allmänt tillgängliga i enlighet med dataskyddsrättsliga bestämmelser.[13] Direktivet som sådant medför inte någon skyldighet att göra personuppgifter tillgängliga, vilket innebär att utlämnandet kräver någon annan rättslig grund (se ovan avsnitt 2.1). Vidareutnyttjande torde dessutom vanligtvis innebära att uppgifterna behandlas för andra ändamål än dem för vilka de ursprungligen samlades in av myndigheten. Principen om ändamålsbegränsning, som förbjuder vidarebehandling

[12] Även i övrigt har bestämmelser i DGA utformats för att utgöra en spegelbild av de undantag som finns i direktiv 2019/1024.

[13] Unionsrätten gör skillnad mellan bestämmelser om tillgång till handlingar och vidareutnyttjande av handlingar. Medan det senare har harmoniserats så bygger unionens rättsliga ram för vidareutnyttjande på och påverkar inte medlemsstaternas bestämmelser om tillgång till allmänna handlingar (artikel 1.3 direktiv 2019/1024 samt artikel 3.3 b förordning 2022/868).

som är oförenlig med dessa ursprungliga ändamål, kan alltså göra det svårt att göra datamängder som innehåller personuppgifter allmänt tillgängliga på det sätt som avses i direktivet (se avsnitt 2.1). Direktivet är tänkt att tillämpas i situationer när det saknar betydelse vem som ska vidareutnyttja de ifrågavarande handlingarna. Det räcker som framgår av artikel 1.2 h att möjligheten att få tillgång till en handling som innehåller personuppgifter begränsats (till exempel att någon måste kunna åberopa särskilda skäl).[14] Det ska alltså i princip röra sig om uppgifter som lämpar sig för att tillgängliggöras som öppna data. Det torde dock, som påpekats i litteraturen, sällan vara fallet vad gäller datamängder som innehåller personuppgifter, vilket gör att vidareutnyttjandet av sådana data normalt i stället kommer att regleras av DGA.[15]

Öppna data-direktivet och DGA innehåller alltså inga undantag från eller inskränkningar av den höga nivå av skydd som stadgas i unionens rättsliga ram för skydd av personuppgifter. Det som lagstiftaren har velat komma åt genom bestämmelserna om vidareutnyttjande av skyddade data i kapitel II i DGA är att myndigheter inte gör sådana personuppgifter tillgängliga trots att det är möjligt enligt unionens dataskyddsrätt, se skäl 6 DGA. Förordningen ska främja sådan datadelning, särskilt för vetenskaplig forskning och innovation, genom att öka myndigheternas tekniska och organisatoriska kapacitet att göra personuppgifter tillgängliga för vidareutnyttjande på ett sätt som överensstämmer med unionens dataskyddsrätt. Att göra det är som lagstiftaren konstaterat både en tidskrävande och kunskapsintensiv uppgift, vilket har resulterat i att sådana data hittills blivit otillräckligt utnyttjade. Förordningen i sig innehåller däremot inga skyldigheter för myndigheter att göra data tillgängliga, utan harmoniserar endast villkoren för vidareutnyttjande. En medlemsstat ska dock säkerställa att dess myndigheter har nödvändiga resurser för att leva upp till förordningens krav, se artikel 5.1 andra stycket DGA.

Artikel 5.3 DGA anger att om en medlemsstat väljer att göra skyddade uppgifter tillgängliga för vidareutnyttjande så ska myndigheten säkerställa att deras skyddade karaktär bevaras. En myndighet får därför kräva att personuppgifterna ska anonymiseras. I sådana fall ska det enligt artikel 5.5 DGA även vara förbjudet för vidareutnyttjare att åter-

[14] Se även artikel 1.2 f i direktiv 2019/1024 som anger att direktivet är inte tillämpligt när tillgång till en handling kräver att någon kan visa att denne har ett särskilt intresse.

[15] Specht-Riemenschneider, Data Governance Act (2023), s. 187 (“Damit sind sämtliche personenbezogene Daten, die unter den Anwendungsbereich der DS-GVO fallen, vom Anwendungsbereich nach Art. 1 Abs. 2 lit. H PSI-RL ausgenommen”). En slutsats som dock vad gäller svensk rätt kan vara för långtgående med hänsyn till det företräde som yttrandefrihetsgrundlagarna åtnjuter enligt 1 kap. 7 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

identifiera de registrerade och denne ska vidta åtgärder för att förhindra sådan återidentifiering.[16] Myndigheten kan också kräva att tillgång till och vidareutnyttjande av data måste ske på distans inom en säker behandlingsmiljö som tillhandahålls eller kontrolleras av myndigheten. När det senare inte kan ske utan att den registrerades rättigheter och intressen hotas kan myndigheten i stället kräva att behandlingen ska utföras i myndighetens lokaler. När behandlingen sker inom en säker behandlingsmiljö får myndigheten enligt artikel 5.4 DGA även ställa upp ytterligare villkor för att garantera systemens säkerhet. Myndigheten får bland annat förbehålla sig rätten att verifiera processen, metoderna och alla resultat av den behandling som utförs av vidareutnyttjaren för att bevara ”integriteten i dataskyddet”.[17] När det inte går att vidareutnyttja data på något av ovanstående sätt och det även saknas rättslig grund för att överföra personuppgifterna ska en myndighet enligt artikel 5.6 DGA i stället bistå en potentiell vidareutnyttjare att inhämta samtycke från de registrerade.[18] Undantag görs när detta medför en oproportionerlig arbetsbörda för myndigheten.

2.3 Dataförmedlingstjänster

Data Governance Act innehåller även en rättslig ram för anmälan av och tillsyn över tillhandahållandet av dataförmedlingstjänster, se artiklarna 10–15. Med dataförmedlingstjänst avses enligt artikel 2.11 en tjänst som syftar till att upprätta affärsförbindelser för datadelning mellan å ena sidan ett obestämt antal registrerade och datainnehavare och å andra sidan dataanvändare.[19] Syftet med att reglera sådana aktörer i förordningen är att säkerställa att dessa fungerar som en neutral tredje part som sammanför nyssnämnda parter, se skäl 33 DGA. Enligt artikel 11 i förordningen måste en sådan leverantör av dataförmedlingstjänster

[16] Artikel 5.5 DGA ålägger även vidareutnyttjaren en skyldighet att inte enbart underrätta Integritetsskyddsmyndigheten vid en personuppgiftsincident som rör den vidareutnyttjade datan, utan även den myndighet som gjort denna tillgänglig enligt DGA.

[17] Det framgår vid en jämförelse med andra språkversioner inte helt klart om detta avser skydd av personuppgifter eller om det är ett olyckligt ordval (”preserve the integrity of the protection of the data” i engelsk språkversion skulle lika gärna kunna avse informationssäkerhet).

[18] En myndighets skyldighet att bistå vid inhämtande av samtycke enligt artikel 5.6 DGA förutsätter att det varken går att vidareutnyttja data genom att anonymisera eller inom en säker behandlingsmiljö. Behandling med stöd av samtycke måste även vara tillåten enligt unionsrätten eller en medlemsstats nationella rätt. Exempelvis kan medlemsstaterna enligt artikel 9.2 a GDPR begränsa denna möjlighet.

[19] Artikel 2.11 led a till d DGA innehåller även ett antal inskränkningar som undantar ett antal förmedlingstjänster från bestämmelserna i kapitel III. Exempelvis innebär dessa att s.k. datamäklare (”data brokers”) i traditionell mening inte omfattas av förordningen. Se Larsson & Ledendal, Personuppgifter som betalningsmedel, Konsumentverket, rapport 2017:4, s. 22.

lämna en anmälan till den behöriga myndigheten för sådana tjänster. När leverantören mottagit en bekräftelse från myndigheten att denne uppfyller de krav som ställs upp i förordningen får leverantören enligt artikel 11.9 använda beteckningen ”leverantör av dataförmedlingstjänster som är erkänd i unionen” samt en gemensam logotyp.[20]

Syftet med de bestämmelser om dataförmedlingstjänster som ställs upp i kapitel III i DGA är i första hand att öka tilliten för sådana tjänster genom att reglera dessa. Förutom ovannämnda anmälningsförfarande innehåller artikel 12 DGA även ett antal krav som ska uppfyllas av den som tillhandahåller en dataförmedlingstjänst. Dessa ska bland annat säkerställa att en sådan mellanman endast använder delade och insamlade data för att tillhandahålla och utveckla dataförmedlingstjänsten som sådan, se artikel 12 a DGA. Kraven är dock inte primärt tänkta som en förstärkning av principen om ändamålsbegränsning enligt dataskyddsförordning, utan ska garantera att dessa inte används på ett sätt som kan komma i konflikt med datainnehavares kommersiella intressen.

Detta gäller dock primärt de tjänster mellan datainnehavare och dataanvändare som anges i artikel 10 a DGA. Dess bestämmelser är även tillämpliga på två andra kategorier av förmedlingstjänster, närmare bestämt tjänster som enligt led b riktar sig till registrerade och sådana datakooperativs tjänster som anges i led c.[21] När det gäller dessa tjänster är det tydligare att lagstiftarens avsikt varit att dataförmedlingstjänsten även ska ta ett särskilt ansvar för att förstärka och förenkla utövandet av den registrerades rättigheter. För dessa gäller därför vissa särskilda krav, bland annat avseende information, som ska förstärka de registrerades rättigheter, se artikel 12 m och n DGA. Genom DGA ska leverantören agera på ett sådant sätt att denne tillvaratar den registrerades intresse. Denne får alltså mer rollen av ett ombud för den senare än en ren datamäklare. Leverantören ska också ha en rådgivande funktion. Om leverantören tillhandahåller verktyg för samtycke ställs dessutom särskilda krav på information vid överföring till tredjeland och att den registrerade ska förses med verktyg för att återkalla sitt samtycke.

Bestämmelserna om dataförmedlingstjänster syftar alltså inte i första hand till att förstärka de registrerades rättigheter, men som konstaterats ovan påverkar förordningen enligt artikel 1.3 inte unionens rättsliga ram för skydd av personuppgifter. DGA innehåller sålunda inga undantag eller lättnader och sådana tjänster måste följaktligen tillhandahållas i full överensstämmelse med kraven i dataskyddsförordningen

[20] En gemensam logotyp har fastställts genom kommissionens genomförandeförordning (EU) 2023/1622 av den 9 augusti 2023 om utformningen av gemensamma logotyper för att identifiera leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som är erkända i unionen.

[21] Artikel 2.15 DGA definierar vad som avses med ”datakooperativs tjänster”.

(se avsnitt 2.1). Det finns också, som beskrivits ovan, genom tjänster som riktar sig till registrerade och datakooperativs tjänster en möjlighet att inom förordningens ramar bygga upp särskilda typer av tjänster som är inriktade på att förstärka de registrerades ställning genom att göra det enklare att tillvarata sina rättigheter enligt bland annat EU:s dataskyddsförordning. Ett exempel är MyData, som arbetat fram ett ramverk för att förstärka registrerades självbestämmande över sina personuppgifter i samband med datadelning.[22] I motsats till modellen med stora plattformar som tenderar att hamna i en intressekonflikt när de monetiserar sina användares personuppgifter genom att ta betalt av annonsörer och andra dataanvändare, kan sådana betrodda mellanhänder spela en viktig roll vid framväxten av en dataekonomi som bygger på respekt för användarnas grundläggande fri- och rättigheter.[23]

2.4 Dataaltruism

Data Governance Act innehåller även bestämmelser om frivillig registrering av organisationer som tillhandahåller data för altruistiska ändamål, se artiklarna 16–25 DGA. Syftet med de bestämmelser om dataaltruism som finns i kapitel IV i förordningen är i första hand att skapa betrodda verktyg för att dela sådan data. För sådana erkända dataaltruismorganisationer gäller enligt artikel 15 DGA som utgångspunkt inte bestämmelserna om dataförmedlingstjänster i kapitel III. Avsikten är att underlätta dataaltruism, vilket enligt artikel 2.16 DGA innefattar frivillig delning av data på grundval av de registrerades samtycke utan någon ersättning när dessa görs tillgängliga för mål av allmänintresse. DGA anger att sådana allmänna intressen bland annat kan innefatta hälso- och sjukvård, bekämpande av klimatförändringar, förbättring av mobiliteten, främjande av utveckling, framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster, politiskt beslutsfattande eller vetenskaplig forskning av allmänt intresse. Förordningen som sådan innehåller dock endast en harmonisering av registreringsförfarandet och vilka villkor som ska gälla för sådana organisationer. Det finns inga krav på att medlemsstater ska införa några nationella arrangemang för dataaltruism, utan artikel 16 DGA ger endast en sådan möjlighet. Samtidigt gäller en registrering i hela unionen och den registrerade organisationen har rätt att använda beteckningen

[22] MyData Global ry är en ideell förening som är registrerad i Finland. Se https://www.mydata.org/participate/declaration/ [2023-08-23].
[23] Se bl.a. Ledendal, Samtycke till behandling av personuppgifter i Karlsson Tuula m.fl. (red.), Festskrift till Rolf Dotevall (2020), s. 411–412.

”dataaltruismorganisation som är erkänd i unionen” och en gemensam logotyp.[24]

Förordningen innehåller liksom beträffande dataförmedlingstjänster (se avsnitt 2.3) inga undantag eller lättnader för registrerade dataaltruismorganisationer, utan deras behandling av personuppgifter måste enligt artikel 1.3 DGA ske i full överensstämmelse med bland annat dataskyddsförordningen (se ovan). Förutom de krav som redan följer av dessa allmänna bestämmelser ställer artikel 20 och 21 DGA även upp särskilda krav på transparens och krav för att skydda de registrerades rättigheter. Dessa kompletteras genom den regelbok som enligt artikel 22 DGA ska fastställas av kommissionen genom delegerade akter. För att främja insamling av data baserat på dataaltruism ska kommissionen enligt artikel 25 DGA även anta genomförandeakter om upprättande och utarbetande av ett europeiskt formulär för samtycke till dataaltruism. En del av dessa krav är säkert nödvändiga för att skapa tillit, men avsaknaden av lättnader har samtidigt kritiserats för att regelbördan och risken rent faktiskt ökar trots att det rör sig om organisationer som bedrivs utan vinstsyfte.[25] Det är alltså inte helt klart hur DGA ska bidra till att skapa nödvändiga incitament för att etablera sådana dataaltruismorganisationer. Det hade till exempel varit möjligt att liksom för myndigheter överväga att sätta ett tak för de sanktionsavgifter som kan tas ut med stöd av EU:s dataskyddsförordning.

3. Digital Markets Act

Den 14 september 2022 antogs förordningen om digitala marknader, Digital Markets Act (DMA), vars syfte är att säkerställa öppna och rättvisa marknader inom den digitala sektorn i hela unionen där grindvakter finns, se artikel 1.1. Digital Markets Act är av konkurrensrättslig karaktär och ska komplettera EU:s konkurrensrätt som är begränsad till vissa fall av konkurrensbegränsande beteende och efterhandstillsyn, jfr skäl 5 i DMA. DMA är enbart tillämplig på centrala plattformstjänster som tillhandahålls eller erbjuds av s.k. grindvakter, se artikel 1.2. En grindvakt är en central plattformstjänst som av Europeiska kommissionen har betecknats som sådan i enlighet med artikel 3 DMA. Grindvakter har en betydande inverkan på den inre marknaden genom att de erbjuder ett stort antal företagsanvändare ingångar för att nå slutanvändare i hela

[24] En gemensam logotyp har fastställts genom kommissionens genomförandeförordning (EU) 2023/1622 av den 9 augusti 2023 om utformningen av gemensamma logotyper för att identifiera leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som är erkända i unionen.

[25] Se även Hennemann & Specht-Riemenschneider, Data Governance Act (2023), s. 56–57.

unionen och på olika marknader, se skäl 6 DMA. DMA omfattar bland annat onlinebaserade förmedlingstjänster, sökmotorer, sociala nätverk, nummeroberoende interpersonella kommunikationstjänster, operativsystem, webbläsare, virtuella assistenter och molntjänster, se artikel 2.2 DMA. För ett betecknande som grindvakt krävs bland annat en årlig omsättning inom unionen på minst 7,5 miljarder EUR samt minst 45 miljoner aktiva slutanvändare i månaden som är etablerade eller befinner sig i unionen och minst 10 000 aktiva företagsanvändare per år som är etablerade i unionen, se artikel 3.2 DMA. Vid betecknande som grindvakt ska kommissionen beakta vissa omständigheter, bland annat nätverkseffekter och datadrivna fördelar, särskilt tillgång till och insamling av personuppgifter, se artikel 3.8 c DMA. Behandling av personuppgifter och konkurrensförhållanden på den digitala inre marknaden har således en nära koppling. Överlappningen mellan dataskyddsförordningen och DMA visar sig främst i form av ett förbud mot att utföra vissa personuppgiftsbehandlingar.[26] I övrigt är överlappningarna begränsade och DMA visar mindre konceptuella likheter med dataskyddsförordningen, vilket bör bero på dess konkurrensrättsliga karaktär.[27]

3.1 Det generella förhållandet

Artikel 1 DMA innehåller konfliktregler som avgränsar förordningens tillämpningsområde i relation till marknadsrättsliga regler, framförallt det konkurrensrättsliga regelverket, se artikel 1.6 DMA. Dataskyddsförordningen nämns inte i artikel 1 DMA. Även om dataskyddsförordningen reglerar det fria flödet av personuppgifter och därmed också har en marknadsinriktad dimension är syftet med DMA ett annat, nämligen att reglera marknader inom den digitala sektorn i hela unionen där grindvakter finns. Det generella förhållandet till dataskyddsförordningen nämns dock på sedvanligt sätt i skäl 12 DMA: förordningen bör tillämpas utan att det påverkar tillämpningen av dataskyddsförordningen (och ePrivacy-direktivet). Överlappningen mellan dataskyddsförordningen och DMA är inte så pass tydlig att det har varit nödvändigt att reglera frågan direkt i förordningstexten. Samtidigt ska grindvakter säkerställa och visa att de skyldigheter som fastställs i artiklarna 5, 6 och 7 DMA efterlevs och de åtgärder som i det sammanhanget vidtas ska i synner-

[26] En annan intressant bestämmelse som inte närmare berörs här är artikel 13.5 DMA, enligt vilken en grindvakt ska göra det möjligt för företagsanvändare att direkt inhämta samtycke till behandling av uppgifter, om detta krävs enligt dataskyddsförordningen eller ePrivacy-direktivet.

[27] En konceptuell likhet är det territoriella tillämpningsområdet i artikel 1.2 DMA som också bygger på effektlandsprincipen.

het tillämpas i enlighet med dataskyddsförordningen och ePrivacy-direktivet, se artikel 8.1 andra meningen DMA.[28] I artikel 2 DMA hänvisas dessutom till dataskyddsförordningens definitioner av begrepp som också används inom ramen för DMA, vilket gäller begreppen ”personuppgifter” (artikel 2.25), ”profilering” (artikel 2.31) och ”samtycke” (artikel 2.32). Sammanlagt ger dessa bestämmelser uttryck för att dataskyddsförordningen vid eventuella konflikter inom sitt tillämpningsområde bör ha företräde framför DMA.

3.2 Förbud mot vissa personuppgiftsbehandlingar

Kärnan i DMA är grindvakters skyldighet till efterlevnad av bestämmelserna i artiklarna 5, 6 och 7 som innehåller såväl förbud som påbud. Till skillnad från en efterhandsbedömning (*ex post*) av kartellsamarbeten och missbruk av dominerande ställningar bygger DMA på att grindvakter på förhand och generellt förbuds vissa otillbörliga metoder samt åläggs vissa skyldigheter, vilket brukar kallas för en *ex ante*-reglering.[29] Den främsta överlappningen mellan dataskyddsförordningen och DMA sker genom artikel 5.2 DMA som förbjuder grindvakter att utföra vissa personuppgiftsbehandlingar. Förbudet gäller a) ackumulering av slutanvändares personuppgifter från tredje parter i syfte att tillhandahålla onlinebaserade annonseringstjänster b) kombination av slutanvändares personuppgifter som samlats in från en central plattformstjänst med sådana som samlats in från andra tjänster, c) korsanvändning av personuppgifter från en central plattformstjänst med sådana från andra tjänster som tillhandahålls separat av grindvakten och d) inloggning av slutanvändare på olika tjänster i syfte att kombinera personuppgifter. Dessa typer av personuppgiftsbehandlingar får av grindvakter enbart genomföras om slutanvändaren har givits det specifika valet och har gett sitt samtycke i den mening som avses i dataskyddsförordningen.[30] Enligt artikel 5.2 tredje meningen DMA påverkar förbudet inte grindvaktens möjlighet att i tillämpliga fall förlita sig på artikel 6.1 c, d och e GDPR, men inte på artikel 6.1 b och f, se skäl 36, sista meningen i DMA. För att säkerställa att ett eventuellt samtycke till behandling av personuppgifter är frivilligt ska grindvakter erbjuda användarna ett mindre individanpassat men likvärdigt alternativ som inte får vara annorlunda

[28] Artikel 8.1 DMA kan jämföras med principen om ansvarsskyldighet enligt artikel 5.2 i GDPR.

[29] Mendelsohn & Budzinski i Schmidt & Hübener (red.), Das neue Recht der digitalen Märkte – Digital Markets Act (2023), § 2, punkt 43 ff.

[30] Om slutanvändaren har nekat eller dragit tillbaka samtycke som givits enligt första stycket får grindvakten inte upprepa sin begäran om samtycke för samma ändamål mer än en gång inom en period på ett år, se artikel 5.2 andra meningen DMA.

eller av sämre kvalitet jämfört med den tjänst som erbjuds de slutanvändare som ger sitt samtycke, se skäl 36, sjätte meningen och skäl 37, första meningen DMA.[31] Skäl 37 DMA innehåller ytterligare information om kraven på ett giltigt samtycke till behandling av personuppgifter som motsvarar kraven i dataskyddsförordningen.

Frågan är hur förbudet i artikel 5.2 DMA rent praktiskt förhåller sig till dataskyddsförordningen. Oklart är i nuläget om kravet på ”likvärdighet” innebär att också den individanpassade versionen måste vara likvärdig, med andra ord är frågan om den version som inte kräver samtycke till behandling av personuppgifter får vara av bättre kvalitet eller erbjuda andra funktioner (i så fall måhända mot betalning). Ett sådant krav kan bli ett problem för s.k. freemium-affärsmodeller som kombinerar en annonsfinansierad gratistjänst med en bättre betalversion. Frågan bör till slut bero på om valet mellan versionerna och därmed samtycket kan anses vara ”frivilligt” i den mening som avses i dataskyddsförordningen. Oklart är också om ett brott mot förbudet i artikel 5.2 DMA automatiskt innebär en överträdelse av EU:s dataskyddsförordning. Förmodligen är så inte fallet, eftersom DMA inte ska påverka dataskyddsförordningens tillämpning. Frågan bör i praktiken vara mest relevant för de olika tillsynsmyndigheternas behörigheter.

4. Digital Services Act

Parallellt till DMA antogs Digital Services Act (DSA) den 19 oktober 2022. I DSA fastställs harmoniserade regler för tillhandahållandet av förmedlingstjänster på den inre marknaden, i synnerhet en ram för förmedlingstjänsters ansvar, regler om särskilda krav på tillbörlig aktsamhet som är skräddarsydda för specifika kategorier av leverantörer av förmedlingstjänster samt regler för genomförandet och kontrollen av efterlevnaden av denna förordning, se artikel 1.2 DSA. Syftet med DSA är att bidra till en korrekt fungerande inre marknad för förmedlingstjänster genom att fastställa harmoniserade regler för en säker, förutsebar och förtroendeskapande onlinemiljö som främjar innovation, och i vilken de grundläggande rättigheterna i stadgan skyddas på ett effektivt sätt, se artikel 1.1. Relationen mellan DSA och dataskyddsförordningen grundar sig på det faktum att förmedlingstjänster, särskilt onlineplattformar har stor betydelse för användarnas rätt till skydd av personuppgifter i en digital miljö, jfr skäl 52 DSA. Den nya förordningen om digitala tjänster

[31] Såvida inte en försämring av kvaliteten är en direkt följd av att grindvakten inte kan behandla sådana personuppgifter eller logga in slutanvändare på en tjänst.

visar flera konceptuella likheter med dataskyddsförordningen.[32] Därutöver innehåller DSA flera bestämmelser som explicit nämner antingen personuppgifter eller dataskyddsförordningen.[33] En överlappning mellan dataskyddsförordningen och DSA sker framförallt i samband med dark patterns, riktad annonsering på sociala medier samt frågan om dataåtkomst.

4.1 Det generella förhållandet

Det materiella tillämpningsområdet av DSA är ”förmedlingstjänster” som utgör en underkategori av begreppet ”informationssamhällets tjänster”. Som förmedlingstjänst definieras enligt artikel 3 g DSA tre olika huvudkategorier av tjänster, nämligen ”tjänster för enbart vidarefordran” (mere conduit, dvs. överföring av information i ett kommunikationsnät), ”cachningstjänster” (tillfällig lagring av information för att effektivisera den vidare överföringen) och ”värdtjänster” (lagring av information på användarens begäran). Enligt artikel 2.4 ska DSA inte påverka tillämpningen av de regler som fastställs i andra unionsrättsakter som reglerar andra aspekter av tillhandahållandet av förmedlingstjänster på den inre marknaden eller specificerar och kompletterar denna förordning. Hit hör bland annat unionsrätten om skydd av personuppgifter, särskilt dataskyddsförordningen och direktiv 2002/58/EG (ePrivacy-direktivet). Skyddet för individer med avseende på behandling av personuppgifter regleras alltså endast av dessa rättsakter och inte av DSA, se skäl 10, andra stycket DSA. Vid tillämpningen av DSA behöver alltid kraven i dataskyddsförordningen beaktas vad gäller lagligheten av behandling av personuppgifter, registrerades rättigheter eller säkerheten kring personuppgifter. Detta gäller framförallt i relation till personuppgiftsbehandlingar som explicit nämns i DSA, se artikel 25.2 DSA avseende dark patterns, se artikel 26.3 och artikel 28.2 DSA avseende riktade annonser baserade på profilering och artikel 40 DSA avseende tredje parts tillgång till personuppgifter. Den nya förordningen om digitala tjänster påverkar inte heller kravet på samtycke till cookies (9 kap. 28 § lagen om elektronisk kommunikation), se skäl 68, andra stycket DSA, alltså när förmedlingstjänster vill placera information på och utläsa den från användarnas terminalutrustning. I övrigt bör dataskyddsförordningen och ePrivacy-direktivet vid eventuella

[32] Exempel är effektlandsprincipen (se artikel 2.1 DSA), regler om riskbedömning och -begränsning (se artikel 34 och 35 DSA), regler om en intern funktion för regelefterlevnad (se artikel 41) eller sanktionsavgifter (se artikel 52 DSA).

[33] Exempel är artikel 28.3 DSA (onlineplattformar ska beakta principen om uppgiftsminimering) eller artikel 38 DSA (rekommendationssystem som bygger på profilering).

normkonflikter inom sina tillämpningsområden anses som *lex specialis* i relation till DSA.

4.2 Dark patterns

En direkt relation till dataskyddsförordningen skapar DSA i samband med regleringen av s.k. dark patterns, se artikel 25 DSA. Leverantörer av onlineplattformar förbjuds numera uttryckligen att utforma, organisera eller driva sina onlinegränssnitt på ett sätt som vilseleder eller manipulerar användare eller på ett sätt som på annat vis väsentligt snedvrider eller försämrar deras förmåga att fatta fria och välgrundade beslut, se artikel 25.1 DSA. Bestämmelsen gäller såväl för datorprogram, webbsidor och applikationer, se artikel 3 k DSA. Tre konkreta exempel på dark patterns anges i artikel 25.3 DSA, att ge större synlighet åt vissa val, att upprepade gånger (särskilt genom popup-fönster) begära att användaren gör ett val och att göra förfarandet för att avsluta en tjänst svårare än att ansluta sig till den. Förbudet ska dock inte tillämpas på metoder som omfattas av dataskyddsförordningen, se artikel 25.2 DSA.[34] Dark patterns omfattas av dataskyddsförordningen i den mån metoden innebär en behandling av personuppgifter. Metoden används bland annat i samband med samtyckesmekanismer. Om dessa mekanismer är utformade på ett sätt som kan medföra en påtryckning på registrerade att tillåta behandling av fler uppgifter än om alternativen skulle presenteras på ett likvärdigt och neutralt sätt, presentera behandlingsalternativen på ett sätt som gör det svårt för registrerade att avstå från att dela sina uppgifter eller en utformning som gör det svårt för dem att justera sina personliga inställningar och begränsa behandlingen kan det strida mot artikel 25 i dataskyddsförordningen och principen om inbyggt dataskydd.[35] Europeiska dataskyddsstyrelsen har antagit riktlinjer specifikt om dark patterns i sociala mediers användargränssnitt.[36] Något oklart är om dark patterns inom dataskyddsförordningens tillämpningsområde är exkluderade från förbudet i artikel 25 DSA. Ett pragmatiskt resultat skulle vara att pröva dataskyddsförordningen först vid bedömningen av dark patterns innan artikel 25 DSA tillämpas.[37]

[34] Samma gäller om metoden omfattas av direktiv 2005/29/EG om otillbörliga affärsmetoder, dvs. marknadsföringslagen.
[35] Europeiska dataskyddsstyrelsen, Riktlinjer 4/2019 om artikel 25 – Inbyggt dataskydd och dataskydd som standard, Version 2.0, 2020-10-20, punkt 70, s. 20.
[36] Se Europeiska dataskyddsstyrelsen, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, 2023-02-14.
[37] Jfr Maamar i Kraul (red.), Das neue Recht der digitalen Dienste – Digital Services Act (2023), § 4, punkt 157.

4.3 Profilering för riktad annonsering

Ett annat fenomen som skapar en direkt överlappning mellan dataskyddsförordningen och DSA är riktad annonsering på onlineplattformar. Onlineplattformar är framförallt olika sociala nätverk, se skäl 13 DSA. Även i det avseendet är grundförutsättningen för en överlappning att metoden bygger på en behandling av användarnas personuppgifter. Leverantörer av onlineplattformar ska vara transparanta vid presentationen av annonser på sina onlinegränssnitt, se artikel 26.1, och ska erbjuda användare en funktion för att dessa ska kunna anmäla om det innehåll de tillhandahåller utgör eller innehåller kommersiella meddelanden, se artikel 26.2, vilket kan bli relevant för influencers. Intressant är att artikel 26.3 DSA numera förbjuder riktad annonsering på onlineplattformar som bygger på profilering med användning av särskilda kategorier av personuppgifter i den mening som avses i artikel 9.1 GDPR. Är leverantören med rimlig säkerhet medveten om att användaren är minderårig är riktad annonsering som bygger profilering med användning av personuppgifter dessutom numera förbjuden, se artikel 28.2 DSA. I båda fallen hänvisas till definitionen av ”profilering” i artikel 4.4 GDPR. Till skillnad från dark patterns, där dataskyddsförordningen behöver prövas först, kompletteras dataskyddsförordningen i fråga om profilering för riktad annonsering av DSA på så sätt att ”presentationen” av riktade annonser kan vara förbjuden enligt DSA för leverantörer av onlineplattformar, även om en behandling av personuppgifter i detta sammanhang skulle vara laglig enligt dataskyddsförordningen. Relationen mellan kraven kan jämföras med relationen mellan kravet på samtycke till cookies och bedömningen av lagligheten av en personuppgiftsbehandling som kan ske i samband med cookies. Båda frågorna måste hållas isär. I övrigt påverkar DSA inte tillämpningen av relevanta bestämmelser i dataskyddsförordningen i samband med annonsering, särskilt de som rör rätten att göra invändningar, automatiserat individuellt beslutsfattande, inbegripet profilering, och i förekommande fall behovet av att inhämta den registrerades samtycke innan personuppgifter behandlas för riktad annonsering, se skäl 68, andra stycket i DSA. Det bör observeras att dataskyddsförordningen inte innehåller ett direkt förbud mot behandling av personuppgifter för riktade annonser utan samtycke, till skillnad från vad nämnda skäl i DSA antyder. EU-domstolen har dock bekräftat att intresseavvägningen inte kan utgöra rättslig grund för en synnerligen omfattande behandling av personuppgifter i samband med riktad reklam på sociala medier.[38]

[38] Se EU-domstolen, dom den 2023-07-04 i mål C-252/21 *Meta Platforms*, EU:C:2023:537, punkt 118.

4.4 Dataåtkomst

En ytterligare fråga som regleras i DSA och som skapar en överlappning till dataskyddsförordningen är dataåtkomst hos förmedlingstjänster. DSA kräver numera att leverantörer av mycket stora onlineplattformar och leverantörer av mycket stora onlinesökmotorer ska ge vissa myndigheter åtkomst till data som behövs för att övervaka och bedöma efterlevnaden av förordningen, se artikel 40.1 DSA. Mycket stora onlineplattformar och mycket stora onlinesökmotorer är sådana som i genomsnitt har 45 miljoner aktiva användare per månad eller mer i EU, se artikel 33.1 DSA. De är skyldiga att ge utvalda forskare åtkomst till data i syfte att bedriva forskning som bidrar till upptäckten, identifieringen och förståelsen av systemrisker i unionen enligt artikel 34.1 samt för bedömning av om riskminskningsåtgärder som leverantören vidtar är lämpliga och effektiva och vilka konsekvenser de har, se artikel 40.4 DSA. De behöriga myndigheterna ska använda de data till vilka åtkomst givits endast för att övervaka och bedöma efterlevnaden av denna förordning och ska ta vederbörlig hänsyn till användarnas rätt till skydd av deras personuppgifter, se artikel 40.2 DSA. Enligt artikel 40.8 d ska forskare, för att kunna få tillgång till data, visa att de är kapabla att uppfylla de särskilda datasäkerhetskrav och konfidentialitetskrav som är förbundna med varje begäran och att skydda personuppgifter i enlighet med dataskyddsförordningen. Kommissionen har dessutom mandat att komplettera DSA genom att fastställa de tekniska villkor enligt vilka leverantörerna ska dela data och de ändamål för vilka dessa data får användas, se artikel 40.13 DSA. Dessa ändamål kan återigen bli relevanta vid bedömningen av behandlingen i enlighet med dataskyddsförordningen. Delegerade akter ska enligt samma stycke också fastställa de särskilda villkor enligt vilka sådan delning av data med forskare kan ske i överensstämmelse med dataskyddsförordningen. Leverantörerna bör också anonymisera eller pseudonymisera personuppgifter utom i de fall detta skulle omöjliggöra det forskningssyfte som eftersträvas, se skäl 98 DSA.

5. Sammanfattning och utblick

Dataskyddsförordningen kan vara tillämplig i samband med vidareutnyttjande av data från den offentliga förvaltningen, tillhandahållandet av dataförmedlingstjänster och datadelning för altruistiska ändamål. På samma sätt kan erbjudandet av centrala plattformstjänster och digitala förmedlingstjänster medföra en behandling av personuppgifter som omfattas av dataskyddsförordningens tillämpningsområde. DGA ska främja datadelning, särskilt för vetenskaplig forskning och innovation,

men den ska inte påverka tillgången till allmänna handlingar, inklusive personuppgifter. Överlappningen mellan dataskyddsförordningen och DGA är därför mer marginell och avgränsningen relativt tydlig.[39] DMA och DSA innehåller däremot några specifika regler som rör behandling av personuppgifter, ett förbud mot vissa personuppgiftsbehandlingar, en kompletterande reglering avseende dark patterns, regler gällande visning av personaliserade annonser som bygger på profilering samt regler avseende dataåtkomst. Överlappningen mellan dataskyddsförordningen och DMA samt DSA är därmed något mer tydlig och konkret.[40] Oavsett konkreta överlappningar är ett genomgående tema att de nya rättsakterna inte ska påverka tillämpningen av dataskyddsförordningen.[41] Därmed har EU:s dataskyddsförordning företräde framför såväl DGA, DMA som DSA vid eventuella normkonflikter. Den behandling av personuppgifter som utförs i samband med vidareutnyttjande av data från den offentliga förvaltningen, vid tillhandahållandet av dataförmedlingstjänster (inklusive dataaltruism), centrala plattformstjänster samt digitala förmedlingstjänster ska ske i överensstämmelse med de krav som ställs upp i dataskyddsförordningen. Varken DGA, DMA eller DSA ger personuppgiftsansvariga rätt att behandla personuppgifter, utan personuppgiftsansvariga som omfattas av de nya rättsakterna behöver ha stöd för sin personuppgiftsbehandling i en av de lagliga grunderna i dataskyddsförordningen. Huruvida dataskyddsförordningens principiella företräde är ett resultat av noggranna avvägningar från lagstiftarens sida i samband med implementeringen av EU:s digitala strategi eller mer ett resultat av att man inte har velat rubba ett redan inarbetat regelverk är emellertid inte helt klart.

Dataskyddsförordningen intar således en central ställning inom EU:s rättsordning och utgör utan tvekan en milstolpe i EU-rättens utveckling. Sedan dess ikraftträdande har förordningen bidragit till ett ökat skydd av fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter i den digitala miljön. Dataskyddsförordningen har också inspirerat efterkommande regelverk rent konceptuellt, till exempel avseende utformningen av det territoriella tillämpningsområdet (effektlandsprincipen). Samtidigt medför den tillsammans med andra rättsakter inom ramen för EU:s digitala strategi en kolossal utmaning för företagens regelefterlevnad. En för stor börda kan teoretiskt leda till att investeringar i innovativa tjänster och produkter inom EU uteblir eller att verksamhet flyttas utomlands. Turerna

[39] DGA reglerar främst icke-personuppgifter, se bl.a. kravet på anonymisering av personuppgifter i artikel 5.3 eller artikel 31 om internationell tillgång och överföring av data som explicit enbart omfattar icke-personuppgifter.
[40] Överlappningen är störst mellan dataskyddsförordningen och DSA.
[41] Samma gäller för ePrivacy-direktivet.

kring transatlantiska överföringar av personuppgifter eller den snabba utvecklingen inom området för generativ AI kan vara tecken på att dataskyddsförordningen inte alltid är helt kompatibel med den allra senaste teknik- och samhällsutvecklingen. Förslagen till Data Act och AI Act kan möjligen ses som en omprövning av dataskyddsförordningens principiella företräde. Förslagen kommer – som det ser ut – bland annat innehålla lagliga grunder för behandling av personuppgifter, exempelvis vad gäller datadelning med offentliga myndigheter vid exceptionella behov eller för utveckling av vissa AI-system i allmänhetens intresse i en regulatorisk sandlåda för AI. Det återstår att se om dataskyddsförordningen i längden kommer förbli ”drottningen” av EU:s digitala årtionde eller om regelverket kommer att revideras för att skapa en annorlunda balans mellan dataskydd och andra intressen. Senast år 2024 ska kommissionen överlämna en ny rapport om tillämpningen och översynen av dataskyddsförordningen till Europaparlamentet och rådet, se artikel 97.1. Det blir i vilket fall spännande att följa när EU ska rustas för den digitala tidsåldern.