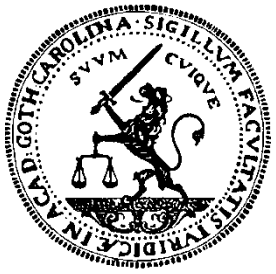

JURIDISKA FAKULTETEN

VID LUNDS UNIVERSITET

Moa Lundgren

Personuppgiftsansvar för offentlig sektor på Facebook

JURM02 Examensarbete

Examensarbete på juristprogrammet

30 högskolepoäng

Handledare: Vilhelm Persson

Termin: VT24

Innehåll

Summary

Facebook can be a tool for Swedish municipalities, regions, and public authorities (*the public sector*) to reach out to citizens. Personal data is processed when one administers a Facebook page and produces content on it, which means that the General Data Protection Regulation becomes applicable.

The aim of this thesis is to examine and analyse the responsibilities of the public sector on Facebook in their role as data controllers. The legal dogmatic research method is used to investigate what the responsibilities of a data controller imply in general and for the public sector on Facebook in particular. The legal dogmatic research method is also used to analyse whether or not the public sector can comply with their responsibilities as data controllers when on Facebook.

The investigation shows that municipalities, regions, and public authorities are data controllers in relation to what they publish on their Facebook pages. They are likely also data controllers in relation to what other users contribute to the pages. It cannot be ruled out that the controllership might be joint together with the users or with Meta, the company behind Facebook. If the tool *Audience Insights* is used to get statistics on the visitors of a Facebook page, the owner of the page becomes a joint controller together with Meta.

The duties of the data controller include ensuring that all processing of personal data follow the basic principles, that there is a lawful ground for the processing, and that the data subjects can exercise their rights. This thesis concludes that municipalities, regions, and public authorities should be able to comply with their responsibilities as data controllers when it comes to their own contributions to their Facebook pages. The actors will however have a more difficult time complying when it comes to other users contributing to the Facebook page. Municipalities, regions, and public authorities are unable to ensure on their own that data subjects can exercise their rights regarding page statistics, however this does not affect the ability to comply with the responsibilities of joint controllership.

It is also the data controller's responsibility to keep a record of their processing activities, to carry out a data protection impact assessment, to handle data breaches and to ensure that any transfers of personal data to third countries can be made in accordance with the regulation. The public sector should be able to fulfil these obligations regarding their processing of personal data on Facebook.

The main conclusion drawn in this thesis is this: The more control a municipality, region, or a public authority has over its processing, the easier it becomes for it to comply with the responsibilities of a data controller.

Sammanfattning

Facebook kan vara ett verktyg för kommuner, regioner och myndigheter (*offentlig sektor*) att nå ut till medborgare med sin verksamhet. Att producera innehåll på Facebook och administrera en Facebooksida innebär att personuppgifter behandlas, vilket i sin tur innebär att EU:s allmänna dataskyddsförordning blir tillämplig.

Syftet med den här uppsatsen är att utreda och analysera den offentliga sektorns personuppgiftsansvar på Facebook. Rättsdogmatisk metod används för att utreda vad personuppgiftsansvaret innebär i allmänhet och vad det innebär på Facebook för offentlig sektor i synnerhet. Metoden används också för att analysera huruvida offentlig sektor kan efterleva de skyldigheter som följer av personuppgiftsansvaret.

Utredningen visar att kommuner, regioner och myndigheter blir personuppgiftsansvariga för det som de själva publicerar och sannolikt också för det som andra tillför Facebooksidan. Det går inte att utesluta att personuppgiftsansvaret eventuellt är gemensamt med användarna eller med Meta – företaget bakom Facebook. Utredningen leder fram till att personuppgiftsansvaret blir gemensamt med Meta när funktionen *Statistik* används för att ta fram data över vilka som besöker Facebooksidan.

I personuppgiftsansvaret ingår att säkerställa att de grundläggande principerna för personuppgiftsbehandling följs, att se till att det finns en laglig grund för personuppgiftsbehandlingen och att säkerställa att de registrerade kan utöva sina rättigheter. Uppsatsens slutsats är att kommuner, regioner och myndigheter har goda förutsättningar att uppfylla sitt ansvar inom ramen för det de själva publicerar, men att de har svårare att uppfylla sitt ansvar inom ramen för det som användare publicerar. Gällande sidstatistiken kan kommuner, regioner och myndigheter inte på egen hand säkerställa att den registrerade kan utöva sina rättigheter, men det gemensamma personuppgiftsansvaret bör trots det kunna uppfyllas.

I personuppgiftsansvaret ingår också att skyldigheter att föra register, göra konsekvensbedömningar, hantera personuppgiftsincidenter och se till att eventuella överföringar av personuppgifter till tredjeland har stöd i dataskyddsförordningen. Här konstateras att den offentliga sektorn kan uppfylla dessa skyldigheter vad gäller personuppgiftsbehandlingen på Facebook.

Den huvudsakliga slutsatsen som kan dras är att ju mer kontroll en kommun, region eller myndighet har över sin personuppgiftsbehandling, desto enklare är det att efterleva skyldigheterna som följer av personuppgiftsansvaret.

Förord

Jag har många att tacka för mycket.

Jag har fyra kvinnor att tacka för att den här uppsatsen kom till. Tack till min svensklärare Camilla, som visade uppskattning för min Powerpoint-presentation om Facebook i femte klass 2010. Tack till mina lärare på språkkonsultprogrammet Anna och Kikki, som fick det juridiska språket att intressera och reta mig så pass mycket att jag kände att jag var tvungen att gå en utbildning till. Och tack till min mentor under min praktik, Mari, för tipset om uppsatsämnet.

Jag har min handledare Vilhelm att tacka för att uppsatsen blev mycket bättre än det utkast jag lämnade in och för att många polletter trillade ner när det kommer till att skriva uppsats i juridik.

Jag har Hanna att tacka för att min tid i Lund blev så rolig, både på korridoren på Helsingkrona nation och på Spolegatan. Man säger ibland att varje brunett behöver en blondin. Det omvända är också sant.

Jag har Josefin att tacka för utbytesterminen i Leiden. Utan hennes nyfikenhet att upptäcka vårt nya gemensamma hemland, hennes självständeaktiga studieteknik och hennes vilja att lära känna mig hade jag inte haft hälften så kul som jag hade.

Jag har juristprogrammets två skarpaste men kanske också mest snedvridna hjärnor att tacka för hela studietiden på juristprogrammet. Tack Pontus, för alla diskussioner om dispaschören, för deltagandet i mina quiz under de ölkvällar vi kallat möten och för allt struntprat i Sveriges roligaste gruppchatt. Och tack Martin, för exakt samma saker och för alla koppar kaffe jag blivit bjuden på (som jag förhoppningsvis har tackat för vid varje tillfälle).

Jag har Salomon att tacka för det osvikliga, eviga stödet, för påminnelserna om vad som är viktigt och för allt, egentligen. Och för korrekturläsningen av uppsatsen såklart, fastän mitt samvete knappt orkade med det.

Och så har jag Mamma och Pappa (med stora begynnelsebokstäver) att tacka. De vet för vad.

Malmö i maj 2024

Moa Lundgren

Förkortningar

Artikel 29-gruppen	Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter och om upphävandet av direktiv 96/56/EG (allmän dataskyddsförordning)
Dataskyddslagen	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
HFD	Högsta förvaltningsdomstolen
Meta	Meta Platforms Ireland Limited
Prop.	Proposition
SOU	Statens offentliga utredningar

1 Inledning

1.1 Bakgrund

Den offentliga förvaltningen ska vara tillgänglig. Kanske är det därför kommuner, regioner och myndigheter har Facebooksidor. Genom att publicera inlägg kan en kommun, region eller myndighet informera om och nå ut med sin verksamhet. En Facebooksida kan också utgöra en kontaktpunkt där allmänheten, eller åtminstone de som har ett Facebookkonto, kan ställa frågor och få svar. Att ha en Facebooksida kan därför vara fördelaktigt, inte minst med tanke på att Internetstiftelsen rapporterar att Facebook är den sociala medieplattform som används mest på en daglig basis i Sverige.[1]

Däremot är det inte helt oproblematiskt att driva en Facebooksida. Att producera innehåll på Facebook och administrera en Facebooksida innebär att personuppgifter behandlas – inlägg och kommentarer kan till exempel innehålla namn eller bilder på individer, och besökarnas personuppgifter kan användas för att upprätta statistik över vilka som besöker Facebooksidan. I takt med digitaliseringen har EU-rätten identifierat skyddet för personuppgifter som allt viktigare. Särskilt central för EU:s (och Sveriges) dataskyddsregelverk är EU:s allmänna dataskyddsförordning[2], som reglerar under vilka förutsättningar personuppgifter får behandlas. En av de centrala mekanismerna i förordningen är *personuppgiftsansvaret*, som i korthet innebär att den som bestämmer varför och hur personuppgifter behandlas ansvarar för att dataskyddsförordningen följs.

Ur ett dataskyddsperspektiv är Facebook ett komplext verktyg. Flera aktörer kan behandla samma personuppgift, vilket kan göra det svårt att avgöra vem som blir personuppgiftsansvarig. Ytterligare en aspekt att ta hänsyn till är att aktörer inom den offentliga sektorn är mer begränsade i sin personuppgiftsbehandling än aktörer inom den privata sektorn. Den norska tillsynsmyndigheten för dataskyddsrättsliga frågor, Datatilsynet, publicerade 2021 en rapport där myndigheten kom fram till att den inte kunde ha en sida på Facebook.[3] Vår svenska motsvarighet har talande nog inte heller någon Facebooksida men inte heller någon rapport om varför. Samtidigt är det få aktörer inom den offentliga sektorn som har följt tillsynsmyndigheternas exempel; Facebooksidorna som tillhör den offentliga sektorn är många. Kan aktörer inom den offentliga sektorn säkerställa att de lever upp till sitt ansvar enligt dataskyddsförordningen om de driver en Facebooksida?

[1] Internetstiftelsen s. 240.

[2] Förordning 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).

[3] Datatilsynet, Risk assessment: should the Norwegian Data Protection Authority create a Page on Facebook? Final report 2021.

1.2 Syfte och frågeställningar

Syftet med den här uppsatsen är att utreda och analysera den offentliga sektorns personuppgiftsansvar på Facebook. Med *den offentliga sektorn* avser jag kommuner och regioner samt kommunala, regionala och statliga myndigheter.

De frågor som styr arbetet är följande:

1. Vad innebär personuppgiftsansvaret för den offentliga sektorn i allmänhet?

2. Vad innebär personuppgiftsansvaret för den offentliga sektorn på Facebook i synnerhet?

3. Kan den offentliga sektorn efterleva de skyldigheter som följer av personuppgiftsansvaret?

1.3 Avgränsningar

Personuppgiftsansvaret är en omfattande reglering. Inom ramen för den här uppsatsen är det inte möjligt att utreda och analysera samtliga skyldigheter som träffar den offentliga sektorns användning av Facebook. Jag har därför valt att fokusera på personuppgiftsansvarets mest centrala skyldigheter för kommuners, regioners och myndigheters användning av Facebook.

Det innebär inledningsvis att jag har valt att utesluta frågor om känsliga personuppgifter (särskilda kategorier av personuppgifter). I artikel 9 dataskyddsförordningen listas åtta kategorier av personuppgifter som omfattas av en starkare reglering. Jag förutsätter genomgående i uppsatsen att de personuppgifter som kommuner, regioner och myndigheter behandlar på Facebook inte faller under artikel 9.

Jag har också valt att utesluta frågor om annonsering och profilering. Om kommuner, regioner eller myndigheter köper annonser på Facebook kan frågor om profilering aktualiseras, eftersom Facebook tillämpar anpassad annonsering.[4] Profilering innebär enligt definitionen i artikel 4.4 dataskyddsförordningen att behandla personuppgifter på automatiserad väg för att bedöma individers personliga egenskaper. Profilering bygger på omfattande personuppgiftsbehandling och aktualiserar flera särskilda bestämmelser i dataskyddsförordningen. Det hade varit utanför uppsatsens omfång att också utreda och analysera frågor som rör annonsering på Facebook och den profilering som det innebär.

[4] Se Meta, ’Information som används för att visa dig annonser’ <https://accountscenter.facebook.com/ad_preferences/faq/?faqID=ad_pref_faq_information_used_to_show_you_ads>.

Slutligen har jag valt att inte i detalj utreda kraven på lämplig säkerhetsnivå (artikel 5.1 f och artikel 32 dataskyddsförordningen). Frågor om lämplig säkerhetsnivå är till stora delar tekniska till sin natur snarare än juridiska. Jag har valt att fokusera på de juridiska frågorna, utan att gå in på några tekniska specifikationer.

1.4 Metod och material

1.4.1 Rättsdogmatik och rättskällor

För att utreda och analysera personuppgiftsansvaret tillämpar jag den rättsdogmatiska metoden. Exakt vad den rättsdogmatiska metoden innebär och omfattar är något omdiskuterat. En beskrivning är att rättsdogmatiken syftar till att beskriva, systematisera och tolka rättande rätt.[5] En annan är att rättsdogmatiken syftar till att rekonstruera gällande rätt – ett uttryck som ska markera att rätten är dynamisk och därför behöver fastställas vid olika tidpunkter.[6] Ytterligare en beskrivning är att metoden syftar till att konstruera en lösning på ett rättsligt problem genom att applicera en rättsregel på problemet i fråga.[7] Enligt vissa tolkningar är rättsdogmatiken strikt begränsad till att utreda och fastställa gällande rätt[8], medan den enligt andra tolkningar också kan omfatta att utvärdera och kritisera rätten och hitta lösningar på problem.[9] Sandgren anser dock att det råder konsensus om grunderna i metoden: den syftar till att fastställa gällande rätt, arbetar inom den gällande rättens ram och använder rättskälleläran för att tolka och systematisera rätten.[10]

I den här uppsatsen ansluter jag mig till Sandgrens tolkning av grunderna för metoden och till tolkningen att rättsdogmatiken också kan utvärdera och kritisera rätten och föreslå lösningar på rättsliga problem. Med andra ord tillämpar jag den rättsdogmatiska metoden för att besvara samtliga tre frågeställningar. Delfråga ett och två är kräver att utreda och fastställa gällande rätt, medan delfråga tre snarare kräver att applicera utredningen i delfråga ett och två på ett rättsligt problem, det vill säga huruvida den offentliga sektorn kan efterleva de skyldigheter som personuppgiftsansvaret innebär på Facebook.

Rent konkret innebär den rättsdogmatiska metoden att söka svar i de rättsliga normerna. För svensk rätts del innebär det att leta svar i lagtext, prejudikat, förarbeten och doktrin.[11] Jag viktar de olika rättskällorna i enlighet med rättskälleläranas hierarki – i första hand konsulterar jag lagtext, i andra hand prejudikat, i tredje hand förarbeten och i fjärde hand doktrin. Eftersom Sveriges dataskyddsregelverk till stora delar regleras på EU-nivå, behöver jag också

[5] Olsen s. 111; Sandgren, Rättsvetenskap för uppsatsförfattare s. 49.
[6] Jareborg s. 4; Sandgren, Rättsvetenskap för uppsatsförfattare s. 49.
[7] Kleineman s. 21.
[8] Se Hellner s. 27; Kleineman s. 24; Sandgren, Rättsvetenskap för uppsatsförfattare s. 49–50.
[9] Jareborg s. 4; Sandgren, Rättsvetenskap för uppsatsförfattare s. 51.
[10] Sandgren, Är rättsdogmatiken dogmatisk? s. 649–650.
[11] Kleineman s. 21, 24.

förhålla mig till EU-rättens rättskällelära. EU-rätten består av primärrätten och sekundärrätten.[12] Primärrätten är den främsta rättskällan inom EU. Till primärrätten räknas EU:s grundfördrag, ändringsfördrag och anslutningsfördrag, protokoll och tilläggsavtal till fördragen samt Europeiska unionens stadga om de grundläggande rättigheterna.[13] Sekundärrätten är den lagstiftning som bygger på EU-fördragen. Sekundärrätten utgörs dels av bindande rättsakter som förordningar, direktiv och beslut, dels av icke-bindande rättsakter (soft law) som rekommendationer, yttranden, resolutioner och meddelanden.[14] Den juridiska doktrinen har också betydelse inom EU-rätten.[15]

Tolkning av EU-rätt ska ske utifrån de tolkningsunderlag som har auktoritativ ställning inom EU-rätten, det vill säga EU-domstolens praxis, EU:s allmänna rättsprinciper, EU-rättsliga förarbeten och relevant soft law.[16] Traditionellt sett har soft law inte haft särskilt stark tolkningsställning inom EU-rätten men på senare tid har ställningen ändrats.[17] Inom dataskyddsrätten har det förekommit att EU-domstolen refererar till rekommendationer i domskälen.[18] Kotsios menar att soft law är en essentiell del av dataskyddsramverket och att rekommendationer och yttranden därför inte kan bortses från.[19]

I den här uppsatsen tolkas främst sekundärrätten – det är dit dataskyddsförordningen hör. I enlighet med EU-rättens tolkningslära stödjer jag min utredning och analys på rättsfall från EU-domstolen och relevanta yttranden och rekommendationer som har utfärdats av organ inom EU. Jag hänvisar också till de beaktandeskäl som anges i ingressen till dataskyddsförordningen, som närmare förklarar innebörden och avsikten med dataskyddsförordningens bestämmelser. Jag använder mig också av doktrin, främst när rättsläget inte går att utredas tillfredsställande med hjälp av de andra källorna.

Nationella tolkningskällor, som svenska förarbeten och rättsfall från svenska domstolar, kan användas när EU-rätten tolkas men bör ge vika för EU-rättsliga tolkningskällor med annat innehåll.[20] Jag hänvisar därför till svenska tolkningskällor när de EU-rättsliga tolkningskällorna inte ger något tillfredsställande svar. Jag använder också svenska tolkningskällor vid de tillfällen där EU-rätten har lämnat åt varje medlemsstat att reglera på nationell nivå.

Slutligen hänvisar jag till källor som inte har ställning som rättskälla varken inom EU-rätten eller svensk rätt. Det rör sig om beslut och uttalanden från

[12] Hettne och Otken Eriksson s. 41–42.
[13] Europeiska unionens publikationsbyrå, ’Europeiska unionens primärrätt’< https://eur-lex.europa.eu/SV/legal-content/summary/the-european-union-s-primary-law.html>.
[14] Hettne och Otken Eriksson s. 41–42.
[15] Hettne och Otken Eriksson s. 121; Rosén s. 252.
[16] Reichel s. 125.
[17] Hettne och Otken Eriksson s. 47; Reichel s. 128.
[18] C-25/17 *Jehovas vittnen* p. 21.
[19] Kotsios s. 50.
[20] Reichel s. 125–126.

Integritetsskyddsmyndigheten[21] och om uttalanden från Meta och från olika kommuner, regioner och myndigheter. Min avsikt med det är inte att fastställa vad som är innehållet i gällande rätt, utan att redogöra för hur rätten har uppfattats av relevanta aktörer.

1.4.2 Närmare om materialet

Uppsatsens mest centrala material utgörs av EU:s allmänna dataskyddsförordning. På nationell nivå har Sverige utfärdat en kompletterande lag till dataskyddsförordningen: dataskyddslagen[22]. Den här kompletterande lagen och dess förarbeten[23] beaktar jag också. Angående den juridiska litteraturen har Ömans kommentar till dataskyddsförordningen[24] en inflytelserik ställning inom den svenska dataskyddsrätten. Därför hänvisar jag återkommande till hans tolkningar.

EU-domstolen har vid flera tillfällen tolkat innebörden av dataskyddsförordningens personuppgiftsansvar. På liknande vis har EU-organen Artikel 29-gruppen[25] och Europeiska dataskyddsstyrelsen[26] utfärdat riktlinjer och rekommendationer om bestämmelsernas innehåll. Flera av avgörandena och riktlinjerna från Artikel 29-gruppen är dock tillkomna före dataskyddsförordningens ikraftträdande och avser dataskyddsförordningens föregångare: dataskyddsdirektivet[27]. Trots att avgörandena och rekommendationerna avser ett annat regelverk bedömer jag att de fortfarande är relevanta. Dataskyddsdirektivet definition av personuppgiftsansvarig är nämligen nästan identisk med dataskyddsförordningens definition.[28] Dessutom har generaladvokat Bobek i ett förslag till avgörande yttrat att tolkningen av dataskyddsförordningens personuppgiftsansvar inte utan mycket goda skäl bör avvika från EU:s redan

[21] Integritetsskyddsmyndigheten hette mellan åren 1973–2020 *Datainspektionen*. I den här uppsatsen hänvisar jag genomgående till myndigheten som *Integritetsskyddsmyndigheten*, även när myndigheten agerade under sitt tidigare namn.

[22] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[23] SOU 2017:39; Prop. 2017/18:105.

[24] Öman, Sören, *Dataskyddsförordningen (GDPR) m.m. – En kommentar*, (27 september 2023, version 2B, Juno).

[25] Artikel 29-gruppen är föregångaren till Europeiska dataskyddsstyrelsen. Artikel 29-gruppen bestod, liksom Europeiska dataskyddsstyrelsen, av företrädare för de nationella tillsynsmyndigheterna.

[26] Europeiska dataskyddstyrelsen är ett oberoende EU-organ som har till uppgift att säkerställa att dataskyddsförordningen tillämpas enhetligt, bland annat genom att utfärda riktlinjer och rekommendationer, se artikel 69 och artikel 70 dataskyddsförordningen.

[27] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

[28] Dataskyddsdirektivet använder termen registeransvarig och följande definition: ”den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter” (artikel 2 d i dataskyddsdirektivet). Jämför dataskyddsförordningens definition av personuppgiftsansvarig: ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter” (artikel 4.7 dataskyddsförordningen).

etablerade rättspraxis.[29] Europeiska dataskyddstyrelsen, som är det organ som utfärdar riktlinjer och rekommendationer för dataskyddsförordningen, har ställt sig bakom flera av Artikel 29-gruppens riktlinjer.[30]

Dataskyddsdirektivet genomfördes i Sverige genom personuppgiftslagen (1998:204).[31] Liksom dataskyddsdirektivet är personuppgiftslagens definition av personuppgiftsansvarig[32] nästan identisk med definitionen i dagens dataskyddsförordning. Därför har jag bedömt att även material som avser personuppgiftslagen kan användas.

För att kunna analysera personuppgiftsansvaret på Facebook använder jag också dokument från den europeiska delen av företaget bakom Facebook: Meta[33]. Eftersom dokumenten har utarbetats av Meta finns det en risk att de kan vara vinklade och inte ger hela bilden, trots att dataskyddsförordningen ställer krav på transparens. Jag har därför behandlat materialet med försiktighet.

Slutligen vill jag kommentera det faktum att stora delar av uppsatsens material existerar i flera språkversioner. Så är det med författningstext, rättsfall och rekommendationer samt dokument från Meta. Jag använder mig av de svenska språkversionerna, när sådana finns.

1.5 Disposition

I delfrågorna ett och två ingår dels att utreda i vilka situationer personuppgiftsansvaret föreligger, dels att utreda vilka skyldigheter som personuppgiftsansvaret för med sig. Därför följer först en kartläggning av vad som utlöser personuppgiftsansvar och hur personuppgiftsansvaret fördelas på Facebook. Därefter utreder och analyserar jag löpande vad personuppgiftsansvaret innebär för den offentliga sektorn på Facebook. Utredningen följer dataskyddsförordningens disposition. Uppsatsen avslutas med en sammanställning av mina slutsatser.

[29] Förslag till avgörande av generaladvokat Bobek i mål C-40/17 *Fashion ID* p. 87.

[30] Europeiska dataskyddsstyrelsen, Endorsement 1/2018.

[31] Se Prop. 1997/98:44.

[32] Personuppgiftsansvarig definieras i 3 § personuppgiftslagen på följande sätt: ”[d]en som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter”. Jämför fotnot 28.

[33] Den europeiska delens fulla namn är Meta Platforms Ireland Limited. Den europeiska delen ägs i sin tur av det amerikanska företaget Meta Platforms Incorporated.

2 Personuppgiftsansvar – en översikt

I det här avsnittet introduceras personuppgiftsansvaret. Jag förklarar först kortfattat vad personuppgiftsansvaret innebär och sedan utreder jag vad som avgör när någon blir personuppgiftsansvarig. Eftersom den här uppsatsen handlar om den offentliga sektorns personuppgiftsansvar finns det också anledning att särskilt utreda vem som blir personuppgiftsansvarig inom en kommun, en region och en myndighet. Därför avslutas det här avsnittet med en sådan utredning.

2.1 Dataskyddsförordningen och ansvar

Ett av dataskyddsförordningens syften är att stärka den enskildes rätt till skydd av personuppgifter.[34] Det gör dataskyddsförordningen bland annat genom att ställa krav på hur personuppgifter får behandlas och genom att förse de som får sina personuppgifter behandlade – de *registrerade*[35] – med ett rättighetspaket som ger dem kontroll över sina personuppgifter. För att säkerställa att syftet realiseras vilar dataskyddsförordningen på en ansvarsprincip.[36] Den som identifieras som personuppgiftsansvarig ska enligt artikel 24.1 dataskyddsförordningen genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att personuppgiftsbehandlingen sker i enlighet med dataskyddsförordningen.

Ansvaret är skadeståndssanktionerat. Om en person lider materiell eller immateriell skada till följd av en överträdelse av dataskyddsförordningen har den personen enligt artiklarna 82.1 och 82.2 rätt till ersättning från den personuppgiftsansvarige. Tillsynsmyndigheten kan också påföra den personuppgiftsansvarige administrativa sanktionsavgifter om dataskyddsförordningen överträds. Sanktionsavgifter varierar beroende på vilken bestämmelser om har överträtts. Om överträdelsen avser de mer administrativa skyldigheterna som föreskrivs i artiklarna 8, 11, 25–39, 42 och 43, kan sanktionsavgiften enligt artikel 83.4 uppgå till 10 000 000 euro eller två procent av den totala globala årsomsättningen. Om överträdelsen istället avser de grundläggande principerna för personuppgiftsbehandling (artikel 5) eller de registrerades rättigheter (artiklarna 12–22) kan de administrativa sanktionsavgifterna enligt artikel 83.5 uppgå till 20 000 000 euro eller fyra procent av den totala globala årsomsättningen.

[34] Skäl 1–2 dataskyddsförordningen. Jämför skäl 9–10, av vilka det framgår att ett annat syfte är att säkerställa en god konkurrens genom en enhetlig dataskyddsreglering.

[35] Se artikel 4.1 dataskyddsförordningen.

[36] Skäl 11 dataskyddsförordningen.

2.2 Ensamt eller gemensamt personuppgiftsansvar?

I artikel 4.7 dataskyddsförordningen definieras personuppgiftsansvar på följande vis:

> *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra fastställer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt

Personuppgiftsansvarig är den som antingen ensamt eller tillsammans med andra bestämmer ändamålen med och medlen för en personuppgiftsbehandling (artikel 4.7 dataskyddsförordningen). Med andra ord går det att identifiera två typer av personuppgiftsansvar: ett ”ensamt” och ett gemensamt.

2.2.1 Ensamt personuppgiftsansvar

Personuppgiftsansvarig är alltså den som bestämmer ändamålen med och medlen för en personuppgiftsbehandling. Att bestämma över ändamålen med personuppgiftsbehandlingen innebär att bestämma *varför* en personuppgiftsbehandling sker, det vill säga i vilket syfte. Att besluta över medlen för personuppgiftsbehandlingen innebär att bestämma *hur* en personuppgiftsbehandling går till, det vill säga vilka tekniska och organisatoriska åtgärder som ska vidtas vid en behandling.[37]

Att den personuppgiftsansvarige är den som fastställer ändamålen och medlen innebär att den personuppgiftsansvarige har en beslutanderätt.[38] Europeiska dataskyddsstyrelsen talar om att enheten ska utöva ett avgörande inflytande på behandlingsändamålet och behandlingssättet.[39] Av förordningstexten går det att utläsa att beslutanderätten kan härröra från faktiskt inflytande eller från uttrycklig juridisk kompetens. Europeiska dataskyddsstyrelsen framhäver dock att begreppet personuppgiftsansvarig är funktionellt, vilket innebär att det är faktiska förhållanden som ska ligga till grund vid en bedömning av vem som är personuppgiftsansvarig. Den som *de facto* bestämmer ändamålen och medlen för personuppgiftsbehandlingen är den som är personuppgiftsansvarig, oavsett om aktören har någon egentlig rätt att göra det.[40] EU-domstolen

[37] Artikel 29-gruppen, WP 169 s. 13; Cimina s. 641; Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 15.

[38] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 12.

[39] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 14.

[40] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 12.

uttalar i flera rättsfall att personuppgiftsansvaret måste tolkas brett för att säkerställa ett komplett skydd för de registrerades personuppgifter.[41]

Personuppgiftsansvaret kan aldrig skrivas över på någon annan eller på något annat sätt avtalas bort – den som har beslutat över ändamålen och medlen är personuppgiftsansvarig.[42] Personuppgiftsbehandling kan dock ibland utföras av ett *personuppgiftsbiträde*, som enligt definitionen i artikel 4.8 dataskyddsförordningen är någon som behandlar personuppgifter för den personuppgiftsansvariges räkning. Europeiska dataskyddsstyrelsen anser att det finns ett visst utrymme för personuppgiftsbiträden att besluta om medlen för personuppgiftsbehandlingen, men bara de medel som är ”icke-väsentliga”.[43] Icke-väsentliga medel gäller mer praktiska aspekter av implementeringen, till exempel valet av en viss typ av programvara eller detaljerade säkerhetsåtgärder.[44] De ska ses i kontrast mot väsentliga medel, som är nära kopplade till behandlingens ändamål och omfattning, till exempel vilken typ av personuppgifter som behandlas, hur länge behandlingen sker, vilka som ska ha åtkomst till personuppgifterna och vilka kategorier av registrerade som behandlingen rör.[45]

2.2.2 Gemensamt personuppgiftsansvar

2.2.2.1 Att gemensamt bestämma ändamålen och medlen

Om flera aktörer gemensamt fastställer ändamålen och medlen för personuppgiftsbehandlingen är de *gemensamt personuppgiftsansvariga* enligt artikel 4.7 och artikel 26 dataskyddsförordningen. Liksom vid bedömningen av (ensamt) personuppgiftsansvar bedöms gemensamt personuppgiftsansvar utifrån faktiska omständigheter snarare än formella.[46]

För att ett gemensamt personuppgiftsansvar ska kunna föreligga ska flera personuppgiftsansvariga *tillsammans*[47] bestämma ändamålen med och medlen för personuppgiftsbehandlingen. Europeiska dataskyddsstyrelsen anser att det kan ske på två sätt. Antingen kan parterna ha en gemensam avsikt ”i enlighet med den vanligaste förståelsen av termen ’gemensamt’” [48] eller genom *konvergerande beslut*.[49] Konvergerade beslut baserar sig på EU-domstolens praxis och är enligt dataskyddsstyrelsen beslut som kompletterar varandra

[41] C-131/12 *Google Spain* p. 32–34; C-210/16 *Wirtschaftsakademie* p. 28; C-25/17 *Jehovas vittnen* p. 66; C-40/17 *Fashion ID* p. 66.

[42] C-210/16 *Wirftschaftsakademie* p. 40; C-40/17 *Fashion ID* p. 78–81; Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 12, 14; Cimina s. 641; Öman, kommentaren till artikel 4 under rubriken ”Sjunde punkten – Personuppgiftsansvarig”.

[43] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 16.

[44] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 16.

[45] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 16.

[46] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 20–21 p. 52.

[47] I artikel 4.7 används ordet *tillsammans*, medan ordet *gemensamt* används i artikel 26. Jag förstår orden som synonyma.

[48] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 21.

[49] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 21.

och är nödvändiga för att behandlingen ska ske; besluten har en påtaglig inverkan på fastställandet av ändamålen och medlen för behandlingen. Behandlingen är möjlig bara tack vare varje parts deltagande i ändamålen och medlen – varje parts behandling är oskiljbar.[50]

Exempel på ett konvergerat beslut finns i rättsfallet *Fashion ID*.[51] I rättsfallet ansåg EU-domstolen att företaget Fashion ID blev gemensamt personuppgiftsansvarigt med Meta. Fashion ID hade integrerat Facebooks gilla-knapp på sin egen webbsida. När webbsidans besökare använde gilla-knappen fick Facebook tillgång till besökarnas personuppgifter. EU-domstolen uttalar att integreringen av gilla-knappen utgjorde ett väsentligt inflytande på den personuppgiftsbehandling som Meta kunde utföra och att Metas personuppgiftsbehandling bara var möjlig tack vare att Fashion ID hade integrerat gilla-knappen. Fashion ID ansågs därmed ha bestämt medlen för personuppgiftsbehandlingen tillsammans med Meta.[52] Angående att gemensamt bestämma syftet med personuppgiftsbehandlingen betonar EU-domstolen att både Fashion ID och Meta behandlade personuppgifterna i ekonomiskt syfte.[53] Europeiska dataskyddsstyrelsens tolkning av EU-domstolens uttalande är att gemensamt personuppgiftsansvar kan uppkomma när aktörerna eftersträvar ändamål som är nära sammankopplade eller kompletterade.[54] I doktrinen hävdas dock att EU-domstolen och Europeiska dataskyddstyrelsens uttalanden lätt missförstås. Varje aktör kan ha helt olika ändamål med behandlingen och fortfarande omfattas av ett gemensamt personuppgiftsansvar. Ändamålet behöver inte vara gemensamt, men beslutet måste vara det.[55]

I doktrinen argumenteras att det i realiteten bara krävs ett gemensamt beslut om ändamålen för att ett gemensamt personuppgiftsansvar ska föreligga – inte också om medlen. Finck anser att EU-domstolens praxis har banat väg för att en aktör bara behöver ha marginellt inflytande över medlen för personuppgiftsbehandlingen för att det ska aktualisera ett gemensamt personuppgiftsansvar – det räcker till exempel med att välja en viss plattform där personuppgifterna behandlas. Det reella kriteriet för gemensamt personuppgiftsansvar är enligt henne att göra personuppgiftsbehandling möjlig.[56] Även Cimina ansluter sig till uppfattningen och anser att det kan vara tillräckligt för gemensamt personuppgiftsansvar att flera aktörer gemensamt fastställer syftet med personuppgiftsbehandlingen.[57]

[50] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 21.
[51] Se C-40/17 *Fashion ID*.
[52] C-40/17 *Fashion ID* p. 78–79.
[53] C-40/17 *Fashion ID* p. 80–81.
[54] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 22.
[55] Sprecht-Riemenschneider och Schneider s. 160.
[56] Finck s. 335.
[57] Cimina s. 646.

2.2.2.2 Inget krav på tillgång till personuppgifterna

Gemensamt personuppgiftsansvar kan föreligga även i situationer där en av aktörerna inte har tillgång till personuppgifterna. I rättsfallet *Jehovas vittnen* konstaterar EU-domstolen att samfundet Jehovas vittnen blev gemensamt personuppgiftsansvarigt tillsammans med samfundets medlemmar för den personuppgiftsbehandling som medlemmarna utförde under sitt predikoarbete. När medlemmarna predikade före de anteckningar som innehöll personuppgifter. Samfundet kände inte till innehållet i antecknarna och hade därmed inte tillgång till några personuppgifter. Däremot organiserade, samordnade och uppmuntrade samfundet predikoarbetet. Enligt EU-domstolen räckte det för att utgöra gemensamt personuppgiftsansvar, eftersom samfundet tillsammans med sina medlemmar deltog i att bestämma ändamålet med och medlen för personuppgiftsbehandlingen.[58] På liknande vis bedömer EU-domstolen i rättsfallet *Wirtschaftsakademie* att gemensamt personuppgiftsansvar kan föreligga även när en av parterna har tillgång till personuppgifter endast i anonymiserad form.[59]

2.2.2.3 Ansvarets omfattning

Enligt EU-domstolens praxis är personuppgiftsansvaret avgränsat till den behandling som den personuppgiftsansvarige faktiskt bestämmer ändamålen och medlen för. I rättsfallet *Fashion ID* aktualiseras frågan om Fashion ID var personuppgiftsansvarig också för den behandling som Meta utförde i ett senare steg. Här konstaterar EU-domstolen att Fashion ID inte var personuppgiftsansvarigt för Metas vidarebehandling, trots att Fashion ID:s personuppgiftsbehandling inom det gemensamma personuppgiftsansvaret var det som möjliggjorde Metas vidarebehandling.[60] Det gemensamma personuppgiftsansvaret innebär alltså inte att en aktör blir personuppgiftsansvarig för delar i en behandlingskedja som aktören inte har något inflytande över.

Det gemensamma personuppgiftsansvaret omfattas av särskilda skyldigheter enligt artikel 26 dataskyddsförordningen. De gemensamt personuppgiftsansvariga under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt dataskyddsförordningen (artikel 26.1). Arrangemanget ska enligt artikel 26.2 på ett lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot den registrerade. Den registrerade har enligt artikel 26.3 rätt att utöva sina rättigheter mot vem den vill av de gemensamt personuppgiftsansvariga.

[58] C-25/17 *Jehovas vittnen* p. 69, 73.

[59] C-210/16 *Wirtschaftsakademie* p. 38.

[60] C-40/17 *Fashion ID* p. 74, 85. Se också Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 22.

2.3 Ansvarig aktör inom offentlig sektor

Trots att det i praktiken är enskilda individer som fattar beslut om varför och hur personuppgiftbehandling sker inträffar det sällan att en fysisk person blir personuppgiftsansvarig i dataskyddsförordningens mening. När personuppgifter behandlas inom en organisation faller nämligen personuppgiftsansvaret typiskt på organisationen som sådan och inte företrädare för den.[61] Enligt Integritetsskyddsmyndigheten är myndigheter personuppgiftsansvariga för personuppgiftsbehandling som sker i myndighetens verksamhet.[62]

I en kommun är de kommunala nämnderna personuppgiftsansvariga för den verksamhet som sker under varje nämnd. Det gäller trots att nämnden bara är begränsat inblandad i personuppgiftsbehandlingen inom verksamheten. Personuppgiftsansvaret faller alltså inte på den juridiska personen kommunen, utan på den ansvariga nämnden.[63]

Min bedömning är att detsamma bör gälla för regioner, eftersom regioner enligt 1 kap. 7 § regeringsformen är en kommun på regional nivå. Flera regioner uppger att varje nämnd är personuppgiftsansvarig för de verksamheter som faller under nämnden.[64] Det finns dock exempel på regioner som uppger att det snarare är regionstyrelsen som är personuppgiftsansvarig.[65] Det förekommer också uppfattningar om att regionen i form av juridisk person är personuppgiftsansvarig.[66]

---

[61] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 11.

[62] Integritetsskyddsmyndigheten, ’Behandling av personuppgifter hos myndigheter’ <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/myndighet/>.

[63] Frydlinger med flera s. 54; Öman, kommentaren till artikel 4, under rubriken ”Sjunde punkten – Personuppgiftsansvarig”.

[64] Se till exempel Region Kronoberg, ’Dataskyddsförordningen (GDPR)’ <https://www.regionkronoberg.se/om-region-kronoberg/dataskyddsforordning-gdpr/>; Region Stockholm, ’Så behandlar vi dina personuppgifter’ <https://www.regionstockholm.se/om-region-stockholm/sa-behandlar-vi-dina-personuppgifter/>; Region Uppsala, ’Behandling av personuppgifter’ <https://regionuppsala.se/politik-och-paverkan/handlingar/diarium/behandling-av-personuppgifter/>.

[65] Se till exempel Region Dalarna, ’Begära dina personuppgifter’ <https://www.regiondalarna.se/om-oss/sakerhet/personuppgifter/begara-dina-personuppgifter/>; Region Kalmar, ’Så hanterar vi dina personuppgifter’ <https://regionkalmar.se/personuppgifter>; Region Östergötland, ’Så behandlar vi dina personuppgifter’ <https://www.regionostergotland.se/ro/om-region-ostergotland/sakerhet-och-krisberedskap/informationssakerhet/sa-behandlar-vi-dina-personuppgifter>.

[66] Se till exempel Region Skåne, ’Så behandlar vi dina personuppgifter’ <https://www.skane.se/supportsidor/sa-behandlar-vi-dina-personuppgifter/>; Region Västerbotten, ’GDPR’ <https://www.regionvasterbotten.se/default.aspx?id=110673>.

3 Vilket ansvar för vad på Facebook?

Det går att urskilja tre typsituationer där personuppgifter behandlas på en kommun, en region eller en myndighets Facebooksida: inlägg som publiceras av kommunen, regionen eller myndigheten i fråga, inlägg och kommentarer från användare och slutligen sidstatistik. I det här avsnittet utreder jag hur personuppgiftsansvaret fördelas i de olika situationerna.

3.1 Ansvar för egen publicering

När kommuner, regioner och myndigheter själva publicerar inlägg på sina Facebooksidor kan det innebära att personuppgifter behandlas. Inläggen kan i text, bild eller video innehålla personuppgifter, och personuppgifterna behandlas när de förekommer i inlägg.[67] Det tycks vara klarlagt att den som driver en Facebooksida bestämmer över ändamålen med den personuppgiftsbehandling som sker i inläggen som administratören själv publicerar.[68] Däremot går det att ifrågasätta om sidans ägare har det inflytande över medlen för personuppgiftsbehandlingen som krävs för att bli personuppgiftsansvarig.

Den som driver en Facebooksida kan inte, till skillnad från Meta, bestämma hur Facebook tekniskt fungerar. Det skulle kunna innebära att sidans ägare inte blir personuppgiftsansvarig. Det finns dock mycket som talar för att sidadministratören ändå anses bestämma över medlen för personuppgiftsbehandlingen i inläggen. Integritetsskyddsmyndigheten anger i beslut baserade på personuppgiftslagen att den som driver en Facebooksida bestämmer över medlen för personuppgiftsbehandlingen när den bestämmer vad de egna inläggen ska innehålla.[69] I doktrinen görs det gällande att varje användare (inklusive sidadministratörer) på sociala nätverk väljer huruvida viss information ska tillhandahållas, på vilken plattform och i vilket format (till exempel text eller bild), och att det innebär att bestämma över medlen för personuppgiftsbehandlingen.[70] Integritetsskyddsmyndighetens uppfattning idag är att den som publicerar något i sociala medier som utgångspunkt är att betrakta som personuppgiftsansvarig för den personuppgiftsbehandling som publiceringen innebär.[71]

---

[67] Jämför artikel 4.1 och 4.3 dataskyddsförordningen.

[68] Edmar s. 205; Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 686-2010 s. 4. Vanliga syften inom den offentliga sektorn med att publicera egna inlägg är att visa upp sin verksamhet och sprida nyheter och information, se till exempel Region Dalarna, ’Region Dalarna’ <https://www.facebook.com/regiondalarna> och Gagnefs kommun, ’Gagnefs kommun’ <https://www.facebook.com/gagnef.se>.

[69] Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 685-2010 s. 5; Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 686-2010 s. 4; Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 687-2010 s. 4.

[70] van Alsenoy m. fl. s. 70; Garrie m. fl s. 131.

[71] Integritetsskyddsmyndigheten, ’Är jag ansvarig för det jag publicerar på sociala medier?’ <https://www.imy.se/vanliga-fragor-och-svar/ar-jag-ansvarig-for-det-jag-publicerar-pa-sociala-medier/>.

Samtidigt finns det ett tydligt stöd för att även Meta är personuppgiftsansvarigt för det den offentliga sektorn publicerar på Facebook. I rättsfallet *Wirtschaftsakademie* slår EU-domstolen fast att det ”i första hand” är Meta som ”ska anses bestämma ändamålen och medlen för behandlingen av personuppgifter för användare av Facebook och för personer som besöker en fanpage som Facebook hyser.”[72] Artikel 29-gruppen anger i sina riktlinjer att den som tillhandahåller ett socialt nätverk är att se som personuppgiftsansvarig, eftersom denne tillhandahåller de grundläggande tjänsterna relaterade till kontohantering.[73] Även i doktrinen uttrycks att den som tillhandahåller ett socialt nätverk är att se som personuppgiftsansvarig. Tillhandahållarens syfte med personuppgiftsbehandlingen är typiskt monetärt (aktiviteten på nätverket ska generera inkomst), och eftersom tillhandahållaren bestämmer hur det sociala nätverket fungerar bestämmer denne också över medlen för personuppgiftsbehandlingen.[74] Integritetsskyddsmyndighetens uppfattning är att ett företag som tillhandahåller ett socialt medium är personuppgiftsansvarigt om företaget har möjlighet att påverka eller bestämma över inläggen.[75] En sådan möjlighet har Meta, som kan radera inlägg. Meta anger dessutom självt att företaget är personuppgiftsansvarigt ”för all aktivitet på Facebook”.[76]

Innebär det här att sidadministratören och Meta blir gemensamt personuppgiftsansvariga för det som administratören själv publicerar på sin Facebooksida? I doktrinen föreslås att det snarare rör sig om ett separat personuppgiftsansvar, alltså att den offentliga sektorn och Meta inte är gemensamt personuppgiftsansvariga utan ansvariga var för sig.[77] Uttalandena är dock från en tid före avgörandena *Wirtschaftsakademie* och *Fashion ID,* som visar att tröskeln är låg för det gemensamma personuppgiftsansvaret. Generaladvokat Bobak argumenterar dock för att tröskeln inte kan vara alltför låg och att det inte kan föreligga ett gemensamt personuppgiftsansvar så fort någon har möjliggjort en personuppgiftsbehandling för någon annan.[78] I rättsfallet *Wirtschaftsakademie* uttalar EU-domstolen följande: ”Enbart den omständigheten att någon använder sig av ett socialt nätverk som Facebook innebär inte att en användare blir medansvarig för detta nätverks behandling av personuppgifter.”[79]

---

[72] C-210/16 *Wirtschaftsakademie* p. 30. Ordet *fanpage* är synonymt med *Facebooksida*.

[73] Artikel 29-gruppen, Opinion 5/2009 s. 5.

[74] van Alsenoy s. 352; van Alsenoy m. fl. s. 70.

[75] Integritetsskyddsmyndigheten, ’Är jag ansvarig för det jag publicerar på sociala medier?’ <https://www.imy.se/vanliga-fragor-och-svar/ar-jag-ansvarig-for-det-jag-publicerar-pa-sociala-medier/>.

[76] Meta, ’Vad är dataskyddsförordningen (GDPR)?’ <https://www.facebook.com/business/gdpr#Facebook-som-personuppgiftsansvarig-kontra-Facebook-som-personuppgiftsbitr%C3%A4de>.

[77] van Alsenoy m.fl. s. 71.

[78] Förslag till avgörande av generaladvokat Michal Bobek i mål C-40/17 *Fashion ID* p. 71–75.

[79] C-210/16 *Wirtschaftsakademie* p. 35.

Utredningen leder mig till slutsatsen att sidadministratören och Meta åtminstone blir separat personuppgiftsansvariga för administratörens egna inlägg. Min slutsats av utredningen är att det förmodligen inte blir fråga om ett gemensamt personuppgiftsansvar men att det inte helt kan uteslutas. Rättsläget är inte helt klarlagt och det finns en möjlighet att den som driver en Facebooksida blir gemensamt personuppgiftsansvarig tillsammans med Meta.

3.2 Ansvar för användares aktivitet

Privatpersoner kan genom sina Facebookkonton integrera med den offentliga sektorns Facebooksidor. När användare kommenterar inlägg delar de i regel personuppgifter om sig själva, antingen genom sina namn, genom sina profilbilder eller genom det som kommentarerna innehåller. Användarnas kommentarer kan också innehålla personuppgifter om någon annan (tredjeman), till exempel genom att en användare taggar någon i en kommentar eller uppger information i en kommentar som kan identifiera tredjeman. Vem är personuppgiftsansvarig för användarnas aktivitet på den offentliga sektorns Facebooksidor?

Med utgångspunkt i det som har beskrivits i avsnitt 3.1 går det sannolikt att tillskriva Meta personuppgiftsansvar för användarnas aktivitet. Meta bestämmer varför personuppgifter behandlas på Facebook och hur plattformen tekniskt fungerar – Meta bestämmer över ändamålen med och medlen för personuppgiftsbehandlingen. Samtidigt finns det också stöd för att hävda att även kommunen, regionen eller myndigheten blir personuppgiftsansvarig. Integritetsskyddsmyndigheten bedömer i beslut baserade på personuppgiftslagen att en Facebooksidas administratör är personuppgiftsansvarig även för de personuppgifter som publiceras av användare. En Facebooksidas administratör kan nämligen bestämma vilka möjligheter användare har att publicera innehåll på sidan, och administratören har en faktisk möjlighet att ta bort personuppgifter som publiceras på sidan av andra användare. Utan valet att upprätta Facebooksidan och fortsätta ha kvar den skulle användare inte ha möjlighet att publicera inlägg och kommentarer på sidan. Därför bestämmer sidans administratör över ändamålen och medlen för personuppgiftsbehandlingen på Facebooksidan även för de personuppgifter som publiceras av användare.[80] I E-delegationens riktlinjer, som förvisso är skrivna utifrån personuppgiftslagen, går att läsa att myndigheter ”torde” ha ett personuppgiftsansvar över sådant som sidans besökare publicerar, om myndigheten kan påverka det som besökarna publicerar och därmed bestämma över ändamålen och medlen för kommentarer och inlägg gjorda av andra.[81] Den som administrerar en Facebooksida har en sådan möjlighet; administratören kan ta bort inlägg som görs av sidans besökare.

[80] Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 685-2010 s. 5; Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 686-2010 s. 4; Integritetsskyddsmyndighetens beslut 2010-07-02 dnr 687-2010 s. 4.

[81] E-delegationen s. 52.

Den enskilda användaren som publicerar personuppgifter i inlägg eller kommentarer blir sannolikt också personuppgiftsansvarig vid sidan av Meta och Facebooksidans administratör. Den enskilde användaren bestämmer nämligen ändamålen med personuppgiftsbehandlingen (till exempel att ställa en fråga till en kommun) och medlen för den (till exempel text i en kommentar).[82] Artikel 2.1 c dataskyddsförordningen föreskriver dock att förordningen inte ska tillämpas på personuppgiftsbehandling som utförs av en fysisk person som ett led i en verksamhet av rent privat natur eller som har samband med dennes hushåll.[83] I skäl 18 till dataskyddsförordningen anges att aktivitet på sociala nätverk kan omfattas av undantaget om privat behandling. Om undantaget är tillämpligt innebär det att enskilda användare inte blir personuppgiftsansvariga för det som de publicerar på Facebooksidan i fråga. Integritetsskyddsmyndighetens uppfattning är dock att undantaget inte är tillämpligt när privatpersoner publicerar personuppgifter i sociala medier, eftersom det innebär en publicering för en bredare krets.[84] Min uppfattning är att det går att argumentera för att undantaget blir tillämpligt om bara ett begränsat antal användare kan se det som publicerats. Det är dock svårt att hävda att undantaget kan tillämpas på publiceringar som sker på Facebooksidor som tillhör offentlig sektor, eftersom vem som helst på internet – även de som inte har konton på Facebook – kan se publiceringen.

Min bedömning är samtliga tre aktörer – den offentliga sektorn, Meta och den enskilda användaren – blir personuppgiftsansvariga på varsitt håll för de personuppgifter som enskilda användare publicerar på den offentliga sektorns Facebooksidor. Den offentliga sektorn har alltså ett ansvar även för användares egen publicering på Facebooksidan. Eftersom rättsläget är oklart för när det föreligger ett gemensamt personuppgiftsansvar vågar jag inte utesluta att ansvaret också kan vara gemensamt.

3.3 Ansvar för sidstatistik

En något dold personuppgiftsbehandling sker i samband med upprättandet av sidstatistik. Den som skapar en Facebooksida får tillgång till verktyget *Statistik*. Med verktygets hjälp går det att se Facebooksidans resultat, det vill säga hur många som sidan når. Genom sidstatistiken kan den som driver en Facebooksida få demografiska data om sin målgrupp och data om hur personer reagerar på och interagerar med inlägg på sidan.[85] Syftet med verktyget är att den som driver en Facebooksida ska få ökad kunskap om sin målgrupp.[86] Upprättandet av sidstatistiken innebär personuppgiftsbehandling –

[82] Se Artikel 29-gruppen, WP163 s. 5; Colcelli s. 1035; Integritetsskyddsmyndigheten, ’Är jag ansvarig för det jag publicerar på sociala medier?’ <https://www.imy.se/vanliga-fragor-och-svar/ar-jag-ansvarig-for-det-jag-publicerar-pa-sociala-medier/>.

[83] Se också C-101/01 *Lindqvist*.

[84] Integritetsskyddsmyndigheten, ’Är jag ansvarig för det jag publicerar på sociala medier?’ <https://www.imy.se/vanliga-fragor-och-svar/ar-jag-ansvarig-for-det-jag-publicerar-pa-sociala-medier/>. Jämför Finck s. 338–339.

[85] Meta, ’Sidstatistik’ <https://www.facebook.com/business/help/633309530105735>.

[86] Meta, ’Sidstatistik’ <https://www.facebook.com/business/help/633309530105735>.

uppgifter om användare som besöker en Facebooksida samlas in med hjälp av kakor när användaren besöker sidan.[87]

Rättsläget som avser sidstatistik på Facebook är klarlagt; EU-domstolen slår i rättsfallet *Wirtschaftsakademie* fast att en Facebooksidas administratör blir gemensamt personuppgiftsansvarig tillsammans med Meta för den personuppgiftsbehandling som sker inom ramen för upprättandet av statistiken. Målet föranleddes av att företaget Wirtschaftsakademie drev en Facebooksida och hade fått ett föreläggande från en tysk tillsynsmyndighet att avaktivera Facebooksidan, eftersom varken Wirtschaftsakademie eller Facebook informerade sidans besökare om att personuppgifter samlades in med hjälp av kakor.[88] I målet konstaterar EU-domstolen att det i första hand är företaget bakom Facebook som bestämmer ändamålen och medlen för behandlingen av personuppgifter för användare av Facebook.[89] EU-domstolen noterar dock att den som skapar en Facebooksida vidtar konfigurationsåtgärder som inverkar på behandlingen av personuppgifter för ändamålet att upprätta statistik. Administratören kan med hjälp av filter som tillhandahålls av Facebook fastställa de kriterier som sidstatistiken upprättas efter. Med andra ord kan administratören bestämma vilka personkategoriers personuppgifter som kommer att användas av Facebook. Administratören kan även begära att få demografiska data om sidans målgrupp, vilket också innebär personuppgiftsbehandling.[90]

EU-domstolen slår avslutningsvis fast att Wirtschaftsakademie, genom sin statistikkonfiguration, medverkat till att fastställa ändamålen och medlen för behandlingen av personuppgifterna tillhörande sidans besökare, och att Wirtschaftsakademie på grund av det blir gemensamt personuppgiftsansvarig med Facebook för behandlingen.[91] Det innebär att den som driver en Facebooksida blir gemensamt personuppgiftsansvarig med Meta för den personuppgiftsbehandling som sker inom ramen för upprättandet av sidstatistiken. EU-domstolen förtydligar i rättsfallet *Fashion ID* att det gemensamma personuppgiftsansvaret inte omfattar eventuell personuppgiftsbehandling som Meta utför i ett senare steg, där Facebooksidans ägare inte är inblandad.[92]

3.4 Kommentar

Utredningen visar att rättsläget inte är helt klarlagt angående vem som ansvarar för vad på en Facebooksida. Jag bedömer att det med relativ säkerhet går att säga att en kommun, region eller myndighet som driver en Facebooksida blir åtminstone separat personuppgiftsansvarig för det som aktören publicerar och för det som användare publicerar på Facebooksidan. Det går också med säkerhet att säga att kommuner, regioner och myndigheter blir gemensamt

[87] C-201/16 *Wirtschaftsakademie* p. 15, 33, 35.
[88] C-210/16 *Wirtschaftsakademie* p. 14–18.
[89] C-210/16 *Wirtschaftsakademie*, p. 30.
[90] C-210/16 *Wirtschaftsakademie*, p. 36–37.
[91] C-210/16 *Wirtschaftsakademie* p. 39.
[92] C-40/17 *Fashion ID* p. 74, 85.

personuppgiftsansvariga med Meta om sidstatistik upprättas. Däremot anser jag att det inte helt går att utesluta att kommuner, regioner och myndigheter kan bli gemensamt personuppgiftsansvariga tillsammans med Meta och enskilda användare. Situationen är komplex och svår att bedöma.

4 Ansvar för att principerna följs

Av artikel 5.1 dataskyddsförordningen framgår att all personuppgiftsbehandling måste följa de principer som listas i artikeln. Det är den personuppgiftsansvarige som ansvarar för att principerna följs (artikel 5.2 och 24.1 dataskyddsförordningen). Bevisbördan för att personuppgiftsbehandlingen följer dataskyddsförordningen ligger enligt samma två artiklar på den personuppgiftsansvarige. I det här avsnittet utreder jag vad principerna innebär och analyserar om den offentliga sektorn kan se till att de efterlevs inom ramen för sitt personuppgiftsansvar på Facebook.

Flera principer är kopplade till en viss rättighet som den registrerade har enligt dataskyddsförordningen. Den registrerades rättigheter utreder och analyserar jag i kapitel 6.

4.1 Laglighet, korrekthet och öppenhet

Personuppgifter ska enligt artikel 5.1 a dataskyddsförordningen behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Principen om laglighet, korrekthet och öppenhet kan ses som tre delprinciper och analyseras i det här avsnittet var för sig.

4.1.1 Laglighet

Att behandlingen ska ske på ett lagligt sätt är en särskild koppling till artikel 6.1 dataskyddsförordningen.[93] Artikel 6.1 föreskriver att varje personuppgiftsbehandling måste stödjas av en av de sex grunder som räknas upp i artikeln för att vara laglig. Laglighetsprincipen innebär också att behandlingen ska vara förenlig med övriga bestämmelser i dataskyddsförordningen och dess kompletterande lagstiftning.[94] För att följa laglighetsprincipen behöver den offentliga sektorn åtminstone säkerställa att det finns en laglig grund för all personuppgiftsbehandling som sker på Facebooksidan. Möjligheten att säkerställa en laglig grund förtjänar ett eget kapitel och analyseras i kapitel 5.

Det är inte helt klarlagt huruvida principen om laglighet innebär att personuppgiftsbehandlingen ska vara förenlig även med annan lagstiftning och rättspraxis, utanför dataskyddsområdet. Högsta förvaltningsdomstolen har slagit fast att motsvarande krav i personuppgiftslagen endast krävde förenlighet med personuppgiftslagen och kompletterande bestämmelser – inte förenlighet med annan lagstiftning.[95] I svensk doktrin anförs att Högsta förvaltningsdomstolens slutsats bör gälla även för dataskyddsförordningen.[96] Samtidigt har det i utländsk litteratur argumenterats för att dataskyddsdirektivets

[93] Prop. 2017/18:105 s. 47; Șchiopu s. 204; skäl 40 dataskyddsförordningen.

[94] Öman, kommentaren till artikel 5, under rubriken ”Led a – Laglighet, korrekthet och öppenhet”. Jämför HFD 2016 ref. 40.

[95] HFD 2016 ref. 40 s. 3–4.

[96] Holtz och Ledendal s. 143.

bestämmelser (som personuppgiftslagen baseras på) innebär att behandlingen ska vara förenlig också med övrig lagstiftning.[97] Det ska också nämnas att Artikel 29-gruppen anser att behandlingen måste vara förenlig med övrig lagstiftning, men att det snarare följer av principen om ändamålsbegräsning.[98] Dataskyddsutredningen verkar ha anslutit sig till att dataskyddsförordningens ändamålsprincip innebär att personuppgiftsbehandlingen ska vara förenlig med övrig lagstiftning.[99]

Det är alltså svårt att säga om personuppgiftsbehandlingen måste vara förenlig även med annan lagstiftning för att vara förenlig med laglighetsprincipen. Om man släpper dataskyddsperspektivet och ser helheten menar jag dock att lösningen blir uppenbar: Personuppgiftsbehandlingen bör inte strida mot övrig lagstiftning. Man kan tänka sig en (kanske något osannolik) situation där en kommun, myndighet eller region publicerar ett inlägg med personuppgifter som till exempel innebär ett intrång i någons upphovsrätt. Enligt min mening är det i en sådan situation oviktigt om behandlingen strider mot laglighetsprincipen, eftersom den strider mot annan lagstiftning.

I personuppgiftsansvaret ingår också att kunna bevisa att laglighetsprincipen följs (se artikel 5.2 och artikel 24.1 dataskyddsförordningen). Min bedömning är att det borde kunna ske genom att den offentliga sektorn gör en noggrann bedömning av vilken laglig grund som är tillämplig innan personuppgiftsbehandlingen påbörjas, och att det man kommer fram till dokumenteras.[100]

4.1.2 Korrekthet

Att personuppgifter ska behandlas på ett korrekt sätt innebär att de ska behandlas på ett sätt som den registrerade kan förvänta sig.[101] Principen om korrekthet ska läsas i relation till den registrerade och innebär att en intresseavvägning ska göras mellan behovet av att genomföra behandlingen och den registrerades personliga integritet.[102] Personuppgiftsbehandlingen ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till den registrerade, och personuppgifterna får inte behandlas på ett sätt som är oväntat eller missvisande för denne.[103] Principen om korrekthet hänger ihop med principen om

[97] Se Öman, kommentaren till artikel 5, under rubriken ”Led a – Laglighet, korrekthet och öppenhet”.

[98] Artikel 29-gruppen, WP 203 s. 19–20.

[99] SOU 2017:39 s. 107.

[100] Se också Myndigheten för digital förvaltning, ’Grundläggande principer för behandling av personuppgifter’ < https://www.digg.se/kunskap-och-stod/metodstod-for-dataskydd-vid-innovation/rattslig-bedomning-av-personuppgiftsbehandlingen/grundlaggande-principer-for-behandling-av-personuppgifter>, som delar min uppfattning.

[101] Krzysztofek s. 61; Törngren, kommentaren till artikel 5.

[102] Integritetsskyddsmyndighetens beslut 2010-11-24 dnr DI-2019-7782 s. 7; Prop. 2017/18:105 s. 47.

[103] Europeiska dataskyddstyrelsen, Riktlinjer 4/2019 s. 17–18; Integritetsskyddsmyndigheten, ’Grundläggande principer’ <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/>; Integritetsskyddsmyndighetens beslut 2010-11-24 dnr DI-2019-7782 s. 7.

öppenhet – det som den registrerade har fått information om är det han eller hon kan vänta sig. Om den personuppgiftsansvarige har upprättat en personuppgiftspolicy och bryter mot den, bryter den personuppgiftsansvarige också mot principen om korrekthet (åtminstone om policyn varit tillgänglig för den registrerade).[104]

Min bedömning är kommuners, regioners och myndigheters personuppgiftsbehandling på Facebook sannolikt är i enlighet med principen om korrekthet, åtminstone personuppgiftsbehandlingen som sker vid de egna inläggen och vid användarnas aktivitet. Det förutsätter dock att kommunen, regionen eller myndigheten i fråga informerar personer som förekommer i inlägg. Användare som själva delar sina personuppgifter på Facebooksidan rimligen måste förvänta sig att personuppgifterna kommer att behandlas av sidans ägare när de publicerar personuppgifterna.

Däremot kan det vara en större utmaning att säkerställa att principen efterlevs när användare publicerar personuppgifter om tredjeman och när sidstatisk upprättas. Det kan vara oväntat för tredjeman att dennes personuppgifter behandlas på en Facebooksida som denne inte har interagerat med, och Facebooksidans besökare kanske inte väntar sig att deras personuppgifter används för att upprätta sidstatistik. Samtidigt framgår det av Metas integritetspolicy att personuppgifter används för att upprätta sidstatistik.[105]

4.1.3 Öppenhet

Principen om öppenhet innebär att all personuppgiftsbehandling ska vara transparant gentemot den registrerade. Principen är särskilt kopplad till dataskyddsförordningens krav på att lämna information till den registrerade.[106] Öppenhetsprincipen syftar till att göra den registrerade medveten om syftet med personuppgiftsbehandlingen och de risker, regler, säkerhetsåtgärder och rättigheter som finns i samband med behandlingen.[107] Öppenhetsprincipen hänger ihop med att säkerställa att den registrerade kan utöva sina rättigheter – om den registrerade inte förstår när och hur personuppgifterna behandlas kan den registrerade inte hävda sin rätt.[108]

Om informationsskyldigheterna i dataskyddsförordningen följs, innebär det alltså att principen om öppenhet uppfylls. Jag analyserar den offentliga sektorns möjlighet att efterleva informationsskyldigheten i avsnitt 6.1.

---

[104] Şandru s. 66–67; Öman, kommentaren till artikel 5, under rubriken ”Led a – laglighet, korrekthet och öppenhet”.

[105] Meta, ’Integritetspolicy’ <https://www.facebook.com/privacy/policy/>.

[106] Skäl 39 dataskyddsförordningen. Se också Artikel 29-gruppen, WP260 s. 6.

[107] Skäl 39 dataskyddsförordningen.

[108] Se Integritetsskyddsmyndigheten beslut 2021-06-07 dnr DI-2019-3375 s. 16. Integritetsskyddsmyndigheten anser att bristfällig information påverkar den registrerades möjligheter att utöva sina rättigheter och att det står i strid med öppenhetsprincipen att tillhandahålla sådan bristfällig information.

Angående den personuppgiftsansvariges möjlighet att bevisa att principen följs anser Krzysztofek att den personuppgiftsansvarige bör låta den registrerade på något sätt bekräfta att denne fått information, till exempel genom att klicka i en ruta eller lämna sin signatur.[109] Min uppfattning är att det räcker att visa att informationen finns öppet tillgänglig och att en bekräftelse är överflödig.

4.2 Ändamålsbegränsning

Personuppgifter ska enligt artikel 5.1 b samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Att ändamålen ska vara särskilda innebär att den personuppgiftsansvarige måste precisera ändamålen – de får inte vara för allmänt hållna.[110] Enligt regeringen är vad som är ett berättigat ändamål direkt kopplat till de rättsliga grunderna i artikel 6.1.[111] Artikel 29-gruppen skriver i sina riktlinjer att ändamålen måste vara förenliga med övrig lagstiftning.[112]

Personuppgifter får enligt artikel 5.1 b inte i ett senare skede behandlas på ett sätt som är oförenligt med det ursprungliga ändamålet.[113] Att ändamålen måste vara preciserade och att personuppgifterna inte får vidarebehandlas på ett sätt som är oförenligt med det ursprungliga ändamålet innebär att den som behandlar personuppgifter måste ha specificerat sitt syfte redan innan behandlingen börjar.[114] Det är alltså inte godtagbart att fastställa ändamålet i efterhand.

Vanliga ändamål för den offentliga sektorns personuppgiftsbehandling på Facebook är att visa upp sin verksamhet, sprida information och nyheter samt svara på medborgarnas frågor.[115] Min bedömning är att de här ändamålen är förenliga med övrig lagstiftning men att de, åtminstone i den form jag har kunnat identifiera dem, är något allmänt hållna. För att kunna leva upp till principen om ändamålsbegränsning behöver sannolikt kommunen, regionen eller myndigheten precisera ändamålen något. Det är också viktigt att kommunen, regionen eller myndigheten noga överväger varför de behandlar personuppgifter på sin Facebooksida innan själva behandlingen börjar; ändamålen ska vara preciserade redan innan personuppgiftsbehandlingen börjar.

---

[109] Krzysztofek s. 64.

[110] Exempel på vaga eller generella är enligt Artikel 29-gruppen ”förbättra användarupplevelsen” och ”marknadsföring”, se Artikel 29-gruppen, WP 203 s. 15–16.

[111] Prop. 2017/18:105 s. 47.

[112] Artikel 29-gruppen, WP 203 s. 19–20.

[113] Motsatsvis innebär det att personuppgifter kan behandlas för andra ändamål än det ursprungliga, om det nya ändamålet inte är oförenligt med det ursprungliga, se artikel 5.1 b och artikel 6.4 dataskyddsförordningen.

[114] Skäl 39.

[115] Se till exempel Region Dalarna, ’Region Dalarna’ <https://www.facebook.com/regiondalarna> och Försäkringskassan, ’Försäkringskassan förälder’ <https://www.facebook.com/foralder>.

Den offentliga sektorn har andra ändamål med personuppgiftsbehandlingen på Facebook än vad Meta har. Meta behandlar personuppgifter i vinstsyfte, vilket inte den offentliga sektorn gör. Som jag tidigare redogjort för utesluter inte olika ändamål att ett gemensamt personuppgiftsansvar kan föreligga.

Så länge kommunen, regionen eller myndigheten har tydliga riktlinjer om hur personuppgifter får vidarebehandlas borde det enligt min bedömning vara enkelt för verksamheten att följa principen om ändamålsbegränsning. Man kan dock tänka sig att Meta kan vidarebehandla personuppgifterna med andra syften än de ursprungliga, vilket riskerar att ske i strid med principen om ändamålsbegränsning. Den risken bör den offentliga sektorn, enligt min bedömning, kunna bortse från. Det följer av EU-domstolens praxis att personuppgiftsansvaret, även det gemensamma, är begränsat till den personuppgiftsbehandling som varje aktör faktiskt bestämmer ändamålen och medlen för.[116]

4.3 Uppgiftsminimering

Enligt principen om uppgiftsminimering i artikel 5.1 c dataskyddsförordningen ska personuppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till varför de behandlas; bara de personuppgifter som behövs för det angivna ändamålet får behandlas.[117] I skäl 39 anges att personuppgifter endast bör behandlas om syftet med behandlingen inte kan rimligen kan uppnås genom andra medel.

För den offentliga sektorns del bör det vara förhållandevis enkelt att se till att principen om uppgiftsminimering efterlevs när det kommer till den egna publiceringen. Kommunen, regionen eller myndigheten i fråga bör ha tydliga riktlinjer för publicering av egna inlägg, och dessa riktlinjer bör föreskriva att ingen extra ”kringinformation” får tillförs inläggen – bara det som är nödvändigt ska med. På så vis har kommunen, regionen eller myndigheter vidtagit åtgärder för att säkerställa att personuppgifterna som behandlas är adekvata och inte för omfattande i förhållande till varför de behandlas.

En särskild situation uppkommer när användare själva förser Facebooksidan med personuppgifter, antingen om sig själva eller om tredjeman. Det är svårt att kommentera hur det påverkar den offentliga sektorns personuppgiftsansvar. Hur väl principen efterlevs måste enligt min uppfattning bero på vad inläggen från användarna syftar till och vad de innehåller för personuppgifter. Ett sätt att se till att principen efterlevs skulle kunna vara att ställa upp riktlinjer för vilken information som får publiceras på Facebooksidan.

Vad gäller sidstatistiken är den offentliga sektorn helt beroende av hur Facebook fungerar. Även om Facebooksidans administratör kan ställa in vilken statistik som ska upprättas, är det utanför administratörens kontroll vilka

[116] C-40/17 *Fashion ID* p. 74, 85.
[117] Öman, kommentaren till artikel 5, under rubriken ”Led c – Uppgiftsminimering”.

uppgifter som faktiskt samlas in. Den offentliga sektorn måste alltså förlita sig på att Meta inte samlar in någon kringinformation när sidstatistiken tas fram. Jag ser det som en risk som är värd att ta i beaktning.

4.4 Riktighet

Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade enligt principen om riktighet i artikel 5.1 d dataskyddsförordningen. I dataskyddsförordningen mening är en personuppgift felaktig bra i förhållande till varför den behandlas. En personuppgift som inte motsvarar verkliga förhållanden kan alltså vara korrekt i dataskyddsförordningens mening.[118] Personuppgifter som är felaktiga i förhållande till varför de behandlas måste rättas, och det är den personuppgiftsansvariges skyldighet att vidta de åtgärder som krävs för att säkerställa att så sker. Huruvida det är nödvändigt att uppdatera personuppgifterna avgörs utifrån ändamålet med behandlingen. Vilka åtgärder som är rimliga att vidta bedöms utifrån omständigheterna i varje enskilt fall, bland annat varför personuppgifterna behandlas, hur många personuppgifter som behandlas och vilka konsekvenser felaktiga personuppgifter kan få för den registrerade.[119]

Jag bedömer att den offentliga sektorn bör kunna efterleva principen om korrekthet när det gäller den egna publiceringen. Sidadministratören har kontroll över sina egna inlägg och kan åtminstone redigera personuppgifter som förekommer i text. Om någon som förekommer i inlägg till exempel har bytt namn kan sidans administratör redigera inlägget och rätta namnet. Principen om riktighet bör också kunna efterlevas inom ramen för sidstatistiken. Om en Facebookanvändare har angett att han eller hon har en annan ålder än vad som verkligen är fallet, är personuppgiften fortfarande korrekt i dataskyddsförordningens mening. Det spelar alltså ingen roll att sidstatistiken blir inkorrekt i förhållande till verkligheten. Om fallet var motsatt och det *hade* spelat roll om uppgifterna är felaktiga i förhållande till verkligheten, hade det inneburit att principen om riktighet kanske inte kan efterlevas. Den som administrerar en Facebooksida kan nämligen inte redigera användares profiler och personuppgifter.

Kommuner, regioner och myndigheter kan få problem med att efterleva principen om riktighet när användare självmant publicerar personuppgifter som är att beakta som felaktiga i dataskyddsförordningens mening. Här kan administratören endast radera uppgifterna och inte rätta dem. I en sådan situation är det tveksamt om principen om riktighet kan efterlevas.

[118] C-434/16 *Nowak*. Jämför Öman, kommentaren till artikel 5, under rubriken ”Led d – Riktighet”.

[119] Öman, kommentaren till artikel 5, under rubriken ”Led d – Riktighet”.

4.5 Lagringsminimering

Enligt principen om lagringsminimering i artikel 5.1 e får personuppgifter bara lagras så länge de behövs för ändamålet med behandlingen. Den personuppgiftsansvarige måste se till att personuppgifter som inte längre behövs antingen raderas eller avidentifieras. Man kan fråga sig om det finns en bortre gräns för hur länge personuppgifter får lagras. Enligt förordningstexten får personuppgifter lagras så länge de behövs för ändamålet. Jag har inte kunnat hitta något som tyder på att det finns en bortre gräns för hur länge personuppgifter får lagras. Hur länge personuppgifterna får lagras bestäms helt och hållet utifrån syftet med personuppgiftsbehandlingen. När syftet är uppfyllt ska uppgifterna raderas eller avidentifieras.

Enligt min bedömning är det svårt att avgöra när personuppgifterna på Facebooksidan inte längre behövs i förhållande till varför de behandlas. Om syftet med att behandla en personuppgift är att informera om kommunens, regionens eller myndighetens verksamhet, är syftet uppfyllt när inlägget är publicerat? När det har nått en viss publik? Min bedömning är att personuppgifter på den offentliga sektorns Facebooksidor förmodligen kan lagras länge, men att principen om lagringsminimering överträds om en Facebooksida finns kvar för en verksamhet som har upphört.

Det kan vara svårt för kommuner, regioner och myndigheter att efterleva principen om lagringsminimering om de skulle behöva radera eller avidentifiera en personuppgift. Det är nämligen åtgärder av teknisk natur, som bara Meta har full kontroll över. Den offentliga sektorn måste förlita sig på att personuppgifterna verkligen raderas.

4.6 Integritet och konfidentialitet

Slutligen ska personuppgiftsbehandlingen ske på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, enligt principen om integritet och konfidentialitet i artikel 5.1 f. Den personuppgiftsansvarige ska genom tekniska eller organisatoriska åtgärder säkerställa lämplig säkerhet för personuppgifterna. Skyldigheten innefattar enligt artikeln både att skydda mot att personuppgifterna behandlas av någon obehörig och att skydda mot att personuppgifterna förloras eller förstörs. Principen om integritet och konfidentialitet är särskilt kopplad till artikel 24.1 och artikel 32. I artikel 32.1 listas exempel på åtgärder som kan vidtas för att säkerställa lämplig skyddsnivå, bland annat pseudonymisering och kryptering.

Till stora delar är det helt utom den offentliga sektorns kontroll hur säkerheten är för personuppgifterna på Facebook. Det är Meta som har kontroll över hur Facebook tekniskt fungerar, inklusive säkerhetsskyddet för personuppgifter. Det är svårt att avgöra hur väl Meta efterlever principen om integritet och konfidentialitet, eftersom informationen som finns tillgänglig är skral. Meta uppger att företaget arbetar med integritet och konfidentialitet både på ett

organisatoriskt och ett tekniskt plan.[120] Samtidigt finns det flera exempel på att data på Facebook har läckt ut till obehöriga.[121] Enligt artikel 32.3 kan Meta ansluta sig till en godkänd uppförandekod eller certifieringsmekanism för att visa att företaget vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå. Jag har inte kunnat hitta att Meta har anslutit sig till någon sådan kod eller mekanism.

Det finns dock åtgärder som jag bedömer att den offentliga sektorn kan och bör vidta för att säkerställa sin efterlevnad av principen om integritet och konfidentialitet. Den offentliga sektorn bör säkerställa att endast behöriga har tillgång till Facebookkontot. Den som har kontots inloggningsuppgifter kan nämligen radera inlägg och därmed även radera personuppgifter, vilket kan innebära att principen om integritet och konfidentialitet inte följs. Dessutom är den personuppgiftsansvarige enligt artikel 32.4 skyldig att säkerställa att anställda som får tillgång till personuppgifter endast hanterar dem i enlighet med instruktion från den personuppgiftsansvarige. Här blir det enligt min mening viktigt att den offentliga sektorn har tydliga riktlinjer för hur Facebooksidan får användas.

4.7 Kommentar

Utredningen visar att kommuner, regioner och myndigheter i flera fall har goda möjligheter att säkerställa att principerna följs. Så länge kommunen, regionen eller myndigheten säkerställer en laglig grund och uppfyller sin skyldighet att informera, efterlevs principerna om laglighet och öppenhet. Ändamålsprincipen kan efterlevas så länge ändamålen tydligt preciseras, och tydliga riktlinjer kan säkerställa att principerna om uppgiftsminimering och integritet och konfidentialitet efterlevs.

Utredningen visar dock också att vissa principer kan vara svårare att efterleva, i regel för att kommunen, regionen eller myndigheten bara har begränsad kontroll över personuppgiftsbehandlingen som sker på deras Facebooksidor. Det kan vara svårt att säkerställa att principen om korrekthet efterlevs när tredjeman får sina personuppgifter behandlade, och det är osäkert om principen om riktighet kan efterlevas eftersom en Facebooksidas administratör inte kan redigera användares inlägg.

[120] Meta, ’Privacy progress update’ <https://about.meta.com/privacy-progress/>.

[121] Se Heiligenstein, ’Facebook Data Breaches. Full Timeline Through 2023’ <https://firewalltimes.com/facebook-data-breach-timeline/>.

5 Ansvar för att säkerställa laglig grund

I artikel 6 dataskyddsförordningen preciseras vad som utgör en laglig behandling av personuppgifter.[122] En personuppgiftsbehandling är laglig om den uppfyller något av de sex villkor som listas i artikeln. Villkoren brukar kallas för laglig eller rättslig grund för personuppgiftsbehandling.[123] Det är den personuppgiftsansvariges skyldighet att se till att varje personuppgiftsbehandling kan stödjas av åtminstone en av grunderna.[124]

Alla lagliga grunder utom samtycke förutsätter att personuppgiftsbehandlingen är *nödvändig*. Kravet på nödvändighet innebär inte att behandlingen ska vara absolut nödvändig eller det enda sättet att uppnå ändamålet. Om en behandling leder till effektivitetsvinster anses den vara nödvändig.[125] Kravet på nödvändighet innebär att man ska undersöka om andra mindre ingripande metoder kan tjäna samma syfte. Om det finns realistiska, mindre integritetskränkande alternativ ska de användas istället.[126]

5.1 Samtycke

Personuppgifter får behandlas om den registrerade lämnar sitt samtycke till det (artikel 6.1 a). Vad som utgör ett giltigt samtycke framgår av artikel 4.11 dataskyddsförordningen: ett samtycke ska vara frivilligt, specifikt, informerat och otvetydigt. Av artikel 7.3 framgår dessutom att ett samtycke när som helst ska kunna återkallas och att det ska vara lika lätt att återkalla ett samtycke som att lämna det.

Att samtycket ska vara frivilligt innebär att den registrerade ska ha en genuin valmöjlighet och att den registrerade utan problem kan vägra eller återkalla sitt samtycke.[127] Ett giltigt samtycke kan enligt skälen till dataskyddsförordningen inte ges om ”det råder en betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet[128] och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar.”[129] Det innebär att det går att ifrågasätta om en registrerad kan lämna ett giltigt samtycke till en personuppgiftsbehandling som utförs av kommuner, regioner och myndigheter. Den offentliga sektorns möjlighet att grunda personuppgiftsbehandling på samtycke är begränsad – men inte helt

[122] Jämför artikel 5.1 a dataskyddsförordningen.

[123] Ibland används även *rättslig grund för personuppgiftsbehandling*.

[124] Det följer av artiklarna 5.1 a, 5.2 och 6.1 dataskyddsförordningen.

[125] C-524/06 *Huber* p. 62.

[126] Artikel 29-gruppen, WP 217 s. 30; Europeiska dataskyddsstyrelsen, Riktlinjer 2/2019 s. 8.

[127] Skäl 42 dataskyddsförordningen.

[128] Enligt regeringen ska regeringsformens terminologi användas för att tolka innebörden av dataskyddsförordningens begrepp *offentlig myndighet*. Det innebär att samtliga statliga och kommunala organ faller in under dataskyddsförordningens begrepp *offentlig myndighet*. Se prop. 2017/18:105 s. 46.

[129] Skäl 43 dataskyddsförordningen.

förbjuden.[130] Europeiska dataskyddsstyrelsen antyder i sina riktlinjer att myndigheter kan grunda sin personuppgiftsbehandling på samtycke i situationer där den registrerade inte går miste om några huvudtjänster. Tjänsten i fråga ska finnas att tillgå även om den registrerade skulle vägra att ge sitt samtycke.[131]

Att samtycket ska vara specifikt ställer krav på att den personuppgiftsansvarige har preciserat sina behandlingsändamål; samtycke till personuppgiftsbehandling ska nämligen ges för ett eller flera specifika ändamål. Om den personuppgiftsansvarige behandlar personuppgifter för flera ändamål måste den registrerade få möjlighet att samtycka till varje ändamålsbehandling.[132] Att samtycket ska vara informerat är kopplat till öppenhetsprincipen i artikel 5.1 a dataskyddsförordningen. Enligt Artikel 29-gruppen ska den registrerade, när den ger sitt samtycke, få information om åtminstone vem den personuppgiftsansvarige är, varför personuppgiftsbehandlingen sker, vilken information som samlas in och att den registrerade har en rätt att återkalla sitt samtycke.[133]

Ett samtycke ska vara otvetydigt. I skäl 32 anges att ett samtycke bör ges genom en entydig bekräftande handling, vilket enligt Europeiska dataskyddsstyrelsen innebär att en medveten handling företas för att samtycka till personuppgiftsbehandlingen.[134] Skriftliga eller muntliga förklaringar är exempel på entydigt bekräftande handlingar, likaså att aktivt kryssa i en ruta när en sida på internet besöks.[135] En Facebooksidas ägare kan inte på ett effektivt sätt se till att de registrerade lämnar sitt samtycke skriftligt eller i form av ett kryss i en ruta. Däremot anges i skäl 32 att samtycke också kan lämnas genom ett beteende som i sammanhanget tydligt visar att den registrerade godtar en behandling av sina personuppgifter. Min bedömning är att det är en entydig bekräftande handling när användare på Facebook själva söker kontakt med kommunen, regionen eller myndigheter och på eget bevåg lämnar ut personuppgifter om sig själv.

Det finns en möjlighet att kommuner, regioner och myndigheter kan grunda sina egna publiceringar på samtycke, men möjligheten är inte helt självklar. Om en kommun, region eller myndighet publicerar personuppgifter som rör någon anställd kan det vara tveksamt om samtycke kan användas som laglig grund, eftersom det råder en maktobalans mellan arbetsgivare och arbetstagare.[136] Integritetsskyddsmyndighetens uppfattning är att samtycke inte kan

[130] Europeiska dataskyddsstyrelsen, riktlinjer 05/2020 s. 8–9; Integritetsskyddsmyndigheten, ’Behandling av personuppgifter hos myndigheter’ <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/myndighet/>; prop. 2017/18:105 s. 56.

[131] Se Europeiska dataskyddsstyrelsen, riktlinjer 05/2020 s. 8–9.

[132] Artikel 29-gruppen, WP 259 s. 12.

[133] Artikel 29-gruppen, WP 259 s. 13–14.

[134] Europeiska dataskyddsstyrelsen, riktlinjer 05/2020 s. 18. Jämför C-673/17 *Planet49*.

[135] Europeiska dataskyddsstyrelsen, riktlinjer 05/2020 s. 21–23; skäl 32 dataskyddsförordningen.

[136] Jämför skäl 75 dataskyddsförordningen.

användas för att publicera bilder på anställda på grund av just maktobalans.[137] Europeiska dataskyddsstyrelsen framhäver dock att samtycke kan användas i anställningsförhållanden om det går att visa att samtycket faktiskt ges frivilligt.[138] Här är därför min bedömning att det kan vara riskabelt att använda samtycke som laglig grund, även om det kan finnas ett visst utrymme för det. Om samtycke skulle användas, bör kommunen, regionen eller myndigheten i fråga använda ett samtyckesformulär för att kunna bevisa att den anställda har lämnat ett giltigt samtycke.[139]

Det finns också utrymme att grunda användares publicering av sina egna personuppgifter på samtycke. Min bedömning är att personuppgiftsbehandlingen på Facebook innebär en situation där den registrerade kan samtycka frivilligt. Så länge det finns andra sätt att kontakta kommunen, regionen eller myndigheten i fråga går den registrerade inte miste om något, vilket med utgångspunkt i Europeiska dataskyddsstyrelsens riktlinjer borde innebära att samtycket faktiskt har lämnats frivilligt. Samtycket kan dessutom återkallas genom att Facebookanvändaren tar bort sin kommentar. Det kan dock bli problematiskt att bevisa att det föreligger ett giltigt samtycke, eftersom den som äger en Facebooksida inte kan införa något samtyckesformulär.

Det är enligt min bedömning osannolikt att samtycke kan användas i någon av de andra situationerna som har beskrivits i den här uppsatsen. När en användare publicerar personuppgifter om tredjeman finns det en risk att tredjeman inte har samtyckt till behandlingen (personen kanske inte känner till personuppgiftsbehandlingen överhuvudtaget). Då går det knappast att hävda att sidadministratören har fått samtycke till personuppgiftsbehandlingen på Facebooksidan. Det är enligt min bedömning också problematiskt att grunda upprättandet av sidstatistiken på samtycke. Meta använder inte samtycke som grund för sidstatistiken, utan *berättigat intresse*.[140] Det talar enligt mig starkt för att Facebooksidans ägare inte heller kan hänvisa till samtycke för sidstatistiken.

5.2 Avtal

Enligt artikel 6.1 b dataskyddsförordningen får personuppgifter behandlas om det är nödvändigt för att fullgöra ett avtal som den registrerade är part till eller för att vidta avtalsförberedande åtgärder på begäran av den registrerade. För att stödja en personuppgiftsbehandling på artikel 6.1 b måste personuppgiftsbehandlingen vara nödvändig för att avtalet ska kunna uppfyllas; huvudföremålet i avtalet kan inte fullgöras om personuppgiftsbehandlingen inte äger

[137] Integritetsskyddsmyndigheten, ’Vi guidar dig: Publicera bilder, filmer och ljud på internet’ <https://www.imy.se/verksamhet/dataskydd/vi-guidar-dig/publicera-bilder-filmer-och-ljud-pa-internet/>.

[138] Europeiska dataskyddsstyrelsen, Riktlinjer 05/2020 s. 9–10.

[139] Se Europeiska dataskyddsstyrelsen, riktlinjer 05/2020 s.

[140] Meta, ’Information om rättslig grund’ <https://www.facebook.com/privacy/policy?section_id=18-LegalBasisInformationConsent>.

rum.[141] Exempel på när personuppgiftsbehandling är nödvändig för att fullgöra ett avtal är när personuppgifter behövs för att fullgöra en betalning eller för att leverera en vara.[142]

Enligt min bedömning är avtal inte den mest självklara lagliga grunden för den offentliga sektorns personuppgiftsbehandling på Facebook. För den offentliga sektorns egen publicering har jag svårt att tänka mig en situation där personuppgiftsbehandlingen på Facebooksidan är nödvändig för att fullgöra ett avtal. Möjligen skulle man kunna tänka sig att en kommun, region eller myndighet ingår ett avtal med en enskild om att publicera inlägg om personen i fråga, till exempel för att marknadsföra ett evenemang med personen. Det förutsätter i så fall att det finns ett avtal som går ut på att just marknadsföra sådana inlägg på Facebooksidan. Om avtalet bara går ut på att personen ska vara en del av evenemanget är det knappast nödvändigt för avtalets fullgörelse att publicera inlägg om evenemanget på Facebook. Att publicera inlägg med anställdas personuppgifter går inte heller enligt min bedömning att göra med stöd av artikel 6.1 b dataskyddsförordningen. Det finns ett anställningsavtal, men det är inte nödvändigt för anställningsavtalets fullgörelse att publicera Facebookinlägg om den anställde.

Den lagliga grunden avtal kräver att den registrerade är (eller kommer vara) part till avtalet. Det spelar alltså ingen roll om den personuppgiftsansvarige är part till avtalet eller inte. Eftersom varje Facebookanvändare ingår ett avtal med Meta när de skapar ett Facebookkonto, skulle man kunna hänvisa till det avtalet för de situationer där Facebookanvändare interagerar med den offentliga sektorns Facebooksidor. Man kan dock fråga sig om det är nödvändigt för avtalets fullgörelse att på Facebook publicera personuppgifter om sig själv eller någon annan. Den lagliga grunden avtal bör överhuvudtaget inte kunna användas när en Facebookanvändare publicerar personuppgifter om någon som inte har ett Facebookkonto. Den som uppgifterna avser, alltså den registrerade, har nämligen inget avtal med Meta (eller den offentliga sektorn).

Angående upprättandet av sidstatistiken går det sannolikt inte att stödja personuppgiftsbehandlingen på den lagliga grunden avtal. I Metas integritetspolicy går det att läsa att den lagliga grunden som används för sidstatistiken är berättigat intresse – inte avtal.[143] En möjlig förklaring kan vara att avtalet om att upprätta sidstatistik är mellan Meta och Facebooksidans ägare, det vill säga, den registrerade är inte part till avtalet.

[141] Europeiska dataskyddsstyrelsen, Riktlinjer 2/2019 s. 9–10.
[142] Europeiska dataskyddsstyrelsen, Riktlinjer 2/2019 s. 11.
[143] Se Meta, ’Information om rättslig grund’ <https://www.facebook.com/privacy/policy?section_id=18-LegalBasisInformationConsent>.

5.3 Rättslig förpliktelse

Personuppgiftsbehandling får också ske om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c). Enligt artikel 6.3 ska den rättsliga förpliktelsen fastställas i antingen unionsrätt eller medlemsstaternas nationella rätt. För svensk rätts del framgår det av 2 kap. 1 § dataskyddslagen att den rättsliga förpliktelsen ska följa av lag eller annan författning, kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Inlägg och kommentarer på Facebooksidor som tillhör offentlig sektor aktualiserar flera rättsliga skyldigheter. Det som publiceras på en kommun, en regions eller en myndighets Facebooksida blir allmänna handlingar enligt 2 kap. tryckfrihetsförordningen.[144] Det betyder bland annat att det kan finnas en skyldighet att lämna ut handlingarna enligt samma kapitel och att arkivera handlingarna enligt arkivlagen (1990:782). Den personuppgiftsbehandling som utförs inom ramen för de här skyldigheterna kan stödjas med den lagliga grunden rättslig förpliktelse. Här ska dock hållas isär att det är utlämnandet och arkiveringen som kan (ska) stödjas av rättslig förpliktelse – inte själva publiceringen av inläggen.

Det finns enligt min bedömning ett visst stöd för att kommuner, regioner och myndigheter kan stödja sina egna publiceringar på den lagliga grunden rättslig förpliktelse. De myndigheter som lyder under myndighetsförordningen (2007:515) har nämligen en skyldighet att tillhandahålla information om myndighetens verksamhet (6 § tredje stycket myndighetsförordningen). I förarbetet till myndighetsförordningen går att läsa att myndigheter bör ha en webbplats och att den bör innehålla grundläggande fakta om myndigheten och annan information som medborgarna tycker är intressant.[145] Det skulle möjligen kunna gå att tolka kravet som att det i dagens kontext innebär en rättslig förpliktelse att också finnas på sociala medier – utredningen skrevs år 2004, när användandet av internet såg annorlunda ut. I propositionen till ett annat regelverk – förvaltningslagen (2017:900) – skriver regeringen däremot att skyldigheten enligt 7 § första stycket förvaltningslagen att vara tillgänglig för kontakter inte ska tolkas som en skyldighet att använda sociala medier.[146]

Om de egna publiceringarna kan grundas på rättslig förpliktelse, kan också möjligen publiceringen från andra användare göra det. Att hantera frågor och

[144] För att någonting ska räknas som en allmän handling måste det enligt 2 kap. 4 § tryckfrihetsförordningen röra sig om en handling (2 kap. 3 §), som antingen förvaras hos en myndighet (2 kap. 9 §) eller är upprättad hos den (2 kap. 10 §). Inlägg och kommentarer är handlingar (2 kap. 3 §). När den offentliga sektorn själv publicerar inlägg och kommentarer på sin Facebooksida är handlingarna upprättade hos myndigheten enligt 2 kap. 10 § tryckfrihetsförordningen. Kommentarer från andra användare är inkomna till myndigheten enligt 2 kap. 9 §, eftersom de görs tillgängliga för myndigheten när de publiceras. Se också E-delegationen s. 27–32.

[145] SOU 2004:23 s. 271.

[146] Prop. 2016/17:180 s. 68.

åsikter från medborgarna kan möjligen läsas in i antingen 6 § tredje stycket myndighetsförordningen eller 7 § första stycket förvaltningslagen. Att upprätta sidstatistik kan däremot enligt min bedömning inte grundas på den lagliga grunden rättslig förpliktelse, eftersom upprättandet av sidstatistik inte följer av vare sig unionsrätt eller svensk rätt.

Vid de tillfällen där kommuner, regioner eller myndigheter behöver behandla personuppgifter på sin Facebooksida för att efterleva den registrerades rättigheter enligt dataskyddsförordningen, blir den lagliga grunden rättslig förpliktelse tillämplig. Det följer av att den är en rättslig förpliktelse att efterleva den registrerades rättigheter.

5.4 Vitala intressen

Artikel 6.1 d föreskriver att personuppgiftsbehandling får ske om det är nödvändigt för att skydda intressen som är av grundläggande betydelse (vitala intressen) för den registrerade eller för en annan fysisk person. Den här grunden tar enligt skäl 46 sikte på situationer där personuppgiftsbehandling är avgörande för någons liv. Grunden kan till exempel användas om någon är medvetslös och vårdpersonal behöver kontrollera blodgrupp.[147]

Jag har svårt att tänka mig en situation där en personuppgiftsbehandling på en kommun, en region eller en myndighets Facebooksida skulle vara avgörande för någons liv. Därför nöjer jag mig med att konstatera att den här lagliga grunden sannolikt inte kan användas av den offentliga sektorn på Facebook.

5.5 Myndighetsutövning eller allmänt intresse

Enligt artikel 6.1 e får personuppgiftsbehandling ske om det är nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Det allmänna intresset respektive myndighetsutövningen måste enligt artikel 6.3 komma till uttryck antingen i unionsrätten eller i medlemsstaternas nationella rätt.

5.5.1 Myndighetsutövning

Begreppet myndighetsutövning är i svensk kontext ett uttryck för samhällets maktbefogenheter över medborgarna, vanligen i form av beslut eller andra liknande åtgärder.[148] Myndigheters verksamhet som inte innebär

[147] Integritetsskyddsmyndigheten, ’Skydda grundläggande intressen’ <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/skydda-grundlaggande-intressen/>.

[148] Prop. 2017/18:105 s. 62.

myndighetsutövning faller med andra ord utanför den lagliga grunden myndighetsutövning. Däremot kan förberedande åtgärder sannolikt stödjas av grunden.[149]

Jag kan inte hitta något stöd för att någon personuppgiftsbehandling på den offentliga sektorns Facebooksidor skulle utgöra myndighetsutövning eller förberedelse för myndighetsutövning.[150] Jag konstaterar därför att den offentliga sektorn inte kan hänvisa till myndighetsutövning för personuppgiftsbehandlingen på sina Facebooksidor.

5.5.2 Allmänt intresse

Begreppet allmänt intresse antyder att något ska beröra många människor på ett bredare plan, i motsats till ett enskilt intresse eller ett särintresse.[151] Intresset ska, enligt artikel 6.3, vara fastställt i antingen unionsrätten eller nationell rätt. Av 2 kap. 2 § dataskyddslagen framgår det att det allmänna intresset måste följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. För Sveriges del betraktas alla uppgifter som riksdagen eller regeringen gett i uppdrag till statliga myndigheter som uppgifter av allmänt intresse; om uppgifterna inte vore av allmänt intresse skulle myndigheterna inte ha ålagts att utföra dem.[152] Detsamma gäller de obligatoriska uppgifter som ålagts kommuner och regioner samt verksamheter som kommuner bedriver inom ramen för sina befogenheter inom kommunallagen (2017:725).[153]

Ser man till hur kommuner, regioner och myndigheter själva motiverar sin personuppgiftsbehandling på sociala medier, verkar de typiskt hänvisa till den rättsliga grunden allmänt intresse.[154] Enligt min mening är det en rimlig hänvisning, åtminstone när det gäller den egna publiceringen och det som användare publicerar. Kopplingen till författning finns enligt min uppfattning i myndighetsförordningen eller i förvaltningslagen. Jag ställer mig däremot tveksam till om personuppgiftsbehandlingen inom ramen för sidstatistiken kan stödjas av grunden allmänt intresse; här finns inte samma stöd i författning.

---

[149] Öman, kommentaren till artikel 5, under rubriken ”Led e – Arbetsuppgift av allmänt intresse eller myndighetsutövning”.

[150] En situation som skulle kunna innebära myndighetsutövning på Facebook är om myndigheten meddelar beslut på sin Facebooksida. Den situationen är dock mycket osannolik.

[151] Brinnen, kommentaren till artikel 6; Öman, kommentaren till artikel 5, under rubriken ”Led e – Arbetsuppgift av allmänt intresse eller myndighetsutövning”.

[152] Prop. 2017/18:105 s. 56–57.

[153] Prop. 2017/18:105 s. 56–57.

[154] Se till exempel Landskrona stad, ’Kommunstyrelsens personuppgiftsbehandling’ <https://www.landskrona.se/kommun-och-politik/sa-behandlar-landskrona-stad-personuppgifter/kommunstyrelsens-personuppgiftsbehandling/>; Stockholms stad, ’Behandling av personuppgifter på Stockholms stads sociala medier’ <https://start.stockholm/om-webbplatsen/personuppgifter-och-dataskydd/behandling-av-personuppgifter-pa-stockholms-stads-sociala-medier/>.

5.6 Berättigat intresse (intresseavvägning)

Slutligen kan personuppgiftsbehandling ske om det är nödvändigt för ett ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, under förutsättning att den registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre (artikel 6.1 f). Artikel 29-gruppen anger i sina riktlinjer att det berättigade intresset måste vara godtagbart enligt lagstiftningen, tillräckligt specifikt och verkligt.[155] Direktmarknadsföring och utövande av rätten till yttrandefrihet och information är exempel på berättigade intressen.[156]

Vanligtvis kan organisationer stödja sin personuppgiftsbehandling på sociala medier med den rättsliga grunden berättigat intresse (artikel 6.1 f).[157] Organisationen har i sådana fall ett berättigat intresse av att finnas på sociala medier (till exempel för att marknadsföra sig eller för att svara på frågor) och det intresset väger tyngre än den enskildes intresse att inte få sina personuppgifter behandlade på sociala medier. I artikel 6.1 *in fine* anges dock att grunden berättigat intresse inte kan användas ”för behandling om utförs av offentliga myndigheter när de fullgör sina uppgifter”.[158] Det är inte helt klarlagt vad bestämmelsen omfattar. Enligt artikel 29-gruppen markerar bestämmelsen att myndigheter bara ska behandla personuppgifter i sin myndighetsutövning om de har tillstånd att göra det.[159] Ömans tolkning är att myndigheter kan använda sig av berättigat intresse när de utför sådant som vilken organisation som helst behöver utföra för att kunna fungera, till exempel personaladministration.[160] Även Brinnen anser att myndigheter kan stödja sig på artikel 6.1 f när de agerar utanför sin myndighetsroll, till exempel som arbetsgivare eller avtalspart.[161] Samtidigt verkar regeringen ge uttryck för att personuppgiftsbehandlingen i myndigheternas övriga verksamhet snarare ska grundas på allmänt intresse.[162]

Min tolkning är att den offentliga sektorn förmodligen inte kan grunda sin personuppgiftsbehandling på Facebook på grunden berättigat intresse. Personuppgiftsbehandlingen på Facebook faller förvisso inte under myndighetsutövning, vilket öppnar för att grunden berättigat intresse kan användas. Med tanke på regeringens och Artikel 29-gruppens uttalanden verkar det dock snarare som att personuppgiftsbehandlingen ska grundas på allmänt intresse.

---

[155] Artikel 29-gruppen, WP 217 s. 26–28.

[156] Artikel 29-gruppen, WP 217 s. 26. Se också skäl 47–50 dataskyddsförordningen.

[157] Edmar s. 202.

[158] Se också skäl 47 dataskyddsförordningen.

[159] Artikel 29-gruppen, WP 217 s. 28.

[160] Öman, kommentaren till artikel 5, under rubriken ”Led f – Intresseavvägning”. Jämför dock Sveriges kommuner och regioner, ’Frågor och svar om GDPR’ <https://skr.se/skr/ekonomijuridik/juridik/dataskyddsforordningengdpr/fragorochsvaromgdpr.14973.html>, som bedömer att administrativa åtgärder snarare ska grundas på allmänt intresse.

[161] Brinnen, kommentaren till artikel 5.

[162] Prop. 2017/18:105 s. 56–57.

5.7 Kommentar

Utredningen visar att den lagliga grund som bäst lämpar sig för kommuners, regioners och myndigheters personuppgiftsbehandling på sina Facebooksidor är allmänt intresse. Det finns ett visst utrymme för den offentliga sektorn att grunda sin behandling på samtycke, men det kan bli problematiskt att säkerställa bevisning för att samtyckena har givits frivilligt. Den lagliga grunden avtal fungerar enligt min bedömning inte riktigt att basera personuppgiftsbehandlingen på. De lagliga grunderna vitala intressen och myndighetsutövning går enligt min bedömning överhuvudtaget inte att tillämpa på personuppgiftsbehandlingen på Facebook. Möjligen har kommuner, regioner och myndigheter en möjlighet att hänvisa till berättigat intresse för sin personuppgiftsbehandling, men utredningen tyder på att det är lämpligare att hänvisa till grunden allmänt intresse.

6 Ansvar för den registrerades rättigheter

En genomgående tanke med dataskyddsförordningen är att stärka de registrerades rätt till skydd för personuppgifter.[163] Förordningen förser därför de registrerade med flera rättigheter som ger dem kontroll över sina personuppgifter. Det är den personuppgiftsansvarige som bär ansvaret för att de registrerade ska kunna utöva sina rättigheter.[164] I det här avsnittet utreder jag de olika rättigheternas innebörd och analyserar om kommuner, regioner och myndigheter kan säkerställa att de registrerade kan utöva sina rättigheter.

6.1 Rätt till information

Dataskyddsförordningen vilar på en tanke om att stärka den registrerades ställning genom att ge denne information om hur dennes personuppgifter behandlas.[165] Artiklarna 13 och 14 dataskyddsförordningen ger därför den registrerade rätt att få information om hur den personuppgiftsansvarige behandlar den registrerades personuppgifter. Artikel 12 innehåller krav på att informationen måste vara klar och tydlig. I det här avsnittet utreder och analyserar jag först artikel 13 och 14, och därefter artikel 12.

6.1.1 Artikel 13 och 14: information som ska tillhandahållas

Artikel 13 och 14 innehåller en förteckning över den information som den personuppgiftsansvarige måste tillhandahålla den registrerade. Den personuppgiftsansvarige ska bland annat informera om ändamålet med personuppgiftsbehandlingen, vilka kategorier av personuppgifter som behandlas, hur länge uppgifterna kommer att behandlas, vilka som kommer ta emot personuppgifterna och vilka rättigheter den registrerade har.

Artiklarna är tillämpliga på olika situationer: artikel 13 är tillämplig när personuppgifterna har hämtats direkt från den registrerade, medan artikel 14 är tillämplig när personuppgifterna har hämtats från någon annan källa. Situationer som omfattas av artikel 13 är när den offentliga sektorn själv publicerar personuppgifter och när användare publicerar sina egna personuppgifter. Även personuppgiftsbehandlingen inom ramen för sidstatistiken omfattas av artikel 13. Artikel 29-gruppen anser nämligen att personuppgifter som inhämtas genom att observera någons beteende faller under artikel 13.[166] När en användare publicerar personuppgifter om tredjeman blir istället artikel 14 tillämplig, eftersom personuppgifterna inte har hämtats direkt från den de angår.

För de situationer som omfattas av artikel 13 gäller att den offentliga sektorn ska informera den registrerade direkt när personuppgifterna tas emot (artikel 13.1). Min bedömning är att det kan vara svårt för den offentliga sektorn att

[163] Se till exempel skäl 7 dataskyddsförordningen.
[164] Det framgår uttryckligen av bestämmelserna i dataskyddsförordningens tredje kapitel.
[165] Skäl 7 och skäl 58–60 dataskyddsförordningen.
[166] Artikel 29-gruppen, WP 260 s. 26.

göra det, åtminstone på ett bra sätt. Att informera de personer som förekommer i den offentliga sektorns egna inlägg borde vara enkelt att göra i enlighet med artikeln, men desto svårare blir det att informera i de övriga fallen som omfattas av artikel 13. En lösning kan vara att ha en personuppgiftspolicy som innehåller informationen som listas i artikel 13 synlig på Facebooksidan. En sådan lösning skulle dock inte täcka in situationer där användare får inlägg från myndigheten i sitt flöde, utan att först ha besökt myndighetens Facebooksida. Problemet skulle dock kunna läkas genom att fästa en kommentar som innehåller en länk till personuppgiftspolicyn.[167] Angående sidstatistiken är min bedömning att användarna informeras genom Metas integritetspolicy.[168]

För de situationer som omfattas av artikel 14 ska den offentliga sektorn enligt artikel 14.3 a informera den registrerade om personuppgiftsbehandlingen inom en rimlig tidsperiod efter det att personuppgifterna togs emot, men senast inom en månad. Artikel 14.5 b innehåller dock ett undantag som föreskriver att ingen information behöver ges om det skulle vara omöjligt att ge informationen eller om det skulle medföra en oproportionerlig ansträngning. Undantaget gäller också för situationer där informationsskyldigheten skulle göra det omöjligt eller avsevärt försvåra uppfyllandet av målet med personuppgiftsbehandlingen. Artikel 29-gruppen framhåller att en avvägning ska göras mellan ansträngningen att informera personen och konsekvenserna för den enskilde att inte få informationen.[169]

Möjligen är undantaget i artikel 14.5 b tillämpligt på när användare publicerar uppgifter om andra. Min uppfattning är att det ofta är enkelt – det vill säga inte en oproportionerlig ansträngning – att hitta kontaktuppgifter till berörd tredjeman på Facebook. Samtidigt anser Integritetsskyddsmyndigheten att det normalt sett är oproportionerligt att informera tredje man om dennes okänsliga personuppgifter förekommer i sedvanlig e-postkorrespondens mellan kollegor och i andra vardagliga meddelanden.[170] Min bedömning är därför att tredjeman sannolikt inte behöver informeras om personuppgifterna är okänsliga. Rör det sig om känsliga uppgifter bör tredjeman enligt min bedömning däremot informeras.

6.1.2 Artikel 12: klar och tydlig information

Informationen som ska ges i enlighet med artikel 13 och 14 måste enligt artikel 12.1 vara koncis, klar, tydlig, begriplig och lätt tillgänglig. Artikeln är särskilt sammankopplad med öppenhetsprincipen.

[167] Jämför Artikel 29-gruppen, WP 260 s. 8 och 19.
[168] Se Meta, ’Integritetspolicy’ <https://www.facebook.com/privacy/policy>.
[169] Artikel 29-gruppen, WP 260 s. 31.
[170] Integritetsskyddsmyndigheten, ’Personuppgifter i e-post’ <www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/personuppgifter-i-e-post/>.

Ett effektivt sätt att efterleva artikel 12.1 är att använda sig av *klarspråk*.[171] Klarspråk innebär att skriva på ett sätt som är vårdat, enkelt och begripligt, det vill säga korrekt, utan komplicerad meningsbyggnad samt målgruppsanpassat.[172] Artikelns krav på klar, koncis, tydlig och begriplig information kan nås genom att skriva vårdat, enkelt och begripligt.[173]

6.2 Rätt till tillgång

Den personuppgiftsansvarige ansvarar enligt artikel 15 dataskyddsförordningen för att, på begäran av en registrerad, ge denne bekräftelse på huruvida personuppgifter om den registrerade behandlas. Enligt samma artikel ska den personuppgiftsansvarige också ge den registrerade tillgång till personuppgifterna som behandlas och information om bland annat varför uppgifterna behandlas, vem som behandlar dem och vilka rättigheter den registrerade har. Om personuppgifterna överförs till tredjeland ska den personuppgiftsansvarige också lämna information om de lämpliga skyddsåtgärder enligt artikel 46 som har vidtagits. Rätten till tillgång syftar enligt skäl 63 till att den registrerade ska kunna kontrollera om personuppgiftsbehandlingen är laglig.

Kommunen, regionen eller myndigheten bör enligt min mening utan större problem kunna efterleva skyldigheten att ge bekräftelse på behandlingen och skyldigheten att lämna den information som listas i artikel 15. Däremot kan det vara svårare att ge den registrerade tillgång till personuppgifterna. Facebook har en funktion när man som enskild användare kan få kopior på sina personuppgifter men funktionen är inte anpassad efter att ägare av Facebooksidor ska kunna få kopior av personuppgifter kopplade till andra användare. I dagsläget skulle kommunen, regionen eller myndigheten manuellt behöva inventera och kopiera de personuppgifter som har begärts ut. Dataskyddsförordningen gör inga undantag för situationer där det skulle vara en oproportionerlig ansträngning att ge ut personuppgifterna. Det kan alltså innebära mycket arbete för den offentliga sektorn att se till att rätten till tillgång kan efterlevas. Det ska också uppmärksammas att sidadministratören inte har tillgång till de personuppgifter som ligger till grunden för sidstatistiken. Det innebär sammantaget att rätten till tillgång kan uppfyllas med en större arbetsinsats för det som sidadministratören själv publicerar och för det som användare publicerar, men inte för sidstatistiken.

6.3 Rätt till rättelse

Personuppgifterna som behandlas ska vara riktiga enligt principen om korrekthet (artikel 5.1 d dataskyddsförordningen). Den registrerade har därför enligt artikel 16 rätt att få felaktiga personuppgifter rättade av den

[171] Jämför Rydzewska-Siemiątkowska s. 1015.
[172] Prop. 2008/09:153 s. 31. Se också 11 § språklagen (2009:600).
[173] Artikel 29-gruppen, WP 260 s. 7–9.

personuppgiftsansvarige. Enligt samma artikel har den registrerade också rätt att komplettera ofullständiga personuppgifter.

Enligt principen om riktighet måste den personuppgiftsansvarige se till att personuppgifterna som behandlas är korrekta och om nödvändigt uppdaterade. Om den personuppgiftsansvarige får reda på att vissa personuppgifter är felaktiga i förhållande till varför de behandlas, måste den personuppgiftsansvarige självmant rätta uppgifterna även om den registrerade inte har utövat sin rätt enligt artikel 16.[174]

Den som administrerar en Facebooksida kan redigera sina egna inlägg. Det innebär att kommuner, regioner och myndigheter kan efterleva rätten till rättelse om de felaktiga personuppgifterna förekommer i deras egna inlägg. Däremot kan sidadministratören inte redigera andras inlägg och kommentarer – bara radera dem. Skulle personuppgifter som förekommer i användares kommentarer behöva rättas, kan sidadministratören inte se till att så sker.

6.4 Rätt till radering

Under vissa förutsättningar har den registrerade rätt att få sina personuppgifter raderade av den personuppgiftsansvarige (artikel 17 dataskyddsförordningen). I artikel 17.1 listas fem situationer som innebär att den registrerade har rätt att få sina personuppgifter raderade:

Inledningsvis ska personuppgifter enligt artikel 17.1 a raderas om de inte längre behövs i förhållande till varför de behandlades. Den här punkten är en konsekvens av principen om uppgiftsminimering (artikel 5.1 c) och principen om lagringsminimering (artikel 5.1 d); när en personuppgift inte längre behövs för sitt ändamål, ska den raderas.[175] Vidare har den registrerade alltid rätt att återkalla sitt samtycke (artikel 7.3). Om den registrerade gör det, och det inte finns någon annan laglig grund för att behandla personuppgifterna, är den personuppgiftsansvarige skyldig att radera uppgifterna enligt artikel 17.1 b. En tredje situation som kräver radering är om den registrerade nyttjar sin rätt att invända mot personuppgiftsbehandlingen (se avsnitt 6.7). Om behandlingen inte kan stödjas av någon annan laglig grund, måste den personuppgiftsansvarige enligt artikel 17.1 c radera uppgifterna. En fjärde situation som kräver radering är om personuppgiftsbehandlingen är olaglig (artikel 17.1 d). En personuppgiftsbehandling är olaglig om det till exempel saknas en giltig laglig grund eller om den registrerade inte har fått information enligt artiklarna 13 och 14 dataskyddsförordningen.[176] Slutligen föreligger en rätt till radering om det finns en rättslig förpliktelse för den personuppgiftsansvarige att radera en personuppgift (artikel 17.1 e). Det kan avse en skyldighet enligt

[174] Brinnen, kommentaren till artikel 16.
[175] Brinnen, kommentaren till artikel 17.
[176] Se Brinnen, kommentaren till artikel 17.

dataskyddsförordningen men också skyldigheter som kommer av andra föreskrifter. Gallringsföreskrifter är ett sådant exempel.[177]

Under vissa förutsättningar gäller inte rätten till radering, trots att någon av situationerna föreligger. Enligt artikel 17.3 gäller inte rätten till radering i den utsträckning som behandlingen är nödvändig för att utöva rätten till yttrandefrihet och informationsfrihet, uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller utföra en uppgifts om är ett led i myndighetsutövning. Rätten till radering gäller enligt artikeln inte heller personuppgiftsbehandling som utförs med statistiska ändamål.

Rätten till radering ställer enligt min mening höga krav på att kommunen, regionen eller myndigheten förstår under vilka förutsättningar rättigheten föreligger. Den offentliga sektorn behöver ha en god förståelse för personuppgiftsbehandlingen och en god förståelse för annan tillämplig lagstiftning, annars finns det en risk att artikel 17 inte tillämpas korrekt. Det kan bli särskilt viktigt med tanke på att inlägg och kommentarer på Facebook blir allmänna handlingar, och att det beroende på arkiverings- och gallringsföreskrifter kan det finnas en rättslig skyldighet för kommunen, regionen eller myndigheten att bevara handlingen. I sådana situationer gäller inte rätten till radering.

Min bedömning är annars att den offentliga sektorn borde kunna se till att rätten till radering kan efterlevas. Den som administrerar en Facebooksida har möjlighet att radera inlägg och kommentarer som publiceras på Facebooksidan, vilket innebär att kommunen, regionen eller myndigheten har en faktisk möjlighet att radera uppgifterna. Den som administrerar en Facebooksida har dock ingen möjlighet att radera personuppgifter som används för att upprätta sidstatistiken, men med tanke på att den personuppgiftsbehandlingen sker i statistiska ändamål gäller inte rätten till radering (artikel 17.3). Det ska dock noteras att administratören är helt beroende av att Meta har byggt plattformen på ett sätt som gör att uppgifterna verkligen raderas permanent. Om personuppgifterna sparas kan inte rätten till radering efterlevas.

6.5 Rätt till begränsning av behandling

Under vissa förutsättningar kan den registrerade begära av den personuppgiftsansvarige att personuppgiftsbehandlingen begränsas (artikel 18 dataskyddsförordningen). Begränsning av behandling innebär enligt definitionen i artikel 4.3 att markera lagrade personuppgifter med syftet att begränsa behandlingen av personuppgifterna i framtiden. Rättigheten kan enligt artikel 18.1 bara krävas följande situationer: när personuppgifternas korrekthet bestrids, när den registrerade kan krävs radering men istället vill att behandlingen ska begränsas, när personuppgifterna inte längre behövs för sitt

[177] Öman, kommentaren till artikel 17, under rubriken ”Första punkten – när det finns skyldighet att radera”.

ursprungliga syfte men behövs av juridiska skäl, och när den registrerade har invänt mot personuppgiftsbehandlingen och väntar på avgörande.

I skäl 67 räknas exempel upp på hur personuppgiftsbehandling kan begränsas. Här anges bland annat att uppgifterna kan flyttas till ett annat databehandlingssystem eller att offentliggjorda uppgifter på en webbplats avlägsnas. Om en registrerad skulle begära begränsning av personuppgifter som den offentliga sektorn behandlar på sin Facebooksida är min bedömning att begränsningen kan genomföras genom att inlägget där personuppgifterna förekommer görs privat. Den offentliga sektorn har dock, enligt min uppfattning, ingen möjlighet att begränsa personuppgiftsbehandlingen som sker inom ramen för användares publicering och inom ramen för sidstatistiken.

6.6 Rätt till dataportabilitet

Dataskyddsförordningen syftar inte bara till att stärka de enskildas rätt till privatliv. Förordningen syftar också till att säkerställa en god konkurrens.[178] Rätten till dataportabilitet är en produkt av det senare syftet.[179] Enligt artikel 20 har den registrerade rätt att få ut sina personuppgifter i ett strukturerat, allmänt använt och maskininläsbart format för att kunna överföra dem till en annan personuppgiftsansvarig.[180] Rättigheten gäller dock bara automatiserad behandling som grundar sig på antingen samtycke eller avtal, och förutsätter att personuppgifterna har hämtats direkt från den registrerade.

Eftersom rätten till dataportabilitet är begränsad till att gälla bara för vissa lagliga grunder, är sannolikheten att den kan krävas begränsad när det gäller den offentliga sektorns användning av Facebook. Vid tillfällen där rättigheten eventuellt föreligger är min bedömning att det blir svårt för kommuner, regioner och myndigheter att efterleva rätten till dataportabilitet. Facebook saknar nämligen en funktion som gör det möjligt för en sidadministratör att få användares personuppgifter som behandlas på Facebooksidan. Kommunen, regionen eller myndigheten i fråga behöver på egen hand identifiera vilka personuppgifter som faller inom rättigheten och se till att de hamnar i ett enligt artikeln godkänt filformat. Det kan vara utmanande, men bör vara möjligt.

6.7 Rätt att göra invändningar

Enligt artikel 21 dataskyddsförordningen har den registrerade rätt att invända mot att dennes personuppgifter behandlas. Rättigheten gäller bara i de situationer där personuppgiftsbehandlingen grundas på allmänt intresse eller myndighetsutövning (artikel 6.1 e) eller på berättigat intresse (artikel 6.1 f). Invändningen ska ske av skäl som hänför sig till den registrerades specifika

[178] Skäl 9 dataskyddsförordningen.

[179] Se Wong och Henderson s. 177.

[180] Exempel på allmänt använda och maskininläsbara format är enligt Öman pdf-filer, text-filer, jpeg-filer och mp3-filer, se Öman, kommentaren till artikel 20, under rubriken ”Första punkten – När det finns rätt till dataportabilitet”.

situation. Den personuppgiftsansvarige ska upphöra med personuppgiftsbehandlingen, om inte denne kan visa att det finns avgörande berättigade skäl för behandlingen och att dessa skäl väger tyngre än den registrerades intressen, rättigheter och friheter. Den personuppgiftsansvarige kan också fortsätta behandla personuppgifterna om behandlingen sker för att fastställa, utöva eller försvara rättsliga anspråk.

Som jag redogjort för i avsnitt 5.5.2 kan den offentliga sektorn grunda sin personuppgiftsbehandling på artikel 6.1 e dataskyddsförordningen (allmänt intresse). Det innebär att den registrerade alltså har en möjlighet att utöva rätten att göra invändningar mot personuppgiftsbehandlingen. Personuppgiftsansvaret är uppfyllt bara den personuppgiftsansvarige prövar rättigheten och agerar efter utfallet. Den offentliga sektorn måste enligt artikeln ha ett *avgörande berättigat skäl* för att få fortsätta med personuppgiftsbehandlingen. Enligt Europeiska dataskyddsstyrelsen bör de grunder som räknas upp i artikel 17.3 dataskyddsförordningen kunna åberopas som avgörande berättigade skäl.[181] Det är dock svårt att uttala sig om ett sådant intresse skulle väga tyngre än den registrerades.[182] Eftersom den registrerade ska hänvisa till skäl som hänför sig till den registrerades specifika situation, är den registrerades intresse olikt i varje enskilt fall.

6.8 Kommentar

Utredningen visar att kommuner, regioner och myndigheter i flera fall kan se till att de registrerades rättigheter efterlevs. Rätten till information, rätten till radering och rätten att göra invändningar kan genomföras utan större problem i de flesta fall. Rätten till tillgång och rätten till dataportabilitet kan med en arbetsinsats uppfyllas för det som kommunen, regionen eller myndigheten själv publicerar och för det som användare publicerar – Facebook saknar en funktion där en administratör kan få fram personuppgifterna automatiskt, vilket innebär att det krävs manuellt arbete.

Utredningen visar också att kommuner, regioner och myndigheter som driver Facebooksidor i många fall inte kan se till att de registrerade kan utöva sina rättigheter. En Facebooksidas administratör kan inte redigera inlägg från användare – bara radera dem – vilket innebär att rätten till rättelse inte kan efterlevas. Inte heller kan administratören begränsa personuppgiftsbehandlingen som sker när användare tillför Facebooksidan personuppgifter. Särskilt vad gäller sidstatistiken kan en Facebooksidas administratör inte alls säkerställa att rättigheterna efterlevs. Det beror på att sidadministratören inte har den kontroll över de berörda personuppgifterna och över Facebook som Meta har.

[181] Europeiska dataskyddsstyrelsen, Riktlinjer 5/2019 s. 9. Se också C-131/12 *Google Spain*.

[182] Se Öman, kommentaren till artikel 21, under rubriken ”Första punkten – Generell rätt att göra invändningar”.

7 Övriga relevanta skyldigheter

Utöver att ansvara för att säkerställa principerna följs och för att den registrerade kan utöva sina rättigheter, har den personuppgiftsansvarige andra skyldigheter enligt dataskyddsförordningen. I det här avsnittet utreder och analyserar jag några av de övriga skyldigheter som jag finner relevanta för den offentliga sektorns personuppgiftsbehandling på Facebook. I tur och ordning utreder och analyserar jag skyldigheten att föra register, skyldigheten att göra en konsekvensbedömning, skyldigheterna relaterade till personuppgiftsincidenter och skyldigheterna relaterade till överföring av personuppgifter till tredjeland.

7.1 Föra register

En förutsättning att följa dataskyddsförordningen är att ha koll över den personuppgiftsbehandling som sker inom verksamheten. [183] Den personuppgiftsansvarige är därför i de flesta fall skyldig att föra register över personuppgiftsbehandlingen enligt artikel 30.[184] I registret ska den personuppgiftsansvarige bland annat uppge namn och kontaktuppgifter för den personuppgiftsansvarige, ändamålen med behandlingen, en beskrivning av kategorierna av registrerade, en beskrivning av kategorierna av personuppgifter, kategorier av mottagare och överföringar till tredjeland. Om det är möjligt ska registret även innehålla de förutsedda tidsfristerna för radering och en beskrivning av de säkerhetsåtgärder som avses i artikel 32.1 dataskyddsförordningen.

Den offentliga sektorn behöver med andra ord se till att registret som förs också tar hänsyn till den personuppgiftsbehandling som sker på Facebooksidan. Min bedömning är att det inte är en enkel uppgift att upprätta ett helt korrekt register, med hänvisning till att jag tidigare bedömt att det inte går att fastställa med säkerhet om det föreligger ett gemensamt personuppgiftsansvar på Facebooksidan eller inte. Brinnen uppmärksammar att ett register enligt artikel 30 inte behöver innehålla en förteckning över vilken rättslig grund som används för varje behandling.[185] Mitt förslag är att den offentliga sektorn utökar sina register med att också innehålla en förteckning över de rättsliga grunder som används vid varje behandling, för att på så vis enklare säkerställa att det faktiskt finns en laglig grund för behandlingen. Om det är tydligt vilken rättslig grund som finns för behandlingen blir det också lättare att utöva den registrerades rättigheter.

[183] Brinnen, kommentaren till artikel 30.
[184] Undantag från skyldigheten att föra register finns i artikel 30.5 dataskyddsförordningen.
[185] Brinnen, kommentaren till artikel 30.

7.2 Konsekvensbedömning

Om en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utföra en konsekvensbedömning. Den här skyldigheten, och vad konsekvensbedömningen ska innehålla, framgår av artikel 35 dataskyddsförordningen. Om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk måste den personuppgiftsansvarige också samråda med tillsynsmyndigheten innan behandlingen påbörjas (artikel 36).

Artikel 29-gruppen har utarbetat nio kriterier för att avgöra om en personuppgiftsbehandling sannolikt leder till en hög risk. Om två av de nio kriterierna uppfylls ska enligt Artikel 29-gruppen en konsekvensbedömning utföras.[186] Enligt min bedömning finns det en möjlighet att den offentliga sektorns personuppgiftsbehandling på Facebook träffas av åtminstone ett kriterium, nämligen personuppgiftsbehandling i stor omfattning. Det finns ingen definition av vad som anses vara personuppgiftsbehandling i stor omfattning. Enligt Artikel 29-gruppen ska hänsyn tas till antalet registrerade som berörs, mängden uppgifter, behandlingens varaktighet och behandlingens geografiska omfattning.[187] Beroende på en Facebooksidas spridning och popularitet är min uppfattning att förhållandevis många kan beröras – när den här uppsatsen skrivs har till exempel Skatteverkets Facebooksida 100 000 följande.[188] I jämförelse nämner Artikel 29-gruppen att journalföring på ett sjukhus kan vara ett exempel på personuppgiftsbehandling i stor omfattning.[189]

Det finns enligt min uppfattning en möjlighet att den offentliga sektorns personuppgiftsbehandling på Facebook också träffas av ytterligare ett kriterium: uppgifter som rör sårbara registrerade. Sårbara registrerade är personer som befinner sig i en maktobalans i förhållande till den personuppgiftsansvarige. Typiska exempel är barn och anställda.[190] Det är svårt att avgöra om alla registrerade alltid är sårbara i förhållande till myndigheter, eller om de bara är sårbara när myndighetsutövning aktualiseras.

Sammantaget är min bedömning att det är svårt att entydigt säga om den offentliga sektorn behöver göra en konsekvensbedömning inför sin användning av Facebook. För att ta det säkra före det osäkra är det kanske att rekommendera att en konsekvensbedömning genomförs även om den inte krävs enligt

[186] Se Artikel 29-gruppen, WP 248 s.10–12. De nio kriterierna är: 1) utvärdering eller poängsättning, 2) automatiskt beslutsfattande med rättsliga eller liknande betydande följder, 3) systematisk övervakning, 4) känsliga uppgifter eller uppgifter av mycket personlig karaktär, 5) uppgifter som behandlas i stor omfattning, 6) matchande eller kombinerande uppgiftsserier, 7) uppgifter som rör sårbara registrerade, 8) innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar, och 9) behandlingen hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal.

[187] Artikel 29-gruppen, WP 248 s. 11. Jämför skäl 91 dataskyddsförordningen.

[188] Se Skatteverket, 'Skatteverket' <https://www.facebook.com/skatteverketdeklarera>.

[189] Artikel 29-gruppen, WP 243 s. 10.

[190] Artikel 29-gruppen, WP 248 s. 11–12.

dataskyddsförordningen. Om det visar sig att en konsekvensbedömning hade behövts men inte genomförts kan det medföra administrativa sanktionsavgifter enligt artikel 83.4.

7.3 Personuppgiftsincidenter

Om en personuppgift, på grund av en säkerhetsincident, oavsiktligt eller olagligt förstörs, förloras eller ändras, eller om någon obehörigen får åtkomst till den, har en personuppgiftsincident skett (artikel 4.12 dataskyddsförordningen). Den personuppgiftsansvarige har en skyldighet att dokumentera personuppgiftsincidenter (artikel 33.5) och i vissa fall också anmäla dem till Integritetsskyddsmyndigheten och informera den registrerade. Närmare bestämt ska anmälan till Integritetsskyddsmyndigheten ske om det är sannolikt att personuppgiftsincidenten medför en risk för en enskild persons rättigheter och friheter (artikel 33.1). Om risken är hög ska även den registrerade som huvudregel informeras (artikel 34). Den personuppgiftsansvarige måste dessutom agera snabbt; om incidenten ska anmälas måste det göras inom 72 timmar från det att incidenten upptäcktes[191] (artikel 33.1), och om den registrerade ska informeras ska det göras utan onödigt dröjsmål (artikel 34.1).

Det kan vara svårt att hålla isär när en personuppgiftsincident ska dokumenteras, anmälas och informeras om. Enligt min mening är dataskyddsförordningen komplicerat skriven i de här delarna, och det kan därför vara svårt för den som driver en Facebooksida att hålla isär när en personuppgift ska dokumenteras, när den ska anmälas och när den registrerade ska få information om den. Det här ställer krav på att det antingen finns tydlig information för medarbetarna om vilka åtgärder som ska vidtas vid en personuppgiftsincident, eller att det finns någon på arbetsplatsen som är väl införstådd med vad som gäller vid personuppgiftsincidenter. Integritetsskyddsmyndigheten har dock en e-tjänst som gör den som anmäler en personuppgiftsincident uppmärksam på om incidenten i fråga behöver dokumenteras, anmälas och/eller informeras om.[192] Min bedömning är därför att det kan bli enklare för den offentliga sektorn att efterleva sina skyldigheter vid personuppgiftsincidenter om Integritetsskyddsmyndighetens e-tjänst används.

[191] Enligt Artikel 29-gruppen har den personuppgiftsansvarige fått vetskap om en incident så fort den personuppgiftsansvarige är rimligt säker på att en incident har ägt rum, Artikel 29-gruppen, WP 250 s. 11.

[192] Se Integritetsskyddsmyndigheten, ’Ny anmälan’ <https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/risk-for-registrerade/>.

7.4 Tredjelandsöverföringar

Dataskyddsförordningen syftar till att säkerställa ett enhetligt och starkt skydd för personuppgifter inom EU.[193] För att dataskyddsförordningens skydd inte ska undergrävas är det därför som utgångspunkt otillåtet att föra över personuppgifter till ett land utanför unionen (artikel 44).[194] Överföring till tredjeland får bara ske om det finns garantier för att dataskyddet i det andra landet lever upp till samma standard. Artikel 44 föreskriver närmare bestämt att den personuppgiftsansvarige måste säkerställa att någon av de *överföringsmekanismer* i kapitel fem dataskyddsförordningen föreligger om personuppgifter ska överföras till tredjeland. Överföring till tredjeland får ske om det föreligger ett beslut om adekvat skyddsnivå (artikel 45), om överföringen omfattas av lämpliga skyddsåtgärder (artikel 46) eller om det finns bindande företagsbestämmelser (artikel 47). Undantagsvis kan personuppgifter föras över till tredjeland i enlighet med de krav som föreskrivs i artikel 49.

När någon driver en Facebooksida finns det en sannolikhet att det kommer ske en överföring av personuppgifterna till tredje land. Meta har nämligen majoriteten av sina servrar i USA.[195] Under en längre tid har överföringar till USA varit problematiska. Genom åren har Europeiska kommissionen fattat två adekvansbeslut som båda har underkänts av EU-domstolen.[196] I juli 2023 fattade Europeiska kommissionen ett adekvansbeslut som återigen möjliggör överföringar till USA. [197] Adekvansbeslutet innebär att överföringar kan ske till de organisationer som har anslutit sig till ramverket *Data Privacy Framework*. Meta Platforms Incorporated är en av de organisationer som har anslutit sig till ramverket.[198] När den här uppsatsen skrivs (våren 2024) föreligger alltså förutsättningar för att föra över personuppgifter till USA. Den offentliga sektorn kan med andra ord fullgöra sitt personuppgiftsansvar vad gäller överföringar till tredjeland. Med tanke på historiken är dock min bedömning att kommuner, regioner och myndigheter bör ha en plan för om EU-domstolen underkänner Data Privacy Framework.

[193] Se särskilt skäl 2, 9 och 10 dataskyddsförordningen.

[194] Skäl 101 dataskyddsförordningen.

[195] Meta, ’Meta Data Centers’ <https://datacenters.atmeta.com/>.

[196] I rättsfallet C-362/14 *Schrems I* underkändes det första adekvansbeslutet: Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (2000/520/EG). I rättsfallet C-311/18 *Schrems II* underkändes det andra adekvansbeslutet: Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

[197] Kommissionens genomförandebeslut (EU) 2023/1795 av den 10 juli 2023 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter enligt ramen för dataskydd mellan EU och Förenta staterna.

[198] Se International Trade Administration, ’Data Privacy Framework List’, <https://www.dataprivacyframework.gov/list>.

8 Särskilda skyldigheter vid gemensamt personuppgiftsansvar

Den som är gemensamt personuppgiftsansvarig har inte bara samma ansvar som någon som är ensamt personuppgiftsansvarig, utan också ett särskilt ansvar enligt artikel 26 dataskyddsförordningen: De gemensamt personuppgiftsansvariga ska fastställa sitt respektive ansvar för att fullgöra sina skyldigheter enligt dataskyddsförordningen. Att inte fastställa sitt respektive ansvar enligt artikeln kan leda till administrativa sanktionsavgifter enligt artikel 83.4.

I det här avsnittet utreder och analyserar jag först skyldigheten att fastställa respektive ansvar i ett inbördes arrangemang, och sedan ansvaret för att se till att de registrerade kan utöva sina rättigheter.

8.1 Fastställa respektive ansvar i inbördes arrangemang

Enligt artikel 26.1 dataskyddsförordningen ska gemensamt personuppgiftsansvariga under öppna former fastställa sitt respektive ansvar att fullgöra sina skyldigheter enligt dataskyddsförordningen. De gemensamt personuppgiftsansvariga ska alltså bestämma vem som ska utföra vilka uppgifter som säkerställer att personuppgiftsbehandlingen följer dataskyddsförordningen. Av artikeln framgår att det är särskilt viktigt att de gemensamt personuppgiftsansvariga fastställer sitt respektive ansvar angående de registrerades rättigheter och skyldigheten att informera de registrerade om personuppgiftsbehandlingen. Artikel 26.2 föreskriver att arrangemanget ska återspegla verkligheten.[199] Enligt Europeiska dataskyddsstyrelsen innebär det att om bara en av de personuppgiftsansvariga har kontakt med den registrerade, så bör den aktören få ansvaret att tillhandahålla de registrerade information och besvara deras förfrågningar.[200]

De gemensamt personuppgiftsansvariga kan enligt artikel 26.1 utse en gemensam kontaktpunkt för den registrerade. Att göra det är frivilligt men rekommenderas av Europeiska dataskyddsstyrelsen. Det underlättar nämligen dels för den registrerade att utöva sina rättigheter, dels för de personuppgiftsansvariga att samordna sina relationer och sin kommunikation gentemot den registrerade.[201]

De gemensamt personuppgiftsansvariga måste se till att hela den gemensamma behandlingen sker i enlighet med dataskyddsförordningen.[202] När gemensamt personuppgiftsansvariga fastställer sina respektive ansvarsområden ska de därför, bland annat, beakta implementeringen av dataskyddsprinciperna, säkerhetsnivån för personuppgifterna, överföring av uppgifter till

[199] Jämför C-210/16 *Wirtschaftsakademie* p. 43; C-40/17 *Fashion ID* p. 70.
[200] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 51.
[201] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 51.
[202] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 48.

tredje land och hur kontakt ska skötas med registrerade och tillsynsmyndigheter.[203] De gemensamt personuppgiftsansvariga behöver ha varsin lagliga grund för personuppgiftsbehandlingen – den ena personuppgiftsansvarige kan inte förlita sig på den andras lagliga grund.[204]

Fastställandet av varje parts respektive ansvar ska enligt artikel 26.1 göras genom ett *inbördes arrangemang*. Dataskyddsförordningen specificerar inte vad som menas med ett inbördes arrangemang. Enligt Europeiska dataskyddsstyrelsen står det de gemensamt personuppgiftsansvariga fritt att komma överens om den juridiska formen för det inbördes arrangemanget. Samtidigt skriver dataskyddsstyrelsen att arrangemanget är bindande för de gemensamt personuppgiftsansvariga och att styrelsen därför rekommenderar att överenskommelsen görs i form av ett bindande dokument, till exempel ett avtal (kontrakt). När arrangemanget finns i formen av ett avtal blir det dessutom, enligt Europeiska dataskyddsstyrelsen, enklare för de personuppgiftsansvariga att kräva ansvar av varandra om överenskommelsen inte följs. Avtalen kan även användas för att visa att de gemensamt personuppgiftsansvariga uppfyller sina skyldigheter enligt dataskyddsförordningen.[205]

Det *väsentliga innehållet* i det inbördes arrangemanget ska enligt artikel 26.2 göras tillgängligt för den registrerade. Enligt Europeiska dataskyddsstyrelsen omfattar det den information som de personuppgiftsansvariga ska informera den registrerade om enligt artiklarna 13 och 14 dataskyddsförordningen. [206] Det innebär information om bland annat vilka de personuppgiftsansvariga är, varför personuppgifterna behandlas, vilken laglig grund som behandlingen stödjer sig på och vilka rättigheter den registrerade har. Arrangemanget bör dessutom, enligt Europeiska dataskyddsstyrelsen, specificera vilken gemensam personuppgiftsansvarig som ansvarar för att säkerställa överensstämmelse med vad.[207] En gemensam kontaktpunkt omfattas enligt dataskyddsstyrelsen av det väsentliga i arrangemanget.[208]

Det saknas närmare ledning av vad *tillgängligt för den registrerade* innebär. Europeiska dataskyddsstyrelsen anser att det är upp till de gemensamt personuppgiftsansvariga att själva besluta om vilket sätt som är mest effektivt. I doktrinen argumenteras för att kriteriet är uppfyllt om det väsentliga i arrangemanget återges i användarvillkor eller i en integritetspolicy.[209]

---

[203] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 48–49.

[204] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 49. Jämför C-40/17 *Fashion ID* p. 70.

[205] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 49–50. Se också Öman, kommentaren till artikel 26, under rubriken ”Första punkten – inbördes fastställda skyldigheter”.

[206] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 51.

[207] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 51.

[208] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 51.

[209] Kamarinou, Millard och Turton s. 302; Öman, kommentaren till artikel 26, under rubriken ”Andra punkten – De personuppgiftsansvarigas roller gentemot den registrerade”.

På Facebook görs arrangemanget i form av ett tillägg till Facebooks användarvillkor.[210] Innehållet i arrangemanget går inte att förhandla eller på något annat sätt ändra. I tillägget anger Meta att företaget har ansvaret för att uppfylla de tillämpliga skyldigheterna i dataskyddsförordningen för behandling av sidstatistiken. Som exempel anges artiklarna 12, 13, 15–21, 33 och 34.[211] Meta anger också att sidadministratören ”bör se till” att den också har en laglig grund för behandling av sidstatistiken, och att sidadministratören ska identifiera sin egen rättsliga grund, sina personuppgiftsansvariga och deras kontaktuppgifter samt kontaktuppgifter till eventuellt dataskyddsombud.[212] I tillägget anger Meta att det uppfyller kravet i artikel 26.2 dataskyddsförordningen genom att ha publicerat tillägget offentligt på internet.[213]

Wendleby och Wetterberg anser att det är problematiskt att arrangemanget upprättas ensidigt från Metas håll med hänsyn till dataskyddsförordningens genomgående krav på att den personuppgiftsansvarige ska ha kontroll och bestämma över personuppgiftsbehandlingen.[214] Jag kan ansluta mig till deras uppfattning. Samtidigt är min bedömning att Metas arrangemang uppfyller kraven i dataskyddsförordningen. Tillägget om sidstatistik tydliggör att skyldigheterna att följa dataskyddsförordningen fördelas så att ansvaret för de flesta skyldigheterna läggs på Meta. Här förtydligas också att Meta bär ansvaret att informera de registrerade och ansvaret att se till att den registrerade kan utöva sina rättigheter – kraven i artikel 2.6 uppfylls alltså.

Vidare bedömer jag att ansvarsfördelningen motsvarar verkligheten. Som jag anför i kapitel 6 i den här uppsatsen är det inte möjligt för en Facebooksidas administratör att se till att den registrerade kan utöva sina rättigheter inom ramen för sidstatistiken – det är det bara Meta som kan göra. I enlighet med rättsläget uppmärksammar Meta sidadministratören på att denne på egen hand behöver säkerställa en laglig grund för sin behandling. Arrangemanget finns dessutom nedskrivet på en webbsida. Det innebär dels att parterna har en konkret överenskommelse att hänvisa till, dels att arrangemanget görs tillgängligt för den registrerade. Kraven på det gemensamma arrangemanget är därför enligt min bedömning uppfyllda, åtminstone inom ramen för sidstatistiken. Om det skulle visa sig att gemensamt personuppgiftsansvar också föreligger i andra situationer, behövs det ytterligare arrangemang.

---

[210] Meta, ’Information om sidstatistik’ <https://www.facebook.com/legal/terms/page_controller_addendum/>.

[211] I korthet: klar och tydlig information (artikel 12), information som ska tillhandahållas om personuppgifterna samlas in från den registrerade (artikel 13), den registrerades rättigheter (artiklarna 15–21), anmälan av personuppgiftincidenter (artikel 33) och information till den registrerade om en personuppgiftsincident (artikel 34).

[212] Meta, ’Information om sidstatistik’ <https://www.facebook.com/legal/terms/page_controller_addendum/>.

[213] Meta, ’Information om sidstatistik’ <https://www.facebook.com/legal/terms/page_controller_addendum/>.

[214] Wendleby och Wetterberg s. 175.

8.2 Ansvaret för de registrerades rättigheter

De gemensamt personuppgiftsansvariga ska, enligt artikel 26.1 dataskyddsförordningen, fastställa sitt respektive ansvar att se till att de registrerade kan utöva sina rättigheter. Enligt samma artikel kan de också utse en gemensam kontaktpunkt som den registrerade kan vända sig till för att utöva sina rättigheter. Samtidigt får den registrerade enligt artikel 26.3 utöva sina rättigheter mot var och en av de personuppgiftsansvariga – även om de personuppgiftsansvariga har satt ut en gemensam kontaktpunkt.

Det står med andra ord den registrerade fritt att vända sig till vem den vill av de personuppgiftsansvariga. Europeiska dataskyddsstyrelsen anser att de gemensamt personuppgiftsansvariga därför redan påförväg bör organisera hur de ska hantera förfrågningar från registrerade. Dataskyddsstyrelsen rekommenderar att den som har ansvaret för en fråga enligt arrangemanget informeras av den som har tagit emot en förfrågan, så att förfrågningar kan hanteras effektivt. Det skulle, enligt dataskyddsstyrelsen, strida mot dataskyddsförordningens syfte att be en registrerad att vända sig till den eventuella gemensamma kontaktpunkten eller till en annan personuppgiftsansvarig; det skulle innebära en för stor börda för den registrerade och försvåra för denne att utöva sina rättigheter.[215]

I Metas arrangemang anges att det är Meta som ansvarar för att de registrerade ska kunna utöva sina rättigheter och att alla förfrågningar som rör de registrerades rättigheter inom ramen för sidstatistiken ska vidarebefordras till Meta i ett särskilt formulär.[216] Upplägget har sannolikt valts för att det bara är Meta som i realiteten kan se till att den registrerade kan utöva sina rättigheter; den som driver en Facebooksida saknar den tekniska kontroll över Facebook som krävs för att ändra, radera, begränsa eller ge ut personuppgifter som används för att upprätta sidstatistik. Enligt den norska tillsynsmyndigheten Datatilsynet innebär situationen att artikel 26.3 inte kan efterlevas.[217]

Jag ansluter mig till att det är problematiskt att den som driver en Facebooksida inte själv kan se till att den registrerade kan utöva sina rättigheter. Sidans ägare blir därför helt beroende av att Meta ser till att den registrerade kan utöva sina rättigheter. Om Meta underlåter att göra det, finns det en risk att Facebooksidans ägare kan behöva betala en administrativ sanktionsavgift (artikel 83.5 b). Jag ser det därför som en risk som varje kommun, region och myndighet behöver beakta inför beslutet att driva en Facebooksida.

[215] Europeiska dataskyddsstyrelsen, Riktlinjer 07/2020 s. 52.

[216] Meta, ’Information om sidstatistik’ <https://www.facebook.com/legal/terms/page_controller_addendum/>.

[217] Datatilsynet s. 33.

9 Slutsatser

I personuppgiftsansvaret ingår bland annat att säkerställa att principerna för personuppgiftsbehandling kan följas, att se till att personuppgiftsbehandlingen kan stödjas av en laglig grund och att den registrerade kan utöva sina rättigheter. I det här avslutande avsnittet presenterar jag de slutsatser jag kan dra av vad skyldigheterna innebär för den offentliga sektorn på Facebook och om skyldigheterna kan fullgöras.

9.1 Svårt att avgöra vilket ansvar

Min utredning visar att en kommun, region eller myndighet som driver en Facebooksida blir personuppgiftsansvarig för det som kommunen, regionen eller myndigheten själva publicerar, det som användare publicerar och den statistik om Facebooksidans resultat som kan upprättas. Ansvaret för sidstatistiken är dessutom gemensamt tillsammans med Meta.

Utredningen visar dock att rättsläget för när ett gemensamt personuppgiftsansvar föreligger är oklart. Min utredning antyder att tröskeln är låg för när beslut om ändamål och medel för personuppgiftsbehandlingen anses vara fattade gemensamt. Det kan innebära att det föreligger ett gemensamt personuppgiftsansvar även i andra situationer. En Facebooksidas ägare kan till exempel bli gemensamt personuppgiftsansvarig tillsammans med Facebookanvändare som interagerar med sidan. Att inte med säkerhet kunna avgöra var gränsen går kan innebära en osäkerhet för aktörer inom den offentliga sektorn som vill finnas på Facebook. Med det gemensamma personuppgiftsansvaret kommer skyldigheter att fastställa vem som ansvarar för vad, att göra arrangemanget tillgängligt för den registrerade och att säkerställa att den registrerade kan utöva sina rättigheter. Det kan vara svårt (kanske till och med omöjligt) att efterleva skyldigheterna om varje kommentar på Facebooksidan innebär ett gemensamt personuppgiftsansvar.

9.2 Varierande möjligheter att följa principerna

Det är en personuppgiftsansvariges skyldighet att se till och kunna bevisa att de grundläggande principerna för behandling av personuppgifter följs. Min utredning visar att kommuner, regioner och myndigheter kan säkerställa att principerna följs inom ramen för det som de själva publicerar. De kan stödja sin personuppgiftsbehandling på den lagliga grunden *allmänt intresse*, och de kan se till att öppet informera om personuppgiftsbehandlingen och följa principen om korrekthet. De har godkända ändamål med sin personuppgiftsbehandling och kan genom tydliga riktlinjer se till att principerna om uppgiftsminimering, lagringsminimering och integritet och konfidentialitet följs (även om det kan vara svårt att avgöra när personuppgiftsbehandlingen inte längre behövs i förhållande till ändamålet). De har också möjlighet att redigera sina egna inlägg, vilket innebär att de kan säkerställa att personuppgifterna hålls korrekta.

I stort kan också kommuner, regioner och myndigheter se till att principerna följs när användare publicerar personuppgifter om sig själva. Om användare publicerar personuppgifter om tredjeman blir det dock svårare att efterleva principerna. Det går att säkerställa en laglig grund (*allmänt intresse*), men enligt min mening går det knappast att hävda att personuppgiftsbehandlingen sker i enlighet med öppenhetsprincipen och principen om korrekthet. Det är alltså tveksamt om kommuner, regioner och myndigheter kan uppfylla sitt ansvar i en sådan situation.

Slutligen visar min utredning att kommuner, regioner och myndigheter har små möjligheter att på egen hand säkerställa att personuppgiftsbehandlingen inom ramen för sidstatistiken sker i enlighet med principerna. Meta kan säkerställa en laglig grund för sin behandling av sidstatistiken, men det är enligt min mening tveksamt om den offentliga sektorn kan göra det.

9.3 Den registrerades rättigheter kan inte alltid säkerställas

Den som administrerar en Facebooksida har begränsade tekniska behörigheter över sidan. Administratören kan redigera och radera sina egna inlägg och göra dem privata (dölja dem). Andras inlägg kan administratören bara radera. Flera av den registrerades rättigheter kräver att Facebooksidans administratör kan ändra, radera eller ge ut personuppgifter. Det innebär att det finns situationer där en kommun, region eller myndighet som driver en Facebooksida inte kan säkerställa att den registrerade kan utöva sina rättigheter. I vissa situationer kan en rättighet bli en omöjlighet, till exempel om någon begär rättelse av en personuppgift som förekommer i en kommentar från en användare. I andra situationer måste den offentliga sektorn förlita sig helt på att Meta kan se till att de registrerade kan utöva sina rättigheter, till exempel inom ramen för sidstatistiken.

9.4 Övriga skyldigheter kan uppfyllas

Det ingår också i personuppgiftsansvaret att föra register, att göra en konsekvensbedömning när det krävs, att hantera personuppgiftsincidenter och att säkerställa att det finns en grund enligt dataskyddsförordningen för att föra över personuppgifter till tredjeland.

Min utredning visar att kommuner, regioner och myndigheter som driver en Facebooksida utan några svårigheter kan leva upp till de här skyldigheterna. Skyldigheterna hör till den offentliga sektorns allmänna arbete med dataskyddsförordningen. Så länge kommuner, regioner och myndigheter gör sig påminda om att de är personuppgiftsansvariga också för personuppgiftsbehandlingen på Facebooksidan, bör det inte vara några problem att uppfylla skyldigheterna. Jag vill dock uppmärksamma att rättsläget kan ändras vad gäller tredjelandsöverföringar. Kommuner, regioner och myndigheter som har Facebooksidor bör vara beredda på det.

10 Avslutning

Trots att kommuner, regioner och myndigheter i flera fall har möjlighet att efterleva sitt personuppgiftsansvar, finns det situationer där det är tveksamt om skyldigheterna kan efterlevas. Ofta är den offentliga sektorn helt beroende av att Meta kan fullgöra personuppgiftsansvarets skyldigheter, eftersom bara Meta har den tekniska kontroll över Facebook som krävs.

Av min utredning kan jag dra följande slutsats: Ju mer (ensam) kontroll den offentliga sektorn har över en personuppgiftsbehandling, desto enklare blir det att efterleva skyldigheterna som kommer av personuppgiftsansvaret. Många situationer kräver att kommunen, regionen eller myndigheten behöver förlita sig på att Meta uppfyller flera av de skyldigheter som personuppgiftsansvaret innebär. Jag låter det vara upp till varje kommun, region och myndighet att avgöra om de anser att det är en risk och om den är värd att ta.

Källförteckning

Offentligt tryck

Sverige

Propositioner
Prop. 1997/98:44 Personuppgiftslag.

Prop. 2008/09:153 Språk för alla – förslag till språklag.

Prop. 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag.

Prop. 2017/18:105 Ny dataskyddslag.

Utredningsbetänkanden
SOU 1997:39 Integritet – Offentlighet – Informationsteknik

SOU 2004:23 Från verksförordning till myndighetsförordning

SOU 2017:39 Ny dataskyddslag: Kompletterande bestämmelser till EU:s dataskyddsförordning

Europeiska unionen

Artikel 29-gruppen
Yttrande 4/2007 om begreppet personuppgifter, 01248/07/EN WP 136, antaget den 20 juni 2007.

Opinion 5/2009 on online social networking, 01189/09/EN WP 163, adopted on 12 June 2009.

Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, adopted on 2 April 2013.

Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, 844/14/EN WP 217, antaget den 9 april 2014.

Riktlinjer om dataskyddsombud, 16/SV WP 243 rev.01, antagna den 13 december 2016, senast granskade och antagna den 5 april 2017.

Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, 17/SV WP 248 rev.01, antagna den 4 april 2017, senast reviderade och antagna den 4 oktober 2017.

Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, 18/SV WP 250 rev.01, antagna den 3 oktober 2017, senast granskade och antagna den 6 februari 2018.

Riktlinjer om samtycke enligt förordning (EU) 2016/679, 17/SE WP 259 rev.01, antagna den 28 november 2017, senast granskade och antagna den 10 april 2018.

Riktlinjer om öppenhet enligt förordning (EU) 2016/679, 17/SV WP 260 rev.01, antagna den 29 november 2017, senast granskade och antagna den 11 april 2018.

Europeiska dataskyddsstyrelsen
Endorsement 1/2018.

Riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, version 2.0, antagna den 8 oktober 2019.

Riktlinjer 4/2019 om artikel 25. Inbyggt dataskydd och dataskydd som standard, version 2.0, antagna den 20 oktober 2020.

Riktlinjer 5/2019 om kriterier för rätten att bli bortglömd av sökmotorer enligt dataskyddsförordningen (del 1), version 2.0, antagna den 7 juli 2020.

Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, antagna den 4 maj 2020.

Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.0, antagna den 7 juli 2021.

Europeiska kommissionen
Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (2000/520/EG).

Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

Kommissionens genomförandebeslut (EU) 2023/1795 av den 10 juli 2023 i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om adekvat skydd av personuppgifter enligt ramen för dataskydd mellan EU och Förenta staterna.

Litteratur

Brinnen, Martin, *Europaparlamentets och rådets förordning 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)*, Lexino 11 mars 2019 (Juno).

Cimina, Veronique: 'The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725.' *ERA Forum* 2021, vol. 21 s. 639–654.

Colcelli, Valentina: 'Joint Controller Agreement under GDPR'. *EU and Comparative Law Issues and Challenges Series* 2019, vol. 3, s. 1030–1047.

Edmar, Malin: *Internetpublicering och sociala medier: En juridisk vägledning*. 7 uppl. Stockholm 2021.

Finck, Michèle: 'Cobwebs of control: the two imaginations of the data controller in EU law.' *International Data Privacy Law* 2021, vol. 11 nr 4, s. 333–347.

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline och Beyer, Sandra: *GDPR – juridik, organisation och säkerhet enligt dataskyddsförordningen*. Stockholm 2018. E-bok.

Garrie, Daniel B., Duffy-Lewis, Maureen, Wong, Rebecca och Gillespie, Richard L.: 'Data Protection: The Challenges Facing Social Networking'. *Brigham Young University International Law & Management Review* 2010, vol. 6 nr 2, s. 127–152.

Hellner, Jan: *Metodproblem i rättsvetenskapen: Studier i förmögenhetsrätt*. Stockholm 2001.

Hettne, Jörgen och Otken Eriksson, Ida: 'EU:s rättskällor', i: Hettne, Jörgen och Otken Eriksson, Ida (red.), *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*. 2 uppl., Stockholm 2011 s. 39–132.

Holtz, Hajo Michael och Ledendal, Jonas: 'Överlappningen mellan dataskydd och marknadsrätt: dataskyddsförordningens tillämpning på marknadsföring och marknadsrättens tillämpning på kommersiell personuppgiftsbehandling.' *Svensk juristtidning* 2020 s. 140–169.

Jareborg, Nils: 'Rättsdogmatik som vetenskap.' *Svensk juristtidning* 2004 s. 1–10.

Kamarinou, Dimitria, Millard, Christopher och Turton, Felicity. ’Responsibilities of Controllers and Processors of Personal Data in Clouds’ i: Millard, Christopher (red.), *Cloud Computing Law*. 2 uppl., Oxford 2021 s. 294–339. E-bok.

Kleineman, Jan: ’Rättsdogmatisk metod’, i: Nääv, Maria och Zamboni, Mauro (red.), *Juridisk metodlära*. 2 uppl., Lund 2018 s. 21–46.

Kotsios, Anderas: *Paying with Data: A Study on EU Consumer Law and the Protection of Personal Data*. Diss. Uppsala universitet, 2022.

Krzysztofek, Mariusz: *GDPR: Personal Data Protection in the European Union*. Alphen aan den Rijn 2021. E-bok.

Olsen, Lena: ’Rättsvetenskapliga perspektiv.’ *Svensk juristtidning* 2004 s. 105–145.

Reichel, Jane: ’EU-rättslig metod’, i: Nääv, Maria och Zamboni, Mauro (red.), *Juridisk metodlära*. 2 uppl., Lund 2018 s. 109–142.

Rosén, Johan: ’De svenska lagförarbetenas vara eller inte vara som rättskälla – effekter av Sveriges anslutning till den Europeiska unionen.’ *Svensk juristtidning* 1996 s. 244–259.

Rydzewska-Siemiątkowska, Joanna: ’Deontic Modality in the GDPR Based Finnish Privacy Notices in the Light of the Transparency Principle’. *International Journal for the Semiotics of Law* 2023, vol. 36 s. 1007–1031.

Sandgren, Claes: *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*. 4 uppl., Stockholm 2018.

Sandgren, Claes: ’Är rättsdogmatiken dogmatisk?’ *Tidsskrift for Rettsvitenskap* 2005, vol. 118 nr 4–5, s. 648–656.

Şandru, Daniel-Mihail: ’The fairness principle in personal data processing’. *Law review* 2019, vol. 10 nr 2 s. 60–69.

Șchiopu, Silviu-Dorin: ’Some Considerations on the Lawfulness of Personal Data Processing by Public Administration Authorities under Regulation (EU) 2016/679’. *Bulletin of the Transilvania University of Brasov* 2018, vol 11 nr 60, s. 203–209.

Specht-Riemenschneider, Louisa och Schneider, Ruben: ‘Stuck Half Way: The Limitation of Joint Control after Fashion ID (C-40/17).’ *GRUR International* 2020, vol. 69 nr 2 s. 159–163.

Törngren, David, *Europaparlamentets och rådets förordning 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),* Lexino 11 mars 2019 (Juno).

van Alsenoy, Brendan. *Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing*. Diss., Katholieke Universiteit Leuven, 2016 <https://lirias.kuleuven.be/1711667&lang=en>.

van Alsenoy, Brendan, Ballet, Joris, Kuczerawy, Aleksandra och Dumortier, Jos. ’Social network and web 2.0: are users also bound by data protection regulations?’. *Identity in the Information Society* 2009, vol. 2 s. 65–79.

Wendleby, Monika och Wetterberg, Dag: *dataskyddsförordningen GDPR: Förstå och tillämpa i praktiken*. 2 uppl., Stockholm 2019.

Wong, Janis och Henderson, Tristan: ’The right to data portability in practice.’ *International Data Privacy Law* 2019, vol. 9 nr 3, s. 173–191.

Öman, Sören, *Dataskyddsförordningen (GDPR) m.m. – En kommentar*, (27 september 2023, Juno).

Övrigt

Datatilsynet, *Risk assessment: should the Norwegian Data Protection Authority create a Page on Facebook? Final report 2021*, Datatilsynet, 2021 <https://www.datatilsynet.no/en/news/2021/norwegian-data-protection-authority-choose-not-to-use-facebook/> (hämtad 22 april 2024).

E-delegationen, *Myndigheters användning av sociala medier – riktlinjer från E-delegationen*. Stockholm 2010.

Europeiska unionens publikationsbyrå. ’Europeiska unionens primärrätt’ <https://eur-lex.europa.eu/SV/legal-content/summary/the-european-union-s-primary-law.html> (hämtad 20 mars 2024).

Försäkringskassan, ’Försäkringskassan förälder’ <https://www.facebook.com/foralder> (hämtad 9 maj 2024).

Gagnefs kommun, ’Gagnefs kommun’ <https://www.facebook.com/gagnef.se> (hämtad 7 april 2024).

Heiligenstein, ’Facebook Data Breaches. Full Timeline Through 2023’ <https://firewalltimes.com/facebook-data-breach-timeline/> (hämtad 9 maj 2024).

Integritetsskyddsmyndigheten, ’Behandling av personuppgifter hos myndigheter’ <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/myndighet/> (hämtad 18 maj 2024).

Integritetsskyddsmyndigheten, ’Grundläggande principer’ <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/> (hämtad 7 april 2024).

Integritetsskyddsmyndigheten, ’Konsekvensbedömning och förhandssamråd’ <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/> (hämtad 3 april 2024).

Integritetsskyddsmyndigheten, ’Ny anmälan’ <https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/risk-for-registrerade/> (hämtad 18 maj 2024).

Integritetsskyddsmyndigheten, ’Personuppgifter i e-post’ <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/personuppgifter-i-e-post/> (hämtad 20 maj 2024).

Integritetsskyddsmyndigheten, ’Skydda grundläggande intressen’ <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/skydda-grundlaggande-intressen/> (hämtad 9 maj 2024).

Integritetsskyddsmyndigheten, ’Vi guidar dig: Publicera bilder, filmer och ljud på internet’ <https://www.imy.se/verksamhet/dataskydd/vi-guidar-dig/publicera-bilder-filmer-och-ljud-pa-internet/> (hämtad 10 april 2024).

Integritetsskyddsmyndigheten, ’Är jag ansvarig för det jag publicerar på sociala medier?’ <https://www.imy.se/vanliga-fragor-och-svar/ar-jag-ansvarig-for-det-jag-publicerar-pa-sociala-medier/> (hämtad 18 mars 2024).

International Trade Administration, ‘Data Privacy Framework List’ <https://www.dataprivacyframework.gov/list> (hämtad 22 april 2024).

Internetstiftelsen, *Svenskarna och internet 2023*, Internetstiftelsen, 2023, https://svenskarnaochinternet.se/app/uploads/2023/10/internetstiftelsen-svenskarna-och-internet-2023.pdf (hämtad 22 april 2024).

Landskrona stad, ’Kommunstyrelsens personuppgiftsbehandling’ <https://www.landskrona.se/kommun-och-politik/sa-behandlar-landskrona-stad-personuppgifter/kommunstyrelsens-personuppgiftsbehandling/> (hämtad 18 maj 2024).

Meta, ’Information om rättslig grund’ <https://www.facebook.com/privacy/policy?section_id=18-LegalBasisInformationConsent> (hämtad 22 april 2024).

Meta, ’Information om sidstatistik’ <https://www.facebook.com/legal/terms/page_controller_addendum/> (hämtad 22 april 2024).

Meta, ’Information som används för att visa dig annonser’ <https://accountscenter.facebook.com/ad_preferences/faq/?faqID=ad_pref_faq_information_used_to_show_you_ads> (hämtad 18 maj 2024).

Meta, ’Integritetspolicy’ <https://www.facebook.com/privacy/policy/> (hämtad 22 april 2024).

Meta, ’Meta Data Centers’ <https://datacenters.atmeta.com/> (hämtad 18 maj 2024).

Meta, ’Privacy progress update’ <https://about.meta.com/privacy-progress/> (hämtad 9 maj 2024).

Meta, ’Sidstatistik’ <https://www.facebook.com/business/help/633309530105735> (hämtad 10 april 2024).

Meta, ’Vad är dataskyddsförordningen (GDPR)?’ <https://www.facebook.com/business/gdpr#Facebook-som-personuppgiftsansvarig-kontra-Facebook-som-personuppgiftsbitr%C3%A4de> (hämtad 22 april 2024).

Myndigheten för digital förvaltning, ’ Grundläggande principer för behandling av personuppgifter’ < https://www.digg.se/kunskap-och-stod/metodstod-for-dataskydd-vid-innovation/rattslig-bedomning-av-personuppgiftsbehandlingen/grundlaggande-principer-for-behandling-av-personuppgifter> (hämtad 9 maj 2024).

Region Dalarna, ’Begära dina personuppgifter’ <https://www.regiondalarna.se/om-oss/sakerhet/personuppgifter/begara-dina-personuppgifter/> (hämtad 18 maj 2024).

Region Dalarna, ’Region Dalarna’ <https://www.facebook.com/regiondalarna> (hämtad 7 april 2024).

Region Kalmar, ’Så hanterar vi dina personuppgifter’ <https://regionkalmar.se/personuppgifter> (hämtad 18 maj 2024).

Region Kronoberg, ’Dataskyddsförordningen (GDPR)’ <https://www.regionkronoberg.se/om-region-kronoberg/dataskyddsforordning-gdpr/> (hämtad 18 maj 2024).

Region Skåne, ’Så behandlar vi dina personuppgifter’ <https://www.skane.se/supportsidor/sa-behandlar-vi-dina-personuppgifter/> (hämtad 18 maj 2024).

Region Stockholm, ’Så behandlar vi dina personuppgifter’ <https://www.regionstockholm.se/om-region-stockholm/sa-behandlar-vi-dina-personuppgifter/> (hämtad 18 maj 2024).

Region Uppsala, ’Behandling av personuppgifter’ <https://regionuppsala.se/politik-och-paverkan/handlingar/diarium/behandling-av-personuppgifter/> (hämtad 18 maj 2024).

Region Västerbotten, ’GDPR’ <https://www.regionvasterbotten.se/default.aspx?id=110673> (hämtad 18 maj 2024).

Region Östergötland, ’Så behandlar vi dina personuppgifter’ <https://www.regionostergotland.se/ro/om-region-ostergotland/sakerhet-och-krisberedskap/informationssakerhet/sa-behandlar-vi-dina-personuppgifter> (hämtad 18 maj 2024).

Skatteverket, ’Skatteverket’ <https://www.facebook.com/skatteverketdeklarera> (hämtad 18 maj 2024).

Stockholms stad, ’Behandling av personuppgifter på Stockholms stads sociala medier’ <https://start.stockholm/om-webbplatsen/personuppgifter-och-dataskydd/behandling-av-personuppgifter-pa-stockholms-stads-sociala-medier/> (hämtad 18 maj 2024).

Sveriges kommuner och regioner, ’Frågor och svar om GDPR’ <https://skr.se/skr/ekonomijuridik/juridik/dataskyddsforordningengdpr/fragorochsvaromgdpr.14973.html> (hämtad 18 maj 2024).

Rättsfallsförteckning

EU-domstolen
C-101/01 *Brottmål mot Bodil Lindqvist*, EU:C:2003:596 (cit. C-101/01 *Lindqvist*).

C-524/06 *Heinz Huber mot Bundesrepublik Deutschland*, EU:C:2008:724 (cit. C-524/06 *Huber*).

C-131/12 *Google Spain SL, Google Inc. mot Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, EU:C:2014:317 (cit. C-131/12 *Google Spain*).

C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:650 (cit. C-362/14 *Schrems I*).

C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein mot Wirtschaftsakademie Schleswig-Holstein GmbH*, EU:C:2018:388 (cit. C-210/16 *Wirtschaftsakademie*).

C-434/16 *Peter Nowak mot Data Protection Commissioner*, *EU*:C:2017:994 (cit. C-434/16 *Nowak*).

C-25/17 *Tietosuojavaltuutettu*, EU:C:2018:551 (cit. C-25/17 *Jehovas vittnen*).

C-40/17 *Fashion ID GmbH & Co.KG mot Verbraucherzentrale NRW eV* (cit. C-40/17 *Fashion ID*), EU:C:2019:629.

C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV mot Planet49 GmbH*, EU:C:2019:801 (cit. C-673/17 *Planet49*).

C-311/18 *Data Protection Commissioner mot Facebook Ireland Ltd, Maximillian Schrems*, EU:C:2020:559 (cit. C-311/18 *Schrems II*).

Förslag till avgörande av generaladvokat
Förslag till avgörande av generaladvokat Bobek i mål C-50/17 *Fashion ID GmbH & Co.KG mot Verbraucherzentrale NRW e.V*, EU:C:2018:1039.

Högsta förvaltningsdomstolen
HFD 2016 ref. 40

Integritetsskyddsmyndigheten (Datainspektionen)
Beslut 2010-07-02 dnr 685-2010.

Beslut 2010-07-02 dnr 686-2010.

Beslut 2010-07-02 dnr 687-2010.

Beslut 2010-11-24 dnr DI-2019-7782.

Beslut 2021-06-07 dnr DI-2019-3375.