LUNDS UNIVERSITET
Ekonomihögskolan

Kimmy Ränzlöw

Vem är personuppgiftsansvarig enligt EU:s allmänna dataskyddsförordning?

En studie i räckvidden för definitionen av (gemensamt) personuppgiftsansvarig.

HARH01

Kandidatuppsats, handelsrätt

Handledare: Jonas Ledendal

Termin för examen: VT 2019

Innehållsförteckning

Förord **11**

Förkortningar **13**

1. Inledning **15**

1.1 Bakgrund 15

1.2 Syfte och frågeställning 16

1.3 Avgränsningar 16

1.4 Metod och material 17

1.5 Forskningsläget 18

1.6 Disposition 18

2. Dataskyddsrättens grunder **21**

2.1 Inledning 21

2.2 Mänskliga rättigheter och personlig integritet 21

2.3 Datalagen, personuppgiftslagen och dataskyddsdirektivet 23

2.4 Dataskyddsförordningen 25

3. Dataskyddsförordningen **27**

3.1 Inledning 27

3.2 Nyheter 27

3.3 Struktur 27

3.4 Grundläggande begrepp 29

3.4.1 Inledning 29

3.4.2 Personuppgifter 30

3.4.3 Behandling 32

3.4.4 Register 34

3.4.5 På automatisk väg 35
4. Personuppgiftsansvarig 36
4.1 Inledning 36
4.2 Bestämmelsen i dataskyddsförordningen 37
4.3 Personuppgiftsansvarig i förhållande till äldre rätt 39
4.4 Bestämmer ändamål och medlen för behandlingen 39
4.4.1 Inledning 39
4.4.2 Bestämmer 40
4.4.3 Ändamålen och medlen för behandlingen 41
4.4.3.1 Soft law 41
4.4.3.2 Praxis 42
4.5 Ensamt personuppgiftsansvarig 43
4.5.1 Inledning 43
4.5.2 Praxis: Jehovan todistajat, mål C-25/17 43
4.6 Gemensamt personuppgiftsansvariga 45
4.6.1 Inledning 45
4.6.2 Praxis: Wirtschaftsakademie, mål C-210/16 46
4.6.3 Praxis: Fashion ID, mål C-40/17 47
4.7 Komplexa organisationer 49
4.7.1 Inledning 49
4.7.2 Koncern 49
4.7.3 Offentliga organisationer 50
4.8 Slutsatser 51
5. Personuppgiftshanterare som inte är personuppgiftsansvariga 53
5.1 Personuppgiftsbiträde 53
5.1.1 Inledning 53
5.1.2 Bestämmelsen i dataskyddsförordningen 53

5.1.3 Personuppgiftsbiträde i förhållande till äldre rätt 54
5.1.4 Olika nivåer av personuppgiftsbiträden 55
5.2 Tjänstelevererande mellanhand, mottagare och tredje part 55
5.2.1 Inledning 55
5.2.2 Tjänstelevererande mellanhand 55
5.2.3 Mottagare 57
5.2.4 Tredje part 58
6. Sammanfattning och diskussion 59
6.1 Inledning 59
6.2 Gränsdragningsproblematiken 59
6.3 Granularitetsproblemet 60
6.4 Diskussion kring mål Fashion ID 61
6.4.1 Personuppgiftsansvaret 61
6.4.2 Granulariteten 63
6.4.3 Samtycket 63
6.4.4 Avtal 64
6.4.5 Olika ansvar 64
6.4.6 Slutsats i mål Fashion ID 65
7. Slutsatser 66
Käll- och litteraturförteckning 69
Rättsfallsförteckning 75

Abstract

Approximately one year ago, on May 25, 2018, the General Data Protection Regulation, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* known as the GDPR, applied all over EU. The regulation didn't come as a surprise, it came into force in May 25, 2016, and was based on the older data protection directive, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, which came into force in 1995 and was implemented in Swedish law through personuppgiftslagen (1998:204) in 1998. Still, there is a relatively great uncertainty regarding interpretation of some of its most fundamental concepts, where one of the most important are the controller. The definition of the concept controller differs only marginally from directive to regulation and although the concept differs between the Swedish translations of the directive and the regulation, this thesis will show they are the same. Thus, in lack of rulings from the regulation, rulings and soft law sprung from the directive will be used in the analysis.

The purpose of this thesis is to clarify the meaning of the General Data Protection Regulations concept *controller*. The concept is fundamental because it determines who has the main responsibility for processing personal data.

To reach the purpose, the following questions are asked:

- Who is the controller, according to the General Data Protection Regulation?
- When would the question of joint controller responsibilities arise?

The thesis starts with a walk through the origin and genesis of personal data protection, from both an international and European perspective, as well as from a Swedish perspective. Hereafter a short review of the GDPRs structure and a brief

analysis of the fundamental concepts personal data, processing and register. The in depth analysis of the concept controller, which is necessary to be able to answer the main questions of the thesis, will follow. Finally, some of the concepts for personal data handlers who are not the controller will be mentioned, before a summary, a discussion and the conclusions will be presented.

The thesis will show my interpretation of the answers to the questions asked: the one determining what, why *and* important measures of how personal data should be processed, is considered, generally speaking, the sole controller. If more than one part could be considered involved in the determination of what, why *or* important measures of how personal data is processed, they will, generally speaking, be deemed joint controllers. However, the thesis will also illustrate the difficulties arising from unclear boundaries in liabilities. Private and corporate innovations put the law enforcement establishment to a test, which may render unpredicted consequences and unclear boundaries – despite some relatively clear definitions. The only thing that can be said with certainty, is that all personal data processing covered by the General Data Protection Regulation requires that someone take responsibility for the same. Whoever this someone might be, may ultimately have to be interpreted in the light of the EU's basic treaties, the statutes and the general legal principles, in combination with the purpose of the General Data Protection Regulation, prejudicing practices and by taking international agreements into account.

Sammanfattning

För ganska exakt ett år sedan, den 25 maj 2018, började 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 om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)*, allmänt känd som GDPR efter engelskans General Data Protection Regulation, tillämpas i hela EU. Förordningen kom inte som någon överraskning utan har varit i kraft sedan den 25 maj 2016 och är baserad på det äldre 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*, som varit gällande från 1995 och implementerad i svensk lagstiftning sedan 1998 genom personuppgiftslagen (1998:204). Ändå finns det en relativt stor oklarhet kring tolkningen av många grundläggande begrepp, inte minst det mest centrala – personuppgiftsansvarig. Uppsatsen visar att begreppen personuppgiftsansvarig och det motsvarande registeransvarig, från det äldre dataskyddsdirektivet, är närmast identiska och att praxis, soft law och doktrin kring direktivet därmed kan nyttjas i analysen av begreppet.

Syftet med denna uppsats är att tydliggöra vad som avses med dataskyddsförordningens begrepp personuppgiftsansvarig. Begreppet är centralt eftersom det bestämmer vem som har det huvudsakliga ansvaret för behandling av personuppgifter.

För att nå syftet ställs frågorna:

- Vem är personuppgiftsansvarig enligt dataskyddsförordningen?
- När uppstår gemensamt personuppgiftsansvar?

Uppsatsen inleds med en redovisning av dataskyddets ursprung och tillkomst ur både ett internationellt och europeiskt perspektiv men även ur ett svenskt perspektiv. Härpå följer en kort genomgång av dataskyddsförordningens struktur

och en analys av de grundläggande begreppen personuppgifter, behandling och register. Därefter görs den nödvändiga fördjupning i begreppet personuppgiftsansvarig som krävs för att kunna besvara frågeställningarna. Sist nämns, lite kort, några av de personuppgiftshanterare som inte är personuppgiftsansvarig, innan sammanfattning, diskussion och slutsatser.

Uppsatsen kommer att visa min tolkning av svaret på frågeställningarna: att den som bestämmer vad, varför *och* väsentliga element av hur personuppgifter samlas in och behandlas kan, generellt sett, komma att anses vara ensamt personuppgiftsansvarig. Likaså visas att den som är delaktig i bestämmandet av vad, varför *eller* väsentliga element av hur personuppgifter samlas in och behandlas kan, generellt sett, komma att anses vara gemensamt personuppgiftsansvarig. Men uppsatsen visar också på de svårigheter som finns att dra några exakta gränser för ansvar. Enskilda och verksamheters innovationsförmågor sätter rättskiparen på prov, vilket kan leda till oanade konsekvenser och otydliga gränsdragningar – trots relativt detaljerade definitioner. Det enda som kan sägas med säkerhet är att all personuppgiftsbehandling som omfattas av dataskyddsförordningen kräver att någon tar ansvar för densamma. Vem denna någon är kan, i slutändan, behöva tolkas i ljuset av EU:s grundläggande fördrag, stadgor och allmänna rättsprinciper i kombination med syftet för dataskyddsförordningen, befintlig praxis och med beaktande av internationella avtal.

Förord

Jag vill rikta ett stort tack till min handledare, Jonas Ledendal, som dels inspirerade mig till fördjupning i dataskyddsförordningen och dels har varit en oumbärlig hjälp genom hela skrivprocessen. Jag vill också rikta ett stort tack till min söta Therese, som står ut med mig och stöttar mig i allt tokigt jag får för mig att göra.

Helsingborg, maj 2019.

Kimmy Ränzlöw

Förkortningar

ABL	Aktiebolagslag (2005:551)
Artikel 29-gruppen	Från artikel 29 i direktiv 95/46/EG, vilken stipulerar att: ”En arbetsgrupp för skydd av enskilda med avseende på behandling av personuppgifter, hädanefter kallad "arbetsgruppen" inrättas härmed. Arbetsgruppen skall vara rådgivande och oberoende.”. (Numera ersatt av EDPB)
Bet.	Betänkande
CETS	Council of Europe Treaty Series
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 om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
Dir.	Regeringens direktiv
Direktiv 95/46	Se dataskyddsdirektivet
EG	Europeiska gemenskapen
EDPB	Europeiska dataskyddsstyrelsen (European Data Protection Board)
EDPS	Europeiska datatillsynsmannen (European Data Protection Supervisor)

EU	Europeiska unionen
EUT	Europeiska unionens officiella tidning
E-handelslag	Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster
FEUF	Fördraget om Europeiska unionens funktionssätt
FN	Förenta Nationerna
GDPR	General Data Protection Regulation
IP	Internet protocol
OECD	The Organization for Economic Cooperation and Development
OSK	Offentlighets- och sekretesslagstiftningskommittén
Prop.	Proposition
PuL	Personuppgiftslag (1998:204)
RF	Kungörelse (1974:152) om beslutad ny regeringsform
Rskr.	Riksdagsskrivelse
SFS	Svensk författningssamling
SOU	Statens offentliga utredningar
SWIFT	Society for Worldwide Interbank Financial Telecommunication

1. Inledning

1.1 Bakgrund

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016, om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), allmänt känd som GDPR efter engelskans General Data Protection Regulation och framgent i uppsatsen kallad dataskydds-förordningen, trädde ikraft den 25 maj 2016 och började tillämpas den 25 maj 2018.[1]

Dataskyddsförordningen ger en behörig tillsynsmyndighet, t.ex. Datainspektionen i Sverige, möjlighet att påföra både en personuppgiftsansvarig och ett personuppgiftsbiträde administrativa sanktionsavgifter vid överträdelse av förordningen. Det kan kosta upp till € 20 000 000:- eller, om det är ett företag och beloppet är större, 4% av företagets globala årsomsättning i sanktionsavgift.[2]

De möjligheter och fördelar personuppgiftsbehandling genererar ser vi många exempel på dagligen – samhället hade inte fungerat utan. Men personuppgifts-behandling kräver omfattande förpliktelser enligt dataskyddsförordningen, främst för personuppgiftsansvarig.

Vid en första anblick ser det enkelt ut; personuppgiftsansvarig är den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Men vad innebär det egentligen att bestämma ändamålen och medlen för behandlingen? Vem skulle, reellt sett, kunna omfattas av dataskyddsförordningens begrepp ”personuppgiftsansvarig”? När kan någon anses vara gemensamt personuppgiftsansvarig?

Lagar och förordningar må se enkla ut att tolka men är det sällan. Risken är stor att några av förpliktelserna inte uppfylls, medvetet eller omedvetet. Konsekvenserna av en felbedömning som innebär att fel eller för få förpliktelser uppfylls kan bli

[1] Dataskyddsförordningen, artikel 99.

[2] Dataskyddsförordningen, artikel 83.

kostsamma. Därför är det av yttersta vikt att utröna vem som faktiskt är personuppgiftsansvarig eller gemensamt personuppgiftsansvarig enligt dataskyddsförordningen. Denna uppsats är avsedd att utreda detta närmare.

1.2 Syfte och frågeställning

Syftet med denna uppsats är att tydliggöra vad som avses med dataskyddsförordningens begrepp personuppgiftsansvarig. Begreppet är centralt eftersom det bestämmer vem som har det huvudsakliga ansvaret för behandling av personuppgifter. Uppsatsen är avsedd för juridiskt bevandrade personuppgiftshanterare i rättsvetenskapligt syfte men den bör också kunna intressera juridikstuderande inom dataskydd. Givet dataskyddsförordningens inverkan torde ämnet intressera både civila och offentliga verksamheter.

För att nå syftet ställs frågorna:

- Vem är personuppgiftsansvarig enligt dataskyddsförordningen?
- När uppstår gemensamt personuppgiftsansvar?

När svar på dessa båda frågor erhållits blir det också tydligare vem som kan anses vara personuppgiftsbiträde – oavsett vad som avtalats – vilket naturligtvis också är av yttersta intresse i sammanhanget.

1.3 Avgränsningar

För att begränsa omfånget och inte frångå huvudsyftet med uppsatsen, avgränsas från en djupare analys kring gränserna för dataskyddsförordningens tillämpning. Varken de uppenbara undantagen i artikel 2.2 om förordningens materiella tillämpningsområde, de begränsningar som skulle kunna utläsas av förordningens territoriella tillämpningsområden i artikel 3 eller andra undantag och begränsningar kommer att undersökas närmare. För att frågan om *vem* som är personuppgiftsansvarig ska aktualiseras förutsätts att dataskyddsförordningen är tillämplig.

Vidare avgränsas uppsatsen från att närmare undersöka de förpliktelser som följer av att vara personuppgiftsansvarig, även om vissa oundvikligen nämns.

Uppsatsen avgränsas också från att undersöka effekterna av villkor för skadestånd och påförande av administrativa sanktionsavgifter vid personuppgiftsansvarigs överträdelse av bestämmelser i förordningen.

1.4 Metod och material

I uppsatsen används traditionell rättsvetenskaplig metod – även kallad rättsdogmatisk metod – vilket innebär att innehållet i gällande rätt har fastställts genom en analys av rättskällor såsom lagstiftning, förarbeten och rättspraxis.[3] Eftersom dataskyddsrätten i huvudsak regleras genom EU-rätten – förordningar gäller inom hela EU enligt sin lydelse, är direktverkande och ska tillämpas av nationella domstolar i sin EU-rättsliga form[4] – har i första hand EU-rättslig metod använts. EU-rättslig metod särskiljer sig främst genom rättskällornas hierarki samt vikten av EU-domstolens metodik och tolkningsmetoder.[5]

Primärrätt (de grundläggande fördragen), rättighetsstadgan, bindande sekundärrätt, internationella avtal, allmänna rättsprinciper och EU-domstolens och tribunalens rättspraxis är bindande rättskällor som rättstillämparen är skylig att rätta sig efter. Vägledande är icke bindande sekundärrätt (s.k. soft law), förarbeten, generaladvokaters förslag till avgöranden, den EU-rättsliga doktrinen och ekonomiska teorier.[6]

Vidare konstateras att EU-rättsliga bestämmelser måste tolkas mot bakgrund av sitt syfte och sammanhang[7] och att EU-domstolens praxis har en betydligt mer framträdande roll än Högsta domstolens domar eftersom auktoritativa tolkningar av EU-rätten helt och hållet är förbehållet EU-domstolen.[8] Intressant att notera är också att EU-domstolen anser att soft law bör följas, med hänsyn till likabehandlingsprincipen.[9]

Givet dataskyddsförordningens ännu relativt begränsade tillämpningsperiod och att det därmed inte finns någon praxis att tillgå från EU-domstolen, används främst de rättskällor som riktar in sig på det äldre Europaparlamentets och rådets direktiv 95/46/EG,[10] hädanefter kallat dataskyddsdirektivet eller direktiv 95/46. Detta

[3] Nääv, Maria & Zamboni, Mauro (red.), Juridisk metodlära, uppl. 2:1, Studentlitteratur, Lund, 2018, 2 kap.

[4] Hettne, J. och Otken Eriksson, I. (red.), *EU-rättslig metod : Teori och genomslag i svensk rättstillämpning*, 2:a uppl., Stockholm, Norstedts Juridik, 2011., s. 177.

[5] A.a., Inledning.

[6] A.a., s. 40.

[7] A.a., s. 36.

[8] A.a., s. 48.

[9] A.a., ss. 46 - 48.

[10] 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.

möjliggörs genom att dataskyddsförordningens begrepp personuppgiftsansvarig respektive personuppgiftsbiträde visas vara närmast identiska till sin definition med dataskyddsdirektivets begrepp registeransvarig respektive registerförare. För att ytterligare stärka denna uppfattning redovisas de nyare begreppens uppkomst.

Materialet uppsatsen utgår ifrån utgörs främst av rättskällorna dataskydds-förordningen, dataskyddsdirektivet och domarna i mål Wirtschaftsakademie[11] och Jehovan todistajat.[12] Även soft law beaktas, främst genom Artikel 29-gruppens[13] yttrande. Bristen på praxis gör att generaladvokatens förslag till avgörande i mål Fashion ID[14] kommer att belysas, trots att detta endast är vägledande.

Doktrin som påverkat uppsatsen mest är främst Brendan van Alsenoys djuplodande doktorsavhandling ”*Regulating data protection; The allocation of responsibility and risk among actors involved in personal data processing.*” även om många andra alster har fungerat som inspirationskällor.

1.5 Forskningsläget

En omfattande skrift på området är tidigare nämnda doktorsavhandling av Brendan van Alsenoy från augusti 2016. I övrigt framstår Artikel 29-gruppens WP 169,[15] som antogs den 16 februari 2010, utgöra mer eller mindre ensam grund för den doktrin som behandlar personuppgiftsansvarig respektive personuppgiftsbiträde.

1.6 Disposition

Uppsatsen inleds med en redogörelse för dataskyddsrättens grunder. Här försöker ursprunget till dataskyddsrätten förklaras, lite kort. Därefter följer en återblick på de lagar och direktiv som ledde fram till dagens dataskyddsförordning.

Efterföljande kapitel ger en översiktlig redogörelse för förordningens största nyheter, i förhållande till dataskyddsdirektivet, samt förordningens uppbyggnadsstruktur. Detta tredje kapitel avslutas med en genomgång av några

[11] Dom av den 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388.

[12] Dom av den 10 juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551.

[13] Från artikel 29 i direktiv 95/46, vilken stipulerar att: ”En arbetsgrupp för skydd av enskilda med avseende på behandling av personuppgifter, hädanefter kallad "arbetsgruppen" inrättas härmed. Arbetsgruppen skall vara rådgivande och oberoende.”.

[14] Förslag till avgörande, föredraget den 19 december 2018, Fashion ID, C-40/17, EU:C:2018:1039.

[15] Artikel 29-gruppen, *WP 169 : Yttrande 1/2010 om begreppen registeransvarig och registerförare*.

grundläggande begrepp i avseendet personuppgiftsbehandling, vilka får anses vara väsentligt att ha kännedom om.

Kapitel fyra avhandlar begreppet personuppgiftsansvarig, dels definitionen i förordningen, dels i förhållande till äldre rätt samt de mekanismer som leder fram till att någon kan anses vara personuppgiftsansvarig. Personuppgiftsansvarig delas sedan upp i ensamt respektive gemensamt ansvarig, där praxis bättre hjälper oss förstå innebörd och skillnader.

För bättre förståelse görs i nästa kapitel en beskrivning av roller som kan komma att hantera personuppgifter men som inte är personuppgiftsansvarig. Här avhandlas, lite mer ingående, personuppgiftsbiträde med definition i förordningen, förhållande till äldre rätt samt mekanismerna som styr bedömningen. Efter en kort redogörelse för den möjliga vidden av detta begrepp, avslutas kapitel fem med en genomgång av andra relevanta roller.

Sjätte kapitlet sammanfattar forskningen och pekar på några av de oklarheter som fortsatt vållar bekymmer samt diskuterar dilemmat kring mål Fashion ID.

Uppsatsen avslutas i sjunde kapitlet med slutsatser dragna utifrån det redovisade materialet som svar på frågeställningarna som ledde fram till uppsatsens uppkomst.

2. Dataskyddsrättens grunder

2.1 Inledning

Dataskyddförordningen må vara relativt ny som lag men den är inte sprungen ur tomma intet. Följande avsnitt sätter dataskyddsrätten i en historisk kontext och ger en förståelse för varför den är nödvändig och vad den vill åstadkomma.

2.2 Mänskliga rättigheter och personlig integritet

> [E]ftersom ringaktning och förakt för de mänskliga rättigheterna har lett till barbariska gärningar som har upprört mänsklighetens samvete, och då skapandet av en värld där människorna åtnjuter yttrandefrihet, trosfrihet och frihet från fruktan och nöd har tillkännagivits som folkens högsta strävan[16]

Så inleds en av punkterna i ingressen till Förenta Nationernas, FNs, ”*Allmän förklaring om de mänskliga rättigheterna*”, som kungjordes år 1948 och antogs av medlemsstaterna den 10 december samma år, om varför det finns ett behov av nämnda skrift. Enligt samma förklaring får ingen utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.[17]

Redan i FNs stadga, som undertecknades den 26 juni 1945, står bland annat att FN ska arbeta för ”att ånyo betyga vår tro på de grundläggande mänskliga rättigheterna, på den enskilda människans värdighet och värde, på lika rättigheter för män och kvinnor samt för stora och små nationer”,[18] vilket utmynnade i den allmänna förklaringen ovan.

Nationernas Förbund hade sedan 1920[19] och första världskrigets slut försökt förhindra krig och främja internationellt samarbete. Av olika anledningar fungerade

[16] FN, *Allmän Förklaring om de mänskliga rättigheterna*, Ingressen.

[17] A.a., artikel 12.

[18] Förenta Nationernas stadga, Ingressen.

[19] Även Sverige blev medlem i Nationernas Förbund redan 1920.

det inte som tänkt.[20] Mitt under andra världskriget gjordes ett omtag. Atlantdeklarationen, framarbetad av USA:s president Franklin D. Roosevelt och Storbritanniens premiärminister Winston Churchill, presenterades på ett möte i Washington i USA den 1 januari 1942. Stadgan förhandlas färdigt och antogs av 50 nationers delegationer, av de 51 som vid tidpunkten var medlemmar, den 26 juni 1945.[21] Sverige blev medlem i FN 1946.[22]

Sverige blev medlem i Europarådet den 5 maj 1949 och var med och grundade organisationen.[23] Med stöd av riksdagens godkännande, lämnat genom bifall till propositionen nr 165 till 1951 års riksdag, hade Sverige den 11 januari 1952 ratificerat Europarådets konvention av den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.[24] Konventionen, som beaktar den allmänna förklaring om de mänskliga rättigheterna som antagits av Förenta nationernas generalförsamling den 10 december 1948,[25] hade blivit lagfäst genom ratificeringen. Ratificeringar av ändringar och tillägg har inneburit att lagen idag heter ”Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna” i den svenska lagsamlingen. Konventionens artikel 8.1 lyder: ”Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.”, vilket även står i lag (1994:1219) och känns igen från FNs allmänna förklaring om de mänskliga rättigheterna. Den personliga integriteten är även grundlagsskyddad i Sverige genom 2 kap., 6 § RF, 2st.: ”Utöver vad som föreskrivs i första stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.” samt 2 kap. 19 § RF ”Lag eller annan föreskrift får inte meddelas i strid med Sveriges åtagande på grund av den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.”.

[20] För en större förståelse av vilka anledningar som låg bakom Nationernas Förbunds upplösande hänvisas till andra källor, exempelvis Nationalencyklopedin.

[21] FN, *FN:s historia*, 2019.

[22] FN, *FN:s medlemsländer*, 2019.

[23] Council of Europe, *Sweden*, 2019.

[24] Prop. 1953:32, (prop. 1951:165, bet. 1951:UU11, rskr. 1951:2).

[25] FN, *Konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna*, Ingressen.

2.3 Datalagen, personuppgiftslagen och dataskyddsdirektivet

I informationsteknikens framväxt under 1960-talet utvecklades ett behov av mer detaljerade regler för att trygga enskilda och skydda deras personuppgifter. I Sverige bemyndigades, den 11 april 1969, chefen på justitiedepartementet att sammansätta en grupp som skulle utreda frågor om offentlighet och sekretess beträffande allmänna handlingar.[26] Gruppen kom att kalla sig Offentlighets- och sekretesslagstiftningskommittén, OSK.[27]

Inkorporerandet av automatisk databehandling i de offentliga myndigheterna ledde initialt till ett behov av en utredning kring offentlighetsprincipen och hur dess efterlevnad skulle tryggas.[28] I tilläggsdirektiv av den 27 maj 1971 ändrades direktivet att omfatta personorienterad automatisk databehandling och att även avse de effekter på enskildas integritet som den nya tekniken kunde medföra.[29] OSK identifierade att även privata aktörer kunde ta del av den omfattande information om enskilda som det offentliga behandlade, för vidare behandling, och att detta inte alltid var önskvärt utan kunde medföra särskilda risker för enskildas integritet.[30] Utredningen resulterade i SOU 1972:47 vilket, efter vidare gängse behandling, utmynnade i proposition 1973:33 och konstitutionsutskottets betänkande 1973:19. Datalag (1973:289), som utfärdades den 11 maj 1973, var ett faktum.

Datalagen trädde ikraft delvis den 1 juli 1973 och, efter bland annat grundlagsändring i tryckfrihetsförordningen, i full kraft den 1 juli 1974.[31] Därmed var Sverige det land i världen som först implementerade en dataskyddslag på nationell nivå.[32] Först i världen med en dataskyddslagstiftning var dock delstaten Hesse i Tyskland som, den 7 oktober 1970, hade antagit sin Datenschutzgesetz.[33]

Men även i Europa jobbades det med dataskydd. I början av 1970-talet antog Europarådets ministerkommitté olika resolutioner om skydd av personuppgifter

[26] SOU 1972:47, s. 3.

[27] A.a., s. 3.

[28] A.a., s. 3.

[29] A.a., s. 8.

[30] A.a., s. 10 f.f.

[31] Freese, J., *Datainspektionen*, SvJT 1979, s. 498.

[32] van Alsenoy, B., *Regulating data protection; The allocation of responsibility and risk among actors involved in personal data processing*, 2016, s. 127 (not 540).

[33] Hessisches Hauptstaatsarchiv, HHStAW Bestand 557, *Datenschutzbeauftragter*, 2007.

med hänvisning till artikel 8 i Europakonventionen.[34] Den 21 januari 1981 öppnades en konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108) för undertecknande (ratificering).[35] Konvention 108 var det första juridiskt bindande internationella instrumentet när det gäller skydd av personuppgifter.[36]

Inom dåvarande EG arbetades det också på dataskydd. Redan 1973 initierade kommissionen en skrivelse till rådet om behovet av en gemensam lagstiftning på området.[37] Men kommissionen backade och ville invänta medlemsstaternas ratificering av Europarådets konvention 108.[38] 1985 insåg kommissionen att det gick för långsamt med ratificeringarna och publicerade en vitbok[39] kallad "Completing the Internal Market", [40] vilken innehöll en tidtabell med estimerat slutförande 1992. 1990 kom en ny publikation från kommissionen med en uppsjö förslag på dataskyddsåtgärder och med ett förslag att rådet skulle utfärda ett direktiv.[41] Efter två års debatterande kom parlamentet med sin "first reading", med över hundra ändringar.[42] Kommissionen replikerade och skickade texten till rådet, som efter ytterligare två år lyckades enas om en formulering.[43] Efter parlamentets "second reading" och kommissionens acceptans av ändringarna blev det slutgiltiga dataskyddsdirektivet, direktiv 95/46, antaget den 24 oktober 1995.

---

[34] Europarådet, ministerkommittén (1973*), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private, 26 september 1973*; Europarådet, ministerkommittén (1974), *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, 20 september 1974.

[35] Europarådet CETS 108, *konvention om skydd för enskilda vid automatisk databehandling av personuppgifter*.

[36] Europarådet, *Details of Treaty No.108*, 2018.

[37] Commission of the European Communities, "*Community Policy on Data Processing*", Communication of the Commission to the Council, SEC(73) 4300 final, 21 November 1973.

[38] Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, OJ L 246, 29/08/1981, CELEX:31981H0679, p. 31.

[39] Vitböcker är EU-kommissionens offentliggjorda förberedande utredningar. "White Paper" på engelska.

[40] Commission of the European Communities, "Completing the Internal Market", White Paper from the Commission to the European Council, COM(85) 310 final, 14 June 1985.

[41] Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, SYN 287 and 288, 13 September 1990, CELEX:51990DC0314.

[42] European Parliament, Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992, 11 March 1992 (First Reading), EUT, 13 april 1992, C 94, s. 173-201, OJ:C:1992:094:TOC.

[43] GEMENSAM STÅNDPUNKT (EG) nr 1/95 antagen av rådet den 20 februari 1995 inför antagandet av Europaparlamentets och Rådets direktiv 95/. . ./EG om skyddet för enskilda personer med avseende på behandlingen av personuppgifter och om det fria flödet av sådana uppgifter (95/C 93/01), CELEX:51995AG0413(01).

Internationellt arbetade OECD,[44] parallellt med Europarådet, EG och Sverige – vilket ytterligare förstärker bilden av ett behov av ett dataskydd – med det som skulle mynna ut i ”OECD:s Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”. OECD började redan 1969 studera datoranvändandet i den publika sektorn. En grupp experter, kallad ”the Data Bank Panel”, studerade och analyserade olika aspekter av personlig integritetsproblematik och gränsöverskridande dataflöden. Tidigt 1978 formades en ny grupp experter på gränsöverskridande databarriärer och dataskydd inom OECD, med syfte att, tillsammans med EG och Europarådet, utforma riktlinjer för att uppnå harmoniserad lagstiftning internationellt. Den 23 september 1980 publicerades de rekommendationer och riktlinjerna som nämnts ovan.[45]

Den 15 juni 1995 tillkallades en parlamentariskt sammansatt kommitté i Sverige, ”Datalagskommittén”.[46] Kommittén hade som uppgift att lämna förslag på bland annat en revision av datalagen och att genomföra dataskyddsdirektivet i svensk lag.[47] I efterföljande SOU 1997:39 och genom därpå följande proposition 1997/98:44 antogs det som numera är känt som PuL, personuppgiftslag (1998:204), vilken trädde ikraft den 24 oktober 1998.

2.4 Dataskyddsförordningen

Efter att Lissabonfördraget[48] trätt i kraft 2009 skrev kommissionen ”Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen”[49] till parlamentet, rådet m.fl. i november 2010. Kommissionen anförde att genom fördraget blev EUs stadga om de grundläggande rättigheterna rättsligt bindande och att det samtidigt infördes en ny rättslig grund[50] som gör det möjligt att utarbeta en omfattande och konsekvent EU-lagstiftning om skydd av enskilda när det gäller behandling av personuppgifter och om det fria flödet av sådana uppgifter.[51] Kommissionen konstaterade att ”[…]

[44] The Organization for Economic Cooperation and Development.

[45] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

[46] Dir. 1995:91.

[47] Prop. 1997/98:44, s. 29.

[48] Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, EUT, 17 december 2017, C 306.

[49] KOMMISSIONENS MEDDELANDE TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN OCH REGIONKOMMITTÉN *Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen*, KOM/2010/0609 slutlig.

[50] Se artikel 16 i fördraget om Europeiska unionens funktionssätt (FEUF).

[51] *Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen*, KOM/2010/0609 slutlig, p. 1., st. 18.

den snabba tekniska utvecklingen och globaliseringen har förändrat omvärlden i grunden och medfört nya utmaningar för skyddet av personuppgifter.”.[52] Det var dags för en revision av dataskyddsdirektivet.

Som bland annat står att läsa i dataskyddsförordningen syftar dataskyddsdirektivet till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.[53] Direktivet har inte kunnat förhindra bristande enhetlighet i genomförandet av dataskyddet i olika delar av unionen.[54] För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater.[55] Därav blev det reviderade dataskyddet en förordning med direktverkande effekt för medlemsländerna.

[52] *Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen*, KOM/2010/0609 slutlig, p. 1., st. 2.

[53] Dataskyddsförordningen, skäl 3.

[54] A.a., skäl 9.

[55] A.a., skäl 10.

3. Dataskyddsförordningen

3.1 Inledning

Innan uppsatsen tar tag i de frågeställningar och den nödvändiga fördjupning som krävs för att uppnå syftet, presenteras dataskyddsförordningen lite kort jämte utredningar kring några av de viktigare grundläggande begreppen.

3.2 Nyheter

Även om mycket är hämtat från dataskyddsdirektivet och lagstiftaren, i vissa fall, har utgått från detsamma tillkom naturligtvis en del förändringar och tillägg i förordningen i förhållande till direktivet. De främsta ändringarna är:[56]

- Nya och uppdaterade grundläggande principer
- Bestämmelser om dataskyddsombud
- Speciella regler gällande barns personuppgifter
- Utökade rättigheter
- Utökat tillämpningsområde
- Sanktionsbestämmelser
- Rätten att bli glömd
- Rätten till dataportabilitet
- Nya säkerhets- och överträdelsebestämmelser
- Bestämmelser om ”one-stop-shop” för invändningar mot behandling
- Riskbaserade bedömningar, riskminimering och incidentrapportering

3.3 Struktur

Dataskyddsförordningen är uppdelad i elva kapitel som vart och ett hanterar ett specifikt område.

[56] Se t.ex. Lambert, P., *Understanding the new European data protection rules*, Florida, CRC Press, 2018, s. 102.

1. Första kapitlet behandlar allmänna bestämmelserna om syftet, materiellt-, inklusive undantag, och territoriellt tillämpningsområde samt innehåller kapitlet de för förordningen viktiga begreppsdefinitionerna.
2. Andra kapitlet handlar om principer; principerna för behandling av personuppgifter, laglighet för behandling, samtycke, särskilda kategorier personuppgifter och behandling som inte kräver identifiering.
3. Tredje kapitlet behandlar den registrerades rättigheter; rätt till insyn och villkor, information och tillgång, rättelse och radering – inkluderat rätt till dataportabilitet, invändningar och profilering men också möjligheterna att lagstifta om vissa begränsningar i rättigheterna.
4. Fjärde kapitlet definierar personuppgiftsansvarigas och personuppgifts-biträdens ansvar, inkluderat tekniska och organisatoriska åtgärder för att behandling ska uppfylla förordningens krav och för att lämplig säkerhets-nivå tillämpas, att föra register över behandling, samarbetsskyldighet med tillsynsmyndigheter, hanterande av personuppgiftsincident, konsekvens-bedömningar, dataskyddsombud, uppförandekoder och certifieringar.
5. Femte kapitlet behandlar överföring av personuppgifter till tredjeländer eller internationella organisationer och under vilka villkor detta får ske; exempelvis när en adekvat skyddsnivå är säkerställd, när lämpliga skyddsåtgärder vidtagits och när en tillsynsmyndighet godkänt bindande företagsbestämmelser men kapitlet behandlar också tillämpliga undantag från dessa villkor.
6. Sjätte kapitlet behandlar tillsynsmyndigheter; deras oberoende, sammansättning, inrättande, behörigheter och befogenheter.
7. Sjunde kapitlet behandlar samarbete tillsynsmyndigheter emellan i unionen, samarbete mellan tillsynsmyndigheter och Europeiska dataskyddsstyrelsen, tvistelösningar mellan tillsynsmyndigheter samt Europeiska dataskyddstyrelsens sammansättning.
8. Åttonde kapitlet behandlar rättsmedel, ansvar och sanktioner; rätt att klaga på tillsynsmyndighet, rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut och mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, rätten till företrädandeorganisationer, rätt till skadestånd från personuppgiftsansvarig eller personuppgiftsbiträde samt reglerna om de ökända sanktionsavgifterna.

9. Nionde kapitlet behandlar bestämmelser om särskilda behandlingssituationer såsom i förhållande till yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, allmänhetens tillgång till allmänna handlingar, anställningsförhållanden, arkivändamål, forskningsändamål eller statistiska ändamål men även i förhållande till de som omfattas av tystnadsplikt och inom kyrkor och religiösa samfund.

10 - 11. Tionde och elfte kapitlet behandlar delegerade akter och kommittéförfarande respektive slutbestämmelser som upphävande av dataskyddsdirektivet och förordningens förhållande till direktiv 2002/58/EG och tidigare ingångna avtal.

3.4 Grundläggande begrepp

3.4.1 Inledning

Givet definitionen av personuppgiftsansvarig i dataskyddsförordningen, blir de grundläggande begreppen ”personuppgifter” och ”behandling” viktiga att utreda. Båda begreppen har närmast likalydande definitioner i artikel 2 a respektive 2 b i det äldre dataskyddsdirektivet jämfört med motsvarande artikel 4.1 respektive 4.2 i den nya dataskyddsförordningen, både i de båda svenska översättningarna såväl som i övriga översättningar. Även i nyare doktrin, rörande dataskyddsförordningen, jämställes dessa båda begrepp med de likalydande begreppen i det äldre dataskyddsdirektivet. Utgångspunkten i denna uppsats blir att det anses fastställt att även tidigare doktrin och praxis kan användas för att fastställa dessa begrepps innebörd och omfattning.

Eftersom dataskyddsförordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register,[57] nämns även lite kort de senaste rönen kring begreppen ”på automatisk väg” och ”register”.

[57] Dataskyddsförordningen, artikel 2.1.

3.4.2 Personuppgifter

Dataskyddsförordningens artikel 4, punkt 1, lyder:

> ”*personuppgifter:* varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”.

Framförallt skäl 26, i ingressen till dataskyddsförordningen, ger vägledning till hur extensivt begreppet personuppgifter ska tolkas i förhållande till direkt eller indirekt identifiering: Man bör beakta samtliga objektiva faktorer, inkluderat kostnader och tidsåtgång såväl som tillgänglig teknik och den tekniska utvecklingen vid tidpunkten för behandlingen, vid bedömning av vilka hjälpmedel som rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen.

Artikel 29-arbetsgruppen har inkluderat en omfattande mängd exempel i sitt yttrande WP 136.[58]

EU-domstolen fastställde en extensiv tolkning i mål Lindqvist,[59] där omnämnandet av olika personer - med namn eller på annat sätt, t.ex. med telefonnummer eller med uppgifter om deras arbetsförhållanden och fritidsintressen - på en hemsida på Internet ansågs utgöra personuppgifter.[60] Även uppgifter rörande såväl löner och pensioner som vem som uppbär denna ersättning[61], uppgifter som avser namn och förnamn på vissa fysiska personer som har inkomster som överstiger vissa nivåer,[62] vissa uppgifter avseende utlänningar,[63] uppgifter som kommunen innehar avseende en person såsom vederbörandes namn och adress[64], arbetstidsregister – vilka avser varje arbetstagares dagliga arbetstid och viloperioder[65] är personuppgifter.

[58] Artikel 29-gruppen, *WP 136 : Yttrande 4/2007 om begreppet personuppgifter*.

[59] Dom av den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596.

[60] A.a., p. 24 - 27.

[61] Dom av den 20 maj 2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294, p. 64.

[62] Dom av den 16 december 2008, Satakunnan och Satamedia, C-73/07, EU:C:2008:727, p. 35 - 37.

[63] Dom av den 16 december 2008, Huber, C-524/06, EU:C:2008:724, p. 43.

[64] Dom av den 7 maj 2009, Rijkeboer, C-553/07, EU:C:2009:293, p. 42.

[65] Dom av den 30 maj 2013, Worten, C-342/12, EU:C:2013:355, p. 19.

Uppgifter som samlas in av privatdetektiver avseende personer som utövar verksamhet som fastighetsmäklare och rör identifierade eller identifierbara fysiska personer[66] är självklart personuppgifter men även ytterligare extensiva tolkningar såsom att en bild av en person som registrerats av en kamera utgör en personuppgift[67] och internetleverantörens insamlade IP-adresser från sina användare – dessa adresser utgör skyddade personuppgifter eftersom de gör det möjligt att exakt identifiera användarna.[68]

Alla dessa domar tyder på att begreppet personuppgift ska tolkas extremt extensivt.

Till listan med personuppgifter måste även sådana uppgifter läggas som gör fysiska personer indirekt identifierbara. Domstolens resonemang i mål Breyer[69] ger perspektiv på *hur* extensivt begreppet ska tolkas. Till skillnad från mål Scarlet Extended,[70] där *fasta* IP-adresser[71] behandlades av internetoperatören – med *direkt access* till de kompletterande upplysningar som krävdes för att en IP-adress skulle kunna identifiera en registrerad, handlar mål Breyer om dynamiska IP-adresser[72] som behandlas genom en från internetoperatören frikopplad hemsida. Målet handlar därmed också om indirekt identifiering och vilka ansträngningar som kan behöva göras för att identifiera någon indirekt. För att det skulle kunna vara möjligt att identifiera en användare, som lämnat spår efter sig i form av en dynamisk IP-adress som registrerats på en viss hemsida, krävs det, förutom IP-adressen, datum, tidsangivelse och att den internetleverantör som tilldelat användaren aktuell IP-adress lämnar ut sådana upplysningar som skulle kunna leda till en identifiering.[73] I tysk rätt, där Breyer målet härstammar ifrån, finns lagliga medel som gör det möjligt, särskilt i händelse av it-attacker, att erhålla sådana upplysningar från internetleverantören och inleda straffrättsliga förfaranden.[74] I svensk rätt regleras

[66] Dom av den 7 november 2013, IPI, C-473/12, EU:C:2013:715, p.26.

[67] Dom av den 11 december 2014, Ryneš, C-212/13, EU:C:2014:2428, p. 22.

[68] Dom av den 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771, p. 51.

[69] Dom av den 19 oktober 2016, Breyer, C-582/14, EU:C:2016:779, p. 31 - 49.

[70] Dom av den 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771.

[71] Fast IP-adress: En av internetoperatören tilldelad [dator]maskinadress, som alltid är samma oavsett när och med vilken apparat man kopplar upp sig mot internet.

[72] Dynamisk IP-adress: En av internetoperatören tilldelad [dator]maskinadress som kan variera mellan ett stort antal IP-adresser från internetoperatörens pool av IP-adresser vid varje enskilt tillfälle man kopplar upp sig mot Internet. Uppkoppling kan ske med t.ex. ett modem, en router, en server eller en faktisk webbläsarapparat som en dator, surfplatta eller smartphone.

[73] Breyer, C-582/14, p. 37.

[74] A.a., p. 47.

sådan utlämning av information genom lag (2003:389) om elektronisk kommunikation (LEK). 6 kap. 22 § LEK listar nio olika möjligheter för myndigheter att begära utlämnande av abonnemangsuppgifter, med allt från en generell regel för myndigheter i samband med delgivning enligt delgivningslagen (2010:1932) till kronofogdemyndighet, skatteverk och finansinspektion i olika situationer samt polismyndighet, säkerhetspolis, åklagarmyndighet eller annan myndighet som ska ingripa mot brott. Med andra ord ges stora, lagliga, möjligheter till indirekt identifiering av en registrerad genom en dynamisk IP-adress i svensk rätt. En dynamisk IP-adress får, åtminstone om IP-adressen härstammar från en tysk eller svensk operatör, därmed anses vara en personuppgift. Det innebär också att alla andra uppgifter, som med liknande eller ännu enklare laglig möjlighet till indirekt identifiering av en fysisk person, ska anses vara personuppgift. Eller uppgifter som bara har en *teoretisk* möjlighet till indirekt identifiering av en person. I mål Nowak[75] lämnas ytterligare exempel på vad ”indirekt identifierbar” kan avse. Målet handlar om yrkesexamen och domstolen anger att examinandens svar avspeglar kunskapsnivå och kompetens inom ett visst område samt, i förekommande fall, vederbörandes tankeprocesser, omdöme och förmåga till kritiskt tänkande.[76] Detta kan vara personuppgifter som gör en person indirekt identifierbar.[77] Med avseende på prov med handskrivna svar innehåller svaren dessutom upplysningar om examinandens handstil, likaså detta utgör personuppgifter som indirekt kan identifiera en person.[78] Även examinators anteckningar, som gjorts i anslutning till svaren, är, av samma anledningar, likaledes att anse vara personuppgifter.[79]

EU-domstolen försätter genom dessa domar ”indirekt” i en avsevärt mer omfattande tillämpningssfär.

3.4.3 Behandling

Dataskyddsförordningens artikel 4, punkt 2 lyder:

[75] Dom av den 20 december 2017, Nowak, C-434-16, EU:C:2017:994.
[76] A.a., p. 37.
[77] A.a., p. 38 - 41.
[78] A.a., p. 37 - 41.
[79] A.a., p. 43 - 44.

> ”*behandling:* en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring”

EU-domstolen har slagit fast att en åtgärd som består i att registrera personuppgifter och använda samt lämna dem till en annan organisation som i sin tur återger dem i en rapport som är avsedd att spridas i stor omfattning har karaktär av behandling av personuppgifter,[80] att en åtgärd som består i att på en webbsida lägga ut personuppgifter ska anses utgöra behandling av personuppgifter,[81] att en verksamhet som består i att uppgifter gällande fysiska personers förvärvsinkomster, kapitalinkomster och förmögenhet samlas in, publiceras i ett tryckalster, utlämnas vidare på CD-ROM-skiva och behandlas i en enhet för SMS-tjänster ska anses utgöra behandling av personuppgifter,[82] att insamling, lagring och översändande av personuppgifter utgör behandling av personuppgifter,[83] att när en sökmotor-leverantör lokaliserar information som har publicerats på internet, indexerar den på automatisk väg, lagrar den tillfälligt och slutligen ställer den till förfogande för internetanvändare omfattas åtgärderna av begreppet behandling av person-uppgifter,[84] att ta personernas fingeravtryck och lagra dem på ett lagringsmedium som är integrerat i ett pass ska anses utgöra behandling av personuppgifter,[85] att en arbetsgivares insamling, registrering, organisering, lagring, inhämtande eller användning av personuppgifter samt översändande av dem till behöriga nationella arbetsmiljömyndigheter utgör behandling av personuppgifter,[86] att kamera-övervakning som lagras kontinuerligt på en hårddisk ska anses utgöra behandling av personuppgifter,[87] att de minnesanteckningar, med bland annat namn och adress,

[80] Dom av den 20 maj 2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294, p. 64.

[81] Lindqvist, C-101/01, p.25.

[82] Dom av den 16 december 2008, Satakunnan och Satamedia, C-73/07, EU:C:2008:727, p. 37.

[83] Dom av den 16 december 2008, Huber, C-524/06, EU:C:2008:724, p. 43.

[84] Dom av den 13 maj 2014, Google Spain och Google, C-131/12 P, EU:C:2014:317, p. 21.

[85] Dom av den 17 oktober 2013, Schwarz, C-291/12, EU:C:2013:670, p. 29.

[86] Dom av den 30 maj 2013, Worten, C-342/12, EU:C:2013:355, p. 20.

[87] Dom av den 11 december 2014, Ryneš, C-212/13, EU:C:2014:2428, p. 19.

som medlemmarna i ett religiöst samfund ägnar sig åt inom ramen för sitt predikoarbete genom dörrknackning och den behandling sparandet och en eventuell återanvändning vid nästa dörrknackningsrunda av dessa uppgifter innebär, utgör behandling av personuppgifter.[88]

Dessa domar tyder på att även begreppet behandling ska tolkas extremt extensivt.

Det är också tydligt att behandling kan bestå av flera steg – en kombination av åtgärder – vilket visas i mål Satakunnan och Satamedia[89] samt mål Worten[90]. Artikel 29-gruppen anförde:

> ” I vissa fall kan olika aktörer behandla samma personuppgifter i en följd. I det här fallet är det sannolikt att de olika behandlingsåtgärderna i kedjan på mikronivå kan uppfattas som frikopplade, eftersom var och en av dem kan ha olika ändamål. Man måste dock kontrollera extra noga om dessa behandlingsåtgärder på makronivå inte bör betraktas som ”en serie åtgärder” som har ett gemensamt ändamål eller som utförs med gemensamt fastställda medel.”[91]

Denna insikt ger stöd för teorin att behandling ska ses i ljuset av, det av personuppgiftsansvarig bestämda, ändamålet. Detta blir viktigt att beakta när personuppgiftsansvarig ska åtskiljas från personuppgiftsbiträde. Det blir också viktigt att inse att samma personuppgifter kan vara utsatta för flera olika behandlingar, med andra ändamål och medel som bestämts av någon annan, vilket kan medföra separat personuppgiftsansvar eller gemensamt personuppgiftsansvar för flera aktörer. Det innebär såklart även att när det är fråga om en part som ”bara” behandlar ett delresultat, från ett led i en kombination av åtgärder i *en* behandling som kräver personuppgiftsansvar, kan det vara fråga om att denne part utför en *annan* behandling som kräver personuppgiftsansvar, om ändamål och medel avviker från definitionen i den första behandlingen.

3.4.4 Register

Ett register har ofta antagits avse någon form av systematisk förvaringslösning i doktrin.[92] Detta med stöd av skäl 15 i dataskyddsdirektivet som anger ”uppbyggt

[88] Jehovan todistajat, C-25/17, p. 34.

[89] Dom av den 16 december 2008, Satakunnan och Satamedia, C-73/07, EU:C:2008:727.

[90] Dom av den 30 maj 2013, Worten, C-342/12, EU:C:2013:355.

[91] Artikel 29-gruppen, *WP 169*, s. 20.

[92] Se t.ex. ICO, *Determining what information is ‘data’ for the purposes of the DPA*, ver. 1.1, 2012, s. 6.

efter vissa kriterier” och ”underlätta tillgång” samt skäl 27 där det specifikt anges att: ”Akter eller grupper av akter liksom dessas omslag, vilka inte är strukturerade enligt särskilda kriterier, faller inte under några omständigheter inom detta direktivs tillämpningsområde.”, vilket även står i skäl 15 i dataskyddsförordningen. I mål Jehovan todistajat förtydligade EU-domstolen begreppet ”register”. Domstolen anger att målet med direktivet ger en vid definition av begreppet ”register” eftersom det omfattar ”varje” strukturerad samling av personuppgifter.[93] Kravet att samlingen av personuppgifter måste vara ”[strukturerad] efter bestämda kriterier” syftar endast till att göra uppgifter om en person lätt tillgängliga.[94] Domstolen betonar specifikt att det inte framgår av direktivet att personuppgifterna måste ingå i särskilda kartotek eller förteckningar eller någon form av sökbart system.[95] I aktuellt fall är de personuppgifter som samlas in strukturerade enligt kriterier som är knutna till syftet med denna insamling av uppgifter.[96] I detta sammanhang är det betydelselöst vilket exakt kriterium och vilken exakt form som valts för samlingen av personuppgifter för att uppnå en viss struktur. [97]

3.4.5 På automatisk väg

En utredning kring register aktualiseras endast om behandling på automatisk väg kan uteslutas, enligt artikel 2.1 dataskyddsförordningen. Dom i mål Lindqvist ger exemplet att publicering på en hemsida åtminstone delvis företas på automatisk väg.[98] Målen Rynês[99] och Buivids[100] visar att överföring av personuppgifter från ett medium (kameralins) till ett annat (hårddisk eller minneskort) utgör behandling på automatisk väg.[101] Slutsatsen att all inblandning av någon form för elektronisk utrustning, om så ett rörpostsystem, på ett eller annat sätt skulle kunna utgöra behandling på åtminstone delvis automatisk väg, ligger nära till hands.

[93] Jehovan todistajat, C-25/17, p. 53, 55 och 56.
[94] A.a., p. 57.
[95] Jehovan todistajat, C-25/17, p. 58.
[96] A.a., p. 60.
[97] A.a., p. 61.
[98] Lindqvist, C-101/01, p.26.
[99] Dom av den 11 december 2014, Ryneš, C-212/13, EU:C:2014:2428.
[100] Dom av den 14 februari 2019, Buivids, C-345/17, ECLI:EU:C:2019:122.
[101] Ryneš, C-212/13, p. 23 och 25 respektive Buivids, C-345/17, p. 35.

4. Personuppgiftsansvarig

4.1 Inledning

Först och främst behöver det poängteras att i doktrinen, så även i denna uppsats, jämställes dataskyddsförordningens artikel 4.7 och 4.8, ”personuppgiftsansvarig” och ”personuppgiftsbiträde” med det äldre dataskyddsdirektivets artikel 2 d och 2 e, ”registeransvarig” och ”registerförare”. Förklaringen ligger i att översättningen av direktivet använde sig av terminologin ur den äldre svenska datalagen.[102] Redan i kommittédirektiv 1989:26 anförde chefen för justitiedepartementet att begreppet registeransvarig ”behöver övervägas och kanske förtydligas och moderniseras”.[103] Datalagskommittén (dir. 1995:91) fick, som tidigare nämnts, bland annat i uppgift att lämna förslag på en revision av datalagen och att genomföra dataskyddsdirektivet.[104] I efterföljande SOU 1997:39 föreslogs visserligen ”persondata-” framför det, i utredarnas tycke, sämre ”personuppgifts-” som prefix till -lag, -ansvarig och –biträde men i prop. 1997/98:44 ändrades prefixet till ”personuppgifts-”, för att göra begreppet mer teknikneutralt, och antogs i PuL.

Ovanstående utredning ger stöd för att det inte har varit någon avsiktlig skillnad i begreppen ”registeransvarig” – ”personuppgiftsansvarig” eller ”registerförare” – ”personuppgiftsbiträde” från den svenska regeringens sida. Följs dessutom transformationsprocessen i EU, från dataskyddsdirektiv till dataskyddsförordning, blir det tydligt att det inte heller från lagstiftarens sida fanns någon avsikt att göra skillnad på begreppen i respektive skrift.[105] Benämningarna är identiska i t.ex. de engelska (”controller” och ”processor”), spanska (”responsable del tratamiento”

[102] Datalagen (1973:28).

[103] Kommittédirektiv 1989:26, ”*Översyn av datalagen*”, s. 1.

[104] Se kap. 2.2.

[105] Från ”Kommissionens meddelande till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén och regionkommittén *Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen*”, KOM(2010) 609 slutlig, 4 november 2010 via bl.a. ”Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)”, COM/2012/011 final - 2012/0011 (COD), 25 januari 2012, till ”Rådets ståndpunkt vid första behandlingen inför antagandet av EUROPAPARLAMENTETS OCH RÅDETS 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)”, 5419/16, 6 april 2016.

och ”encargado del tratamiento”), tyska (”Verantwortlicher” och ”Auftragsverarbeiter”) och franska (”responsable du traitement” och ”sous-traitement/traitant”) varianterna av det äldre dataskyddsdirektivet och den nyare dataskyddsförordningen. Generaladvokat Michal Bobek skrev: ”Om denna nya lagstiftning inte innehåller ett särskilt eller systematiskt undantag i fråga om de relevanta definitionerna, vilket inte verkar vara fallet, eftersom artikel 4 i dataskyddsförordningen i princip har behållit de centrala begrepp som fanns artikel 2 i direktiv 95/46 (samtidigt som några nya har lagts till), skulle det emellertid vara ganska förvånande om tolkningen av dessa centrala begrepp, inbegripet begreppen registeransvarig, behandling eller personuppgifter, skulle skilja sig avsevärt från befintlig rättspraxis (utan mycket goda skäl).” i sitt förslag till avgörande i mål Fashion ID.[106]

Kontentan blir att rättskällor kring det tidigare dataskyddsdirektivet kan användas i bedömningen av vem som ska anses vara personuppgiftsansvarig och personuppgiftsbiträde enligt dataskyddsförordningen idag.

4.2 Bestämmelsen i dataskyddsförordningen

Den fullständiga definitionen av personuppgiftsansvarig, enligt dataskyddsförordningens artikel 4.7, lyder:

> ”*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; 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”

Vem som *kan* vara personuppgiftsansvarig ges av artikel 4, punkt 7, direkt i inledningen: ”*personuppgiftsansvarig:* en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ […]”. Det framstår inte finnas någon avgränsning för t.ex. fysiska personer, varken ålder, sysselsättning eller position. Inte heller finns det någon avgränsning för några sammanslutningsformer men en

[106] Fashion ID, C-40/17, p. 87.

myndighet har sanktionsavgiftsrabatt, i Sverige.[107] Ingen och ingenting är egentligen uteslutet från möjligheten att bedömas vara personuppgiftsansvarig, så länge man kan anses kunna bestämma ändamål och medel för behandlingen. Ett visst motstånd mot att tillmäta fysiska personer personuppgiftsansvar finns dock. Artikel 29-gruppen anser att man ska sträva efter att hålla ett företag eller organ ansvarigt,[108] en strävan som har bekräftats av EU-domstolen.[109]

Till skillnad från det tidigare dataskyddsdirektivet, där det viktigaste och direktivets främsta mål var att ge skydd för enskilda personer med avseende på otillåten behandling av personuppgifter, har dataskyddsförordningen till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.[110] Det innebär dock inte att det numera är oviktigt att skydda enskilda från otillåten behandling av personuppgifter[111] utan även fortsatt måste någon kunna anses vara ansvarig för behandlingen.[112] I denna strävan, att ge enskilda skydd mot otillåten behandling av personuppgifter, kan en för förordningen ändamålsenlig tolkning av personuppgiftsansvarig vara nödvändig.[113]

Vidare, i artikel 4.7, anges att personuppgiftsansvarig kan man vara ”[…] ensamt eller tillsammans med andra […]”. I punkt 34 i dom Google Spain och Google[114] anger EU-domstolen att ”[syftet] med [den med artikel 4.7 dataskyddsförordningen likalydande] artikel 2.d är en vid definition av begreppet ’ansvarig’ […]”.[115] Domstolen anger att begreppet registeransvarig kan avse flera aktörer.[116] Med andra ord ensamt personuppgiftsansvarig eller gemensamt personuppgiftsansvarig, som det uttrycks i doktrin och senare praxis. Dessutom introducerar dataskyddsförordningen en reglering som just avser gemensamma personuppgiftsansvariga, i artikel 26. Den anger att om två eller flera gemensamt

[107] 6 kap. 2 § Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[108] Artikel 29-gruppen, *WP 169*, s. 15.
[109] Jehovan todistajat, C-25/17, p. 75.
[110] Se t.ex. dataskyddsdirektivet, artikel 1.1 samt skäl 10 och dataskyddsförordningen, artikel 1.1.
[111] Se t.ex. dataskyddsförordningen, skäl 39, artikel1.1, 5.1, samt artikel 24.1.
[112] Se t.ex. dataskyddsförordningen, skäl 45.
[113] Artikel 29-gruppen, *WP 169*, ss. 4 - 5.
[114] Dom av den 13 maj 2014, Google Spain och Google, C-131/12 P, EU:C:2014:317.
[115] Wirtschaftsakademie, C-210/16, p. 28.
[116] A.a., p. 29.

fastställer ändamål och medel, så är man gemensamt personuppgiftsansvariga. Man ska även, under öppna och tillgängliga former, fastställa sitt respektive ansvar.

4.3 Personuppgiftsansvarig i förhållande till äldre rätt

Som tidigare nämnts skiljer dataskyddsförordningens definition av personuppgiftsansvarig inte nämnvärt mot dataskyddsdirektivets registeransvarig. Dataskyddsdirektivet implementerades i svensk lag genom PuL där, vilket tidigare visats, det ”nya” begreppet personuppgiftsansvarig användes och definierades som ”Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter”,[117] en uppenbarligen lite förenklad variant av direktivets formulering. Förenklingen ligger främst i uttrycket ”den”, vilket i förordningen och direktivet anges vara ”[d]en fysiska eller juridiska person, den myndighet, den institution eller det andra organ” men förenklingen ligger även i uteslutandet av begränsningen att nationell rätt eller unionsrätt/gemenskapsrätt inte kan utse personuppgiftsansvarig enligt däri särskilda angivna kriterier.

I den ännu äldre datalagen[118] definierades registeransvarig som ”den för vars verksamhet personregister föres, om han förfogar över registret.”,[119] där personregister definierades som ”[…] föres med hjälp av automatisk databehandling […]”.[120] Det senare var en starkt bidragande orsak till det i Sverige inledda reformeringsarbetet 1995 eftersom lagstiftaren, bland annat, ville göra dataskyddslagen teknikoberoende.[121]

4.4 Bestämmer ändamål och medlen för behandlingen

4.4.1 Inledning

Såsom Artikel 29-gruppen anfört är ”[b]egreppet registeransvarig … ett funktionellt begrepp som är avsett att lägga ansvaret där det faktiska inflytandet ligger och bygger alltså på en faktabaserad snarare än en formell analys”.[122] Näst efter kravet på att förordningen överhuvudtaget är tillämplig, både materiellt, territoriellt och

[117] 3 § PuL.
[118] Datalag (1973:289).
[119] 1 § Datalag (1973:289).
[120] A.a.
[121] Prop. 1997/98:44, s. 38.
[122] Artikel 29-gruppen, *WP 169*, s. 9.

under förutsättning att det faktiskt sker en behandling av personuppgifter, är de viktigaste parametrarna som styr bedömningen av vem som är personuppgiftsansvarig begreppen ”bestämmer” samt ”ändamål och medel för behandlingen”.

Artikel 29-gruppen argumenterar ”[a]tt bestämma ändamål och medel kan också sägas vara detsamma som att bestämma ’varför’ och ’hur’ vissa behandlingsverksamheter utförs. […] Vilken vikt som ska läggas vid ändamål eller medel kan variera beroende på det särskilda sammanhang som behandlingen utförs inom. […] Beslutet om ’ändamålet’ för uppgiftsbehandling är förbehållet för den ’registeransvarige’. […] Beslutet om ’medlen’ för behandlingen kan delegeras av den registeransvarige i fråga om tekniska och organisatoriska frågor.”. [123]

4.4.2 Bestämmer

För att utröna vem som *bestämmer* bör det göras en utredning kring *hur* ett bestämmande kan se ut. Artikel 29-gruppen anger att det krävs en tolkning av direktivet som garanterar att ”den som bestämmer” lätt och tydligt kan identifieras i de flesta sammanhang och menar att det finns tre typer av bestämmande: uttrycklig rättslig behörighet, underförstådd behörighet och faktiskt inflytande.[124]

Uttrycklig rättslig behörighet att bestämma innebär att registeransvarig genom de särskilda kriterierna i nationell lagstiftning eller EU-lagstiftning för att utse den registeransvarige, enligt andra delen av definitionen i artikeln, har fastställs. Som exempel nämns vissa länders nationella lagstiftning, där offentliga myndigheter anges vara ansvariga för den behandling som sker inom ramen för deras uppdrag eller där ett visst organ pekas ut att utföra ett visst uppdrag (t.ex. socialförsäkring) och på så sätt blir registeransvarig.[125]

Underförstådd behörighet att bestämma härrör från gemensamma rättsliga bestämmelser eller etablerad rättspraxis för vissa områden (civilrätt, handelsrätt, arbetsrätt osv.). Som exempel nämns arbetsgivaren i fråga om uppgifter om anställda, utgivaren i fråga om prenumerantuppgifter och föreningen i fråga om uppgifter om medlemmar eller bidragsgivare. Behandlingsverksamheten betraktas

[123] Artikel 29-gruppen, *WP 169*, ss. 12 - 15.
[124] A.a., s. 11.
[125] A.a., s. 10.

som en naturlig del av den funktionella rollen hos en (privat) organisation som i slutändan leder till ansvar även i fråga om dataskydd.[126]

Faktiskt inflytande på bestämmandet grundar sig på en bedömning om de faktiska omständigheterna. I många fall omfattar detta en bedömning av de avtalsmässiga förbindelserna men avtalsvillkoren är inte avgörande under alla omständigheter, eftersom det i så fall skulle vara möjligt för parterna att helt enkelt fördela ansvaret enligt sina egna önskemål. Som exempel nämns målet SWIFT[127] där transaktionsbolaget beslutade att göra vissa personuppgifter – som ursprungligen behandlades för kommersiella ändamål på ett finansinstituts vägnar – tillgängliga även för kampen mot finansiering av terrorism, på begäran av det amerikanska finansdepartementet i stämningar som departementet utfärdat. Transaktionsbolaget, SWIFT, bedömdes vara registeransvariga för denna del av behandlingen och hade brustit i sina åtaganden att informera de registrerade och övriga skyldigheter det anstår en registeransvarig enligt dataskyddsdirektivet. Artikel 29-gruppen anser denna kategori bestämmande särskilt viktig eftersom den gör det möjligt att ta upp och fördela ansvar även i fråga om otillåtna beteenden. [128] Ytterligare praxis som visar denna typ av bestämmande är t.ex. målen Wirtscahftsakademie och Jehovan todistajat, vilka redogörs för ingående senare i uppsatsen.

4.4.3 Ändamålen och medlen för behandlingen

4.4.3.1 Soft law

Ändamålen och medlen står, som tidigare nämnts, för behandlingens ”varför” och ”hur” enligt Artikel 29-gruppen. Eftersom beslutet om ändamålet är förbehållet den registeransvarige, innebär ett fastställande av behandlingens ändamål alltid att man identifierar den registeransvarige.[129] Det krävs en pragmatisk inställning till ”varför”, där större vikt läggs vid självbestämmande i fråga om att bestämma om ändamål.[130] Skulle underleverantören ha behandlat uppgifterna om inte den registeransvarige hade bett dem om det och på vilka villkor? Om en underleverantör

[126] Artikel 29-gruppen, *WP 169*, s. 10.

[127] Se t.ex. EUROPEAN DATA PROTECTION SUPERVISOR, *EDPS opinion on the role of the European Central Bank in the SWIFT case*; Artikel 29-gruppen, *WP 128 : Yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society for Worldwide Interbank Financial Telecommunication).*

[128] Artikel 29-gruppen, *WP 169*, ss. 11 - 12.

[129] A.a., ss. 14 - 15.

[130] A.a., s. 13.

har inflytande på ändamålet och utför behandlingen (även) för eget syfte, t.ex. genom att använda mottagna personuppgifter för att skapa mervärdestjänster, så är den underleverantören registeransvarig (eller eventuellt gemensamt registeransvarig) för en annan behandlingsverksamhet.[131] Det råder inga tvivel om att det i att bestämma ändamålen med behandling även ligger att bestämma vilka uppgifter som ska behandlas för att uppnå dessa ändamål.[132]

Att fastställa ”medlen” omfattar både tekniska och organisatoriska frågor och beslutet kan vara delegerat.[133] Medlen bör utgöra en rimlig metod för att uppnå ändamålet och den registeransvarige bör ha fullständig information om vilka medel som används.[134] En person eller en enhet som beslutar om *väsentliga* element av medlen, exempelvis hur länge uppgifter ska sparas eller vem som ska få tillgång till uppgifterna, fungerar som registeransvarig för denna del av uppgiftsanvändningen och måste därför uppfylla samtliga skyldigheter som en registeransvarig har.[135] När parter bildar infrastruktur och fattar beslut om de väsentliga elementen i de medel som ska användas, kvalificerar de sig som gemensamt registeransvariga – i varje fall när det gäller medlen – även om de inte nödvändigtvis har samma ändamål.[136]

4.4.3.2 Praxis

Till skillnad från föregående redovisade delbegrepp, *personuppgifter* och *behandling*, så är det sällan det har ifrågasatts hur ett bestämmande av ändamålen och medlen ska göras genom förhandsavgöranden i EU-domstolen.

I de absolut flesta fall, med koppling till dataskydd och som varit uppe till förhandsavgörande i EU-domstolen, är frågan om vem som bestämmer ändamålen och medlen närmast obefintlig. Oftast handlar avgörandena om otillåten behandling eller huruvida direktivet överhuvudtaget är tillämpligt. Domstolen anser sig veta vem som bestämmer ändamål och medel. Exempelvis konstaterar domstolen att sökmotorleverantören själv bestämmer ändamål och medel för behandlingen i mål Google Spain och Google.[137] I mål Wirtschaftsakademie fastställer EU-domstolen

[131] Artikel 29-gruppen, *WP 169*, s. 14.
[132] A.a.
[133] A.a.
[134] A.a.
[135] A.a.
[136] A.a., s. 19.
[137] Google Spain och Google, C-131/12 P, p. 33.

att Wirtschaftsakademie, genom att acceptera Facebooks villkor för cookies och statistikinsamling när man skapade en fanpage, har medverkat till att ha fastställt ändamålen och medlen för Facebooks personuppgiftsbehandling.[138] I mål Jehovan todistajat fastställer EU-domstolen att valet av ändamål och medel inte behöver vara skriftligt och att påverkan på behandling av personuppgifter i eget syfte kan anses bidra till att bestämma ändamål och medel.[139]

4.5 Ensamt personuppgiftsansvarig

4.5.1 Inledning

En förutsättning för att kunna bedömas som *ensamt* personuppgiftsansvarig torde naturligtvis vara att man är ensam om att bestämma ändamål med och de väsentliga elementen av medlen[140] för behandlingen av personuppgifter. Är endast en part inblandad i all hantering och behandling av personuppgifter, råder inga tveksamheter. Fysiska personer i beroendeställning hanteras dock annorlunda och anses inte alltid vara en separat part.[141] Artikel 29-gruppen argumenterade kring detta principalansvar, som tidigare nämnts, i sin WP 169.[142] Alltså kan anställda, föreningsmedlemmar, samfundsmedlemmar och andra i organiserad form engagerade enskilda fysiska personers agerande försvåra bedömningen, beroende på vilken personuppgiftsbehandling de utför och i vilket syfte.

Även om ett datautbyte sker mellan två parter som samarbetar i t.ex. en kedja, utan gemensamma ändamål eller medel i en gemensam serie av åtgärder, bör detta betraktas som en dataöverföring mellan två separata registeransvariga.[143]

4.5.2 Praxis: Jehovan todistajat, mål C-25/17

Finska datasekretessnämnden beslutade förbjuda Jehovan todistajat (Jehovas vittnen), i egenskap av registeransvarig, att samla in eller behandla personuppgifter inom ramen för medlemmarnas predikoarbete om inte de rättsliga villkoren för behandling av sådana uppgifter har iakttagits. Samfundet Jehovan todistajat ansåg

[138] Wirtschaftsakademie, C-210/16, p. 39.
[139] Jehovan todistajat, C-25/17, p. 67-68.
[140] Artikel 29-gruppen, *WP 169*, s. 14.
[141] Se t.ex. dataskyddsförordningen, artikel 39.1 a och 47.1 a.
[142] Artikel 29-gruppen, *WP 169*, s. 15.
[143] A.a., s. 19.

sig inte vara registeransvariga eftersom anteckningarna gjordes av enskilda medlemmar, utan att samfundet fick del av uppgifterna och överklagade beslutet. Högsta förvaltningsdomstolen i Finland konstaterade att medlemmar av samfundet gör minnesanteckningar om okända personer som de har mött, exempelvis de besökta personernas namn och adress samt uppgifter om deras religiösa övertygelse och familjeförhållanden. Uppgifterna samlas in för att kunna återfinnas vid ett eventuellt senare besök, utan att de berörda personerna samtyckt därtill eller informerats därom.[144] Men huruvida registeransvaret låg hos samfundet eller de enskilda medlemmarna behövde förvaltningsdomstolen inhämta vägledning av EU-domstolen för att kunna utröna.

EU-domstolen inleder med att förklara att begreppet ”registeransvarig” i artikel 2 d i dataskyddsdirektivet inte nödvändigtvis avser en enda fysisk eller juridisk person, med hänvisning till dom i mål Wirtschaftsakademie.[145] Domstolen hänvisar även till dom i mål Wirtschaftsakademie när den fastställer att syftet med denna bestämmelse också är att genom en vid definition av begreppet ”registeransvarig” säkerställa ett effektivt och heltäckande skydd för de berörda personerna,[146] när den anger att ett gemensamt ansvar inte nödvändigtvis innebär att olika aktörer har samma ansvar för samma typ av behandling av personuppgifter - ansvaret för var och en av dem ska bedömas med beaktande av alla relevanta omständigheter i fråga - [147] och när den anger att det inte heller krävs att var och en har tillgång till aktuella personuppgifter för att kunna anses gemensamt ansvariga för samma behandling.[148] Vidare anger domstolen att en fysisk eller juridisk person som i eget syfte påverkar behandlingen av personuppgifter, och därigenom bidrar till att bestämma ändamål och medel för behandlingen, kan anses vara registeransvarig.[149] Predikoarbete utgör en viktig verksamhet för samfundet och samfundet har inte bara allmän kunskap om att sådan verksamhet äger rum utan uppmuntrar, organiserar och samordnar självt sina medlemmars predikoarbete.[150] Det får anses klarlagt att samfundet Jehovan todistajat deltar i att bestämma ändamålet med och medlen för

[144] Jehovan todistajat, C-25/17, p. 15.
[145] A.a., p. 65.
[146] A.a., p. 66.
[147] A.a., p. 66.
[148] A.a., p. 69.
[149] A.a., p. 68.
[150] A.a., p. 70 - 71.

behandlingen av personuppgifter som rör besökta personer.[151] Detta bekräftar Artikel 29-gruppens tolkning av begreppet registeransvarig, såsom redogjorts för tidigare.

Av vikt att nämna är också domstolens klargörande att ingen bestämmelse i dataskyddsdirektivet ger grund för att valet av ändamål och medel för behandlingen av personuppgifter ska ske utifrån skriftliga riktlinjer eller instruktioner från den registeransvariges sida [vilket hävdats av samfundet].[152]

Därefter tar EU-domstolen frågan ett steg längre och bekräftar även Artikel 29-gruppens angivna strävanssyfte med direktivet; att principalansvar ska ligga till grund för bedömningen, i den mån det är möjligt.[153] Domstolen menar nämligen att insamlingen av personuppgifter och dessa uppgifters vidare bearbetning utförs för samfundets egna syften och fastställde därefter att ett religiöst samfund kan anses *ensamt* ansvarigt för behandlingen av personuppgifter som insamlats av dess medlemmar inom ramen för predikoarbetet.[154]

4.6 Gemensamt personuppgiftsansvariga

4.6.1 Inledning

Det är sällan att endast en part är inblandad. Med alla molntjänster, redovisningsbyråer, reklambyråer, betalningstjänster, konsulter, transporttjänster, hälsovård med mera, som de flesta måste använda i sitt dagliga (företags-) liv, är det bara att inse att personuppgiftsbehandling sker på många olika sätt, med många inblandade aktörer. Därmed är det lätt att inse att det även kan bli komplicerat eller innebära problem att utkräva (rätt) ansvar.

Artikel 29-gruppen menar att när det gäller gemensamt registeransvar kan parternas deltagande i det gemensamma beslutet ta olika former och måste inte delas lika.[155] När det handlar om flera aktörer kan de ha ett mycket nära förhållande (och t.ex. dela samtliga ändamål och medel för en behandling) eller ett lösare förhållande (och t.ex. endast dela ändamål eller medel, eller delar av dem).[156] Dessa, Artikel 29-

[151] Jehovan todistajat, C-25/17, p. 73.
[152] A.a., p. 67.
[153] Artikel 29-gruppen, *WP 169*, s. 15.
[154] Jehovan todistajat, C-25/17, p. 71 respektive p. 75.
[155] Artikel 29-gruppen, *WP 169*, s. 19.
[156] A.a.

gruppens tolkningar av dataskyddsdirektivet, kan sägas ha kodifierats i dataskyddsförordningens artikel 26.

Men, som tidigare nämnts, det faktum att olika enheter samarbetar i behandlingen av personuppgifter, t.ex. i en kedja, innebär inte att de alltid är gemensamt registeransvariga eftersom ett datautbyte mellan två parter, utan gemensamma ändamål eller medel i en gemensam serie av åtgärder, endast bör betraktas som en dataöverföring mellan två separata registeransvariga.[157]

4.6.2 Praxis: Wirtschaftsakademie, mål C-210/16

Wirtschaftsakademie Schleswig-Holstein GmbH, nedan kallad WA, erbjuder utbildning genom en fanpage[158] som Facebook hyser. Den tyska delstaten Schleswig-Holsteins datainspektionsmyndighet förelade WA att avaktivera sin fanpage eftersom varken WA eller Facebook informerade besökarna om att denna samlade in personuppgifter samt behandlade dessa uppgifter. WA överklagade beslutet och gjorde gällande att man varken var ansvarig för de cookies[159] Facebook skapat, som möjliggjorde insamling av personuppgifter, eller för den behandling som Facebook därefter gjorde med de insamlade personuppgifterna. Ärendet togs till domstol där den tyska federala förvaltningsdomstolen vände sig till EU-domstolen för vägledning.

Inledningsvis hänvisar EU-domstolen till punkt 66 i dom Google Spain och Google, via dom Rynês,[160] ”[att] direktiv 95/46, såsom framgår av artikel 1 och skäl 10 i direktivet, avser att säkerställa en hög skyddsnivå när det gäller fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter.” [161] och till punkt 34 i dom Google Spain och Google, ”[syftet] med artikel 2 d är en vid definition av begreppet ’ansvarig’

[157] Artikel 29-gruppen, *WP 169*, s. 19.

[158] En typ av hemsida, skapad i Facebooks plattform, under villkor stipulerade av Facebook som måste accepteras av fanpage-skaparen. En fanpage är även tillgänglig för besökare utanför Facebooks plattform och kräver således inte att besökare har skapat ett eget Facebookkonto och accepterat Facebooks villkor för personuppgiftsbehandling.

[159] Kallas även ”kakor” i vissa svenska översättningar. En typ av spårningsfil som genereras av programkod på en hemsida, vid besök på sidan. Filen sparas på besökarens webbläsarapparat och används av hemsidan för att ”komma ihåg” vad som görs och gjorts av besökaren och för att anpassa hemsidans innehåll. Filen kan även lagra personuppgifter och kan komma att delas med andra hemsidor för anpassat innehåll, riktad reklam eller annan behandling. Det finns väldigt många olika sorters cookies och de kan vara väldigt olika avancerade. För en djupare beskrivning och mer information om cookies hänvisas till andra källor.

[160] Ryneš, C-212/13, p. 27.

[161] Wirtschaftsakademie, C-210/16, p. 26.

[…]".[162] Domstolen anger att begreppet registeransvarig kan avse flera aktörer.[163] Vidare konstateras att Facebook ska anses bestämma ändamål och medel för den personuppgiftsbehandling som sker, för Facebooks användare.[164] Däremot ger en administratör av en fanpage, genom att godkänna användarvillkoren, Facebook möjlighet att placera kakor i en besökares utrustning (gemensamt bestämma "hur" insamling sker [egen tolkning]) oavsett om denne har ett konto hos Facebook eller ej.[165] Dessutom kan en administratör påverka de kriterier för statistik (bestämma "ändamål" [egen tolkning]) som upprättas även om statistiken bara skickas till administratören i anonymiserad form.[166] EU-domstolen gör ett viktig förtydligande i detta mål: "Under alla omständigheter krävs inte enligt direktiv 95/46, när flera aktörer har ett gemensamt ansvar för samma behandling, att var och en av dessa har tillgång till de berörda personuppgifterna.".[167]

EU-domstolen fastställde att en administratör av en fanpage hos Facebook kan anses vara gemensamt registeransvarig med Facebook.[168]

Detta bekräftar ännu en gång Artikel 29-gruppens tolkning av begreppet registeransvarig: genom det faktiska bestämmandets och dess fördelning. Trots att WA egentligen inte kan påverka själva behandlingen. Facebook kan däremot påverka, och gör de facto lite som de vill med behandling av personuppgifter - har vi fått erfara.[169]

4.6.3 Praxis: Fashion ID, mål C-40/17

Sakerna ställs på sin spets i detta mål. Var går gränserna för gemensamt personuppgiftsansvar? Kan någon vara gemensamt ansvarig för *all* behandling, om man gemensamt bara beslutat om en liten del av behandlingen eller genom att "bara" göra vidare behandling möjlig?

Först och främst måste det poängteras att i detta mål handlar det om generaladvokatens förslag till avgörande, målet har ännu inte avgjorts av EU-

[162] Wirtschaftsakademie, C-210/16, p. 28.
[163] A.a., p. 29.
[164] A.a., p. 30.
[165] A.a., p. 32 - 35.
[166] A.a., p. 36 - 38.
[167] A.a., p. 38.
[168] A.a., p. 44.
[169] Se t.ex. CNBC, *Here's everything you need to know about the Cambridge Analytica scandal*, 2018.

domstolen. Så som frågorna ställts kan domstolen komma till slutsatsen att frågan om registeransvarig inte behöver besvaras och även om den anser att frågan ska besvaras kan domstolen givetvis komma till helt andra slutsatser än advokaten.

Målet handlar om nätbutiken Fashion ID GmbH som har inkorporerat ett insticksprogram, Facebooks ”Gilla”-knapp, på sin webbplats. Detta gör att användarens IP-adress och webbläsarsträng skickas till Facebook när användaren besöker butikens webbplats. Uppgifterna översänds automatiskt när Fashion ID:s webbplats aktiveras, oavsett om användaren klickar på ”Gilla”-knappen eller inte och oavsett om användaren har ett Facebook-konto eller inte.[170] Fashion ID kan inte påverka [den efterföljande] uppgiftsbehandlingen men har uppenbart inflytande på orsakandet.[171] Generaladvokaten refererar till Wirtschaftsakademie gällande att registeransvarig kan vara flera aktörer och till Jehovan todistajat (och Google Spain och Google) avseende en extensiv tolkning av begreppet.[172] Vidare resonerar generaladvokaten, med hjälp av domarna i ovan nämnda mål, att visserligen får Fashion ID inte något annat i utbyte av Facebook än förmodad viss reklam i deras plattform när någon klickar på ”Gilla”-knappen och någon ”konfiguration” likt den i Wirtshaftsakademie, som medverkar till att fastställa ändamål och medel, verkar inte förekomma.[173] Å andra sidan kunde man, igen enligt nämnda domar, vara gemensam registeransvarig i fall där man inte hade tillgång till ”resultatet av det gemensamma arbetet” eller ens tillgång till de insamlade uppgifterna.[174] Dessutom skulle det, menar generaladvokaten, kunna sägas att man gemensamt bestämt konfigurationen av de insamlade uppgifterna enbart genom att integrera insticksprogrammet på sin webbplats.[175]

”Vem är då *inte* en gemensam registeransvarig?” [Frågar advokaten sig själv.]

Via ett resonemang inkluderande ”en galax lång, långt borta” och ytterligheter som att elbolag skulle kunna anses vara gemensamt registeransvariga genom att ha gjort behandling möjlig med leverans av ström, landar generaladvokaten i domstolens uttalande ”aktörer [kan] vara involverade i olika skeden av behandlingen och i olika

[170] Fashion ID, C-40/17, p. 21.
[171] A.a., p. 51.
[172] A.a., p. 61.
[173] A.a., p. 68.
[174] A.a., p. 70.
[175] A.a., p. 69.

utsträckning".[176] Advokatens slutsats blir att det är logiskt att frågan om kontroll bedöms utifrån den särskilda åtgärden i fråga och inte utifrån en diffus blandning som utgörs av allt som kan kallas behandling.[177] För att två (eller flera) personer ska anses vara gemensamt registeransvariga måste de ha samma ändamål och medel för behandlingen av personuppgifter.[178] I förevarande mål motsvarar det relevanta stadiet (de relevanta åtgärderna) för behandlingen insamlingen och översändandet av personuppgifter som sker genom Facebooks "Gilla"-knapp.[179] För denna behandling är Fashion ID och Facebook gemensamt registeransvariga.[180] Den vidare behandling som Facebook gör senare, är Fashion ID *inte* gemensamt ansvariga för.[181]

Argumentation kring generaladvokatens resonemang presenteras i kap. 5.4.

4.7 Komplexa organisationer

4.7.1 Inledning

Många verksamheter, både privata och offentliga, är komplexa till sin uppbyggnad som t.ex. koncerner med holdingbolag, moderbolag, dotterbolag och filialer eller departement, myndigheter, verk, institutioner och avdelningar. De flesta av dessa komplexa organisationer har en viss hierarkisk bestämmanderätt men ingående förgreningar kan också framstå som mer eller mindre självbestämmande fristående enheter. Vem är personuppgiftsansvarig för behandling av personuppgifter här?

4.7.2 Koncern

En koncern som sådan kan inte vara personuppgiftsansvarig. Den är inte en egen juridisk person eller någon annan av dataskyddsförordningens uttalade objekt som skulle kunna vara personuppgiftsansvarig.[182] Alltså måste någon av de i koncernen ingående juridiska personerna vara personuppgiftsansvarig, ensamt eller gemensamt.[183] Det är inte möjligt, ens inom en koncern, att själv bestämma och utse valfri ansvarig juridisk person genom delegering och avtal. På samma sätt och av

[176] Fashion ID, C-40/17, p. 97; Wirtschaftsakademie, C-210/16, p. 43; Jehovan todistajat, C-25/17, p. 66.
[177] Fashion ID, C-40/17, p. 99.
[178] A.a., p. 100.
[179] A.a., p. 102.
[180] A.a., p. 108.
[181] A.a., p. 107.
[182] 1 kap. 11 § ABL och dataskyddsförordningen, artikel 4.7.
[183] Se även dataskyddsförordningen, skäl 37.

samma anledning som tidigare redogjorts för, ligger ansvaret hos den som bestämmer ändamål och medel. Det är där det faktiska bestämmande ligger som avgör vem som är personuppgiftsansvarig.[184] Dessutom förstås det, av mål Google Spain och Google som i relevant mening visserligen handlar om territoriellt tillämpningsområde, att ansvaret landar uppåt i hierarkin om det finns ”ett oupplösligt samband”[185] mellan personuppgiftsbehandlingen och den egentliga bestämmanderätten. Som exempel på ett oupplösligt samband nämner Artikel 29-gruppen en dagstidning som är tillgänglig via internet genom prenumeration.[186] Med huvudkontor i ett land och filialer i andra länder, alla med syftet att också sälja annonser och marknadsföra men med ”lokala” utgåvor, ligger bestämmanderätten, om än bara ekonomiskt, hos huvudkontoret som därmed också är personuppgiftsansvariga. Sambanden, inte minst det redaktionella materialet, mellan huvudkontoret och de lokala filialerna är oupplösliga. Som motsats nämns ett socialt nätverk som i koncernen även har ett dotterbolag som sysslar med vindistributionsverksamhet. Vindistributionsverksamheten behandlar inga personuppgifter som har anknytning till det sociala nätverket och varken medlemskap i nätverket eller marknadsföring av respektive verksamhet har några gemensamma kopplingar. Rent tekniskt finns det, i sista hand, en ekonomisk koppling - de är ju en del av samma koncern - men det finns inget oupplösligt samband mellan verksamheterna. Alltså skulle personuppgiftsansvaret anses stanna hos vindistributören.[187]

4.7.3 Offentliga organisationer

Motsvarande resonemang som för koncerner gäller för offentliga organisationer om inte personuppgiftsansvaret är specifikt reglerat genom nationell lagstiftning eller EU-lagstiftning.[188] Genom lagstiftning kan personuppgiftsansvaret vara reglerat antingen genom direkt utpekning av ett ansvarigt organ alternativt genom att

[184] Se kap. 3.4, Bestämmer ändamål och medlen för behandlingen.

[185] Google Spain och Google, C-131/12 P, p. 56.

[186] Artikel 29-gruppen, *WP 179 update : Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain*, annex 2, ss. 1 - 2.

[187] A.a., s. 1.

[188] Artikel 29-gruppen, *WP 169*, s. 10.

lagstiftningen föreskriver vilka personuppgifter som ska behandlas och i vilket syfte, vilket kan vara delegerat till ett utsett organ som på så sätt blir ansvarigt.[189]

4.8 Slutsatser

Praxis visar att även om man som organisation varken bestämmer vilka personuppgifter som behandlas, hur de behandlas eller ens har tillgång till uppgifterna, kan organisationen anses ha gemensamt personuppgiftsansvar tillsammans med andra organisationer.[190] Andra organisationer kan bli ensamt personuppgiftsansvariga trots att de varken bestämmer vilka personuppgifter som behandlas, hur de behandlas eller ens har tillgång till uppgifterna när det rör sig om flera olika fysiska personers, medlemmars, egna olika behandlingar.[191] Finns det ett samröre mellan en fysisk person och en organisation kan organisationen anses vara ensamt eller gemensamt personuppgiftsansvarig.

Kontentan blir att Artikel 29-gruppens riktlinjer förmodligen håller. Det svåra verkar bli att bryta ner behandlingen till en nivå där en ändamålsenlig tolkning av förordningen kan göras. All behandling av personuppgifter kräver ansvar. Ansvar medför förpliktelser. Bestämmer man att personuppgiftsbehandling ska (får) ske, bestämmer man antingen (gemensamt) ändamål (för den behandling som gör vidare behandling möjlig), alternativt bestämmer man medel. Oavsett är man (gemensamt) personuppgiftsansvarig, har ansvar och har därmed förpliktelser enligt förordningen. Vidare kan konstateras att principalansvaret är omfattande så länge organisationen kan ha nytta av och därmed kan härledas till enskilda medlemmars och, i förlängningen, anställdas personuppgiftsbehandling. Helt enligt Artikel 29-gruppens riktlinjer.

En prövning kan, vid varje givet tillfälle och inte minst i komplexa organisationer, vara nödvändig för att bestämma vem som de facto är personuppgiftsansvarig.

Som parentes nämns följande: en effekt av den EU-rättsliga metoden syns i mål Wirtschaftsakademie. I målet begärde federala förvaltningsdomstolen i Tyskland ett förhandsavgörande från EU-domstolen avseende om det kvarstår, inom ramen för ”lämpliga bestämmelser” enligt artikel 24 [i direktiv 95/46], flera nivåer med

[189] Artikel 29-gruppen, *WP 169*, s. 10.
[190] Wirtschaftsakademie, C-210/16.
[191] Jehovan todistajat, C-25/17.

utrymme för ansvar?[192] Redan innan frågorna ställdes till EU-domstolen hade förvaltningsdomstolen nämligen uteslutit att Wirtschaftsakademie skulle kunna vara ansvariga för behandling av personuppgifter enligt artikel 2 d, direktiv 95/46.[193] Till skillnad från hur det fungerar i domstolsväsendet i Sverige – där inget annat än det som yrkats får behandlas – så väljer EU-domstolen helt sonika att bortse från det faktum att förvaltningsdomstolen tolkat artikel 2 d fel och därmed ställt ”fel” frågor. EU-domstolen formulerar istället om den hänskjutande domstolens frågor och öppnar därmed upp för möjligheten att lämna ett resonemang, skäl och svar som passar bättre med vad EU-domstolen vill uppnå. Detta helt i enlighet med artikel 267 FEUF som säger att Europeiska unionens domstol ska vara behörig att meddela förhandsavgöranden angående tolkningen av fördragen och giltigheten och tolkningen av rättsakter som beslutas av unionens institutioner, organ eller byråer. Syftet med förfarandet med förhandsavgörande är att säkerställa en enhetlig tillämpning av unionsrätten i samtliga medlemsstater och att skapa ett effektivt samarbete mellan EU-domstolen och de nationella domstolarna.[194] Har den hänskjutande domstolen redan i sitt resonemang som ledde fram till frågan som ställts i begäran om förhandsavgörande tänkt fel, måste den grundläggande definitionen klargöras.

[192] Wirtschaftsakademie, C-210/16, p. 24.1.

[193] A.a., p. 23.

[194] Se t.ex. Hettne, J. och Otken Eriksson, I. (red.), 2011, s.285; Worten, C-342/12, p. 30.

5. Personuppgiftshanterare som inte är personuppgiftsansvariga

5.1 Personuppgiftsbiträde

5.1.1 Inledning

Som tidigare utretts är dataskyddsförordningens begrepp personuppgiftsbiträde att jämställa med det äldre dataskyddsdirektivets begrepp registerförare. [195] Rättskällor som behandlar direktivet i detta avseende kan därför nyttjas.

Utredningen kring personuppgiftsansvarig ger oss en bättre förståelse för hur tolkning av begreppet personuppgiftsbiträde ska göras och ger oss förståelsen av personuppgiftsbiträdets begränsade möjligheter till självbestämmande. Exempel på begränsade möjligheter till självbestämmande lyfts fram i målet SWIFT, i Artikel 29-gruppens skrift WP 169 och i generaladvokatens förslag till avgörande i mål Fashion ID.

5.1.2 Bestämmelsen i dataskyddsförordningen

Definitionen av ett personuppgiftsbiträde enligt dataskyddsförordningen lyder:

> *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,[196]

Men ytterligare krav ställs. Personuppgiftsbiträden måste ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning, för att få anlitas av en personuppgiftsansvarig.[197] För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter ålägger nämligen förordningen personuppgiftsansvariga och

[195] Se kap. 3.1, Inledning.

[196] Dataskyddsförordningen, artikel 4.8.

[197] A.a., artikel 28.1.

personuppgiftsbiträden samma ansvar.[198] Fördelning av ansvar kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när en behandling utförs på en personuppgiftsansvarigs vägnar.[199]

När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.[200] I avtalet eller rättsakten ska det särskilt föreskrivas att personuppgiftsbiträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, säkerställer konfidentialitet, ska vidta åtgärder för lämplig säkerhetsnivå enligt artikel 32, ska respektera de villkor som avses i punkterna 2 och 4 [i artikel 28] för anlitandet av ett annat personuppgiftsbiträde, ska hjälpa den personuppgiftsansvarige att fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter, ska radera eller återlämna uppgifter efter avslutad behandling, ska kunna visa på efterlevnad av förordningen och bidra till granskningar.[201] Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om han anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.[202]

5.1.3 Personuppgiftsbiträde i förhållande till äldre rätt

Personuppgiftsbiträdesrollen har genomgått stora förändringar i samband med dataskyddsförordningen. Först och främst är förordningen *direkt* och *uttryckligen* tillämplig på personuppgiftsbiträden, dataskyddsdirektivet och PuL var bara indirekt tillämpligt. Dessutom *ska* personuppgiftsbiträden uttryckligen samarbeta med tillsynsmyndigheter, tidigare var det underförstått. Vidare har krav på dokumentation, säkerhet och incidentrapportering införts samt skyldigheten att beakta reglerna om dataskyddsombud och överföring av personuppgifter till

[198] Dataskyddsförordningen, skäl 13.
[199] A.a., skäl 79.
[200] A.a., artikel 28.3.
[201] A.a., artikel 28.3 a - h.
[202] A.a., artikel 28.3, 2 st.

tredjeländer eller internationella organisationer tillkommit. Sist men inte minst omfattas numera även personuppgiftbiträde av implicit ansvar och reglerna kring sanktionsavgifter.[203]

5.1.4 Olika nivåer av personuppgiftsbiträden

Definitionen av personuppgiftsbiträden omfattas av samma vida begrepp som personuppgiftsansvarig, ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ” och inga undantag synes tillgängliga. Personuppgiftsbiträden kan i sin tur anlita ett eller flera andra personuppgifts-biträden för delbehandling av personuppgiftsansvarigs personuppgifter, enligt artikel 28.2, men bara med personuppgiftsansvarigs allmänna eller särskilda tillåtelse. Naturligtvis kan dessa biträden i sin tur anlita ett eller flera biträden, som också anlitar ett eller flera biträden och så vidare. Samtidigt ställs samma krav på personuppgiftsbiträden som är anlitade av ett personuppgiftsbiträde som på personuppgiftsbiträden som är anlitade av en personuppgiftsansvarig, det görs ingen skillnad på var i kedjan personuppgiftsbiträdet hamnar enligt förordningen.

För att lösa de avtalstekniska problemen som kan uppstå i komplicerade kedjor av personuppgiftsbiträden torde personuppgiftsansvarig kunna delegera möjligheten att ingå avtal med biträdes biträde genom fullmakt.

5.2 Tjänstelevererande mellanhand, mottagare och tredje part

5.2.1 Inledning

Det finns ytterligare ett par roller i dataskyddsförordningen som är värda att nämna i detta sammanhang. Gemensamt för dem alla är att de kan komma att hantera personuppgifter men de är varken personuppgiftsansvariga, personuppgiftsbiträde eller ens en registrerad.

5.2.2 Tjänstelevererande mellanhand

Tjänstelevererade mellanhänder, som det kallas i dataskyddsförordningen, [204] och deras ansvarsfrihet regleras främst genom direktiv 2000/31/EG, "Direktiv om

[203] van Alsenoy, B., 2016, s. 269.

[204] Dataskyddsförordningen, artikel 2.4.

elektronisk handel", implementerat i svensk lag som Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster, E-handelslagen.[205] Ordet mellanhand nämns visserligen inte i den svenska lagen men det förekommer i direktivet den baseras på, om än odefinierat, och avser en tjänsteleverantör som endast förmedlar eller lagrar information genom tjänster som normalt utförs mot ersättning och som tillhandahålls på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.[206]

Artikel 2.4 i dataskyddsförordningen nämner särskilt artiklarna 12 – 15 i direktiv om elektronisk handel, vilka primärt handlar om definitionen av vilka tjänsteleverantörer som berörs och om ansvarsfrihet. En grundläggande förutsättning för ansvarsfrihet för en tjänsteleverantör är bland annat att behandling av personuppgifter i dataskyddsförordningens mening inte sker.[207] Både överföring (förmedling) och lagring är att betrakta som behandling av personuppgifter,[208] så det är motsägelsefullt. Å andra sidan *bestämmer* en tjänstelevererande mellanhand inget som är specifikt relaterat till någon personuppgiftsbehandling genom tjänsten, lika lite som ett elbolag bestämmer om till vad, varför eller hur strömmen de levererar ska användas. Personuppgifter ”råkar” bara kunna vara en del av den information som kan passera i ett kommunikationsnät eller som lagras i ett moln.

En förmedlande mellanhand får inte initiera överföring, välja mottagare, välja information eller ändra i information som överförs i mellanhandens kommunikationsnät.[209] Däremot får information genomgå automatisk, mellanliggande och tillfällig lagring som sker endast för att effektivisera vidare överföring.[210]

Vid lagringstjänster krävs att tjänsteleverantören inte är medveten om att det förekommer, i händelse av att det skulle visa sig förekomma, olaglig information

[205] Prop. 2001/02:150.

[206] 1 § 1 st., E-handelslagen; Direktiv 200/31/EG, artikel 12 - 14.

[207] 1 § 2 p., E-handelslagen; Direktiv 2000/31/EG, artikel 1.5 b.

[208] Dataskyddsförordningen, artikel 4.2.

[209] 16 §, E-handelslagen.

[210] 17 §, E-handelslagen.

eller olaglig verksamhet och att så snart han får sådan kännedom eller medvetenhet utan dröjsmål förhindrar vidare spridning av informationen.[211]

Frångår en tjänstelevererande mellanhand ovanstående principer blir de, med andra ord, personuppgiftsansvariga för den behandling som utförs utöver uppdraget som mellanhand och ska följa de förpliktelser som åtföljs av detta ansvar avseende den utökade behandlingen.

Ansvarsfriheten gäller innehållet i informationen som förmedlas eller lagras och avser skadestånd och sanktionsavgifter under förutsättning att kraven, såsom oförändrad information och förhindrande av vidare spridning, efterlevs.[212] En tjänsteleverantör kan dock dömas till ansvar för brott som avser innehållet i informationen, om brottet har begåtts uppsåtligen.[213]

5.2.3 Mottagare

> *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte.[214]

Denna kategori är den som framstår som minst omskriven. Å andra sidan är definitionen relativt tydlig och skiljer sig inte konceptuellt från definitionen i dataskyddsdirektivet.[215] Begreppet infördes i dataskyddsdirektivet som ett led i att åstadkomma transparens av personuppgiftsbehandling i förhållande till en registrerad.[216] Detta syfte återspeglas tydligt även i dataskyddsförordningen.[217]

---

[211] 18 §, E-handelslagen.

[212] 16 - 18 §§, E-handelslagen.

[213] 19 §, E-handelslagen.

[214] Dataskyddsförordningen, artikel 4.9.

[215] Dataskyddsdirektivet, artikel 2 g.

[216] GEMENSAM STÅNDPUNKT (EG) nr 1/95 antagen av rådet den 20 februari 1995 inför antagandet av Europaparlamentets och Rådets direktiv 95/. . ./EG om skyddet för enskilda personer med avseende på behandlingen av personuppgifter och om det fria flödet av sådana uppgifter (95/C 93/01), CELEX:51995AG0413(01), se exempelvis artikel 10 och 11.

[217] Se bl. a. dataskyddsförordningen, skäl 61, artikel 13.1 e & f, 14.1 e & f, 14.3 c, 15.1 c och 19.

5.2.4 Tredje part

> *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.[218]

Artikel 29-gruppen beskriver denna kategori som en ”återstod”, det är ingen av de andra definierade parterna och inte helt olikt den traditionella civilrättens definition: en person som varken ingår i en enhet eller i ett avtal.[219]

Som exempel nämns att ”personer som arbetar för en annan organisation, även om den tillhör samma koncern eller holdingföretag, i allmänhet är tredje män”.[220] I det här fallet rör det sig således om en aktör som inte har någon särskild legitimitet eller något särskilt tillstånd i fråga om behandling av personuppgifter.[221]

En tredje part kan även få personuppgifter överförda till sig. En tredje part som tar emot personuppgifter – oavsett om det är lagligt eller ej – blir i princip en ny registeransvarig.[222] För att tredje part ska ha laglig rätt att få personuppgifter överförda till sig krävs ett berättigat intresse.[223] Datainspektionen nämner exempel såsom överföringar av personuppgifter mellan flera separata personuppgifts-ansvariga inom koncerner, där mottagarna anses vara tredje part.[224] Det berättigade intresset kan vara för att förhindra bedrägerier eller för direktmarknadsföring.[225]

[218] Dataskyddsförordningen, artikel 4.10.
[219] Artikel 29-gruppen, *WP 169*, ss. 31, 33.
[220] A.a., s. 30.
[221] A.a., s. 33.
[222] A.a., s. 31.
[223] Dataskyddsförordningen, skäl 47 och 69, artikel 6.1 f, 13.1 d och 14.2 b.
[224] Se kap. 5.3, Mottagare.
[225] Datainspektionen, *Intresseavvägning*, 2019.

6. Sammanfattning och diskussion

6.1 Inledning

Först och främst behöver det påminnas om att dataskyddsförordningen reglerar *behandling* av personuppgifter. För det andra behöver det förtydligas att behandling kan vara en, en kombination av eller en del av en kombination av *åtgärder*. Del av en kombination av åtgärder kan vara allt ifrån en enkel åtgärd till en kombination av åtgärder, en kombination som i sin tur kan bestå av flera delar i flera nivåer i komplexa behandlingsstrukturer. För det tredje behöver det påpekas att *avtal* varken är konstituerande eller ansvarsfördelande enligt dataskyddsförordningen. Det är den *faktiska* bestämmanderätten som styr hur ansvarsfördelningen ser ut.

Bestämmanderätten kan delas upp i två huvudgrupper: ”vad och varför” samt ”hur”. *Vad* (vilka personuppgifter) som behandlas och *varför* behandling sker bestäms alltid av personuppgiftsansvarig, ensamt eller gemensamt med andra personuppgiftsansvariga. *Hur* behandling ska ske kan delas upp i väsentliga och oväsentliga element. De väsentliga elementen bestäms alltid av en personuppgifts-ansvarig, ensamt eller gemensamt med andra personuppgiftsansvariga, de oväsentliga elementen kan delegeras till personuppgiftsbiträde som också kan utföra själva behandlingen efter ansvarigs instruktioner.

Lagstiftning kan däremot fördela ansvar enligt andra principer men gäller främst offentliga organ.

6.2 Gränsdragningsproblematiken

Numera är det relativt tydligt hur extensivt begreppen personuppgifter och behandling ska tolkas.[226] De uppenbara problem som istället uppstår, för att kunna svara på uppsatsens huvudfråga om vem som är personuppgiftsansvarig, är gränsdragningen för vad som ska betecknas som *bestämmande* och framförallt kring *gemensamt bestämmande*, när flera parter är inblandade. Praxis visar att man

[226] Se kap. 2.4.2, Personuppgifter och 2.4.3, Behandling.

kan riskera att bli gemensamt personuppgiftsansvarig för all behandling, om man så bara kan göra en enkel åtgärd för konfiguration som påverkar *varför*.[227] Om generaladvokatens argumentation i mål Fashion ID anammas av EU-domstolen skulle bestämmandet av det faktum *att* behandling av personuppgifter görs möjlig, där ingen åtgärd för konfiguration föreligger eller andra möjligheter att påverka den fortsatta behandlingen finns, begränsa det gemensamma personuppgiftsansvaret till den del av behandlingen som kan härledas till den gemensamma behandling som gör fortsatt behandling möjlig. Vilket, i förevarande mål, omfattar insamlingen och överföringen av personuppgifter.

Vidare kan frågan om principalansvarets gränser gällande personuppgiftsansvarig ställas. Praxis visar att så länge en organisation kan ha nytta av enskildas behandling av personuppgifter, med ett förmodat oupplösligt samband – både mellan den enskilda och organisationen och mellan personuppgiftsbehandlingen och organisationen – så träder principalansvaret in.[228] Gränsen för vad som ska anses vara till nytta för organisationen är oklar men samma praxis visar att den inte behöver vara av ekonomisk karaktär. Likaså kan man tänka sig att gränsen för vad som ska anses vara enskilda individers koppling till en organisation är oklar. Måste man vara anställd, medlem eller på annat sätt företräda organisationen? Skulle principalansvaret kunna träda in om man t.ex. är i familj med någon som har koppling till en organisation, om behandlingen av personuppgifter är till nytta för och har ett oupplösligt samband med organisationen?

Att fastställa var den faktiska bestämmanderätten ligger är också ett gränsdragningsproblem, inte minst i komplexa organisationsstrukturer. Det krävs en noggrann analys av maktstrukturer och oupplösliga samband, vilket inte alltid är en enkel uppgift.

6.3 Granularitetsproblemet

Öppenhetsprincipen i dataskyddsförordningen förutsätter att det är klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas. Det krävs också att all information och

[227] Wirtschaftsakademie, C-210/16, p. 36.

[228] Jehovan todistajat, C-25/17.

kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig.[229] Som konstateras av Artikel 29-gruppen kan ”[…] fördelningen på flera registeransvariga också kan leda till oönskad komplexitet och bristande tydlighet i fråga om ansvarsfördelningen. Detta kan leda till att hela behandlingen blir otillåten på grund av bristande insyn och strider mot principen om rättvis behandling.”[230] Med generaladvokatens resonemang i mål Fashion ID ökar granulariteten avsevärt och det kan, i komplexa arrangemang, innebära att hela behandlingen blir otillåten. Generaladvokaten bemöter inte denna problematik.

6.4 Diskussion kring mål Fashion ID

6.4.1 Personuppgiftsansvaret

Generaladvokaten vill begränsa det gemensamma personuppgiftsansvaret till den del av behandlingen som kan härledas till den *gemensamma behandling* som gör fortsatt behandling möjlig, i det här fallet insamlingen och överföringen. Men generaladvokaten gör en tankevurpa i sitt resonemang, enligt min mening. Han drar nämligen slutsatsen att domstolen skulle kommit fram till sina domslut i målen Jehovan todistajat och Wirtschaftsakademie mer eller mindre för att dessa båda ”[…] ’gjort det möjligt’ att samla in och översända personuppgifter […]”[231] och anser att i så fall borde, i förlängningen, även elbolaget vara gemensamt personuppgiftsansvarig eftersom de ”gjort det möjligt”.[232] Därför ger han sig också ut i ett resonemang kring att två eller flera aktörer måste ”ha *samma ändamål och medel*”, det vill säga situationer där båda definitionerna förekommer i kombination, för att kunna anses vara gemensamt personuppgiftsansvariga.[233] Fördelen skulle bli att endast den som de facto har kontroll över och har möjlighet att påverka insamlade uppgifter samt kan påverka den efterföljande behandlingen därmed skulle anses vara ensamt personuppgiftsansvarig för detta. En sådan tolkning skulle emellertid kräva att Artikel 29-gruppen skrev om sina yttranden och att EU-domstolen ändrade sin praxis.

[229] Se bl.a. dataskyddsförordningen, skäl 39, artikel 12, 13, 14 och 15.
[230] Artikel 29-gruppen, *WP 169*, s. 24.
[231] A.a., p. 73.
[232] A.a., p. 74.
[233] A.a., p. 100.

Själv ser jag ingen anledning att ändra tolkning, yttrande och praxis. Enligt direktiv och förordning räcker det inte med att ”göra behandling möjlig” för att kunna anses vara ansvarig. Man måste *bestämma* också. Elbolaget har ju varken varit med om att *bestämma* ”*vad*”, ”*varför*” eller de, för förordningens begrepp personuppgiftsansvarig likaledes grundläggande, väsentliga elementen av ”*hur*”, rörande själva behandlingen och blir därmed automatiskt befriad från ansvar.

Enligt gällande rätt skulle Fashion IDs personuppgiftsansvar kunna härledas till ett bestämmande av *medel*, ett väsentligt element i *hur*, även för den fortsatta behandlingen. Medlen för behandlingen, åtminstone en väsentlig del av medlen, är insticksprogrammet. Det må vara Facebook som bestämt hur insticksprogrammet ska bete sig men bestämmandet att detta insticksprogram ska användas utan att informera de registrerade görs uteslutande av Fashion ID, gällande deras hemsida. Alltså uppstår gemensamt personuppgiftsansvar genom gemensamma beslut kring de väsentliga medlen för all personuppgiftsbehandling relaterad till insticksprogrammet, för de personuppgifter som kan härledas komma från Fashion IDs hemsida. Personuppgiftsbehandlingen går nämligen, ur min synvinkel, inte att separera. All behandling sker genom Facebooks försorg, automatiskt och direkt, i en serie åtgärder där Fashion ID endast är med och bestämmer de väsentliga element av *hur*. Det gemensamma personuppgiftsanvaret inträder oavsett om man kan komma fram till någon form av *varför*, ett varför som diskuteras vara osäkert i målet.

Men det måste finnas mer. Om insamlingen skett efter regelrätt inhämtande av samtycke från Facebook först när en besökare klickade på ”gilla”-knappen, hade Fashion ID fortfarande kunnat anses vara gemensamt personuppgiftsansvarig för den behandling som Facebook gör endast tack vare det faktum att man integrerat deras ”gilla”-knapp på sin hemsida? Fashion ID är ju fortfarande med och bestämmer om en väsentlig del av *hur*, även om det inte sker någon behandling förrän efter godkänt samtycke… Och det är väl där den springande punkten ligger. Det sker ingen behandling. Inte förrän besökaren samtyckt till Facebooks förfrågan. Alltså bestämmer Fashion ID inte längre något väsentligt element av hur. Finns det däremot ett gemensamt beslut om *varför*, t.ex. en ökad frekvens av annonser i flödet hos Facebook när besökaren tryckt och accepterat samtycke, då är Fashion ID

gemensamt personuppgiftsansvarig igen och behöver se till att samtycke även inhämtats för deras räkning, innan behandlingen påbörjas.

6.4.2 Granulariteten

Alternativet till en ökad detaljnivå och risken att behandlingen i sin helhet blir otillåten, skulle kunna vara om EU-domstolen i mål Fashion ID istället vidhåller sin praxis från mål Wirtschaftsakademie, där Wirtschaftsakademie ansågs gemensamt personuppgiftsansvariga för all personuppgiftsbehandling. I enlighet med resonemanget ovan blir därmed Fashion ID gemensamt personuppgiftsansvarig, skyldig att förvissa sig om den efterföljande behandlingens innebörd och åläggs skyldigheten att informera de registrerade om densamma. Därmed skulle man uppfylla öppenhetsprincipen och principen om rättvis behandling. Dessutom skulle behandlingen vara tillåten, ur komplexitetssynvinkel.

6.4.3 Samtycket

Vidhållandet vid nuvarande praxis löser även problemet med vem som ska inhämta samtycke. Den gemensamt personuppgiftsansvariga vars resurs är den som möter en potentiellt registrerad initialt, för insamling av personuppgifter, och därmed medverkar till vidare personuppgiftsbehandling, torde vara bäst lämpad att inhämta samtycke till den fortsatta behandlingen. Det torde även ligga i resursägarens intresse. Uppdelat personuppgiftsansvar, med krav på att var och en av de personuppgiftsansvariga skulle inhämta samtycke för sin behandling, skulle nämligen kunna generera ett otal antal samtyckesdialoger. En användare hade kanske svårligen kommit fram till den sökta hemsidan eller, på ett rimligt sätt, kunnat få möjligheten att lämna samtycke till vidare behandling till någon annan - i t.ex. ett fysiskt möte. Det ger definitivt bristande insyn och är ingen rättvis behandling av registrerade. Tysklands ombud konstaterar att det inte finns något hinder för att en sådan lösning, där samtycke inhämtas av initial resurs, regleras genom avtal.[234] Naturligtvis finns det heller inget som hindrar att man separerar personuppgiftsansvaret, om insamling och behandling endast sker för en parts räkning, efter regelrätt samtycke, t.ex. först när besökare klickar på ”gilla”-knappen. Det viktiga är att samtycke till behandling, till *all* behandling när flera parter med gemensamt personuppgiftsansvar ”delar” på uppgifterna, har inhämtats

[234] Fashion ID, C-40/17, p. 79.

innan insamling, överföring eller annan behandling påbörjas.[235] Vid gemensamt personuppgiftsansvar bör den information som behöver lämnas till en registrerad i samband med samtycke, med enkelhet kunna finnas med i de avtalsvillkor eller användarvillkor som accepteras i och med integreringen av ett insticksprogram eller vad det än är som föranleder en överföring av personuppgifter för vidare behandling. Är informationen tillgänglig kan den, likaledes relativt enkelt, medfölja avtal och villkor nedströms i komplexa förhållanden och presenteras för en tilltänkt registrerad.

6.4.4 Avtal

Nästa tankevurpa som generaladvokaten gör, enligt min mening, är att förvilla sig bort i en diskussion om behovet av ett stort antal avtal kring ansvarsfördelning,[236] vilket man varken enligt direktivet eller förordningen kan avtala bort. Istället kunde kanske *ett* standardavtal tänkas fungera för alla i liknande situationer. Ett endaste standardavtal, där den part som har kontroll över personuppgifterna förpliktigades att efterleva dataskyddsförordningens skyldigheter rörande sådant som bara den som har kontroll över uppgifterna kan uppfylla.[237] Men inte bara på den registrerades begäran utan också på den gemensamt personuppgiftsansvarigas begäran. Förslagsvis kompletteras avtalet med ett skadeståndsskydd, i händelse att part som inte har möjligheten att påverka personuppgifter eller dess behandling drabbas av skadestånd eller sanktionsavgifter till följd av kontrollerande parts underlåtenhet, vilket kan bli fallet givet dataskyddsförordningens utformning.[238] Ett sådant avtal fördelar inte det direkta ansvaret gentemot en registrerad i förordningens mening, utan bara den ekonomiska fördelningen mellan parterna i händelse av skada eller sanktioner.

6.4.5 Olika ansvar

Ovanstående framstår inte förhindrande till beaktandet av ”att den omständigheten att det finns ett gemensamt ansvar inte nödvändigtvis behöver innebära att de olika aktörer som medverkar vid behandlingen av personuppgifter har likvärdigt ansvar.

---

[235] Dataskyddsförordningen, artikel 6.1 a.; Se även Artikel 29-gruppen, *WP 208 : Yttrande 2/2013 med vägledning om inhämtande av samtycke för kakor*; *WP 187 : Yttrande 15/2011 om definitionen av begreppet samtycke.*

[236] Fashion ID, C-40/17, p. 85, 86.

[237] I enlighet med dataskyddsförordningen, artikel 26.

[238] Se t.ex. dataskyddsförordningen, artikel 26.3.

… dessa aktörer [kan] vara involverade i olika skeden av behandlingen och i olika utsträckning, så att ansvaret för var och en av dem ska bedömas med beaktande av alla relevanta omständigheter i fråga”,[239] i enlighet med tidigare praxis. Även om man anses vara gemensamt personuppgiftsansvarig för *all* behandling, så kan man fortfarande bara anses ha medverkat vid *samma behandling* till en begränsad del.[240]

6.4.6 Slutsats i mål Fashion ID

Fashion ID är gemensamt personuppgiftsansvarig med Facebook för all behandling av personuppgifter som följer av den personuppgiftsinsamling som sker via Fashion IDs hemsida genom Facebooks integrerade ”gilla”-knapp, så länge personuppgiftsbehandlingen sker direkt, automatiskt och utan föregående uttryckliga samtycke från besökare. Bedömningen grundas i att Fashion ID anses ha bestämt väsentliga element av *hur* personuppgiftsbehandling ska göras, i och med integrerandet av Facebooks ”gilla”-knapp på sin hemsida.

[239] Wirtschaftsakademie, C-210/16, p. 43.

[240] Relevant i förhållande till dataskyddsförordningen, artikel 82, *Ansvar och rätt till ersättning*, p. 3 och 4.

7. Slutsatser

För att kunna anses vara personuppgiftsansvarig krävs att någon form av behandling av personuppgifter, om så endast en uppgift, sker enligt dataskyddsförordningens definition av behandling. Behandling omfattar inte bara själva utvinnandet av information från en mängd personuppgifter, oavsett syfte, utan även kringåtgärder såsom insamling, överföring och lagring. Från nedtecknande av personuppgifter på papper till överföring från kameralins till minneskort, där lagringen på minneskortet allena är ytterligare en egen form för behandling. Med inblandning av någon form för elektronisk apparatur kan förmodligen all hantering av personuppgifter anses vara behandling delvis företagen på automatisk väg.

Undantag från personuppgiftsansvar finns bland annat för tjänstelevererande mellanhänders behandling, gällande överföring och lagring, och för fysisk persons behandling som är av rent privat natur.

Vem är ensamt personuppgiftsansvarig enligt dataskyddsförordningen?

Den som bestämmer vad, varför *och* väsentliga element av hur.

Det vill säga:

1. Den som bestämmer *vad* som ska samlas in – vilka personuppgifter, beaktande att även indirekt identifierbara uppgifter, som till och med kan kräva domstolsbeslut för att få åtkomst till kompletterande information, kan vara personuppgifter. Inkluderat kunskapsnivå, tankebanor, handstil, dynamiska IP-adresser och transportmönster.
2. Den som bestämmer *varför* personuppgifter ska samlas in – om så bara för att det är bra att ha eller för att man kan.
3. Den som bestämmer väsentliga element av *hur* behandlingen ska göras eller ens vara möjlig – inkluderat genom vilka medel som används vid insamlingen (t.ex. integrerade tredjeparts insticksprogram på en webbsida eller uppmaningen att skriva på papper), hur länge uppgifter ska lagras (om så bara under själva behandlingen), vilka metoder som ska tillämpas för att nå önskat resultat och vilka kriterier som är relevanta eller ska styra.

Den som ensamt bestämmer alla tre momenten ovan, kommer att anses vara *ensamt* personuppgiftsansvarig enligt dataskyddsförordningen.

Tänk speciellt på:

Framförallt det sista kriteriet, *väsentliga element av hur*, är osäkert och inte lika tydligt definierat i praxis, soft law eller doktrin som de två andra. Nuvarande information tyder på att även detta begrepp ska tolkas extensivt.

Vid personuppgiftsbehandling av fysisk person i beroendeställning till en organisation är det högst sannolikt att *och* kan komma att bytas ut mot *eller*, motsvarande gemensamt personuppgiftsansvar nedan, vid bedömning av ansvar. Konsekvensen blir, också högst sannolikt, att principalansvaret renderar organisationen *ensamt* personuppgiftsansvarig – trots begränsat bestämmande. Framförallt vid den bedömningen att organisationen har uppmuntrat eller haft någon form för nytta av behandlingen.

När uppstår gemensamt personuppgiftsansvar?

Gemensamt personuppgiftsansvar uppstår när mer än en part är med och bestämmer vad, varför *eller* väsentliga delar av hur - enligt definition ovan.

Tänk speciellt på:

Ett medbestämmande kan ta sig många uttryck. En medbestämmande part kan bestämma om insamlandet av en ”extra” personuppgift men det kan även gälla bestämmande om begränsningar, t.ex. vid val av mjukvara för insamling eller annan behandling. Detta påverkar *vad*. Även om man varken får del av personuppgifter eller resultat av behandling kan det betraktas som ett medbestämmande av *varför* så snart det finns någon form för vinning eller utbyte av tjänster mellan två eller flera parter. Åtminstone när det är grundat genom hantering av personuppgifter.

Vid komplexa strukturer är det den som innehar den *faktiska* bestämmanderätten som blir åtminstone gemensamt personuppgiftsansvarig, om inte ensamt. Inom koncerner får man även beakta *oupplösliga samband*, vilka kan påverka bedömningen och leda till att ett huvudkontor eller moderbolag anses vara ensamt eller gemensamt personuppgiftsansvariga för en filials personuppgiftsbehandling.

Speciellt om avtal

Inga avtal kan ändra på personuppgiftsansvar, det är en bedömning av *faktisk* bestämmanderätt som avgör. Oavsett om bestämmanderätten är uttrycklig, underförstådd eller baserad på inflytande.

Slutord

Även om ett försök till ett praktiskt och användbart tillvägagångssätt för att utröna vem som är personuppgiftsansvarig lämnats ovan, så är min uppfattning att det enda man kan säga med säkerhet är att all personuppgiftsbehandling som omfattas av dataskyddsförordningen kräver att någon tar ansvar för densamma. Vem denna någon är kan dock, i slutändan, behöva tolkas i ljuset av EU:s grundläggande fördrag, stadgor och allmänna rättsprinciper i kombination med syftet för dataskyddsförordningen, befintlig praxis och med beaktande av internationella avtal.

Käll- och litteraturförteckning

Offentligt tryck

Sverige

Kommittédirektiv 1989:26, ”Översyn av datalagen”.

Dir. 1995:91, Ny datalag m.m. .

SOU 1972:47, Data och integritet.

SOU 1997:39, Integritet ´ Offentlighet ´ Informationsteknik.

Prop. 1951:165, angående godkännande av Sveriges anslutning till Europarådets konvention angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. (Bet. 1951:UU11, Rskr. 1951:2).

Prop. 1953:32, angående avgivande av förklaring enligt artilkel 46 i den europeiska konventionen angående skydd.

Prop. 1997/98:44, Personuppgiftslag.

Europeiska unionen

Commission of the European Communities, “Community Policy on Data Processing”, Communication of the Commission to the Council, SEC(73) 4300 final, 21 November 1973.

Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, OJ L 246, 29/08/1981, p. 31, CELEX:31981H0679.

Commission of the European Communities, “Completing the Internal Market”, White Paper from the Commission to the European Council, COM(85) 310 final, 14 June 1985.

Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the

Community and information security, COM(90) 314 final, SYN 287 and 288, 13 September 1990, CELEX:51990DC0314.

European Parliament, Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992, 11 March 1992 (First Reading) O.J. 13 april 1992, C 94 s. 173-201, OJ:C:1992:094:TOC

GEMENSAM STÅNDPUNKT (EG) nr 1/95 antagen av rådet den 20 februari 1995 inför antagandet av Europaparlamentets och Rådets direktiv 95/. . ./EG om skyddet för enskilda personer med avseende på behandlingen av personuppgifter och om det fria flödet av sådana uppgifter. EUT C 93, 13 april 1995, s. 0001, CELEX:51995AG0413(01).

Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, EUT C 306, 17 december 2007, CELEX:12007L/TXT.

KOMMISSIONENS MEDDELANDE TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN OCH REGIONKOMMITTÉN, Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen, KOM/2010/0609 slutlig, 4 november 2010, CELEX:52010DC0609.

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), COM/2012/011 final - 2012/0011 (COD), 25 januari 2012, CELEX:52012PC0011.

Rådets ståndpunkt vid första behandlingen inför antagandet av EUROPAPARLAMENTETS OCH RÅDETS 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/EC (allmän dataskyddsförordning)”, 5419/16, 6 april 2016, CELEX:52016AG0006(01).

Artikel 29-gruppen, *WP 128 : Yttrande 10/2006 om behandling av personuppgifter hos SWIFT (Society for Worldwide Interbank Financial Telecommunication).*

Artikel 29-gruppen, *WP 136 : Yttrande 4/2007 om begreppet personuppgifter.*

Artikel 29-gruppen, *WP 169 : Yttrande 1/2010 om begreppen registeransvarig och registerförare*.

Artikel 29-gruppen, *WP 179 update : Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain*.

EUROPEAN DATA PROTECTION SUPERVISOR, *EDPS opinion on the role of the European Central Bank in the SWIFT case*.

Europarådet CETS 108, Konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.

Europarådet, ministerkommittén (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private, 26 september 1973, doc.id: 0900001680502830.

Europarådet, ministerkommittén (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 september 1974, doc.id: 16804d1c51.

FN, Allmän Förklaring om de mänskliga rättigheterna.

FN, Konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Förenta Nationernas stadga.

Litteratur

van Alsenoy, Brendan, *Regulating data protection; The allocation of responsibility and risk among actors involved in personal data processing*, KU Leuven, 2016.

Hettne, Jörgen och Otken Eriksson, Ida (red.), *EU-rättslig metod : Teori och genomslag i svensk rättstillämpning*, 2:a uppl., Stockholm, Norstedts Juridik, 2011.

Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*, uppl. 2:1, Studentlitteratur, Lund, 2018.

Lambert, Paul, *Understanding the new European data protection rules*, Florida, CRC Press, 2018.

Artiklar

Freese, Jan., *Datainspektionen*, SvJT 1979, s. 498.

Internetkällor

CNBC, *Here's everything you need to know about the Cambridge Analytica scandal*, 21 mars, 2018. https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html, senast hämtad kl. 18:33, 22 april 2019.

Datainspektionen, *Intresseavvägning*, 2019. https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/intresseavvagning/, senast hämtad kl. 14:16, 30 april 2019.

Europarådet, *Details of Treaty No. 108*, 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108, senast hämtad kl. 12:13, 9 april 2019.

Europarådet, *Sweden*, 2018. https://www.coe.int/sv/web/portal/sweden, senast hämtad kl. 17:01, 8 april 2019.

FN, *FN:s historia*, 2019. https://fn.se/vi-gor/vi-utbildar-och-informerar/fn-info/fn-som-organisation/fns-historia/, senast hämtad kl. 16:30, 8 april 2019.

FN, *FNs medlemsländer*, 2019. https://fn.se/vi-gor/vi-utbildar-och-informerar/fn-info/fn-som-organisation/medlemslander/, senast hämtad kl. 16:41, den 8 april 2019.

Hessisches Hauptstaatsarchiv, HHStAW Bestand 557, Datenschutzbeauftragter, 2007. https://arcinsys.hessen.de/arcinsys/detailAction.action?detailid=b2988, senast hämtad kl. 20:23, 8 april 2019.

ICO, Determining what information is 'data' for the purposes of the DPA, ver. 1.1., 2012. https://ico.org.uk/media/for-

organisations/documents/1609/what_is_data_for_the_purposes_of_the_dpa.pdf, senast hämtad kl. 18:04, 15 maj 2019.

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum, senast hämtad kl. 14:22, 10 april 2019.

Rättsfallsförteckning

Europeiska unionen

EU-domstolen

Dom av den 20 maj 2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294.

Dom av den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596.

Dom av den 16 december 2008, Satakunnan och Satamedia, C-73/07, EU:C:2008:727.

Dom av den 16 december 2008, Huber, C-524/06, EU:C:2008:724.

Dom av den 7 maj 2009, Rijkeboer, C-553/07, EU:C:2009:293.

Dom av den 24 november 2011, Scarlet Extended, C-70/10, EU:C:2011:771.

Dom av den 30 maj 2013, Worten, C-342/12, EU:C:2013:355.

Dom av den 17 oktober 2013, Schwarz, C-291/12, EU:C:2013:670.

Dom av den 7 november 2013, IPI, C-473/12, EU:C:2013:715.

Dom av den 13 maj 2014, Google Spain och Google, C-131/12 P, EU:C:2014:317.

Dom av den 11 december 2014, Ryneš, C-212/13, EU:C:2014:2428.

Dom av den 19 oktober 2016, Breyer, C-582/14, EU:C:2016:779.

Dom av den 20 december 2017, Nowak, C-434-16, EU:C:2017:994.

Dom av den 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388.

Dom av den 10 juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551.

Dom av den 14 februari 2019, Buivids, C-345/17, ECLI:EU:C:2019:122.

Förslag till avgörande, föredraget den 19 december 2018, Fashion ID, C-40/17, EU:C:2018:1039.