bara vara dataskyddsombud (dso): lillebrors stol, bestick och bordsskick

*Olle Pettersson**

1. Inledning

Rollen dataskyddsombud (”DSO”) har tidigare beskrivits som en rådgivare och revisor[1] som inte ska besluta om personuppgiftsbehandling,[2] en mellanhand som manifesterar principen om ansvarsskyldighet,[3] samt en orkesterdirigent som bäddar in kulturell och regulatorisk praxis och mekanismer i verksamheter för att effektivt uppnå efterlevnad av **gällande dataskyddsregler**[4].[5] Rollen har numera också liknats vid en relativt oberoende lillebror till tillsynsmyndigheterna för reglerna (dataskyddsmyndigheterna eller ”storasystrarna”).[6]

Rollen blev till genom EU:s reform av **tidigare dataskyddsregler**[7] och reglerar utnämning, ställning och uppgifter. Ställningen ger DSO (”utförare”) skydd bland annat mot repressalier från organisationen

* Författaren vill utan inbördes ordning tacka följande personer för synpunkter på denna text: Johan Borre, Martin Brinnen, Hans-Olof Lindblom, Joakim Söderberg, David Törngren, Monika Wendleby, Daniel Westman och Paulo Zavala.

[1] Andra menar att ”revisor” blir missvisande eftersom DSO inte ska kontrollera om verksamhetens mål uppfylls, se exempelvis Wendleby, Dataskyddsombud ska vara oberoende – analys, 2022-08-12, JPinfonet.

[2] Westman, Dataskyddsförordningen, artikel 39, Karnov 2022-07-01 (JUNO).

[3] Magnusson Sjöberg, Dataskyddsförordningen, artikel 38, Lexino 2020-09-04 (JUNO).

[4] Förordning (EU) 2016/679 (EU:s dataskyddsförordning, DSF) (kompletterad i svensk rätt i lagen [2018:218] med kompletterande bestämmelser till DSF, DSL, och domstolsdatalagen [2015:728], DDL), direktiv (EU) 2016/680 (EU:s brottsdatadirektiv, BDD) (implementerad i svensk rätt i brottsdatalagen [2018:1177], BDL), förordning (EU) 2018/1725 (motsvarighet till DSF för EU:s institutioner och organ, EU DSF) och direktiv 2002/58/EG (EU:s e-Dataskyddsdirektiv, eDD) (som EU-kommissionen år 2017 föreslagit ska ersättas med en EU-förordning, vilket dock inte ännu lett till lagstiftning, se förslag COM(2017) 10 final, eDSF).

[5] Alvarez Rigaudias & Spina i Kuner, Bygrave, & Docksey (red.), The EU General Data Protection Regulation (GDPR): a commentary (Oxford University Press, 2020) (”Oxfordkommentaren till DSF”), kommentaren till artikel 37, avsnitt C.7.

[6] Se avsnitt 3.3.3 nedan.

[7] Direktiv 95/46/EG (EU:s dataskyddsdirektiv, DD) (vilket implementerades i svensk rätt i personuppgiftslagen [1998:204], PUL) och förordning (EG) nr 45/2001 (regler för EU:s institutioner och organ, förordning 45/2001).

som utnämnt DSO (”utnämnare”)[8]. EU-domstolen (”EUD”) har uttalat att skyddet inte får äventyra förverkligandet av målen med dataskyddsreglerna, vilket exempelvis skulle ske om utnämnare inte kunde avsätta DSO som inte har de kvalifikationer som krävs eller som inte utför uppdraget på rätt sätt.[9] Det väcker följdfrågor, bland annat vilka kvalifikationer som krävs för att utföra uppdraget och vad som är rätt sätt att göra det.

Svaren beror nog på omständigheterna, men även vem man frågar. Enligt en undersökning anser många DSO att de inte har tillräcklig tid och att det är otydligt vad de ska åstadkomma.[10] Vissa DSO har gjort gällande att utnämnare har svårt att förstå varför de ska ha ett DSO, inte har bett om det och saknar kunskap om rollens uppdrag och funktion.[11]

Europeiska dataskyddsstyrelsen (”EDPB”),[12] som tidigare antagit riktlinjer om rollen,[13] genomför under år 2023 en gemensam åtgärd för att tydliggöra rollen. I Sverige sker det genom att Integritetsskyddsmyndigheten (”IMY”)[14] genomför tillsyn av cirka fyrtio utnämnare, och bland annat frågar om ledningen tydligt definierat DSO:s uppgifter, om vilka arbetsuppgifter DSO har, om DSO har tillräckliga resurser, och om DSO:s råd följs.[15] Förhoppningsvis leder åtgärden till tydliga och enhetliga svar på alla tänkbara frågor.[16]

I det följande beskrivs först kort gällande och tidigare reglering. Vidare diskuteras vad som bör vara vägledande för tolkningen av bestämmelserna. Därefter diskuteras några praktiska utmaningar[17] för DSO:s position,

[8] Ordet ”utnämnare” avser i denna text den aktör som utnämnt DSO, vilket kan vara en personuppgiftsansvarig eller ett personuppgiftsbiträde (eller både och) enligt gällande dataskyddsregler.

[9] Dom i Leistritz (C-534/20, EU:C:2022:495, punkt 35).

[10] IMY rapport 2023:1, Dataskyddsarbetet i praktiken – En studie av förutsättningar för arbetet med dataskyddsfrågor i verksamheter som är skyldiga att ha dataskyddsombud, s. 8, 15 och 17.

[11] Lindgren Schelin, IMY:s webbplats, sidan ”Dataskyddsombudens svar oroar”, 2023-01-28.

[12] Cheferna för EU:s dataskyddsmyndigheter (tillika EU:s klubb för storasystrar inom dataskydd).

[13] Riktlinjer om dataskyddsombud WP 243 rev.01 (”WP 243”), senast granskade och antagna den 5 april 2017 av arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG (”Artikel 29-arbetsgruppen”), som sedan förordning (EU) 2016/679 trädde i kraft har ersatts av EDPB, som i sin tur antog dem som sina egna vid sitt första möte den 25 maj 2018.

[14] Artisten tidigare känd som Datainspektionen, tillsynsmyndighet (och storasyster) i Sverige.

[15] IMY, pressmeddelande, 2023-06-12.

[16] Om inte annat lär väl utnämnare vilja veta vad fan de får för pengarna och utförare om de får fan för pengarna (och ingen av dem vilja behöva måla fan på väggen om storasyster skulle sparka in dörren i en gryningsräd och ropa ”habeas DSO:us!” eller ”var är lillebror och vad gör han, *egentligen*?”).[a]

[a] Denna fotnot är lika absolut strikt nödvändig som stenen är sval mot pannan.

[17] Som framkommit i diskussioner med olika intressenter, som här inte bör nämnas (förutom DSO Voldemort).

uppgifter och förhållningssätt – eller, putslustigt uttryckt, lillebrors stol, bestick och bordsskick – och hur de kan lösas.[18] Sist några avslutande ord.

2. Gällande och tidigare reglering samt vad som bör vara vägledande

2.1 Gällande reglering

Rollen DSO är reglerad i tre regelverk på EU-nivå (DSF, EU DSF och BDD) som delvis kompletteras med bestämmelser på nationell nivå (nedan ”regleringen om DSO”)[19]. I korthet innebär regleringen att aktörer som behandlar personuppgifter på sätt som typiskt sett medför förhöjda risker för enskildas fri- och rättigheter ska *utnämna* ett DSO, som ska ha en oberoende *ställning* och som i vart fall ska utföra vissa *uppgifter* på ett visst sätt.[20]

Rollen bör tolkas enhetligt eftersom syftet bakom och huvuddragen i regleringen är samma i regelverken.[21] Övriga regelverk bör till exempel kunna vägleda när en fråga inte i detalj är reglerad i ett av dem men i de andra (såsom gällande avsaknaden av stadganden om repressalieförbud och intressekonflikter i BDD)[22] eller när bara ett av dem tolkats av EUD (såsom gällande repressalieförbud och intressekonflikter i DSF)[23].[24]

2.2 Tidigare reglering

Innan regleringen om DSO infördes fanns en liknande roll, personuppgiftsombud (”PUO”). Rollen var olika detaljerad i de EU-regelverk som gällde nationellt (DD)[25] respektive för EU:s institutioner och organ (för-

[18] Författarens inställning överensstämmer inte nödvändigtvis med tidigare eller nuvarande arbetsgivares.
[19] Artiklarna 37–39 i DSF (kompletterade i svensk rätt avseende tystnadsplikt i 1 kap. 8 § DSL och 10 § i DDL), 32–34 i BDD (implementerade i svensk rätt genom 3 kap. 13–15 §§ i BDL) och 43–45 i EU DSF.
[20] Den närmare regleringen beskrivs i relevanta delar inom ramen för respektive praktisk utmaning nedan.
[21] På så vis anförs i WP 243 not 2 att med hänsyn till likheterna mellan bestämmelserna är den vägledning som ges där för DSO enligt DSF även relevant för DSO enligt BDD.
[22] Se artiklarna 33 i BDD, 38.3 andra meningen och 38.6 i DSF samt 44.3 andra meningen och 44.6 i EU DSF.
[23] Se domar i Leistritz (C-534/20, EU:C:2022:495), X-FAB Dresden (C-453/21, EU:C:2023:79) och KISA (C-560/21, EU:C:2023:81).
[24] Se HFD 2021 ref 10 och EUD:s dom i kommissionen mot Tyskland (C-518/07, EU:C:2010:125, punkt 28).
[25] Artiklarna 18 och 20 i DD.

ordning 45/2001)[26]. Enligt DD var det frivilligt att utse PUO i de flesta medlemsstater som valde att införa rollen (”nationellt PUO”), bland annat Sverige, medan förordning 45/2001 gjorde det obligatoriskt och var mer detaljerad (”EU PUO”).

Enligt huvudregeln i DD skulle tillsynsmyndigheten informeras om all behandling av personuppgifter som omfattades av reglerna innan den fick påbörjas.[27] Medlemsstaterna fick dock fastställa undantag om de införde krav på att ett PUO utnämnts. Motiveringen angavs vara att olämpliga administrativa formaliteter kunde undvikas när ett PUO utnämnts och getts i uppgift att på ett fullständigt oberoende sätt försäkra sig om att utnämnarens behandlingar inte skulle kränka enskildas fri- och rättigheter.[28] PUO skulle ha som uppgift att på ett oberoende sätt säkerställa den interna tillämpningen av nationella bestämmelser som antagits till följd av DD. PUO skulle också föra ett register över behandlingar med information om dem[29] och fråga tillsynsmyndigheten i tveksamma fall om en viss behandling ändå behövde anmälas till tillsynsmyndigheten för förhandskontroll.[30]

Enligt implementeringen i Sverige (PUL)[31] skulle ett **nationellt PUO** vara en fysisk person som efter förordnande av den utnämnande verksamheten självständigt skulle se till att personuppgifter behandlades på ett korrekt och lagligt sätt av utnämnaren och påpeka brister.[32] PUO var skyldig att anmäla till tillsynsmyndigheten om PUO hade anledning att misstänka att utnämnaren bröt mot reglerna och inte vidtog rättelse så snart det kunde ske efter påpekande.[33] PUO skulle även samråda med tillsynsmyndigheten vid tveksamhet om hur reglerna skulle tillämpas och hjälpa registrerade att få rättelse när deras behandlade personuppgifter var felaktiga eller ofullständiga.[34] PUO hade också i uppgift att föra ett register över behandlingar som annars skulle ha anmälts med viss information om dem.[35]

Enligt EU-förordningen 45/2001 skulle ett **EU PUO** ha en rad uppgifter.[36] Dessa var att ansvara för att: utnämnaren och registrerade informerades om sina rättigheter och skyldigheter, besvara framställ-

[26] Artiklarna 24–27 och bilaga i förordning 45/2001.
[27] Artikel 18.1 i DD.
[28] Skäl 49 i DD.
[29] Artikel 18.2 i DD.
[30] Artikel 20.2 i DD.
[31] Se 36–40 §§ PUL.
[32] Se 3 och 38 §§ första stycket PUL.
[33] Se 38 § andra stycket.
[34] Se 38 § tredje stycket och 40 § PUL.
[35] Se 39 § PUL.
[36] Artikel 24 i förordning 45/2001.

ningar från Europeiska datatillsynsmannen (EDPS)[37] och inom ramen för sin behörighet samarbeta med EDPS på begäran eller eget initiativ, på ett oberoende sätt se till att bestämmelserna i förordningen tillämpades internt, hålla ett register över de behandlingar som utfördes av utnämnaren med viss information och anmäla behandlingar som kunde innebära särskilda risker till EDPS. PUO skulle utses på grundval av personliga och yrkesmässiga kvalifikationer och i synnerhet expertkunskaper om dataskydd. Valet av PUO fick vidare inte leda till en intressekonflikt mellan uppdraget och andra offentliga uppdrag. PUO skulle utses för en period av mellan två och fem år, kunde återväljas för en period på högst tio år och fick endast avsättas av utnämnaren efter medgivande av EDPS om PUO inte längre uppfyllde kraven för att kunna utföra sina uppgifter. Utnämningen skulle registreras hos EDPS. Vidare skulle PUO av utnämnaren tilldelas den personal och de medel som behövdes för att kunna utföra sina uppgifter. PUO fick vid utförandet av sina uppgifter inte ta emot några instruktioner. Dessutom skulle utnämnare anta ytterligare bestämmelser för genomförande i enligt med förordningens bilaga, som i synnerhet skulle avse PUO:s arbetsuppgifter, skyldigheter och befogenheter.

Vidare skulle utnämnaren underrätta sitt PUO innan en behandling eller en serie behandlingar med samma eller närbesläktade ändamål företogs, lämna viss information om behandlingen och omedelbart meddela senare ändringar av den.[38] PUO skulle föra ett register över sådana anmälda behandlingar som skulle hållas allmänt tillgängligt samt samråda med EDPS om det var tveksamt om en viss behandling innebar sådana särskilda risker för de registrerades fri- och rättigheter som medförde att den ändå skulle kontrolleras på förhand av EDPS efter anmälan från PUO.[39]

2.3 Varför vägledning kring tidigare regelverk har begränsad fortsatt betydelse

EU-domstolens tolkning avseende tidigare regler som upphävts och ersatts av nya regler (såsom regleringen av PUO respektive DSO), är i princip tillämplig även på de nya reglerna, förutsatt att bestämmelserna i fråga i allt väsentligt har samma räckvidd.[40] Någon praxis från EU-

[37] Som var tillsynsmyndighet för förordning 45/2001 och numera är det för gällande regelverk, EU DSF.
[38] Artikel 25 i förordning 45/2001.
[39] Artikel 26 i förordning 45/2001.
[40] Se EUD:s dom M.I.C.M. (C-597/19, EU:C:2021:492, punkt 107).

domstolen gällande PUO finns dock i huvudsak inte,[41] men i litteraturen anförs ändå att eftersom regleringen av DSO liknar regleringen av EU PUO bör vägledning från EDPS om EU PUO[42] anses vara särskilt värdefull för tolkningen av regleringen om DSO.[43]

Mot det kan anföras att under lagstiftningsarbetet med reglerna om DSO togs vissa likheter med EU PUO som fanns med i förslaget (om minimumperioder)[44] bort och att förslaget om att införa motsvarande krav (specificerade kvalifikationer)[45] inte ledde till några ändringar. Därutöver kan nämnas att i motiveringen till det ursprungliga förslaget om DSO i DSF, som i huvudsak antogs, angavs att rollen byggde vidare på rollen nationellt PUO i DD.[46] Det är samtidigt tveksamt att hämta vägledning från nationellt PUO i och med skillnaderna i nationella implementeringar.[47] I svenska förarbeten till regleringen om DSO anförs visserligen att rollen inte innebär några större skillnader gällande uppgifterna, men också att regleringen om DSO är mer utförlig avseende kvalifikationer och uppgifter. Vidare ger den ett tydligare uppdrag att bistå tillsynsmyndigheten och medför nya uppgifter som har karaktär av intern rådgivning.[48] I litteraturen anförs att mycket talar för att DSO är en helt ny yrkesroll.[49]

Inget hindrar att för DSO-rollen inspireras av tidigare vägledning om PUO, men värdet av den bör inte överdrivas eller hindra tolkningar som bättre uppfyller dataskyddsreglernas mål utifrån nu gällande förutsättningar och de större förändringar som har gjorts i dem.

En större nyhet i gällande dataskyddsregler är ansvarsskyldigheten,[50] som innebär att personuppgiftsansvariga behöver kunna visa att de

[41] Det som finns är att EUD uttalat att skyldigheten att införa en viss behandling i behandlingsregistret (vilket PUO ansvarade för enligt den tidigare regleringen) inträder först när behandlingen påbörjas, se dom i Volker und Markus Schecke och Eifert (C-92/09 och C-93/09, EU:C:2010:662, punkterna 95–101).

[42] Se EDPS, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 2010-10-14, som alltså gäller EU PUO (EDPS har även antagit ett ställningstagande om DSO enligt EU DSF, Position paper on the role of Data Protection Officers of the EU institutions and bodies, 2018-09-30).

[43] Se Oxfordkommentaren till DSF, kommentaren till artikel 37, avsnitt B.1.

[44] Se artikel 35.7 i förslaget till DSF.

[45] Se Europaparlamentet, betänkande om förslag till DSF (A7-0402/2013) och den antagna texten efter första behandlingen (P7_TA(2014)0212), ändringsförslag 50 och 126.

[46] Se kommissionen, COM/2012/011 final (förslaget till DSF), 3.4.4.4. Avsnitt 4.

[47] För en genomgång, se the Confederation of European Data Protection Organisations (CEDPO), Comparative analysis of data protection officials role and status in EU and more, 2012, och EU-kommissionen, SEC(2012) 72 final, (”konsekvensbedömning avseende förslaget till DSF”), bilaga 6 avseende DSO.

[48] Se förarbetena till DDL (prop. 2017/18:113 s. 24) respektive BDL (prop. 2017/18:232 s. 203).

[49] Se Magnusson Sjöberg, C., Dataskyddsförordningen, artikel 37, Lexino 2020-09-04 (JUNO).

[50] Artiklarna 5.2 och 24 i DSF, 4.1 och 26 i EU DSF och 4.4 och 19 i BDD.

följer dataskyddsreglerna. DSO är en hörnsten i detta arbete,[51] vilket bland annat kommer till uttryck genom att vägledning för utnämnarens genomförande av lämpliga åtgärder och för att visa efterlevnad framför allt kan ges genom bland annat riktlinjer från EDPB *eller anvisningar från* DSO.[52]

En annan större nyhet är EDPB och dess uppgifter. Enligt det ursprungliga förslaget till DSF skulle kommissionen ha haft befogenhet att precisera kraven i många frågor, bland annat DSO:s kvalifikationer, uppgifter, ställning, befogenheter och resurser.[53] Förslaget antogs dock inte i denna del. Istället inrättades EDPB, som har getts i uppgift att se till att dataskyddsreglerna tillämpas enhetligt, och för det syftet i synnerhet bland annat ska utfärda riktlinjer, rekommendationer och bästa praxis för att främja en enhetlig tillämpning av dem[54].[55] EDPS har inte uttryckligen getts några sådana uppgifter, men ingår i EDPB, tillhandahåller dess sekretariat och har i uppgift att delta i EDPB:s verksamhet.[56]

Mot denna bakgrund och i ljuset av ovan nämnda argument för att tolka och tillämpa regleringen om DSO enhetligt, bör EDPB, och alltså gärna även EDPS i möjligaste mån, ta fram gemensamma riktlinjer om rollen. De bör för den välja lösningar utifrån vad som bäst säkerställer efterlevnaden av nu gällande regler och uppfyllnad av de övergripande syftena med dem[57]. Dessa riktlinjer bör bygga vidare på den vägledning som redan lämnats i WP 243 och bland annat adressera och klargöra de praktiska utmaningar som beskrivs i det följande.

3. Praktiska utmaningar

3.1 Ombudets position (”lillebrors stol”)

Vissa praktiska utmaningar är kopplade till att utnämnaren behöver säkerställa att DSO:s stol är rätt placerad i – eller i förhållande till – den egna verksamheten samt har de kvalifikationer som krävs för att utföra uppdraget.

[51] Se WP 243, s. 5.
[52] Se skäl 77 i DSF.
[53] Se artiklarna 35.11 och 37.2 i förslaget till DSF.
[54] Artikel 70.1 e i DSF.
[55] För en närmare beskrivning av EDPB:s roll och uppgifter, se Elisabeth Jilderyds bidrag i denna skrift.
[56] Artiklarna 68.3 och 75 i DSF samt 57.1 k i EU DSF.
[57] Vilket bland annat är att säkerställa en hög skyddsnivå för fysiska personer inom EU och, för att uppnå detta ändamål, säkerställa en konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande fri- och rättigheter vid behandling av personuppgifter i hela EU.

3.1.1 Om ombudet bör vara internt eller externt

Utnämnare behöver ta ställning till om DSO ska anställas (internt DSO) eller anlitas (externt DSO). Det är svårt att säga annat än att vad som är lämpligast beror på omständigheterna.

Fördelar med ett ***internt* DSO** är att tillgänglighet för utnämnares personal, verksamhetskännedom och ömsesidigt förtroende mellan DSO och utnämnare kan bli bättre. Nackdelarna är att det kan uppstå intressekonflikter, till exempel på grund av den lojalitet som normalt uppstår hos anställda gentemot sina arbetsgivare, eller på grund av incitament för att bortse från brister vars korrigerande skulle ha väsentlig negativ inverkan på utnämnarens måluppfyllnad, såsom att omfattas av bonussystem kopplade till måluppfyllnad.[58] För- och nackdelar med ett ***externt* DSO** kan, men behöver inte vara, de omvända. Andra fördelar med ett externt DSO är att de kan dra nytta av erfarenheter från kännedom om bästa praxis från flera verksamheter och förmodligen är lättare att avsätta om det visar sig att kvalifikationerna inte är tillräckliga eller att uppdraget inte utförs på rätt sätt.

3.1.2 Om flera personer kan utses till ombud för en aktör

En utmaning ligger i att avgöra om bara en eller om flera personer kan utnämnas till DSO för en aktör och om det är någon skillnad om DSO är internt eller externt. Om flera DSO utnämns uppstår frågan om vems anvisning som gäller om de har olika uppfattningar.

I regleringen anges att ”*ett*” DSO ska utnämnas.[59] Vidare anges att ”*ett enda*” DSO får utnämnas för flera myndigheter med hänsyn till deras struktur och storlek,[60] eller en koncern om DSO är lätt att nå på varje verksamhetsställe,[61] alltså singular.

I litteraturen anförs att tanken verkar vara att en utnämnare bara får utnämna *ett* enda DSO men noteras att saken inte tolkats så i svenska förarbeten[62].[63] Den *andra* delen av bestämmelsen om internt och externt DSO,[64] har i WP 243 tolkats så att tjänsteavtalet kan ingås med *en person eller en organisation* och där beskrivs även vad som är viktigt när upp-

[58] Det är till exempel enligt enkätundersökningar som gjorts inte ovanligt att samtliga medarbetare i vissa företag omfattas av sådana bonusprogram, vilket inte framstår som förenligt med kravet på oberoende.
[59] Artiklarna 37.1 i DSF, 43.1 i EU DSF och 32.1 i BDD.
[60] Artiklarna 37.3 i DSF och 43.2 i EU DSF.
[61] Artikel 37.2 i DSF.
[62] Prop. 2017/18:113 s. 24 och prop. 2017/18:232 s. 201.
[63] Öman, Dataskyddsförordningen (GDPR) m.m.: En kommentar (2022, version 2A, JUNO), kommentaren till artikel 37.
[64] Artikel 37.6 i DSF, som stadgar att DSO antingen 1) får ingå i utnämnarens personal (internt DSO) *eller* 2) utföra uppgifterna baserat på ett tjänsteavtal (externt DSO).

gifterna utförs av *flera personer*.[65] Det tycks därmed som att tillsynsmyndigheterna när det gäller *externt* DSO inte anser att det finns något hinder mot att flera personer utnämns till DSO, vilket är rimligt. Det bör inte vara annorlunda om DSO är *internt*. IMY förefaller till exempel inte göra någon skillnad, utan anger i sin kommentar till bestämmelsen generellt att ”*[DSO] kan antingen vara en anställd i organisationen eller en konsult som utför uppgifterna som extern tjänsteleverantör*” och att ”*[e]n grupp av enskilda personer kan också utföra [DSO:s] uppgifter, under ansvar av en utsedd huvudkontakt och ansvarig person*”.[66]

Oavsett om flera personer är utsedda till DSO internt eller externt bör det, som IMY därvid rekommenderar (i linje med WP 243), för att skapa rättslig klarhet, underlätta god organisation och förebygga intressekonflikter inom gruppen, finnas en tydlig och skriftlig fördelning av uppgifterna dem emellan.[67] För att uppfylla ansvarsskyldigheten bör denna uppdelning göra det möjligt att i efterhand bedöma om det finns grund för att avsätta någon av dem om uppgifterna inte har utförts på rätt sätt. Om flera DSO utsetts bör det finnas rutiner för vad som gäller om de är av olika uppfattningar i en viss fråga, som tillser att deras oberoende respekteras. Mängden kompetenser som DSO behöver ha och omfattningen av uppgifterna talar för att en grupp kan behöva utses, särskilt i större verksamheter.[68] En annan fördel med flera DSO är att om någon utav dem får en intressekonflikt kan de andra fortfarande upprätthålla den oberoende kontrollen.

3.1.3 *Vilka andra befattningar, uppdrag och uppgifter som ombudet kan ha*

Vissa utmaningar uppstår i och med att utnämnare behöver avgöra vilka andra befattningar, uppdrag och uppgifter som deras DSO kan ha därutöver. Detta till exempel gällande utnämnares arbete med informationssäkerhet utifrån andra krav, hantering av enskildas begäranden om att få utöva sina dataskyddsrättigheter, samt bestämmande av innehåll i utnämnarens dataskyddspolicy och andra interna regler för dataskydd.

I regleringen anges att DSO *får* fullgöra andra uppgifter och uppdrag, men att utnämnaren ska se till att det inte leder till intressekonflikter.[69]

[65] WP 243, s. 14.
[66] IMY:s webbplats, sidan ”Om dataskyddsombud i dataskyddsförordningen”, senast uppdaterad den 8 februari 2023, kommentaren till artikel 37.6.
[67] Se IMY:s webbplats, sidan ”Om dataskyddsombud i dataskyddsförordningen”, senast uppdaterad den 8 februari 2023.
[68] Se prop. 2017/18:232 s. 201, där det anförs att i större myndigheter kan det vara svårt för en enda person att ensam utföra de uppgifter som ett DSO ska ha i framtiden, vilket även torde gälla för andra än myndigheter.
[69] Artiklarna 38.6 i DSF och 44.6 i EU DSF.

IMY har i kommentar (och i linje med WP 243) angett att ”*[e]n tumregel kan vara att [DSO] inte ska tillhöra högsta ledningen (till exempel verkställande direktör, högste verkställande beslutsfattare, finansdirektör, chefsläkare, marknadsföringschef, personalchef eller it-chef)*”, men att ”*[ä]ven andra funktioner lägre ned i organisationsstrukturen kan vara olämpliga om de innebär att besluta om behandling av personuppgifter.*”[70]

Det kan vara frestande att som utnämnare kombinera tjänsten som DSO med **ansvaret för att leda och samordna arbetet med informationssäkerhet** (informationssäkerhetschef, informationssäkerhetssamordnare eller chief information security officer, ”CISO”).[71] I litteraturen anförs dock att det kan vara svårt, om ens möjligt, att samtidigt vara DSO och it- eller säkerhetsspecialist, eftersom det kan innebära att granska sig själv.[72] Å andra sidan behöver befattningar som typiskt sett har beslutsbefogenheter gällande behandling, exempelvis CISO, i praktiken inte ha det och därmed innebära risk för intressekonflikter.[73]

EUD har förtydligat att bedömningen av om ett visst uppdrag riskerar att leda till en intressekonflikt med uppdraget som DSO ska göras utifrån omständigheterna i det enskilda fallet. Relevanta faktorer för bedömningen kan vara utnämnarens organisatoriska struktur och interna regler. Det viktiga är att sidouppgifterna inte skadar utförandet av DSO:s uppgifter eller oberoendet. DSO kan inte vara med och bestämma varför och hur personuppgifter behandlas och samtidigt oberoende kontrollera att det görs på rätt sätt.[74] Bedömningen bör, i likhet med vad som gäller för fastställande av personuppgiftsansvar och gemensamt personuppgiftsansvar,[75] ta sikte på faktisk snarare än formell bestämmanderätt.

[70] Se IMY:s webbplats, sidan ”Om dataskyddsombud i dataskyddsförordningen”, senast uppdaterad den 8 februari 2023 samt WP 243, s. 19. Det bör inte förstås på så sätt att DSO inte alls får besluta om behandling av personuppgifter, alltså inte heller i utförande av sina uppgifter som DSO (exempelvis i urval av och metod för sin övervakning och kontroll). Om någon annan bestämmer det är DSO inte oberoende. En annan sak är att DSO inte oberoende kan kontrollera efterlevnad av egen behandling, vilket också måste kunna granskas.

[71] Se definition och synonymer av termen ”CISO” i MSB:s termbank.

[72] Magnusson Sjöberg, C., Dataskyddsförordningen, artikel 38, Lexino 2020-09-04 (JUNO).

[73] Se den franska tillsynsmyndigheten (CNIL) om CISO (RSSI) som DSO, 2022-04-05, Guide pratique RGPD – Délégués à la protection des données, s. 16. Se även kommentaren till ovan nämnda term i MSB:s termbank. Där anges att organisationer kan benämna rollen på olika sätt (t.ex. informationssäkerhetskoordinator, informationssäkerhetsambassadör, informationssäkerhetsansvarig) och att ibland görs även skillnad utifrån nivå (strategisk, taktisk, och operativ), så att t.ex. informationssäkerhetssamordnare är en annan person än informationssäkerhetschefen, men att uttrycket CISO enbart bör användas om högsta nivån. Vidare anges att ansvarsområdet även kan avspeglas i benämningen (t.ex. är it-säkerhetschef på en lägre nivå än informationssäkerhetschef).

[74] X-FAB Dresden (C-453/21, EU:C:2023:79, punkterna 41–42 och 44–45).

[75] Se till exempel Medinas förslag i Belgiska staten (C-231/22, EU:C:2023:468, punkt 65) och Emilious förslag i Nacionalinis visuomenės sveikatos centras (C-683/21, ECLI:EU:C:2023:376, punkterna 27, 28 och 41).

En annan utmaning ligger i att det inte är ovanligt att DSO involveras i den praktiska hanteringen av enskildas begäranden om att få utöva sina dataskyddsrättigheter (**rättighetsutövande**). Det är i sig naturligt att DSO involveras, dels eftersom enskilda *får* kontakta DSO med avseende på alla frågor som rör behandlingen av deras personuppgifter och utövandet av deras rättigheter enligt dataskyddsreglerna,[76] dels eftersom utnämnaren kan tänkas be DSO om råd i den hanteringen.

DSO ska dock inte fatta beslut gällande enskildas begäranden om att få utöva sina rättigheter, till exempel avslå en begäran. Detta dels eftersom det endast är den personuppgiftsansvarige som kan besluta om det,[77] dels eftersom det skulle leda till en intressekonflikt med den kontrollerande uppgiften.

Det bör dock inte anses vara en intressekonflikt att DSO medverkar i den slutliga handläggningen när ett beslut fattas i den mening som avses i förvaltningslagen[78], så länge DSO inte är med och fattar beslutet. Därigenom har DSO även möjlighet att få sin avvikande mening antecknad.[79] DSO bör dock inte vara föredragande, eftersom det omfattar att föreslå en viss utgång i beslutet vilket kan komma i konflikt med den kontrollerande uppgiften. Som framhålls i litteraturen är det generellt en bra praxis att låta dataskyddsansvariga,[80] och inte DSO, föredra beslutsfrågor rörande dataskydd (och det bör vid sådana föredragningar framgå vilka råd DSO har gett).[81] För att undvika att DSO i praktiken fattar beslut om vilken information som registrerade ska få eller inte få i rättighetshanteringen, eller röjer sådant som omfattas av sekretess, bör DSO främst förmedla information mellan utnämnaren och den registrerade och närmast agera brevlåda.

När det gäller **bestämmandet av innehåll i utnämnarens policy** och andra interna regler för dataskydd, det vill säga strategier för dataskydd, är det förmodligen inget DSO bör ha beslutanderätt över eftersom DSO ska kontrollera dessa.[82] Det kan vara en utmaning i mindre verksamheter, som kan sakna annan dataskyddskompetens. En universallösning

[76] Artiklarna 38.4 i DSF och 44.4 i EU DSF.

[77] Till exempel har Kammarrätten i Sundsvall i dom den 12 april 2021 i mål nr 252-21 upphävt underinstansernas avgöranden, där en kommuns DSO hade fattat beslut om att neka en enskilds begäran om att få utöva sina rättigheter (med motiveringen att de begärda uppgifterna inte utgjorde personuppgifter). Kammarrättens motivering var att den personuppgiftsansvarige, det vill säga kommunen, genom det överklagade beslutet inte hade hanterat eller tagit ställning till begäran, vilket den borde ha gjort.

[78] Se 28–31 §§ förvaltningslagen (2017:900).

[79] Se 30 § andra stycket förvaltningslagen.

[80] Ett samlingsbegrepp som Wendleby myntat och som kan användas för att hänvisa till jurister, IT-personal med flera som har tydliga arbetsuppgifter kopplade till behandling av personuppgifter.

[81] Wendleby, ”Gör ert dataskyddsombud rätt saker? – analys”, 2020-05-19, JPifonet.

[82] Artikel 39.1 b sista ledet i DSF.

för att ta tillvara DSO:s expertis utan att riskera oberoendet, kan dock vara att i interna regler ställa krav på att DSO ska informeras om förslag till nya och förändringar av befintliga och konsulteras i beredningen i lämplig omfattning.

3.1.4 *Hur visa att ombudet involveras i god tid och på korrekt sätt*

Enligt regleringen ska utnämnaren se till att DSO på ett korrekt sätt och i god tid deltar i alla frågor som rör dataskyddet.[83]

Ett sätt bland flera att visa att involveringen sker på ett **korrekt sätt** lär vara att i interna regler fastställa att nya och förändrade interna regler om dataskydd ska stämmas av med DSO. Av WP 243 framgår också att vid behov kan utnämnare ta fram riktlinjer eller program för dataskydd och i dem fastställa i vilka situationer DSO ska rådfrågas.[84]

När det gäller **omfattningen** innebär ordvalet ”*rör*” i regleringen mer än bara frågor som direkt *gäller* dataskyddet, utan alltså även frågor som *kan få följder* för dataskyddet. Det senare kan vara svårt att avgöra för utnämnare, vilket gör att, så som IMY bland annat anger i kommentar till bestämmelserna,[85] utnämnare bör ”*bjuda in [DSO] att regelbundet delta i möten på högsta och mellanliggande förvaltningsnivå, låta [DSO] delta i beslut som har följder för dataskyddet och förmedla all relevant information till [DSO] så att [DSO] i god tid kan ge lämpliga råd*”.[86] Med ”*delta i beslut*” menar IMY inte att DSO ska vara med och fatta besluten (i och med att det skulle innebära en intressekonflikt), utan, som det uttrycks i WP 243, ”delta *när* beslut med följder för dataskyddet *fattas*”. Det innebär förmodligen att DSO bör stå som kopiemottagare för utskick inför och efter möten på högre ledningsnivåer (såsom beslutsunderlag, protokoll och anteckningar) och i vart fall få tillgång på begäran.

När det gäller **tidpunkten** för involveringen betonas i WP 243 att det är viktigt att det sker så tidigt som möjligt. Där påpekas också att när det gäller konsekvensbedömningar avseende dataskydd föreskrivs uttryckligen att DSO ska göras delaktigt redan i ett tidigt skede.[87] Vidare anges att det bör vara en standardrutin i utnämnares styrning att se till att DSO informeras och rådfrågas redan från början, eftersom det underlättar efterlevnaden och främjar en strategi för inbyggt dataskydd. Där-

[83] Artiklarna 38.1 i DSF, 33.1 i BDD och 44.1 i EU DSF.
[84] Se WP 243, s. 16.
[85] Visserligen till den om *rapporteringslinjen*, men med skrivningar hämtade från WP 243 om *involveringen*.
[86] Se IMY:s webbplats, sidan ”Om dataskyddsombud i dataskyddsförordningen”, senast uppdaterad den 8 februari 2023 samt WP 243, s. 16.
[87] Artikel 35.2 i DSF.

till framhålls vikten av att DSO ses som en diskussionspartner och ingår i relevanta arbetsgrupper som har ansvar för dataskyddet.

3.1.5 *Internt ombuds organisatoriska placering och närmsta chef*

Ett internt DSO behöver, som anställd, ha en organisatorisk placering och en närmsta chef.

En utmaning ligger i att hitta rätt **organisatorisk placering** för internt DSO. Regleringen innehåller inget krav på var DSO ska vara placerad. Det kan därför exempelvis vara i avdelningar för IT, risk, regelefterlevnad, juridik eller administration.[88] Bäst är nog i en oberoende kontrollfunktion (exempelvis en avdelning eller funktion för regelefterlevnad, även benämnd ”compliance”), om en sådan finns. Detta eftersom sådana redan har krav på att vara oberoende från verksamheten enligt andra regler. Det är dock viktigt att DSO även kontrollerar de behandlingar som de utför i enlighet med dessa regler (exempelvis för att motverka ekonomisk brottslighet, såsom penningtvätt).[89] DSO bör inte vara chef för en sådan funktion, eftersom det innebär rätt att besluta om dessa behandlingar.

När det gäller **närmsta chef** kan konstateras att regleringen visserligen anger att DSO ska *rapportera* direkt till utnämnarens *högsta* förvaltningsnivå.[90] Ordet ”rapportera” syftar här dock inte på arbetsrättsligt underordnad,[91] utan på att det är till ledningen som DSO ska rapportera om resultatet av sin övervakning och kontroll av utnämnarens efterlevnad av olika skäl[92]. DSO kan alltså ha en lägre chef som närmsta chef som har det arbetsrättsliga personalansvaret för DSO och den lönesättande funktionen. Om denna chef är någon som fattar väsentliga beslut om behandling bör det finnas fastställda garantier som gör att denne inte kan filtrera eller hindra DSO:s rapportering till ledningen, exempelvis vid avstämningar innan fastställande. Dessa garantier bör även tillses att chefen inte påverkar utförandet av uppgifterna, så som en chef för en domstol inte ska lägga sig i enskilda domares dömande.

[88] CNIL, 2022-04-05, Guide pratique RGPD – Délégués à la protection des données, s. 34.
[89] Se exempelvis de faktiska omständigheterna i dom i Pankki S (C-579/21, EU:C:2023:501).
[90] Artiklarna 38.3 tredje meningen i DSF och 44.3 tredje meningen i EU DSF. Den senare anger till högsta ”*ledningsnivå*”, vilket bör innebära samma sak.
[91] CNIL, 2022-04-05, Guide pratique RGPD – Délégués à la protection des données, s. 34.
[92] Ordningen bidrar till att ledningen görs medveten om brister och åtgärdsplaner och ges möjlighet och incitament att agera utifrån DSO:s anvisningar (se skäl 77 i DSF), vilket bör vara relevant för att bedöma om uppsåt eller oaktsamhet föreligger som är av betydelse, eller en förutsättning för, beslut om administrativa sanktionsavgifter; se därvid generellt generaladvokaten Emiliou i förslag till avgörande i Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:376, punkterna 80–83).

3.1.6 *Vad som är tillräcklig motivering när ombudets råd inte följs*

Av regleringen följer att utnämnare inte får lämna instruktioner till DSO om hur uppgifterna ska utföras,[93] vilket enligt WP 243 bland annat omfattar vilken tolkning DSO gör av dataskyddsreglerna.[94]

Det innebär inte att utnämnare inte kan föra en diskussion med DSO eller lämna synpunkter under DSO:s beredning av rapporter och råd. Det innebär inte heller att utnämnare måste följa DSO:s råd om de gör en annan tolkning. Enligt WP 243 måste dock DSO:s åsikt alltid ges tillbörlig vikt och vid eventuell oenighet rekommenderas att utnämnare ”*som god praxis dokumenterar skälen till att [DSO:s] råd inte har följts*”.[95] Något uttryckligt stadgande om en sådan skyldighet finns inte i regleringen, men anges följa av ansvarsskyldigheten.[96]

Att tolka in en motiveringsskyldighet är rimligt, särskilt eftersom utnämnare generellt getts möjlighet att visa sin efterlevnad och att lämpliga åtgärder vidtagits genom att följa DSO:s anvisningar.[97] Det kan dock vara utmanande att avgöra vad som är en tillräcklig motivering.

Vad som är tillräckligt bör förmodligen avgöras från fall till fall. Det bör dock generellt inte krävas en specifik och detaljerad motivering om skälen framgår av dokumentationen. Om till exempel anledningen till att DSO:s råd inte följs är att utnämnaren gjort en annan bedömning av rättsläget än DSO, bör det vara tillräckligt att dokumentera denna anledning och bedömningarna på ett sätt som gör att det i efterhand enkelt och klart går att utläsa varför utnämnaren ansett att skyldigheterna iakttagits trots att DSO:s råd inte följts.[98] Utnämnare bör som god praxis låta DSO ta del av och kommentera motiveringen innan beslut fattas som avviker från DSO:s råd. Detta för att undvika missförstånd och eftersom det är möjligt att DSO initialt bedömt att det inte varit nödvändigt att mer utförligt redovisa sin motivering till ett visst råd som lämnats till utnämnaren.

[93] Artiklarna 38.3 första meningen i DSF och 44.3 första meningen i EU DSF.
[94] WP 243, s. 17.
[95] WP 243, s. 16.
[96] WP 243, s. 21, not 36 (där för motsvarande krav gällande DSO:s involvering i konsekvensbedömningar).
[97] I sig en anledning för tillsynsmyndigheter att när brister uppdagas vid tillsyn regelmässigt fråga om utnämnaren konsulterat och agerat i enlighet med DSO:s anvisningar och begära in underlag för det.
[98] Se för ett liknande resonemang EUD:s dom HYA m.fl. (C-349/21, punkterna 53–54 och domslutet).

3.1.7 *Vilka kvalifikationer ombudet bör ha och hur de bör upprätthållas*

Vissa utmaningar ligger i att dels avgöra vilken förmåga DSO ska ha, dels vilka yrkesmässiga kvalifikationer ett DSO ska ha och hur de ska upprätthållas.

Av regleringen följer att utnämnare ska utse DSO baserat på yrkesmässiga kvalifikationer och, i synnerhet, utöver förmåga att fullgöra uppgifterna, sakkunskap om regler och praxis avseende dataskydd[99] och stödja DSO i upprätthållandet av denna sakkunskap[100].

I WP 243 anges att den **sakkunskapsnivå** som krävs inte definieras strikt men måste stå i proportion till mängden behandlade uppgifter samt hur känsliga och komplexa behandlingen och uppgifterna är. Vidare anges att även om bestämmelserna inte specificerar de **yrkesmässiga kvalifikationerna**, är det relevant att DSO har sakkunskap om regler och praxis inom dataskydd och djupgående förståelse av DSF samt användbart med kunskap om utnämnarens organisation och sektor. Vidare anges att DSO bör ha en god förståelse av utnämnarens behandling och vara insatt i dennes informationssystem samt datasäkerhets- och dataskyddsbehov. Slutligen anges att **förmåga** bör tolkas som att det både rör ställningen samt personliga kvaliteter (till exempel integritet och hög yrkesetik).[101]

Det är utifrån denna övergripande vägledning inte helt lätt att avgöra vilka krav som kan och bör ställas. Som ovan framgått (avsnitt 2.3) antogs inte de förslag som lades fram under lagstiftningsarbetet om att i regleringen närmare specificera DSO:s kvalifikationer och den ursprungliga delegationen för kommissionen att göra det kan sägas ha getts till EDPB. Det vore därför lämpligt att EDPB och EDPS i vägledning närmare specificerar det, gärna i form av riktmärken. Dessa kan inspireras av riktmärken från etablerade branschorganisationer, men bör till skillnad från vissa av dessa inte kräva viss ålder eftersom det är irrelevant.

När det gäller **upprätthållandet av sakkunskaperna och professionell vidareutbildning** bör det faktiska bestämmandet av vad som är nödvändigt lämnas upp till varje DSO att avgöra efter eget omdöme med hänsyn till egna behov. Det bör inte till exempel så som för advokatkåren fastställas ett visst minsta antal timmar utbildning per år eftersom behoven kan variera, men bör i likhet med vad som gäller för dem finnas krav på att utbildningsaktiviteter dokumenteras,[102] till exempel i DSO:s årsrapport eller liknande.

[99] Artiklarna 37.5 i DSF, 43.4 EU DSF och 32.2 i BDD.
[100] Artiklarna 38.2 i DSF, 44.2 i EU DSF och 33.2 i BDD.
[101] WP 243, s. 13 f.
[102] Se Advokatsamfundets Riktlinjer för professionell vidareutbildning av advokater, punkt 2.1 och 2.5.

3.2 Ombudets uppgifter (”lillebrors bestick”)

Vissa praktiska utmaningar är kopplade till att utnämnaren behöver säkerställa att DSO utför sina obligatoriska uppgifter på rätt sätt i – eller i förhållande till – den egna verksamheten.

3.2.1 Hur ombudet bör utföra sina huvuduppgifter och hur det bör dokumenteras

Enligt regleringen är DSO:s två huvuduppgifter att informera och ge utnämnare råd om deras skyldigheter enligt dataskyddsreglerna och att övervaka deras efterlevnad av dem, inbegripet utnämnares interna regler.[103] Uppgifterna ska utföras på ett riskbaserat sätt.[104]

IMY anger i sin kommentar till **bestämmelserna om huvuduppgifterna** (i linje med WP 243) att DSO ”*ska alltså övervaka efterlevnaden av [dataskyddsreglerna]*”, vilket ”*till exempel [kan] innebära att [DSO]: samlar in information om hur personuppgifter behandlas i organisationen, analyserar och kontrollerar om personalen följer [dataskyddsreglerna] samt utfärdar rekommendationer till [utnämnaren]*”.[105] Vidare anger IMY i sin kommentar till **bestämmelsen om det riskbaserade sättet** (i linje med WP 243) att DSO ”*ska prioritera och bör inrikta sitt arbete på problem som kan innebära en större risk för dataskyddet*”, men ”*ska förstås inte försumma uppgiftsbehandlingar som innebär en jämförelsevis lägre risk*”. Vidare anger IMY att ”*[s]yftet med detta pragmatiska tillvägagångssätt är att hjälpa [DSO] att ge goda råd till personuppgiftsansvariga om: vilka metoder de bör använda för konsekvensbedömningar, vilka områden som bör genomgå en intern eller extern revision av dataskyddet, vilka interna fortbildningsverksamheter som bör tillhandahållas till anställda eller ledningspersonal som ansvarar för uppgiftsbehandling samt vilken typ av behandling som de bör ägna mer av sin tid och sina resurser åt*”.[106]

DSO ska alltså fokusera sitt arbete utifrån riskerna, främst för de registrerades fri- och rättigheter, men även för bristande efterlevnad (vilket, som påpekas i litteraturen, ofta, men inte alltid är samma sak)[107]. En utmaning ligger i att konkretisera detta och en annan i att avgöra

[103] Artiklarna 39.1 a och b i DSF.
[104] Artikel 39.2 i DSF.
[105] Se IMY:s webbplats, sidan ”Om dataskyddsombud i dataskyddsförordningen”, senast uppdaterad den 8 februari 2023 samt WP 243, s. 20.
[106] Se IMY:s webbplats, sidan ”Om dataskyddsombud i dataskyddsförordningen”, senast uppdaterad den 8 februari 2023 samt WP 243, s. 22.
[107] Johnssén & Edvardsen, Data Protection Officer (BCS, The Chartered Institute for IT, 2021), s. 230.

vilken dokumentation som krävs för att visa att det har gjorts och på rätt sätt.

Lösningen för båda utmaningarna bör ligga i att med beaktande av utnämnarens verksamhet arbeta strukturerat utifrån en dokumenterad metod och en plan baserad på en riskanalys (riskbedömning). I litteraturen lyfts att ett sätt att göra det praktiska arbetet hanterbart, särskilt för mindre verksamheter, är att utgå ifrån ett så kallat årshjul, där olika åtgärder (exempelvis kartläggningar, kontroller, råd och stöd) inom delområden utförs vid olika tidpunkter under året och med intervall och av en omfattning som beror på omständigheterna i fallet (såsom tidigare konstaterade brister och riskbedömningar).[108] Verksamhetsanpassade och meningsfulla nyckelriskindikatorer[109] bör identifieras och mätas och angreppsättet bör vara holistiskt och ta stöd i en standard eller ett ramverk.[110]

På andra områden som också handlar om efterlevnad av regler som kräver riskbaserade förhållningssätt, finns vedertagna ramverk för att säkerställa och kunna visa efterlevnad genom intern styrning och kontroll, såsom COSO[111] för revision.[112] Som påpekas i litteraturen måste intern styrning och kontroll visserligen anpassas och dimensioneras utifrån verksamhetens unika situation, men det finns goda skäl för verksamheter att utgå från ramverk som är gedigna och har *legitimitet genom tillsynsmyndigheters acceptans*.[113] Detta skapar nämligen förutsebarhet om förväntningar. Även om DSO, till skillnad från en internrevisor, inte ska kontrollera måluppfyllnad, finns i dessa ramverk användbara verktyg för att effektivt kontrollera, påvisa och säkerställa efterlevnad även av dataskyddsreglerna.

På dataskyddsområdet finns flera standarder, ramverk och verktyg, både fritt tillgängliga och kommersiella.[114] Det är dock inte enkelt att

[108] Wendleby, Dataskyddsförordningen GDPR: för dataskyddsombud och andra ansvariga (Sanoma utbildning, 2020), s. 275–323 (kontrollplan och riskbaserat kontrollarbete) och s. 282–284 (årshjul).
[109] Till exempel avseende utbildning av personal, rättighetsbegäranden och personuppgiftsincidenter.
[110] Johnssén & Edvardsen, Data Protection Officer (BCS, The Chartered Institute for IT, 2021), s. 153 och 256.
[111] Committee of Sponsoring Organizations of the Treadway Commission.
[112] Som även informerat regler för det allmänna, se förordning (2007:603) om intern styrning och kontroll.
[113] Arwinge & Davaine, Optimera intern styrning och kontroll (Studentlitteratur, 2022), s. 94.
[114] Se exempelvis Korff och Georges, The Data Protection Officer Handbook, 2019-07-30, del 3 (s. 144–245); Hoskins, How to be a decent DPO: letters to aspiring privacy pros (självpublicerad, 2021), s. 124–133; Johnssén & Edvardsen, Data Protection Officer (BCS, The Chartered Institute for IT, 2021), kapitel 6 (s. 256).

veta vad som fungerar eller krävs. Riskerna med att landa fel (exempelvis inlåsningseffekter, resursslöseri) gör det viktigt att välja rätt.[115]

Ett omfattande, men fritt tillgängligt ramverk är den brittiska tillsynsmyndighetens (ICO) ramverk för ansvarsskyldighet (som innehåller tio huvudområden, 73 underområden och 339 kontroller).[116] Det ger ett holistiskt och flexibelt angreppsätt för att tillse och kunna visa efterlevnad samt förutsebarhet till verksamheter om tillsynsmyndighetens förväntningar.[117] Sådant underlättar acceptans och adaptering i praktiken bland DSO och utnämnare.[118]

Tillsynsmyndigheterna bör genom EDPB tydliggöra sina förväntningar genom att enas om och offentliggöra något liknande. Det skulle underlätta för berörda och minska kostnaden för att verkställa efterlevnaden. Det gäller för såväl DSO (som behöver utföra och/eller kontrollera), utnämnare (som behöver utvärdera och besluta om utförandet) och tillsynsmyndigheterna (som behöver överblickbar och tillförlitlig information om efterlevnad för att effektivt kunna prioritera faktisk kontroll av efterlevnad och informationsinsatser).

3.2.2 *Om ombudet får och bör föra behandlingsregistret*

Utnämnaren ska enligt reglerna föra ett register över behandling som utförts under dess ansvar och föra ett register över alla kategorier av behandling som utförts för annans räkning.[119]

I WP 243 betonas att det är utnämnaren och inte DSO som är ansvarig, men att inget hindrar att utnämnaren tilldelar DSO uppgiften att föra registret. Vidare påpekas att detta var en uttrycklig uppgift för PUO under den tidigare regleringen. Därtill anförs att registret är ett av de verktyg som gör det möjligt för DSO att fullgöra sina uppgifter att övervaka efterlevnaden samt informera och ge råd till utnämnaren och är en nödvändig förutsättning för efterlevnad och som sådant en effektiv ansvarsåtgärd.[120]

Även om tillsynsmyndigheterna genom det ovan nämnda anför goda skäl för att lägga uppgiften på DSO, är argumentationen inte helt övertygande. Behandlingsregistret är, likt andra administrativa skyldigheter i dataskyddsreglerna, såsom att fastställa en tydlig ansvarsfördelning

115 Hoskins, How to be a decent DPO: letters to aspiring privacy pros (självpublicerad, 2021), s. 126.
116 Se ICO:s webbplats (”ico.org.uk”), sidan ”Accountability Framework”, besökt 2023-07-30.
117 ICO anger att de är de mest troliga men inte uttömmande sätten att uppfylla ICO:s förväntningar.
118 Hoskins, How to be a decent DPO: letters to aspiring privacy pros (självpublicerad, 2021), s. 129.
119 Artiklarna 30.1 och 30.2 i DSF.
120 WP 243, s. 22.

mellan gemensamt personuppgiftsansvariga eller strategier för dataskydd, ett *medel* för att säkerställa att personuppgiftsansvariga iakttar de garantier som föreskrivs i dataskyddsreglerna till skydd för de registrerades fri- och rättigheter.[121] Den som har det operativa ansvaret för en sådan skyldighet kan visserligen *självutvärdera* sitt iakttagandet därav, men inte anses *oberoende* kontrollera detta, vilket är en obligatorisk uppgift. Om utnämnare ändå lägger uppgiften att föra registret på DSO är det viktigt att de ser till att DSO har tillräckliga resurser för sina obligatoriska uppgifter. De behöver också säkerställa att registret faktiskt förs korrekt genom oberoende kontroller av någon annan än DSO, eftersom DSO genom att föra registret fått en intressekonflikt för sin kontroll av det.

3.2.3 *Ombudets information och råd vid utbildning och konsekvensbedömningar*

DSO ska bland annat informera och ge utnämnare och deras anställda råd om deras skyldigheter enligt dataskyddsreglerna[122] och på begäran ge råd om konsekvensbedömningar[123]. DSO ska samtidigt övervaka och kontrollera efterlevnaden, bland annat information till och utbildning av personal[124] och genomförandet av konsekvensbedömningar[125]. Detta kan leda till utmaningar i att avgöra vad DSO och utnämnare kan göra utan att det medför intressekonflikter och otillåtna instruktioner.

När det gäller **utbildning av personal** ligger utmaningen i att avgöra vad DSO respektive utnämnare ska göra. I svenska förarbeten och litteratur anges att det kan vara olämpligt att lägga det på DSO på grund av att det omfattas av det som ska kontrolleras.[126] Samtidigt konstateras i annan litteratur att även om det är utnämnarens ansvar att utbildningen har en lämplig process och är tillräckligt omfattande genomförs den i praktiken ofta av DSO.[127]

DSO bör kunna hålla i en utbildning som utnämnare bestämt innehållet i, exempelvis om vad som följer av interna regler, utan att det ses som en intressekonflikt eller otillåten instruktion. Om DSO inte håller med om innehållet i en utbildning som utnämnaren fastställt, kan DSO vid utbildningstillfällen ange det som ett led i sin uppgift att informera

[121] Se EUD:s dom i Bundesrepublik Deutschland (C-60/22, EU:C:2023:373, punkt 65).
[122] Artiklarna 39.1 a i DSF, 45.1 a i EU DSF och 34 a i BDD.
[123] Artiklarna 39.1 c i DSF, 45.1 e i EU DSF och 34 c i BDD.
[124] Artiklarna 39.1 b i DSF, 45.1 b i EU DSF och 34 b i BDD.
[125] Samma artiklar som ovan nämnts.
[126] Sandén, Brottsdatalagen – En kommentar (2023, version 1D, JUNO), kommentaren till 3. kap. 14 §.
[127] Johnssén & Edvardsen, Data Protection Officer (BCS, The Chartered Institute for IT, 2021), kapitel 6, s. 162.

de anställda om deras skyldigheter och ta upp det i sin rapportering. DSO bör även på liknande sätt som tillsynsmyndigheterna generellt kunna informera utnämnare och deras personal på lämpligt sätt om sin tolkning av reglerna, bästa praxis och omvärldsbevakning.

När det gäller **konsekvensbedömningar** ligger utmaningen i att avgöra vad DSO ska utlåta sig om och om DSO, genom att inte invända mot en konsekvensbedömnings slutsats om att behandlingen ska fortsätta, kan sägas ”godkänna” behandlingen på ett sätt som innebär en intressekonflikt för den senare kontrollen av den. Så bör det dock inte anses vara. Institutet konsekvensbedömning[128] är ett arv från tidigare reglering om förhandskontroll, det vill säga en slags skyddsåtgärd, som i kombination med institutet förhandssamråd, syftar till att motverka att personuppgifter behandlas i strid med reglerna eller med onödiga risker genom att tillse att förhandskontrollen sker på lämplig nivå (DSO eller tillsynsmyndigheten). DSO bör kunna lämna den vägledning som krävs för att uppnå detta syfte, vilket kan göras genom att svara på de frågor som utnämnare i WP 243 rekommenderas fråga DSO om.[129]

3.3 Ombudets förhållningssätt (”lillebrors bordsskick”)

Vissa utmaningar gäller DSO:s förhållningssätt till verksamheten, de registrerade och tillsynsmyndigheten.

3.3.1 Ombudets förhållningssätt till verksamheten

En utmaning finns i att avgöra vilket förhållningssätt DSO ska ha till verksamheten. DSO kan antingen inspireras av hur tillsynsmyndigheterna agerar, och ha distans till den egna organisationen och fokusera på efterhandskontroll. DSO kan också, mot bakgrund av rollens förutsättningar, vara mer ”handgriplig” och proaktiv och fokusera på förhandskontroll.

Eftersom DSO, till skillnad från tillsynsmyndigheterna, inte har några formella korrigerande befogenheter, behöver DSO sälja in värdet av god efterlevnad till utnämnare[130] och övertyga snarare än övertala dem.[131]

[128] För en närmare beskrivning, se Monika Wendlebys bidrag i denna skrift.
[129] WP 243, s. 20 f., bland annat om konsekvensbedömningens slutsatser (det vill säga om behandlingen ska fortsätta eller inte och vilka skyddsåtgärder som ska vidtas) överensstämmer med dataskyddsreglerna.
[130] EDPS, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, s. 10.
[131] En god start är att i tillämpliga fall hjälpa sina utnämnare och deras personal att förstå varför de ska ha ett DSO trots att de inte har bett om det och bistå med kunskap om rollens uppdrag och funktion.

Enligt WP 243 spelar DSO en central roll i främjandet av en dataskyddskultur och bör ha som främsta prioritering att möjliggöra efterlevnad av dataskyddsreglerna.[132] Vad ”dataskyddskultur” innebär definieras inte i WP 243, men i litteraturen anförs att det är DSO:s främsta uppgift,[133] vilket ändå framstår som rimligt.

Nyckeln bör ligga i att kommunicera på ett enkelt och tydligt sätt kring de skyldigheter som reglerna innebär utifrån väl avvägda prioriteringar. DSO bör i möjligaste mån involveras i ett tidigt skede i utvecklings- och förändringsinitiativ och fungera som diskussionspartner. För att kunna göra det bör DSO vara insatt i och nyfiken på den verksamhet som utnämnaren bedriver. DSO bör inte vara rädd för att vända på stenar och ställa följdfrågor om något är oklart. När väsentliga utmaningar och brister uppdagas i DSO:s övervakande och kontrollerande roll bör DSO vara rak i sin kommunikation med utnämnaren samt ställa krav på åtgärdsplaner och följa upp och validera att de genomförs. DSO bör om möjligt ge råd om lösningen på problemen, men bör fokusera på beskrivning och förklaring av problemen, eftersom utnämnare ofta kan vara bättre lämpade att hitta den bästa konkreta lösningen.

DSO har genom sin inbäddade position en möjlighet att känna verksamheten på ett sätt som tillsynsmyndigheten inte har. Det är viktigt att DSO behåller sitt oberoende, särskilt för kontrollens tillförlitlighet och dess intressenters förtroende för den, men det bör vara ännu viktigare att DSO motverkar att målen med reglerna förfelas och att höga risker realiseras. Det är till exempel inte lämpligt att DSO i fall där det är osäkert hur en viss rättsregel ska förstås, oavsett om det beror på avsaknad av vägledning eller kännedom om den, använder kravet på oberoende som en ursäkt för att inte själv (efter bästa förmåga) söka svaret, ta ställning till vilken väg som är bäst och lämna tydliga anvisningar till utnämnaren.

3.3.2 Ombudets förhållningssätt till de registrerade

Som ovan framgått *får* registrerade kontakta DSO i alla frågor som rör behandling av deras personuppgifter och rättighetsutövande. I litteraturen påpekas att det inte innebär att det är DSO:s uppgift att tillgodose deras rättigheter, exempelvis en begäran om tillgång till sina personuppgifter,[134] eller avslå den (vilket som ovan nämnts kan leda till intressekonflikter).

[132] WP 243, s. 14.
[133] Wendleby, Dataskyddsförordningen GDPR: för dataskyddsombud och andra ansvariga (Sanoma utbildning, 2020).
[134] Se Öman, Dataskyddsförordningen (GDPR) m.m.: En kommentar (2022, version 2A, JUNO), kommentaren till artikel 38.

Enligt WP 243 ska DSO utreda klagomål från registrerade och av förbudet mot instruktioner,[135] följer att utnämnare inte får instruera DSO om hur utredningen ska göras.[136] Om EDPB anser att DSO ska göra detta (och inte bara övervaka att utnämnaren gör det) bör vägledning lämnas om vad som är bästa praxis för sådan utredning och om registrerade har rätt att få ta del av resultatet av den, och i så fall i vilken mån. Om så, bör det i vart fall innebära en rätt att få veta att DSO utrett klagomålet och lämnat erforderliga råd, likt vid tillsynsmyndigheternas laglighetskontroll av brottsbekämpande myndigheter.[137]

DSO ska genom sin övervakning och kontroll vara en garant för de registrerades rättigheter, särskilt i situationer där avvägningar gjorts i reglerna för att värna motstående intressen som gör att kontrollen inte kan utövas av de registrerade. Till exempel argumenterade generaladvokaten i EU-domstolens mål Pankki S för att registrerade inte ska ha rätt att få reda på namnen på anställda i en bank som i enlighet med bankens instruktioner läst deras uppgifter i samband med en internrevision. Detta med motiveringen att det är tillräckligt med möjligheten till oberoende kontroll bland annat genom DSO.[138] En sådan rätt skulle nämligen kunna förfela syftet att förebygga och motverka ekonomisk brottslighet. Detta eftersom anställda som utför sådana arbetsuppgifter som ett led i sina arbetsgivares skyldigheter, skulle kunna utsättas för, eller vara rädda för, otillbörlig påverkan från de som utnyttjar rätten i sådana syften[139]. För att detta ska fungera bör DSO generellt agera på ett sätt som upprätthåller förtroendet för oberoendet och inte gå utnämnarens ärenden.

[135] Artiklarna 38.3 första meningen i DSF och 44.3 första meningen i EU DSF.
[136] WP 243, s. 17.
[137] Se exempelvis generaladvokat Medinas förslag i Ligue des droits humains (C-333/22, EU:C:2023:488, punkterna 41–42 och 61–74).
[138] Förslag i Pankki S (C-579/21, EU:C:2022:1001, punkt 70–80 och dom (C-579/21, EU:C:2023:501).
[139] En begäran om tillgång kan förmodligen inte nekas även om det står klart att den avser ett syfte som inte är relaterat till dataskydd och att utöva kontroll över sina personuppgifter. Detta av de skäl som anförts i förslag av generaladvokat Emiliou i målet FT (C-307/22, EU:C:2023:315, punkterna 15–30). Samtidigt bör, med ledning av domar i kommissionen mot Polen (C-204/21, EU:C:2023:442, punkt 376), Luxembourg Business Registers (C-37/20 och C-601/20, EU:C:2022:912, punkt 42), och Diamantis (C-373/97, EU:C:2000:150, punkterna 33–34), ett syfte att begå olagliga handlingar göra en begäran uppenbart orimlig enligt artikel 12.5 i DSF (på samma sätt som enligt artiklarna 57.4 jämte 77.1) och inte vara något som rättsordningen skyddar.

3.3.3 *Ombudets förhållningssätt till tillsynsmyndigheten*

En utmaning ligger i hur DSO ska förhålla sig till tillsynsmyndigheterna och om de ska fungera som deras förlängda arm ute i verksamheterna[140] och vad som i så fall ligger i det.

Av regleringen i DSF och BDD framgår att DSO ska samarbeta med tillsynsmyndigheten,[141] samt vid behov samråda i frågor som rör behandling, inbegripet förhandssamråd, och vid behov samråda i alla andra frågor om så är lämpligt.[142] I regleringen i EU DSF[143] tydliggörs att samråd ska ske på DSO:s eget initiativ eller tillsynsmyndighetens begäran.[144] Vidare klargörs att samråd ska ske vid tvivel om behovet av dels en anmälan eller meddelande om en personuppgiftsincident, dels en konsekvensbedömning eller ett förhandssamråd.[145]

Det kan argumenteras för att i kravet på oberoende ligger att DSO ska vara självständig i förhållande till tillsynsmyndigheterna och inte ta några instruktioner från dem. Mot det kan anföras att DSO visserligen måste kunna tänka och agera självständigt, och exempelvis lämna motiverade bedömningar av rättsläget i oklara frågor på ett sätt som betraktas som anvisningar som utnämnare kan följa för att påvisa efterlevnad. Samtidigt krävs för att systemet ska fungera och målen med reglerna uppfyllas utan orimliga samhällskostnader att DSO arbetar *med* och inte *mot* tillsynsmyndigheterna. DSO och tillsynsmyndigheterna tillhör i regleringen samma oberoende familj, men enligt ordalydelsen är det endast tillsynsmyndigheterna som ska vara ”*fullständigt* oberoende”[146].[147] Förhållandet kan liknas vid det mellan storasyster och lillebror, där lillebror behöver lyssna på, lära av och förstå vad storasyster – som ofta har mer erfarenhet, insyn och överblick – säger och tycker.[148]

För att lillebror ska kunna dra åt samma håll behöver storasyster förmedla hur och vad hon tänker, genom regelbunden dialog, som måste kunna initieras från båda håll. En utmaning finns i att vissa DSO upplever att tillsynsmyndigheterna inte är tillgängliga för dialog och att de i

[140] Vilket bland annat Lindgren Schelin, IMY:s generaldirektör i perioden mars 2018–augusti 2023, gjort gällande i sitt avslutande tal vid IMY:s konferens ”Dataskyddet 50 år” den 25 maj 2023.
[141] Artiklarna 39.1 d i DSF och 34 d i BDD.
[142] Artiklarna 39.1 e i DSF och 34 e i BDD.
[143] Som bör vägleda tolkningen av de andra regelverken i enlighet med vad som anförts i avsnitt 2.1.
[144] Artikel 45.1 g i EU DSF.
[145] Artikel 45.1 d, e och f i EU DSF.
[146] Begreppet tolkat i EUD:s dom i kommissionen mot Tyskland (C-518/07, EU:C:2010:125, punkterna 18–19).
[147] Jämför i DSF artiklarna 52.1 (tillsynsmyndigheterna) och 69.1 samt skäl 139 in fine (EDPB) samt skäl 97 (DSO). I DD användes ordet ”fullständigt” bara i skälen (49) och inte alls om EU PUO i förordning 45/2001.
[148] Därmed inte sagt att storasyster alltid har rätt.

för hög grad lämnas att själva bedöma onödigt svåra frågor. Ett annat klagomål är variation i stödet till DSO mellan tillsynsmyndigheterna, vilket upplevs som orättvist.

En lösning är att tillsynsmyndigheterna genom EDPB enas om vad som är en lämplig ordning och miniminivå samt drar nytta av varandras arbeten. Det bör i vart fall finnas en särskild utsedd person på varje tillsynsmyndighet med helhetsansvar för DSO och en kanal genom vilken DSO kan samråda med tillsynsmyndigheten i den mening som avses i reglerna.

Frågor och slutsatser i sådana samråd bör generellt kunna ge värdefullt underlag för tillsynsmyndigheternas generella vägledning och tillämpning, i synnerhet med hänsyn till den expertis som DSO som kollektiv har. För förutsebarheten är det dock viktigt att tillsynsmyndigheterna är tydliga med hur sådana samråd hanteras i förhållande till tillsynsverksamheten. För att DSO faktiskt ska våga genomföra sådana samråd krävs nog att det klargörs att de inte används som underlag för att informera tillsynsverksamhet såsom tips, klagomål och anmälningar. Exempelvis bör en begäran om samråd från ett DSO gällande en potentiell brist hos utnämnaren, som är beroende av tolkningen i en oklar rättsfråga, inte leda till att tillsynsmyndigheten svarar med att öppna ett tillsynsärende.

En annan sak är om det är tydligt att DSO:s avsikt inte är att samråda i en viss fråga, utan att uppmärksamma tillsynsmyndigheten på sin utnämnares problem och brister, eller avsaknad av eller oskäligt dröjsmål med att vidta åtgärder för att komma till rätta med dem, i form av överträdelser av dataskyddsreglerna. Det finns inga formella hinder för DSO att anmäla överträdelser, men heller ingen skyldighet. Enligt den tidigare regleringen av nationellt PUO i Sverige hade PUO dock en sådan skyldighet.[149]

I förarbetena till BDL föreslogs en anmälningsskyldighet även för DSO som inte infördes. Trots detta påpekades att det är viktigt att DSO uppmärksammar tillsynsmyndigheten på problem och brister, särskilt om utnämnaren inte rättar sig efter DSO:s påpekanden.[150]

Lämpligheten av att lägga ett sådant ansvar på DSO kan diskuteras. Det kan medföra att samma situation kan komma att behandlas olika beroende på vem som är DSO. Det kan också antas vara svåra beslut för DSO, både att ta och landa rätt i. Eftersom många frågor i dataskyddsreglerna fortfarande är oklara kan en väsentlig brist enligt DSO visa sig vara oväsentlig eller inte en brist alls. Det är heller inte i sig säkert att en anmälan leder till ett bättre resultat och kan skada relationen till

[149] Se 38 § andra stycket PUL.
[150] Prop. 2017/18:232 s. 205.

utnämnaren och försvåra utförandet av uppdraget i övrigt. DSO kan förvisso precis som vem som helst anmäla överträdelser anonymt enligt visselblåsningsreglerna[151], men i praktiken vore det nog inte förenligt med att DSO ska agera på ett transparent sätt i förhållande till utnämnaren.[152] Det är inte heller svårt att föreställa sig att DSO inte är objektiv i frågan och inte kan bortse från hur det påverkar möjligheten att utöva yrket eller få andra uppdrag. Det kan också riskera att gynna DSO som inte anmäler när de borde göra det och utnämnare som medvetet väljer dem.[153]

Om det är önskvärt att sådana anmälningar görs, bör det införas som en uttrycklig skyldighet och kombineras med tydliga instruktioner om när det förväntas ske. En bättre ordning vore i så fall att lägga skyldigheten på verksamheterna själva anmäla sina egna överträdelser, i likhet med skyldigheten att anmäla personuppgiftsincidenter (vilket i sig inte nödvändigtvis också är överträdelser)[154], så som gäller för vissa finansiella företag avseende sådana överträdelser av externa regler som är att anse som händelser av väsentlig betydelse.[155]

4. Avslutning

Som framgått ovan finns utmaningar i rollen som kanske gör att det inte är så *bara* att vara DSO. Rollen står förmodligen inför en intressant utveckling i när- och framtid, som utövare och utnämnare kommer att behöva följa med i och anpassa sig efter. Det bör samtidigt framhållas att rollen inte bara bjuder på negativa utmaningar, utan är full av givande inslag. Det är på goda grunder nog få DSO som inte är stolta över förtroendet och innebörden i att vara DSO och det kommer förmodligen bara att bli bättre i takt med att rollen förtydligas.

De flesta av svårigheterna ligger nu i att dataskyddsreglerna i sig ännu inte är klara och hur man som DSO förhåller sig till det och bäst hjälper sin utnämnare att lotsa skutan framåt.

En del av det beror nog på att regelverken är en mosaik av idéer, stilar och koncept från olika europeiska traditioner som sammanfogats för att skapa något stort och spektakulärt, såsom DSF, som beskrivits

[151] Lag (2021:890) om skydd för personer som rapporterar om missförhållanden, som genomför direktiv (EU) 2019/1937 (visselblåsardirektivet).
[152] CNIL, 2022-04-05, Guide pratique RGPD – Délégués à la protection des données, s. 34.
[153] Mot vilket DSO Lindgren i litteraturen förvisso anför att det finns saker som DSO måste göra, även om det är farligt, annars är man ingen DSO, utan bara en liten lort.
[154] Se generaladvokat Pitruzzellas förslag i Natsionalna agentsia za prihodite (C-340/21, EU:C:2023:353, punkterna 29–37).
[155] Se Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse (FFFS 2021:2).

som EU:s flaggskepp bland lagstiftningsakter. Det har gjort att rutinerade rävar inom fältet har liknat regleringen vid den katalanska kyrkan Temple Expiatori de la Sagrada Família (Heliga Familjens Botgöringstempel) i Barcelona i Spanien av arkitekten Gaudí.[156] Frågorna kommer behöva klarna över tid genom vägledning från EUD.

En annan del är att många intressenter och aktörer av olika slag och storlek har olika åsikter om hur dataskyddsreglerna bör tillämpas och inflytande över det. Precis som i alla stora familjer som bryr sig mycket om både frågor och varandra uppstår stormar i vattenglas och det utbyts ibland hätska ord, där man kan behöva påminna varandra om att spänna av och skämta lite för att bli sams igen. Som DSO är man en liten, men viktig del i den familjen, som behöver lyssna på de större djuren och försöka simma lugnt. Det är också klokt att tala med små bokstäver eftersom ingen utom EUD tycks veta vad lagstiftaren *egentligen* vill med det hele.[157]

En sista del man bör ha med sig i värvet är att det tar tid för många att komma till insikt och freds med att dataskyddet aldrig blir färdigt och att det är som det ska. Resan är målet.

Till dig som står och velar om rollen är något att ha eller för dig, kanske följande lånade, men parafraserade, ord från Tranströmer[158] kan ge riktning i beslutet och mening till resan.[159]

Dataskyddets bågar
Inne i den väldiga katalanska kyrkan
trängdes registrerade och tillämpare i halvmörkret.
Valv gapade bakom valv och ingen överblick.
Några bestämmelser fladdrade.
En lagstiftarvilja utan ansikte omfamnade oss
och viskade genom hela uppgiften:
”*Skäms inte för att ni är dataskyddare, var stolta!*
Inom dataskyddet öppnar sig valv bakom valv oändligt.
Det blir aldrig färdigt, och det är som det ska.”
Vi var blinda av tårar
och föstes ut på den solsjudande piazzan
tillsammans med mr och mrs DSF, herr BDD och
signora eDD ”snart” eDSF,
och inne i dem alla öppnade sig valv bakom valv oändligt.

[156] Se exempelvis Ustaran, ”In Conversation With Eudardo Ustaran” (Privacy Pros Podcast, 2022), 12 min.
[157] En anledning till att benämna sig som ”dso” snarare än ”DSO” och till att så görs i titeln på denna text.
[158] Som förmodligen var DSO i någon mörk tunnel när ingen såg.
[159] Tomas Tranströmer, original ”Romanska bågar” i samlingen För levande och döda (Bonniers, 1989).