DATASKYDDSFÖRORDNINGEN

Grundläggande om GDPR till Sund Affärsbyrå och deras kunder

20 JANUARI 2020

DATASKYDDSOMBUD
Stefan Johansson

Innehållsförteckning

Inledning

Syftet med denna informationsbroschyr är att inom Sund Affärsbyrå och bland dess kunder sprida grundläggande kunskap om centrala delar av dataskyddsförordningen. Därigenom skapas en gemensam kunskapsbas, som väsentligt underlättar ömsesidig förståelse och dialog. Med centrala delar menas både grundläggande förståelse för förordningens principiella uppbyggnad och för de delar som varje organisation oavsett storlek måste uppfylla. Datainspektionens första sanktionsbeslut ger väsentlig information om tillvägagångssättet för påförande av sanktionsavgifter. Därför avslutas broschyren med en analys av det beslutet. Broschyren kan läsas antingen från början till slut, eller i den ordning läsaren själv vill. För tydlighets skull påpekas att ingenting i denna skrift innebär någon juridisk rådgivning i något konkret fall. Allt är generell information.

För frågor och synpunkter:
Stefan Johansson
Dataskyddsombud
stefan@datakollen.se

1. Dataskyddsförordningens bärande principer

Kunskap om förordningens bärande principer syftar till att sätta samtliga artiklar i ett sammanhang. Dels till varandra och dels till förordningens övergripande mål

1.1 Dataskyddsförordningens kontext och syfte

EU:s allmänna dataskyddsförordning, även kallad GDPR[1], trädde i kraft den 25 maj 2018. Alla som hanterar personuppgifter med anknytning till EU måste beakta dataskyddsförordningen. Antingen för att man är personuppgiftsansvarig eller personuppgiftsbiträde etablerad i någon medlemsstat, eller för att de personuppgifter som behandlas avser nu levande fysiska personer som befinner sig inom unionens gränser. Detta gäller oavsett om själva behandlingen utförs i en medlemsstat eller ej.

Ovanstående känner många känner till. Därefter spretar kunskapsläget betydligt. Överdrifter och felaktigheter är tyvärr mer regel än undantag. Förordningens ikraftträdande föregicks av en intensiv verksamhet i många organisationer. Rena skräckscenarier målades inte sällan upp och en viss domedagsstämning var ganska vanligt förekommande. Efter ikraftträdandet byttes den intensiteten på många håll ut mot en slapp likgiltighet. Om den inledande paniken var överdriven, så är den efterföljande nonchalansen farlig. Faran lurar på många håll. Dels innehåller dataskyddsförordningen skarpa sanktioner med risk för både höga avgifter och behandlingsförbud, vilket gymnasienämnden i Skellefteå blivit de första att erfara.[2] Dels blir vi blinda för de risker vårt alltmer digitaliserade samhälle utsätter oss själva och andra för, både som representanter för en organisation och som privatpersoner. Identitetsstölder, bedrägerier och kapningsattacker är bara tre exempel på konkreta risker som konstant ökar på alla plan i samhället.

En annan typ av risk representeras av alla de företag och organisationer som samlar in mängder av specifika uppgifter från miljontals människor, med eller mot deras vilja, och använder informationen till att kartlägga och profilera hela populationer på individnivå, med allt från oönskad reklam till manipulation av demokratiska val som följd. Allt detta kan ske i bakgrunden av vanlig internetanvändning. Cambridge Analytica är den mest kända aktören i sammanhanget och fallet erbjuder den intresserade insikter i dessa processer.

Om ovanstående risker skulle få enskilda människor att avstå från internetanvändning eller utöva självcensur av rädsla för övervakning och kartläggning skulle samhällsutvecklingen påverkas klart negativt. Inte bara för att effektivitetsvinster skulle utebli utan även för att yttrande- och informationsfriheten skulle inskränkas.[3] Dataskyddsförordningen kan sägas vara ett rättsligt medel med syfte att motverka att det uppkopplade samhället övergår i ett övervakningssamhälle med totalitära förtecken, samtidigt som det fria flödet av personuppgifter inte hämmas.

---

[1] Akronymer gör en text svårläslig och bör därför användas så lite som möjligt i skrift. Av det skälet används det svenska ordet dataskyddsförordningen. Förordningens fullständiga namn lyder: Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG – Allmän dataskyddsförordning.

[2] Fallet behandlas i avsnitt 7.

[3] Agrell, Wilhelm och Pettersson, Tobbe (red.) Övervakning och integritet – teknik, skydd och aktörer i det nya kontrollandskapet, Carlsson Bokförlag, 2016, s. 214.

Dataskyddsförordningens övergripande syfte är således att utveckla den digitala ekonomin med respekt för mänskliga rättigheter. Den digitala ekonomin ska helt enkelt inte byggas på digitalt slaveri. Därför har unionens medlemsländer tillsammans skapat en enhetligt giltig och tillämplig rättslig ram för dataskydd. Dataskyddsförordningen är den ramen.

1.2 Begreppet personuppgift

Dataskyddsförordningen handlar uteslutande om behandling av personuppgifter. Uppgifter som inte är personuppgifter hamnar utanför förordningens tillämpningsområde, oavsett deras betydelse och vikt. Andra lagar och avtal kan skydda sådana uppgifter, men inte dataskyddsförordningen. Vad kännetecknar då en personuppgift?

Definitionen finns i Art. 4.1:
”varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk 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,”

De begreppsliga byggstenarna är alltså:

- Varje upplysning…
- …som avser en identifierad eller identifierbar fysisk person…
- …en identifierbar person är en person som direkt eller indirekt kan identifieras…
- …med hänvisning till en identifierare…

följt av en icke uttömmande exempelkatalog avseende vad som särskilt ska betraktas som identifierare.

Som synes är definitionen mycket bred. I praktiken kan nästan vad som helst vara en personuppgift, t.ex. ”AIK:aren på Sund,” ”filosofen på finansdepartementet,” eller ”den store” om dessa benämningar gör att en fysisk person kan identifieras. Uppgiften i sig kan alltså vara alldaglig eller allvarlig, det spelar ingen roll. Det avgörande är om uppgiften på ett eller annat sätt går att knyta till en person.

Slutsats: varje uppgift som på ett eller annat sätt kan knytas till en fysisk nu levande person är en personuppgift.[4]

Konsekvens: alla organisationer hanterar personuppgifter.

Den ofta förekommande replikväxlingen:

- Har ni tagit tag i GDPR hos er?
- Nja, vi har ju inga sådana uppgifter, så det där rör inte oss.

Visar således på ett djupgående missförstånd om vad och vem som berörs av lagen.

I Art. 2 anges förordningens materiella tillämpningsområde: om unionsrätten gäller, då gäller även dataskyddsförordningen. Endast viss statlig och myndighetsbunden verksamhet undantas, samt fysiska personers verksamhet som antingen är av rent privat natur, eller har samband med det egna hushållet. I alla andra fall måste förordningen följas.

[4] Att endast nu levande människor omfattas av förordningen framgår av skäl 27. Det är upp till varje medlemsland hur de vill hantera avlidna människors personuppgifter.

Möjligen kan grunden till ovanstående missförstånd finnas i Art. 9. I den artikeln anges *särskilda kategorier av personuppgifter*.[5] Dessa kategorier av uppgifter anses av lagstiftaren vara så skyddsvärda att behandling av dem per definition är förbjuden. De möjliga undantagen från förbudet listas i Art. 9.2. Hanteras uppgifter som omfattas av Art. 9.1, men inga undantag i Art. 9.2 kan tillämpas, då måste behandlingen upphöra. Behandlingar som innehåller uppgifter som faller in under Art. 9.1 genomgår således två rättsliga prövningar. Först måste en rättslig grund enligt Art. 6 finnas. Därefter måste ett undantag enligt Art. 9.2 vara tillämpligt. Att inte respektera detta är både sanktionerat med de högsta avgifterna, Art. 83.5, samt förbud att fortsätta behandlingen.

Men, huruvida personuppgifter faktiskt är särskilt integritetskänsliga eller ej kan inte utläsas direkt av deras legala kategoritillhörigheter[6]. Olika människor betraktar olika uppgifter ur olika synvinklar. Vissa människor anser t.ex. att detaljerade resultaträkningar avseende specifika resultatenheter i det egna företaget, deklarationsunderlag, vem man åt lunch eller pratade med, platsdata[7] m.m. som mycket integritetskänsliga uppgifter. Samtidigt som andra människor anser dessa typer av uppgifter vara harmlösa. Det ingår i den personuppgiftsansvariges grundansvar[8], enligt Art. 24.1, att för varje enskild behandling bedöma och dokumentera riskerna. Detta gäller alltid.

Behandlingens risk ska kartläggas och bedömas efter dess ursprung, art, sannolikhetsgrad och allvar, skäl 77. Risken bör minskas i enlighet med bästa praxis.

Riskbedömningen ska vara objektiv och utgå från behandlingens art, omfattning, sammanhang och ändamål, vilket framgår av skäl 76. Per definition finns ingen riskfri behandling.

Ur ett praktiskt perspektiv bör den personuppgiftsansvariges bedömning en behandling landa i ett generellt ställningstagande, så att alla personuppgifter i den behandlingen behandlas lika. Möjligheten finns att vissa anser dataskyddet vara överdrivet, medan andra anser det vara otillräckligt. Den personuppgiftsansvarige kan inte göra mer än fatta sina dataskyddsbeslut på ovanstående grunder och sedan stå för detta.

Att alla organisationers behandlingar måste följa dataskyddsförordningen innebär dock inte att alla alltid måste göra lika mycket för att leva upp till kraven. Lösningen kallas för den riskbaserade metoden, ämnet för nästa avsnitt.

1.3 Den riskbaserade metoden

Den riskbaserade metoden innebär i korthet att ju högre risk för fysiska personers rättigheter och friheter en behandling medför, desto större krav ställs på personuppgifternas skydd. I

[5] Kallas ofta för *känsliga personuppgifter*, vilket är en begreppslig kvarleva från 13§ personuppgiftslagen. I dataskyddslagen (SFS 2018:218) används också det begreppet istället för det nya, 3 kap 1§. Det viktigaste i sammanhanget är att lagen definierar ett antal kategorier av uppgifter och föreskriver vad som gäller för dem. Någon särskild känslighetsbedömning görs alltså inte.

[6] Art. 10 innehåller uppgiftstyper som lagstiftaren bedömt vara ännu känsligare. Undantagen där är ännu snävare än för Art. 9.1. Datainspektionens sanktionsbeslut mot Mr. Koll från 13 december 2019, iarienr. DI-2018-22737, handlar bland annat om överträdelse av denna artikel. Länk till beslutet: https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-mrkoll.pdf

[7] För dem som t.ex. har skyddat boende eller förföljs av en stalker kan platsdata handla om liv och död.

[8] Med *grundansvar* avses att varje personuppgiftsbehandling alltid åtföljs av ett visst mått av ansvar, som visserligen kan variera från fall till fall, men som aldrig kan vara noll.

detta skydd ingår kravet på laglig grund för behandling, att de grundläggande dataskyddsprinciperna följs och att de registrerades rättigheter respekteras. Metoden bör ses som verktyg för en proaktiv hållning. Fokus ska ligga på förebyggande av negativa effekter, istället för att enbart reaktivt hantera inträffade skador. Med negativa effekter avses både sådana som kan komma av att behandlingen genomförs precis som planerat och sådana som kan komma av att personuppgifter förstörs, försvinner eller hamnar i orätta händer. Risk ur förordningens synvinkel är alltså inte bara obehörigas intrång eller informationsförlust. Alla behandlingar anses per definition inkräkta på fysiska personers integritet sker. Därför finns kravet på att den risken också ständigt måste bedömas och hanteras. Mer om det i avsnitt 3.

Den riskbaserade metoden fanns redan i det ersatta dataskyddsdirektivet, men har fått en större roll och uppmärksamhet nu. Kanske har denna uppmärksamhet bidragit till missförståndet att endast vissa typer av personuppgifter faller under lagens tillämpningsområde. Principen är mycket viktig. Den undantar dock aldrig någon behandling från kravet att följa förordningen. Den modifierar bara detaljnivån på de lösningar och resonemang som krävs för att en behandling ska anses vara förenlig med förordningen.

Det lagtekniska syftet kan sägas vara att ge lagen en flexiblare tillämpning, utan att göra den otydlig eller rättsosäker. Behandlingar med hög risk ska åtföljas av starkt skydd, utan att behandlingar med låg risk avkrävs oproportionerligt högt skydd. Detta ska uppnås utan att begreppet hög risk måste kvantifieras i lagtexten. All it-relaterad lagstiftning har nämligen ett grundläggande problem, som kommer av tidens olika betydelse för olika verksamheter. Fem år för ett lagstiftningsförfarande är lite. Fem år för it-utveckling är mycket. Ett fullgott dataskydd år ett kan mycket väl vara verkningslöst år tre. Lagregler kan inte skrivas om på så kort tid. På något sätt måste ändå dessa två verkligheter, den rättsliga och den it-tekniska, kopplas ihop för att människors och organisationers liv och verksamheter ska kunna framskrida i acceptabla och någorlunda förutsägbara banor. Den riskbaserade metodens funktion inom rättsinformatiken kan således jämföras med t.ex. skälighetsbedömningar inom civilrätten,[9] d.v.s. vara ett skydd mot otidsenlig och stelbent rättstillämpning utan att öppna dörren till rättsosäkerhet och godtyckligt dömande.

Metoden framgår till viss del av t.ex. skäl 89 och 90, samt Art. 24, 32 och 35, men kan inte påstås vara uttömmande och fullständigt formulerad i något enskilt skäl eller artikel. Den riskbaserade metoden kan ses som en princip som genomsyrar hela förordningens skyddstänkande. Möjliga tecken på att den riskbaserade metoden är tänkt att påverka en specifik artikels tillämpning är att olika uttryck på temat *”risker av varierande sannolikhetsgrad och allvar”* och *”sannolikt hög risk”* har använts.

Den riskbaserade metoden kan sägas handla om att dataskyddsförordningens syften ska kunna uppnås på smidigast möjliga sätt. Samtidigt lägger den riskbaserade metoden över ansvaret på dem som ska följa lagen, att de faktiskt vet vilka behandlingar de har och vilka potentiella risker de därmed utsätter fysiska personer för. Detta är en annan bärande princip i dataskyddsförordningen och kallas för ansvarsskyldighetsprincipen, som behandlas i nästa avsnitt.

1.4 Ansvarsskyldighetsprincipen

Principen innebär att den personuppgiftsansvarige är skyldig att både följa förordningens regler och kunna visa att så är fallet. Det räcker alltså inte med att göra rätt, den personuppgiftsansvarige måste också ha en dokumentation som visar att man gör rätt.

[9] Se t.ex. avtalslagens (SFS 1915:218) 33 och 36 §§.

Principen nämns första gången i Art. 5.2, i anslutning till de grundläggande dataskyddsprinciperna, sedan också i Art. 24.1, där den personuppgiftsansvariges grundansvar specificeras. En minnesregel lyder: *det är lika fel att göra fel som att inte kunna visa att man gör rätt.* Ansvarsskyldighetsprincipen medför nämligen en legal placering av bevisbördan på den ansvariges respektive biträdets sida. Det är inte tillsynsmyndigheten som ska visa att fel har begåtts. Tillsynen inskränker sig till att bedöma om berörd parts dokumentation visar att de har gjort rätt.

Personuppgiftsbiträdet ansvarar för att följa de regler som gäller dennes verksamhet, samt att kunna visa det, Art. 28. Följer av att personuppgiftsbiträdet endast får behandla personuppgifter på den personuppgiftsansvariges skriftliga instruktioner. Överträds instruktionernas gränser så blir personuppgiftsbiträdet personuppgiftsansvarig i de delar som ligger utanför gränserna. Detta kan få allvarliga följder för såväl den ursprungligt personuppgiftsansvarige samt för det biträde som gått över sitt uppdrags gränser.

1.5 Skadestånd och ekonomiska sanktioner

Både personuppgiftsansvariga och personuppgiftsbiträden kan bli skadeståndsskyldiga respektive utsättas för diverse administrativa sanktioner ifall de inte lever upp till kraven som förordningen ställer på dem, Art. 79 och 82 - 84.

Beträffande skadestånd krävs att en fysisk person lidit materiell eller immateriell skada, Art 82.1. Hur stor denna skada måste vara är emellertid oklart, samt hur beviskraven ser ut. Ett fall i Tyskland[10] där en person fått ett oönskat marknadsföringsmail finns. Domstolen ansåg att fallet var för bagatellartat för att föranleda skadeståndsansvar. Domstolen är första instans, så domen har inget egentligt prejudikatvärde. Domstolen har kritiserats för att den tog för lätt på frågan och missade möjligheten att få frågan prövad i EU-domstolen[11]. Fortsättning i frågan lär komma, särskilt med tanke på den möjlighet till grupptalan som finns genom Art. 80. En konsekvens av grupptalan är, att om t.ex. 10.000 personer bedöms ha rätt till skadestånd på 5.000 kr p.g.a. av oönskad marknadsföring, då blir totala notan för den skadeståndsskyldige 5.000 x 10.000 = 5 miljoner kronor. Ogenomtänkta rutiner kan således snabbt skapa stora merkostnader för den ansvarige.

Kan den personuppgiftsansvarige eller personuppgiftsbiträdet i fråga visa att den inte på något sätt är ansvarig för den händelse som orsakade skadan, då undgår de ansvar, Art. 82.3. *"Inte på något sätt är ansvarig"* är ett högt beviskrav. Det säger också att den ansvarige respektive biträdet förefaller ha ett ansvar för allt-eller-inget. Vikten av en fullgod dokumentation framträder alltså även här.

Villkoren för när och hur administrativa sanktionsavgifter ska dömas ut regleras i Art. 83. Deras påförande ska i varje enskilt fall vara *"effektivt, proportionellt och avskräckande."* I Sverige ansvarar Datainspektionen för att så sker.

Det finns två nivåer på sanktionsavgifter, beroende på vilka bestämmelser frågan gäller. Den lägre nivån är antingen upp till 10 miljoner euro eller 2% av den globala årsomsättningen, Art. 83.4. Den högre nivån är 20 miljoner euro eller 4% av den globala omsättningen, Art.

[10]Domstol var Amtsgericht i Dietz, målnr: Az. 8 C 130/18, dom avkunnades 7 november 2018.
[11] Se t.ex. https://blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-claims-for-immaterial-damages-under-gdpr/ och https://www.datenschutz.org/dsgvo-gewaehrt-schmerzensgeld-deutsche-gerichte-bislang-nicht/

83.5. I bägge fallen gäller det belopp som blir högst.[12] Sättet att räkna kan slå proportionellt sett mycket hårt mot mindre organisationer, vars omsättning inte når upp till de angivna eurobeloppen. Detta framgår t.ex. i Sveriges andra fall av utdömda sanktionsavgifter[13], där beloppet om €35.000, ca 385.000 kr, motsvarade 8% av den antagna årsomsättningen.

Alla tillsynsmyndighetens beslut kan överklagas till domstol, Art. 78. Detta har skett med den första sanktionsavgift som utdömts i Sverige. Hur det blir i fallet med den andra sanktionsavgiften är ännu inte klart.

Observeras bör att de administrativa sanktionsavgifterna fokuserar på förordningens efterlevnad, vilket kan uttryckas som att frågan är om berörd part har fullgjort sina förpliktelser enligt ansvarsskyldighetsprincipen och den riskbaserade metoden. Om skada har uppstått eller inte, samt hur stor den i så fall är, är en bedömningspunkt bland flera avseende såväl val av sanktioner som eventuella sanktionsavgifters storlek, Art. 83.2(a) och (c). Att skada har uppstått är alltså inte avgörande för om administrativa sanktionsavgifter kan påföras eller ej. Inte heller är skaderekvisitets uppfyllande nödvändigt för att en behandling ska kunna förbjudas.

1.4 Tillsynsmyndigheternas samverkan

Alla EU:s medlemsstater måste ha minst en ansvarig tillsynsmyndighet som ska övervaka förordningens tillämpning och bidra till att förordningen tillämpas enhetligt inom hela EU, Art. 51. Tillsynsmyndigheten ska inom sin egen stats territorium utföra de uppgifter med de behörigheter som förordningen anger, Art. 55.1. Alla tillsynsmyndigheter inom EU ska samverka med varandra och ha en överordnad styrelse,[14] enligt Art. 60 – 76. Tillsynsmyndigheternas samverkan är det enskilda ämne som upptar störst utrymme i hela dataskyddsförordningen.

Den som utför personuppgiftsbehandlingar, oavsett i vilken roll, kan alltså bli föremål för tillsyn av ett annat lands tillsynsmyndighet. Om frågan gäller gränsöverskridande behandlingar är huvudregeln att tillsynsmyndigheten i det land där den ansvarige eller biträdet i fråga har sitt enda eller huvudsakliga verksamhetsställe vara enda motpart, Art. 56.6[15]. De närmare villkoren för myndigheternas samverkan finns i nämnda artiklar och ska inte närmare diskuteras här, men denna aspekt av förordningen är viktig att känna till.

2. Personuppgiftsbehandlingens rollfördelning

Innan en personuppgiftsbehandling påbörjas bör man ha klart för sig i vilken roll man ämnar behandla personuppgifterna. Lagtexten definierar två roller och skiljer tydligt på vilka befogenheter respektive roll har. Rollfördelningen är i lagtexten tydlig och enkel, men det är

[12] CNIL, Frankrikes datainspektion, utfärdade redan i januari 2019 en avgift om 50 miljoner euro till Google.
[13] Datainspektionens beslut från 13 december 2019 rubricerat: Tillsyn enligt kreditupplysningslagen (1973:1173) och EU:s dataskyddsförordning 2016/679 - Nusvar AB, ärendenr DI-2018-22737.
[14] Europeiska dataskyddsstyrelsen, förkortas oftast EDPB, European Data Protection Board, Art. 68.
[15] Detta har lett till stora belastningar på Irlands och Luxemburgs tillsynsmyndigheter, då de amerikanska it-jättarna har sina europeiska huvudkontor i dessa länder. Andra tillsynsmyndigheter har framfört kritik mot denna så kallade *one stop shop model*. De anser att tillsynen av it-jättarna måste gå snabbare från ärendestart till beslut, annars hotas hela förordningens trovärdighet. Artikeln i frågan finns på: https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605

långt ifrån alltid klart på vilken sida om befogenhetsgränsen den egna organisationen befinner sig.

2.1 Personuppgiftsansvarig eller personuppgiftsbiträde?

Dataskyddsförordningens två roller för behandling av personuppgifter är personuppgiftsansvarig, Art. 24 och 26, eller personuppgiftsbiträde, Art. 28.

Personuppgiftsansvarig är den *"som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter,"* Art. 4.7.

Personuppgiftsbiträde är den *"som behandlar personuppgifter för den personuppgiftsansvariges räkning,"* Art. 4.8.

I dataskyddsförordningens mening kan inte personuppgifter behandlas utan att någon är personuppgiftsansvarig, medan personuppgiftsbiträden inte nödvändigtvis finns för varje behandling. Avtal och egna uppfattningar spelar roll, men frågan är inte helt dispositiv.[16] Det är de faktiska omständigheterna i det specifika fallet som avgör vem som verkligen bär ansvaret. De inblandade måste således agera i enlighet med sina avtal och beslut för att dessa ska ha rättslig verkan, om frågan skulle prövas av myndigheter och domstol.

Bägge rollerna har ett skadeståndssanktionerat ansvar gentemot fysiska personer för det fall de inte efterlever förordningens bud, Art. 82, samt står var för sig under myndighetstillsyn, Art. 51. Tillsynsmyndigheterna har breda befogenheter, Art. 58. Sanktionsavgifterna regleras som nämnts ovan i Art. 83.

Frågan som ursprungligen antogs vara enkel att lösa, men som har visat sig motspänstig i många fall, är att bedöma vilka handlingar som ryms inom definitionen att bestämma *ändamål och medel* för behandlingen. Frågan är av avgörande betydelse för vem som får göra vad med vilka uppgifter, samt vilka avtal som måste upprättas. En felaktig eller osmidig placering av personuppgiftsansvaret kan alltså leda till att förordningen de facto inte efterlevs eller att efterlevnaden är onödigt administrativt krånglig och dyr.

Om två eller flera parter[17] är inblandade i en och samma behandling är följande möjligt:

- Självständigt personuppgiftsansvariga = inget avtal krävs, kan vara klokt ibland, men i de flesta fall behövs inget avtal
- Gemensamt personuppgiftsansvariga = datadelningsavtal krävs
- Personuppgiftsansvarig och personuppgiftsbiträde = biträdesavtal krävs

2.1.1 Ansvarig-biträdesrelationen för redovisningskonsulter

Under förberedelserna inför dataskyddsförordningens ikraftträdande ansågs en redovisningskonsult per definition alltid bli ett personuppgiftsbiträde. Tanken var troligen att eftersom kunden kommer med sina uppgifter och vill få en tjänst utförd, så måste personuppgiftsansvaret fördelas likadant, d.v.s. kunden blir personuppgiftsansvarig och redovisningskonsulten blir personuppgiftsbiträde. Detta resonemang fördes, och förs

[16] Dispositiva bestämmelser innebär att parterna själva bestämmer och att deras gemensamma beslut avgör vad som gäller. Typexemplet är att säljare och köpare kommer överens om priset på en bil.

[17] En part är en fysisk eller juridisk person med rättskapacitet, d.v.s. som kan och får ingå avtal med andra. Om flera anställda inom samma organisation deltar i behandlingen har ingen betydelse för denna fråga. Dessa kallas medhjälpare och saknar självständigt ansvar enligt dataskyddsförordningen. Annat ansvar enligt andra avtal och regler kan naturligtvis finnas.

fortfarande, i många kund-leverantörsrelationer. Det faktum att leverantören tillhandahåller en tjänst till kunden ses som avgörande för att all behandling som därvid aktualiseras utförs för kundens räkning. Kunden anses således bestämma över behandlingens ändamål och medel som en automatisk konsekvens av sitt beslut att anlita leverantören.

Resonemangets fördel är att personuppgiftsansvaret placeras utan tankemöda. Nackdelarna är att ett personuppgiftsbiträdesavtal med tillräckligt detaljerade instruktioner måste upprättas och ingås mellan parterna. Det ligger helt på kundens ansvar att instruera leverantören om behandlingen av personuppgifter, t.ex. vilka uppgifter som ska behandlas i vilket syfte, samt i övrigt kontrollera och övervaka biträdet för att uppfylla sina skyldigheter som personuppgiftsansvarig. Biträdet kan sägas utgöra den ansvariges förlängda arm och får enbart behandla de uppgifter den personuppgiftsansvarige tillhandahåller för de specifika ändamål som denne föreskriver. Biträdet måste även ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att biträdet fullgör sina lagstadgade skyldigheter, samt möjliggöra och bidra till att den personuppgiftsansvarige, själv eller genom bemyndigat ombud, kan granska och inspektera att biträdet agerar i enlighet med sina ord. Hela relationen mellan ansvarig och biträde regleras av Art. 28

Att kunden samtidigt som den anlitar en redovisningskonsult meddelar vilka personuppgifter som ska behandlas i vilket syfte är kanske inte verklighetens vanligaste scenario. Är det vanligare att konsulten talar om för kunden vilka uppgifter som behövs för att uppnå ett visst syfte? De konkreta former under vilka uppdraget ges och utförs har stor betydelse för fastställandet av vilken relation som faktiskt föreligger. Att kunden ansvarar för sin redovisning är inte samma sak som att kunden per automatik är den personuppgiftsansvarige i relationen till sin redovisningskonsult.

Om kunden säger *”fixa min redovisning”* och sedan i stort enbart agerar i enlighet med vad konsulten meddelar blir det administrativt mycket omständligt att skapa en ansvarig-biträdesrelation. Den konkreta nyttan med ett sådant arrangemang kan diskuteras, likaså om det i händelse av prövning skulle stå sig.

Om kunden däremot säger *”gör så här med de här uppgifterna,”* d.v.s. har detaljerade instruktioner som är framtagna av egen kraft, då ter sig ansvarig-biträdesrelationen mer naturlig.

Sammanfattningsvis, ju större frihet redovisningskonsulten har att själv bestämma om och hur behandlingen ska utföras, d.v.s. rent konkret bestämma behandlingens ändamål och medel, desto mindre är sannolikheten att det faktiskt föreligger någon ansvarig-biträdesrelation. Förhållandet mellan kunden och konsulten kan då istället betraktas som ett utlämnande mellan två personuppgiftsansvariga. Även i dessa fall kan det finnas behov av att skriftligen klargöra och dokumentera personuppgiftsansvaret, men i de tämligen få fall där detta skulle kunna tänkas aktualiseras, kan det göras tämligen enkelt. I alla händelser, administrationen och genomförandet blir i samtliga fall betydligt enklare än att försöka få till och upprätthålla en ansvarig-biträdesrelation.

2.1.2 Två självständigt ansvariga

Relationen mellan två självständigt personuppgiftsansvariga är den relation som skapar minst administration parterna emellan, ur dataskyddsförordningens perspektiv. Vardera parten är ensam ansvarig sina egna förpliktelser, både att uppfylla dem och att dokumentera uppfyllelsen och varje part står ensam under Datainspektionens tillsyn.

2.1.3 Gemensamt ansvariga

Parterna måste upprätta ett datadelningsavtal mellan varandra där varje parts ansvarsområde specificeras. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade. Exakt vad detta betyder är oklart. Kanske krävs någon form av publicering, kanske räcker det med att kunna svara på en förfrågan från en registrerad. Denna skyldighet finns dock alltid ändå, Art. 13. Parternas interna ansvarsfördelning till trots kan den registrerade utöva samtliga sina rättigheter mot valfri part. De inbördes konsekvenserna av detta får parterna reda ut mellan varandra i efterhand.

2.2 Nödvändiga avtal mellan behandlande parter

Skriftliga avtal krävs i två fall. När ett biträde anlitas eller när två eller fler är gemensamt ansvariga för en behandling.

2.2.1 Personuppgiftsbiträdesavtal

Kraven på ett biträdesavtal är utformade som minimikrav och återfinns i Art. 28.3. Eftersom dessa är så viktiga för Sunds verksamhet återges de här:

a. endast behandla på dokumenterade instruktioner från den ansvarige, vilka ska innehålla huruvida överföringar får ske till tredjeland eller internationell organisation. Utanför kravet dokumenterad instruktion från den ansvarige faller sådana behandlingar som biträdet är skyldig att utföra enligt nationell rätt eller EU-rätt, vilka biträdet måste informera om innan biträdesavtalets behandling inleds om inte sådan information är förbjuden enligt ett viktigt allmänintresse, om detta är fastlagt i nationell rätt eller EU-rätt.
b. Att biträdet säkerställer att endast behöriga personer behandlar uppgifterna och att behandlingen sker under avtalad eller lagstadgad tystnadsplikt
c. Att biträdet uppfyller samtliga säkerhetskrav enligt Art 32.
d. Att biträdet endast får anlita underbiträden efter ingångna underbiträdesavtal; i vilka bl.a. ska framgå den specifika behandling som ett underbiträde ska utföra, samt att varje underbiträde har samma skyldigheter gentemot den ansvarige som biträdet själv har och att den ansvarige måste skriftligen godkänna varje underbiträde, alternativt inte ha några invändningar om ett allmänt skriftligt förhandsgodkännande finns.
e. Att biträdet, med tanke på behandlingens art, genom tekniska och organisatoriska åtgärder kan hjälpa den ansvarige att besvara begäranden om utövande av de registrerades rättigheter enligt Art. 12 – 22
f. Att biträdet, med beaktande av den information denne har att tillgå samt typen av behandling ifråga, ska bistå den ansvarige vid dennes uppfyllande av säkerhetsföreskrifterna i Art. 32 – 36
g. Att biträdet vid avslutad avtalsrelation antingen raderar eller återlämnar alla uppgifter till den ansvarige, samt raderar alla eventuella kopior på uppgifterna, såvida inte EU-rätt eller nationell rätt föreskriver annorlunda
h. Att biträdet ger den ansvarige, eller dennes utsedda revisor, tillgång till all information som visar att alla skyldigheter enligt Art. 28 har fullgjorts, samt att den ansvarige eller av denne utsedd revisor kan genomföra inspektioner och granskningar som visar informationen stämmer. Om biträdet anser att den ansvariges instruktion enligt h strider mot förordningen eller andra nationella eller EU-rättsliga dataskyddsbestämmelser ska biträdet meddela den ansvarige det.

Biträdesavtalet måste vara tillräckligt konkret för att kunna ligga till grund för bedömningen om det har uppfyllts eller ej. Det räcker således inte att avtala om att *"tillräckliga organisatoriska och tekniska säkerhetsåtgärder ska vidtas"*, avtalet ska specificera vilka dessa är. I annat fall vore det tillräckligt om parterna avtalade att de ska följa lagen. Ett sådant avtal vore dock meningslöst, eftersom parterna är skyldiga att följa lagen oavsett något avtal dem emellan eller ej.

Avtalet ska även kunna ligga till grund för bedömningen huruvida de förpliktelser som däri stadgas är tillräckliga för att dataskyddsförordningens krav uppfylls. Därmed är ett avtal som säger att parterna ska se till att dataskyddsförordningens krav uppfylls i praktiken samma sak som att inget avtal finns, eftersom alla former av konkreta, specifikt angivna åtgärder saknas. Med andra ord, svepande och generella formuleringar i generalklausulstil duger inte.

2.2.2. Datadelningsavtal

Kravet på ett datadelningsavtal är att det ska *"på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot de registrerade,"* Art. 26.2. Det finns alltså ingen lista att följa. En möjlig slutsats av detta är att parterna i ett avtal mellan varandra specificerar:

- Behandlingens gemensamma ändamål[18] och dess rättsliga grund
- Vem som gör vad[19]
- Vem som ansvarar för vilka av de registrerades rättigheter[20]
- Hur och när behandlingen avslutas.

Datadelningsavtalet rör hur uppgifterna får behandlas av respektive part. Att samtliga parter är personuppgiftsansvariga innebär att ingen har något ansvar för någon annans behandling, även om parterna är solidariskt ansvariga gentemot de registrerade. Samtliga parter måste således uppfylla alla krav som ställs på en personuppgiftsansvarig.

2.3 Artikel 30-register, ett för ansvariga och ett annat för biträden

Varje personuppgiftsansvarig och varje personuppgiftsbiträde är skyldig att föra ett register över sina behandlingar, Art. 30. Den organisation som har bägge rollerna måste alltså föra två olika register, ett för vardera rollen.

2.3.1 Artikel 30-register för personuppgiftsansvariga

Beträffande personuppgiftsansvarig specificeras registrets innehåll i Art. 30.1:

- Namn och kontaktuppgifter på den personuppgiftsansvarige, eller gemensamt ansvariga, ansvariges företrädare och dataskyddsombud.
- Behandlingens ändamål.

[18]Parternas inflytande över detta behöver inte vara lika stort. Det räcker med att en part har något inflytande för att det gemensamma ansvaret ska aktiveras, enligt EU-domstolen i fallet C-25/17, Jehovas vittnen, p. 68.
[19] Det gemensamma ansvaret består oavsett om parterna har lika stor tillgång till alla uppgifter, C-25/17, Jehovas vittnen, p. 69, se även HFD 2012 ref. 21.
[20] En registrerad kan vända sig till vem som helst av parterna med en förfrågan. För att undvika dubbelarbete, eller att en förfrågan inte kan besvaras, bör därför parterna tydligt klargöra detta mellan varandra. Gentemot de registrerade är parterna solidariskt ansvariga för allt, Art. 82.4 och p.5.

- Beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- Kategorierna av mottagare som uppgifterna har eller ska lämnas ut till samt om mottagarna finns i tredjeland eller i internationella organisationer.
- Om överföringar sker till tredjeland eller till internationella organisationer, vilka dessa är, samt dokumentation av lämpliga skyddsåtgärder, ifall överföringarna är av sådan art som nämns i Art. 49.1.
- Förutsedda tidsfrister för radering av uppgifterna, om möjligt.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder enligt Art. 32.1.

Dessa uppgifter måste alltså finnas i ett register, som måste vara skriftligt och på begäran kunna göras tillgängligt för tillsynsmyndigheten.

2.3.2 Artikel 30-registret för personuppgiftsbiträden

Beträffande personuppgiftsbiträden specificeras registrets innehåll i Art 30.2:

- Namn och kontaktuppgifter för personuppgiftsbiträdet eller biträdena, om flera är involverade, och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar. Om tillämpligt, även den ansvariges och biträdets företrädare, samt dataskyddsombudet.
- De kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.
- Om överföringar sker till tredjeland eller till internationella organisationer, vilka dessa är, samt dokumentation av lämpliga skyddsåtgärder, ifall överföringarna är av sådan art som nämns i Art. 49.1.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder enligt Art. 32.1.

Både för personuppgiftsansvariga och för biträden anges att vissa uppgifter endast behöver registreras *"om möjligt."* Detta skrivsätt finns på flera platser i förordningen. Nivån på när något inte längre anses möjligt ligger alltid högt. Det måste även kunna visas att något inte är möjligt, på sakligt godtagbara grunder.

I Art. 30.5 anges ett antal villkor för när något register enligt Art. 30.1 och p.2 inte behöver föras. Dessa villkor är:

- Den organisation som är personuppgiftsansvarig eller biträde sysselsätter färre än 250 personer
- Behandlingen i fråga kommer sannolikt inte medföra någon risk för de registrerades fri- och rättigheter.
- Behandlingen är tillfällig.
- Behandlingen rör inte särskilda kategorier av personuppgifter enligt Art. 9.1 eller uppgifter om fällande domar i brottmål eller andra lagöverträdelser som innefattar brott, Art. 10.

Det är den personuppgiftsansvariges eller biträdets ansvar att kunna visa att Art. 30.5 är tillämplig på varje behandling. Det går alltså inte att få något undantag i klump, bara för att man är färre än 250 personer. Varje enskild behandling måste uppfylla undantagskraven och detta måste kunna visas. Man undgår alltså i praktiken inget administrativt arbete genom att

hävda att undantaget gäller. Därför torde det vara mer arbetsekonomiskt att registrera alla behandlingar i sitt register och därigenom slippa ett bedömningsmoment. Dessutom slipper man också risken för felbedömningar.

Personuppgiftsbiträdet har till största delen utfört sitt dokumentationsansvar när artikel 30-registret är skapat. Så är inte fallet för den personuppgiftsansvarige.

2.4 Dokumentationskravet går längre för personuppgiftsansvariga: Datakollen

En av dataskyddsförordningens grundpelare är att den personuppgiftsansvarige ansvarar för och kan visa att förordningens samtliga krav uppfylls. Detta krav kallas för ansvarsskyldighetsprincipen och beskrivs i avsnitt 1.4.

Emellertid anges i förordningen bara minimikrav och principer, samt några förbud. Någon metod för hur arbetet kan genomföras för att bli rätt finns inte angiven. Men utan en klart definierad arbetsmetod med en tydlig struktur på resultatet kan inte dokumentationsarbetet leda fram till det som förordningen kräver. I synnerhet inte när verkligheten dessutom ska vara i överensstämmelse med den dokumentation som finns. Sett över några års tid blir situationen fullständigt ohanterlig. Tillväxt, personalomsättning, organisatoriska förändringar, nya tekniska lösningar, för att bara nämna några grunder, bidrar alla till att öka omfattningen och mängden av nödvändig dokumentation, inklusive att gallra bort uppgifter och samlingar som inte längre är relevanta. Utan metod och struktur i detta arbete kommer det de facto inte ha någon större betydelse. Detta inkluderar regelbunden översyn och uppdatering av dokumentationen, samt att rutiner för lagenlig personuppgiftsbehandling finns och följs.

Den organisatoriska utmaningen blir således tvåfaldig:

- dokumentationen vara formellt korrekt
- dokumentationen ska återspegla verkligheten

Själva dokumentationsarbetet bör dessutom bedrivas på ett arbetsekonomiskt och för verksamheten utvecklingsfrämjande sätt.

Detta är även utgångspunkterna för dokumentationstjänsten Datakollen.

3. Tekniska och organisatoriska säkerhetsåtgärder

Dataskyddsförordningen handlar om dataskydd, som namnet avslöjar. Detta dataskydds primära skyddsobjekt är fysiska personers grundläggande fri- och rättigheter, särskilt rätt till skydd av personuppgifter. Det effektivaste sättet att skydda personuppgifter är att inte behandla dem alls. Därefter krävs att de *principer för behandling av personuppgifter* som återfinns i Art. 5.1 uppfylls, innan behandlingen påbörjas. Dessa principer är:

a. Lagligt, korrekt[21] och öppet gentemot de registrerade (öppenhetsprincipen)
b. Särskilda, uttryckligt angivna och berättigade ändamål (ändamålsprincipen)

[21] Det engelska ordet i denna punkt är *fair*. Ordet *korrekt* ska alltså förstås i den betydelsen, d.v.s. som schysst, ärligt, rättvist, hederligt och liknande. Det handlar om den personuppgiftsansvariges uppträdande gentemot de registrerade.

c. Adekvata, relevanta och inte för omfattande i förhållande till det ändamålet (uppgiftsminimeringsprincipen)
d. Korrekta[22] och om nödvändigt uppdaterade (riktighetshetsprincipen)
e. Inte sparas i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt (lagringsminimeringsprincipen)
f. Säkerställa uppgifternas integritet och konfidentialitet.

Förordningens synvinkel kan uttryckas så, att dataskyddsarbetet börjar med att medvetet behandla så få personuppgifter under så kort tid som möjligt. Självklart på giltig rättslig grund och med full respekt för de registrerades rättigheter. Först efter detta avgränsande inledningsarbete tar säkerhetsåtgärderna vid. Att ovanstående principer kan uppfyllas ska alltså säkerställas redan på planeringsstadiet, innan behandlingen har påbörjats.

3.1 Typer av åtgärder

Efter att ha fastställt att viss personuppgiftsbehandling är nödvändig för att kunna lösa specifika uppgifter, krävs tekniska och organisatoriska säkerhetsåtgärder som säkerställer att personuppgifterna inte förstörs, försvinner, manipuleras eller kommer i orätta händer, samt att hela förordningen efterlevs. Schematiskt kan åtgärderna delas upp enligt följande:

Tekniska: hur ett it-system för personuppgiftsbehandling är uppbyggt. Inbegriper bland annat hård- och mjukvarufrågor, fysisk placering av hårdvara, kryptering, lösenord, brandväggar m.m.

Organisatoriska: hur it-systemet ifråga ska hanteras och av vem, hur dokumentationen och övriga efterlevnadsfrågor ska lösas. Handlar bland annat om var vilken typ av uppgifter ska bearbetas och sparas, vem som ska göra det, vem som ska få tillgång till dem m.m.

Säkerhetsarbetets två ben måste samverka mot ett gemensamt mål för att någon verklig säkerhet ska uppnås. Många organisationer anlitar extern kompetens för att hantera tekniken. Den anlitade parten blir då oftast personuppgiftsbiträde. Som redan har påpekats i avsnitt 2.2.1 krävs i så fall ett korrekt biträdesavtal. Detsamma gäller eventuella underbiträden. Personuppgiftsansvariga som tar hjälp av utomstående, vilka de facto hamnar i biträdesposition, utan att ha korrekta avtal för detta tar en potentiellt sett både stor och onödig risk. Det resonemanget gäller också för eventuell extern hjälp att hantera de organisatoriska kraven.

3.2. Risk- och konsekvensanalyser

Det grundläggande kravet för att korrekta och rimliga säkerhetsåtgärder ska kunna tillämpas är att varje uppgiftssamling förses med en risk- och konsekvensanalys. Detta krav ligger implicit i Art. 24, som anger den personuppgiftsansvariges ansvar. Arbetet med att säkerställa rätt nivå av skydd kräver ett kontinuerligt och systematiskt arbete för att identifiera, analysera och förvalta risker som påverkar, eller kan påverka, efterlevnaden av dessa krav.

[22] I denna punkt ska ordet *korrekta* förstås i betydelsen riktiga, d.v.s. uppgifterna ska vara med verkligheten överensstämmande. Ofta används därför ordet *riktighet* istället. Därför används här begreppet *riktighetsprincipen.* Risken för mental sammanblandning bedöms minska då, jämfört med om det mer ordalydelse trogna korrekthetsprincipen hade använts.

Att införa korrekta och rimliga säkerhetsåtgärder avseende personuppgiftsbehandling skiljer sig inte principiellt från annat säkerhetsarbete. Det handlar om att få en bild av de risker och konsekvenser som finns och hur dessa ska hanteras. Generellt uttryckt, vilka risker bör accepteras, modifieras eller helt undvikas med tanke på deras konsekvenser. Konsekvenserna måste i sin tur ställas i relation till skyddsåtgärdernas kostnader.

Kontinuiteten i arbetet är av central betydelse. En risk som kanske accepteras idag, när konsekvenserna anses vara hanterbara, kan imorgon vara oacceptabel. Förändringar sker både i omvärlden och internt. De konkreta åtgärder som hanterar organisationens risker och konsekvenser måste därför övervakas över tid. Personuppgiftsansvaret rymmer även krav på att dataskyddsarbetet ses över och uppdateras vid behov, Art. 24.1 och Art. 32.1d, vilket leder över till nästa avsnitt.

3.3 Planen och verkligheten: kongruens

Det krävs alltså att säkerhetsåtgärderna är i nivå med förordningens krav för den specifika behandlingen och att de är tydligt dokumenterade. Dessutom måste dokumentationen representera verkligheten. Påpekandet är i och för sig en självklarhet, men sätter ljuset på några viktiga punkter:

- Det som faktiskt görs ska dokumenteras.
- Dokumentationen ska vara lätt tillgänglig för egenkontroll och justeringar.
- Säkerhetsarbetet måste hållas aktuellt i det dagliga arbetet.

Dessa punkter ställer vissa krav på en organisations arbetsrutiner. Krav som dessutom aldrig försvinner. För även om arbetsrutinerna förblir som de har varit så kan omvärlden förändras och därmed även riskbilden ändras.

3.4 Säkerhetspolicy

Artikel 32 anger de säkerhetskrav som personuppgiftsansvariga och personuppgiftsbiträden måste möta. Artikeln är utformad i enlighet med den riskbaserade metodens modell, som beskrevs i avsnitt 1.3. Detta kommer till uttryck genom orden *”säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.”* Vid riskbedömningen ger, som alltid, skäl 75 ledning.

Ordet *lämplig*[23] spelar en stor roll vid artikelns tillämpning. Exakt vilka åtgärder som är lämpliga att vidta framgår inte av artikeltexten, men målen för säkerhetsåtgärderna specificeras i Art. 32.1b som:

”förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna.”

Vidare anges i Art. 32.2 att säkerhetsåtgärdernas viktigaste punkter är att skydda personuppgifterna som överförts, lagrats eller på annat sätt behandlats från:

- oavsiktlig förstöring, förlust eller ändring
- obehörigt röjande
- obehörig åtkomst

[23] På engelska används ordet *appropriate.*

Slutligen framgår av Art. 32.4 att varje fysisk person som under en ansvarigs eller ett biträdes överinseende får tillgång till personuppgifter måste omfattas av den ansvariges instruktion, beträffande åtgärder som säkerställer den lämpliga säkerhetsnivån.

Konkret anger alltså Art. 32.4 att den personuppgiftsansvarige måste ha en säkerhetspolicy som talar om för de anställda vad de konkret ska göra för att de personuppgifter de får tillgång till alltid hanteras säkert. Detsamma gäller i relationen mellan den ansvarige och eventuella biträden, inklusive dennes personal och eventuella underbiträden. En väsentlig punkt i den policyn är avtalad sekretess. Detta framgår inte direkt av ordalydelsen, men är en logisk konsekvens av hur artikeln rent praktiskt ska kunna tillämpas.

4. De registrerades rättigheter

De registrerades rättigheter anges i Art. 12 – 22. Överträdelse av dessa bestämmelser är sanktionerad med de högsta avgifterna, Art. 83.5. Personuppgiftsansvariga och biträden har således starka incitament att ta rättigheterna på allvar. Grunden till dessa rättigheters ställning finns i den så kallade *öppenhetsprincipen*[24], som uttrycks i Art. 5.1a, den första av de grundläggande dataskyddsprinciperna. Den kan i korthet beskrivas som att fysiska personer har rätt att:

- få veta hur deras personuppgifter behandlas och behandlingens konsekvenser
- kunna förstå personuppgiftsansvarigas kommunikation
- utöva sina rättigheter utan hinder

Andemeningen kan sägas vara att personuppgifter inte ska behandlas i det fördolda, utan att de registrerade har en aning om att det sker, i vilket syfte det sker eller dess konsekvenser.

För att rent allmänt förstå öppenhetsprincipens funktion kan man gå tillbaka till dataskyddsförordningens grundläggande syfte, att vara en rättighetslagstiftning för enskilda individer. Om den registrerade inte ens vet om registreringen, hur ska han eller hon då kunna utöva några rättigheter? Öppenhetsprincipen och de registrerades rättigheter är hur EU vill motverka att internetåldern övergår i den typ av hemlig massövervakning, som totalitära organisationer och stater utövar, utan att enskilda individer har några möjligheter att skydda sig. Det sker redan idag en omfattande och till största delen hemlig övervakning och kartläggning av allt som alla gör på internet, även i demokratiska rättsstater. Öppenhetsprincipen kan då betraktas som ett sätt att sprida kunskap om läget, samt uppmana till betänksamhet bland enskilda.

I vardagen, för de ansvariga och deras biträden, är nog de potentiella sanktionerna, skadeståndsansvaret och administrativa problem[25] de största skälen för att ta dessa frågor på allvar, men kännedom om det övergripande syftet kan kanske hjälpa till att skapa intern acceptans för åtgärder som kanske uppfattas som onödigt merarbete.

[24] I ”Riktlinjer om öppenhet och information till de registrerade” WP260 rev.01 har Artikel 29-gruppen, föregångaren till Europeiska dataskyddstyrelsen, EDPB, redogjort för sin syn på hur denna centrala princip bör förstås.

[25] Med administrativa problem avses den verksamhetsstörning som uppstår om förfrågningar inte kan hanteras inom ramen för den dagliga verksamheten.

4.1 Informationskrav och integritetspolicy

Personuppgifter kan komma den personuppgiftsansvarige tillhanda på två sätt. Antingen direkt från den registrerade eller via en mellanhand. I bägge fallen har den ansvarige en informationsplikt gentemot den registrerade. Kommer uppgifterna direkt från den registrerade gäller Art. 13, kommer de via en mellanhand gäller Art. 14.

Tidsfristerna för att lämna informationen är antingen när uppgifterna erhålls, Art. 13.1, eller senast inom en månad, Art. 14.3a. Ska uppgifterna användas för att kommunicera med de registrerade får informationen lämnas senast vid första kommunikationstillfället, Art. 14.3b. Ska uppgifterna lämnas till annan mottagare får informationen lämnas senast när uppgifterna lämnas ut för första gången, Art. 14.3c.

Kraven på informationens innehåll framgår av Art.13 och Art 14.
Formkraven på informationen återfinns i Art.12. Huvudregeln är att informationen är skriftlig, vilket inbegriper i elektronisk form. Informationen får vara muntlig om den registrerades identitet bevisats på andra sätt, Art. 12.1.[26]

Informationen ska vara *"i en koncis, klar och tydlig, begriplig och lätt tillgänglig form,"* Art. 12.1. Det finns en spänning mellan detta krav och den informationsmängd som krävs enligt Art. 13 och 14. Den spänningen, eller konflikten, måste den personuppgiftsansvarige lösa efter eget huvud.[27] Syftet är att motverka informationströtthet hos den registrerade, d.v.s. att en undran dennes sida besvaras med så mycket information att denne helt enkelt struntar i svaret. Tidsåtgången för att förstå blir för stor.

Det enklaste sättet att praktiskt lösa informationskravet är att skapa en integritetspolicy och att sedan antingen bifoga den i sin helhet, som länk, eller hänvisa till en adress.

4.2 Relationskategorier och uppgiftskategorier

En personuppgiftsansvarig hanterar olika personuppgifter för olika syften och från olika människor. Av Art 30.1c framgår att behandlingsregistret ska innehålla kategorier av registrerade och kategorier av personuppgifter. Eftersom det kategoriseringskravet finns och dessutom i ett grundläggande krav, blir det arbetsekonomiskt att strukturera sin informationsplikt på liknande sätt.

Relationskategorier kan uttryckas som en grupp människor vars personuppgifter förekommer i en behandling p.g.a. minst en gemensam egenskap hos dessa människor. Det är t.ex. anställda, anställdas anhöriga, kunder, potentiella kunder, leverantörer, samarbetspartners etc.

Uppgiftskategorier handlar om den typ av personuppgifter som ingår i en specifik behandling, t.ex. namn, kontaktuppgifter, hälsouppgifter, inkomstuppgifter etc.

---

[26] Det mesta av informationen till de registrerade är av generell art, varför identifikationskravet framstår som något överdrivet. Sett ur den personuppgiftsansvariges synvinkel kan rätten att informera muntligt knappast betraktas som annat än ett komplement som i enstaka fall kan vara smidig att använda. Som helhet framstår den muntliga informationsrätten av tämligen underordnad betydelse.

[27] Punkter 34, 36 och 38 i "Riktlinjer om öppenhet och information till de registrerade" WP260 rev.01 tar upp detta. Rekommendationen är att det viktigaste tas först i en lättförståelig form och att mer detaljerad information ges ju längre in i texten som den registrerade vill gå. Kallas för *skiktad metod*, på engelska *layered approach.*

Alla relations- och uppgiftskategorier kan ingå i samma integritetspolicy, eller så kan olika policys kan göras för olika relationskategorier. Det väsentliga är att registrerade erhåller den information de enligt lag har rätt till, samt att den är lätt att förstå. Naturligtvis måste den ansvarige också lätt kunna kontrollera vad som står var och vid behov kunna uppdatera det.

4.3 Cookies

Användningen av cookies[28] faller in under två olika regelverk, den så kallade cookielagen och dataskyddsförordningen. Cookielagen utgörs av 6 kap 18§ i lagen om elektronisk kommunikation, LEK (SFS 2003:389)[29]. Cookielagen gäller för alla typer av spårning online, så kallade tracking teknologier, och är alltså trots sitt namn inte begränsad till enbart cookies.

Att cookies EU-rättsligt regleras av både ett direktiv och en förordning har två stora följder:

1. Cookies faller till viss del under varje enskilt medlemslands nationella rätt.
2. Gränserna mellan regelverken är oklara.[30]

Dessutom kan, som i Sveriges fall, regelverken ha olika tillsynsmyndigheter. Tillsynsmyndighet för cookielagen är Post- och Telestyrelsen, PTS, och för dataskyddsförordningen är det Datainspektionen.

Cookielagen[31] lyder:

---

[28] En cookie är en liten textfil som skickas från webbplatsen till besökarens webbläsare. Cookies skickas antingen direkt från den besökta webbplatsen (så kallade förstapartscookies) eller från en annan organisation som levererar tjänster till den aktuella webbplatsen, såsom ett analys- och statistikföretag (så kallade tredjepartscookies). Det finns två sorters cookies, den ena typen kallas sessioncookie och den andra kallas permanent cookie. Sessioncookies används för att webbsidorna ska fungera korrekt under besöket. En sessionscookie lagras inte på besökarens dator utan försvinner när webbläsaren stängs av. En permanent cookie lagras däremot datorn och gör till exempel så att en webbsida kan känna igen datorns IP-adress och därmed webbläsaren vid nästa besök. Den som har skapat cookien bestämmer vad den ska ha för funktion. Många funktioner på internet bygger på användning av cookies. Se t.ex. denna artikel ur tidningen PC för alla: https://pcforalla.idg.se/2.1054/1.623681/overvakning-internet

[29] LEK reglerar användningen av telenät och radio som kommunikationsmedel och är den lag som införlivar e-privacydirektivet 2002/58/EG i svensk rätt. Direktivet ändrades en del genom direktivet 2009/136 EG. Dessa ändringar inbegrep direktivets artikel 5.3, som är cookielagens direkta ursprung. E-privacydirektivets fullständiga namn lyder: Europaparlamentets och Rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

[30] Dataskyddsförordningens Art. 95 stadgar att förordningen inte ska innebära några ytterligare förpliktelser i förhållande till dem som aktörer redan uppfyller under e-privacydirektivet. Med tanke på att direktivet är olika genomfört och tolkat i de olika medlemsländerna blir efterlevnaden av Art. 95 per definition olika i olika länder. I förordningens skäl 173 står också att e-privacydirektivet bör ändras så att förhållandet mellan de två regelverken kan klargöras. Tanken var att detta skulle ske genom en e-privacyförordning, som skulle vara klar ungefär samtidigt som dataskyddsförordningen. Detta arbete har dock inte varit framgångsrikt och för närvarande kan ingen säga när någon sådan förordning kan vara klar. Att det handlar om flera år är dock ställt utom allt rimligt tvivel.

[31] För jämförelsens skull återges här även gällande direktivtext, artikel 5.3 i 2009/136/EG: *Medlemsstaterna ska se till att lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, i enlighet med direktiv 95/46/EG, bland annat om ändamålen med behandlingen av uppgifterna. Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.*

Uppgifter får lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Detta hindrar inte sådan lagring eller åtkomst som behövs för att överföra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som är nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt.

Det anses allmänt att cookielagen skiljer mellan två typer av cookies. De som är tekniskt nödvändiga för att kommunikationen mellan webbplatsen och besökarens webbläsare ska fungera och alla övriga. För tekniskt nödvändiga cookies krävs inget samtycke, däremot för alla övriga. Undantaget är dock varje cookie som är *"nödvändig för att tillhandahålla en tjänst som användaren eller abonnenten uttryckligen har begärt."* Lagen säger inget om hur innehållet i detta uttryck ska fastställas.

Av naturliga skäl blir EU-domstolens avgöranden extra viktiga i detta oklara legala landskap. Domstolen har i närtid avgjort två mål angående bruket av cookies.

Den 29 juli 2019 föll dom i det så kallade Fashion ID-målet, målnr C-40/17. Det tyska företaget Fashion ID hade lagt upp en "gilla-knapp" från Facebook på sin webbplats. Att knappen fanns innebar att utvald information om alla webbplatsens besökare automatiskt överfördes till Facebook, oavsett om besökaren använde knappen eller ej och oavsett om besökaren hade ett facebookkonto eller ej. Besökaren fick ingen information om denna överföring och kunde inte heller vägra den. Domslutet i korthet:

- Fashion ID är personuppgiftsansvarig för installationen av knappen. Facebook är personuppgiftsansvarig för behandlingen av den information som når dem. Både delat och gemensamt personuppgiftsansvar föreligger.
- Både Fashion ID och Facebook måste ha berättigat intresse för att behandlingen ska vara tillåten.
- Fashion ID måste informera besökaren om knappens funktion och inhämta besökarens samtycke, så långt som Fashion ID bestämmer över ändamål och medel för behandlingen.

Den 1 oktober 2019 avkunnades dom i det andra målet kallat Planet49, målnr C-673/17. Det tyska företaget Planet49 hade anordnat en pristävling på sin webbplats. En mängd samarbetspartners och sponsorer var inblandade. Tävlingsdeltagarna samtyckte genom sitt deltagande till att dessa fick skicka reklam och erbjudanden till dem. Deltagarna var också fria att välja vilka de ville erhålla marknadsföring från. Om deltagarna inte gjorde några aktiva val så valde Planet49 åt dem. Valen kunde när som helst ändras. En klickruta med samtycke var förkryssad. Deltagarna var alltså tvungna att ta bort samtycket för att det inte skulle ges automatiskt. Domen i korthet:

- Samtycke genom förkryssad ruta är inte giltigt.
- Informationen om cookies på en webbplats måste innehålla deras funktionstid, samt möjligheten för tredje part att få tillgång eller inte till dessa cookies.

Sett ur ett helhetsperspektiv ger dessa två fall ganska mager ledning avseende hur cookies ska hanteras, även om några viktiga frågor har besvarats. Även om en förkryssad ruta är ett för grovt medel för att inhämta giltigt samtycke, så kvarstår problematiken med alla de webbplatsbesökare som inte gör något aktivt val utan bara surfar vidare på en sida. Detta är och lär under överskådlig framtid förbli det vanligaste sättet att hantera cookieinformationen på, oavsett hur begriplig och lätt tillgänglig den är. Just nu framstår det som möjligt att

likställa fortsatt surfande med samtycke till cookieplacering, under förutsättning att denna samtyckeshantering tydligt framgår. Frågan kan dock ställas om den relevanta skillnaden mellan denna variant och den förkryssade rutan. Den frågan har dock ännu inte hamnat hos EU-domstolen. Rättsläget förefaller överlämna frågan åt den personuppgiftsansvariges egna rättsliga argumentationsförmåga.

Att webbplatsbesökare måste informeras om funktionstid på och vem som har tillgång till de cookies som används är helt klart. Att ett giltigt samtycke behövs för att cookies ska få placeras på besökarens webbläsare är också klart. Men exakt hur ett giltigt samtycke inhämtas och exakt vilken information som måste lämnas är som sagt fortfarande oklart.

5. Personuppgiftsincidenter

All proaktivitet till trots kan fortfarande oönskade händelser inträffa. De kan ha olika orsaker och olika konsekvenser. Dataskyddsförordningen kräver att ett antal åtgärder vidtas när en personuppgiftsincident av tillräckligt allvar har inträffat.

5.1 Vad är en personuppgiftsincident?

Begreppet definieras i Art. 4.12:
en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats

Definitionen är vidsträckt. I praktiken berörs allt som på något sätt påverkar uppgifternas *tillgänglighet*, *integritet* och *konfidentialitet*. En personuppgiftsincident är således per definition en säkerhetsincident.

Med *tillgänglighet* menas att uppgifterna ska kunna nås av behörig person när det behövs och att de inte förstörs eller förloras[32]. Med *integritet*, kallas även för riktighet, menas både att uppgifterna inte obehörigt eller oavsiktligt kan ändras.[33] Med *konfidentialitet* menas att endast behöriga personer får åtkomst till uppgifterna. En incident berör inte nödvändigtvis bara en av dessa händelsekategorier.

5.2 Anmälan till Datainspektionen

Om det är osannolikt att personuppgiftsincidenten medför risk för fysiska personers rättigheter och friheter, då behövs ingen anmälan göras till Datainspektionen. I annat fall är det ett krav. Anmälan ska göras när den personuppgiftsansvarige får vetskap om incidenten, eller senast inom 72 timmar från denna tidpunkt. Kan inte fristen om 72 timmar hållas ska anmälan åtföljas av en motivering till förseningen. Detta framgår av Art. 33.1. I Art. 33.3 anges vad en incidentanmälan åtminstone måste innehålla. I korthet:

- Vad har hänt?
- Vilka kategorier av registrerade berörs och ungefär hur många?
- Vilka uppgiftskategorier berörs och ungefär hur många?

[32] Förlust täcker både fallet att uppgifterna helt har förlorats, t.ex. ett USB-minne med ett register har tappats bort och fallet att uppgifterna fortfarande finns, men att den ansvarige inte kommer åt dem, t.ex. att en krypteringsnyckel har försvunnit eller att uppgifterna har krypterats av en it-brottsling som kräver en lösensumma (så kallad *ransomeware*).
[33] Det är även en riktighetsaspekt att det märks om uppgifterna har utsatts för sådan ändring.

- Namn och kontaktuppgifter till dataskyddsombudet eller annan kontaktpunkt för mer information.
- Beskrivning av incidentens sannolika konsekvenser.
- Beskrivning av vidtagna eller föreslagna åtgärder för att åtgärda incidenten.
- Om lämpligt, beskrivning av åtgärder för att mildra incidentens potentiella negativa effekter.

Om det inte är möjligt att tillhandahålla all information samtidigt så får den delas upp i omgångar utan onödigt ytterligare dröjsmål, enligt Art. 33.4. Artikeln täcker huvudsakligen in det fall att en incident har skett, men större utredning krävs för att kunna fastställa exakt vad som har skett och vad det innebär.[34] Ett ytterligare syfte med regeln är att ansvariga uppmuntras att anmäla inträffade incidenter och alltid har möjlighet att senare komplettera en anmälan.

Datainspektionen har två blanketter för anmälan av personuppgiftsincidenter, en ifall endast registrerade i Sverige berörs och en ifall det handlar om gränsöverskridande behandlingar.[35] En intressant detalj är att anmälan måste skickas med fysisk post. Detta för att anmälan kan vara sekretessbelagd[36] och alltså inte bör skickas med vanlig e-post. Hänsyn tas till postgångens tid för bedömningen om tidsfristen på 72 timmar har hållits eller ej.

5.3 Anmäla till berörda registrerade

Om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter måste även de registrerade informeras, Art. 34.1. Detta ska ske utan onödigt dröjsmål, kvantifierad tidsangivelse saknas.

Informationen ska innehålla en tydlig och klar beskrivning av incidentens art och dessutom åtminstone:

- Namn och kontaktuppgifter till dataskyddsombudet eller annan kontaktpunkt för mer information.
- Beskrivning av incidentens sannolika konsekvenser.
- Beskrivning av vidtagna eller föreslagna åtgärder för att åtgärda incidenten.
- Om lämpligt, beskrivning av åtgärder för att mildra incidentens potentiella negativa effekter.

Ovanstående information behöver dock inte skickas om något av följande villkor är uppfyllt:

- Uppgifterna är oläsbara för obehöriga personer, t.ex. genom kryptering.
- Ytterligare vidtagna åtgärder säkerställer att den höga risken blivit osannolik.
- Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller de registrerade informeras på ett lika effektivt sätt.

Någon färdig blankett för detta finns inte, utan den ansvarige måste själv skapa formen för informationen.

---

[34] Artikel 29-gruppens WP250rev.01, Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/67, s.16.

[35] Blanketterna finns på Datainspktionens webbplats. https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/personuppgiftsincident/anmala-personuppgiftsincident/

[36] 18 kap 8§ 3 offentlighets- och sekretesslagen (SFS 2009:400) samt dataskyddsförordningens Art 54.2.

5.4 Incidentberedskap

Grunden för om Datainspektionen och de registrerade ska informeras bygger på en riskbedömning. Risknivån för när anmälan till Datainspektionen måste göras är *"inte osannolik"* och risknivån för när de registrerade måste informeras är *"hög."* Eftersom den personuppgiftsansvarige bär informationsansvaret måste även denne göra riskbedömningen. Skäl 75 ger ledning för hur riskerna bör bedömas. Det mest praktiska är att göra alla riskbedömningar innan en eventuell incident inträffar. Detsamma gäller skapandet av den arbetsprocess som krävs för att kunna hålla tidsgränsen om max 72 timmar och se till att rätt information går till rätt mottagare. Felaktig hantering av anmälnings- och informationsplikterna är sanktionerat enligt Art. 83.4, varför avgifter är en möjlig påföljd.

Incidentberedskapen bör således minst innehålla:

- Anmälningsansvarig person
- Rätt anmälningsadress
- Riskbedömning av varje uppgiftssamling
- Mall avseende anmälnings- och informationsinnehåll

Den viktigaste punkten är att vara klar över de olika riskernas potentiella konsekvenser, enligt skäl 75.

6. Hemsidespublicering av generell information

Den egna webbplatsen är ett bra medel för att nå ut med generell information om hur man arbetar med dataskyddsförordningen. Informationens riktighet är mycket viktig. Det man skriver att man gör måste man också göra.

6.1 Integritetspolicy

Som framgår av avsnitt 4.1 är hemsidespublicering av integritetspolicyn, för att därefter kunna hänvisa till den via länk eller adress, ett enkelt sätt att lösa sin informationsplikt i många fall. Främst naturligtvis i fallet att någon besöker hemsidan som första och enda kontakt med organisationen.

Vill man inte använda sig av hemsidespublicering måste informationen framföras på annat sätt, främst då genom bifogade elektroniska eller fysiska dokument. Det går även att framföra muntligt, men är på grund av bevisfrågan sällan att rekommendera. Hur ska det objektivt kunna styrkas vilken information som givits till vem vid vilken tidpunkt, om det handlar om muntligt framförd information?

Det går att bestämma att viss integritetspolicy avseende vissa relationskategorier ska framföras på ett sätt och att andra policyer till andra kategorier på annat sätt. Det viktiga är att fatta ett beslut och att följa det.

6.2 Cookiepolicy

Som framgår av avsnitt 4.3 är den legala hanteringen av cookies till stor del oklar. Så mycket är dock säkert, att den hemsida som använder cookies måste innehålla en cookiepolicy. Vidare måste besökaren ge sitt uttryckliga samtycke till placeringen av cookies innan dessa de facto placeras. Undantag från informationsplikt och inhämtande av samtycke görs endast för tekniskt nödvändiga cookies.

Av praktiska och pedagogiska skäl är det dock klokt att ha en cookiepolicy även om man endast använder tekniskt nödvändiga cookies. Dels visar man tydligt för besökarna att man förstått cookielagstiftningen, dels skapar man en intern säkerhet beträffande det egna förhållningssättet i frågan.

6.3 Säkerhetspolicy

Personuppgiftsansvariga är skyldiga att ha en relevant säkerhetspolicy som de följer. Vissa väljer att offentliggöra den, medan andra väljer det motsatta. Det finns ingen skyldighet för de ansvariga eller deras biträden att informera om hur de arbetar med den tekniska och organisatoriska säkerheten avseende de personuppgifter de behandlar. Det vanligaste argumentet för ett offentliggörande, t.ex. genom en hemsidespublicering, är viljan att vara öppen och visa kunder, partners och övriga intressenter att man tar frågan på allvar och har koll på vad man gör. Det vanligaste argumentet mot ett offentliggörande är att man inte vill tala om för eventuella angripare vilka rutiner och system de behöver ta sig förbi för att kunna lyckas med sina onda avsikter. Varje organisation är fri att träffa sitt eget val, med hänsyn till just den egna situationen.

7. Datainspektionen första administrativa sanktionsavgift

Gymnasienämnden i Skellefteå kommun blev föremål för den första sanktionsavgiften i Sverige för överträdelse av dataskyddsförordningen. Fallet rör användande av ansiktsigenkänningsteknik för närvarokontroll i en gymnasieskola. Datainspektionen ansåg i sitt beslut den 20 augusti 2019, DI-2019-2221, att behandlingen var oproportionell och att det saknades laglig grund för att behandla känsliga personuppgifter. Någon konsekvensbedömning hade inte genomförts och något förhandssamråd hade inte sökts, trots att detta borde ha skett. Beslutet är överklagat och fallet ligger nu hos Förvaltningsrätten i Stockholm, mål nr 20 577-19.

7.1 Tillsynsärendets inledning och beslutet

I sin tillsynsplan för 2019-2020,[37] beslutad 19 mars 2019, listade Datainspektionen skolan som en bransch de avsåg utöva tillsyn över och tog även upp just ansiktsigenkänning som en särskild punkt. Enligt plan skulle fokus ligga på det rättsliga stödet för att behandla personuppgifter. Tillsynsärendet i fråga inleddes med en tillsynsskrivelse den 19 februari 2019 och gymnasienämndens svar inkom den 15 mars 2019[38]. Ärendet var således i full gång när tillsynsplanen publicerades.

Datainspektionen skriver i sitt beslut att de fick kännedom om projektet i Skellefteå via media[39]. Enligt sin tillsynspolicy[40] följer inspektionen dels sin i förväg fastställda tillsynsplan, så kallad riskbaserad tillsyn, dels reagerar den på omvärldshändelser. Det faktum att tillsynen av gymnasienämnden i Skellefteå inledes efter uppmärksamhet i media visar att verklig bevakning av omvärldshändelser finns och har betydelse.

---

[37] Diarienr DI-2019-841, se länk:
https://www.datainspektionen.se/globalassets/dokument/datainspektionens-tillsynsplan-2019-2020.pdf

[38] Kompletteringar med bilagor kom den 2 april. Ytterligare kompletteringar kom den 16 och 19 augusti. Beslutet fattades som nämnts den 20 augusti.

[39] Projektet beskrevs i ett inslag på Svt i december 2018.
https://www.svt.se/nyheter/lokalt/vasterbotten/ansiktsigenkanning-testades-pa-skola-sa-gick-det-till
Tidningen voister.se publicerade också en artikel om projektet den 19 februari 2019.
https://www.voister.se/artikel/2019/02/skolan-med-ansiktsigenkanning/

[40] Datainspektionens policy för tillsyn, diarienr DI-2019-1280 med beslutsdatum 2019-01-31. Se länk:
https://www.datainspektionen.se/globalassets/dokument/datainspektionens-policy-for-tillsyn.pdf

Beslutet är välmotiverat och välformulerat. Det innebär att tillsynsfallets resultat är av generellt intresse.

7.2 Sanktionsavgiftens storlek och grunder

Avgiftens storlek sattes till 200.000 kr. Huruvida beloppet är högt eller lågt är en fråga om perspektiv. Med tanke på antalet inblandade personer och projektets tidsrymd är beloppet proportionellt sett mycket högre än vad Google påfördes av CNIL[41], fastän läget i absoluta tal är det omvända.

Tillsynsmyndighetens grundläggande villkor för påförande av sanktionsavgifter framgår av Art. 83.1. Påförandet ska i varje enskilt fall vara *"effektivt, proportionellt och avskräckande."* Om flera av dataskyddsförordningens bestämmelser överträdes i samband med en och samma behandling, får inte avgiften överskrida maxbeloppet för den allvarligaste överträdelsen, Art. 83.3. Datainspektionens beslut bygger på överträdelse av fyra bestämmelser: Art 5, Art. 9, Art. 35 och Art. 36. Överträdelser av Art. 5 och 9 är var för sig sanktionerade med förordningens högsta belopp, Art. 83.5. För överträdelser av Art. 35 och 36 gäller i bägge fallen den lägre beloppsgränsen, Art. 83.4.

Fyra artiklar anses ha överträtts. Även om två av artiklarna har dubbelt så hög sanktionsnivå som de andra två, så är det klart att var och en av de aktuella överträdelserna var för sig mycket väl kan föranleda avgifter på den utdömda nivån. Sett ur det perspektivet kan avgiften framstå som låg.

Exakt hur Datainspektionen resonerat för att fastställa sanktionsbeloppet framgår inte. Olika bedömare har i olika sammanhang framfört synpunkten att avgiften är låg respektive hög. Oavsett uppfattning i den frågan, så bör man hålla i minnet att det i förordningstexten finns stöd för betydligt högre avgiftsnivåer för överträdelse av de fyra artiklar som det i fallet handlar om. Detta för framtida fall. Det kan inte hållas för otroligt att Datainspektionen succesivt höjer beloppen, så att nästa fall där samma artiklar berörs resulterar i högre avgift.[42] Det legala utrymmet för ett sådant agerande finns.

7.3 Fallets rättsfrågor

De fyra ovan nämnda artiklarna representerar fyra olika rättsfrågor. I beslutet diskuteras samtliga utförligt och resonemangen är av allmängiltigt intresse.

7.3.1. Grundläggande dataskyddsprinciper, Art. 5

Datainspektionen resonerar kring Art. 5.1b, ändamålsbegränsning, och Art. 5.1c, uppgiftsminimering. Dessa artiklar tolkas mot bakgrund av skäl 39. Sammantaget finner Datainspektionen att närvarokontroll genom ansiktsigenkänning via kamera är en för omfattande metod. Genomförandet har varit alltför integritetsingripande och därigenom också varit oproportionerligt i förhållande till ändamålet. Närvarokontroll kan ske på andra sätt som är mindre integritetskränkande för eleverna. De argument som gymnasienämnden anför till stöd för sin behandling bedöms som alltför svaga. Därför anses behandlingen ha genomförts i strid med Art. 5. Behandlingar som strider mot Art. 5 får inte utföras.

[41] I det fallet, som ännu inte är avslutat, uppgår avgiften till 50 miljoner euro. Googles årsomsättning 2018 uppgick till 136 miljarder dollar. De höga siffrorna motsvarar alltså knappt 0,04% av årsomsättningen.
[42] Det andra fallet, DI-2018-22737 med sanktionsavgifter har högre nivå, €35.000. Se även under avsnitt 1.5.

Datainspektionen tar alltså det faktum att närvarokontroll kan göras med mindre ingripande medel som ett argument för att ansiktsigenkänning är ett oproportionellt medel för att uppnå nämnda ändamål. Denna tolkning kan principiellt sett diskuteras. Att något går att göra på ett annat sätt kan inte betyda att det med automatik måste göras så. I så fall vore teknisk utveckling omöjlig. I det aktuella fallet handlar det dock om ansiktsigenkänning, en teknologi som står högt på listan över dem som Europeiska dataskyddsstyrelsen anser vara starkt integritetsingripande. Kanske menar Datainspektionen att närvarokontroll i skolan med sådan teknik per definition är oproportionellt, men det uttryckliga resonemanget förs inte exakt så. Gymnasienämndens argumentation tvingar dock inte Datainspektionen att i detta läge hantera den här anförda synpunkten.

Konsekvensen av bedömningen är att behandlingen är otillåten från start.

7.3.2 Behandling av särskilda kategorier av personuppgifter, Art. 9

Datainspektionen bedömer närvarohantering i skolan vara en uppgift av allmänt intresse och ett krav som skollagen ställer. Den rättsliga grunden för gymnasienämndens behandling av personuppgifter är således Art. 6.1e och i vissa delar även Art. 6.1c. De uppgifter som har behandlats är dock biometriska uppgifter. Dessa ingår otvetydigt bland dem som täcks av Art 9.1. Som påpekades i avsnitt 1.2 måste således något av undantagen i Art. 9.2 kunna tillämpas, annars är behandlingen olaglig.

Gymnasienämnden stödjer sig i första hand på Art. 9.2a, att eleverna samt deras målsmän har samtyckt till behandlingen. Reglerna för ett giltigt samtycke finns i Art. 7. Av skäl 42 och 43 framgår att samtyckets frivillighet är en fundamental förutsättning för dess giltighet. I skäl 43 poängteras att samtycke inte bör accepteras som laglig grund om betydande ojämlikhet råder mellan parterna. Detta bör särskilt gälla om den ansvarige är en offentlig myndighet. Gymnasienämnden anser att de inhämtat ett frivilligt samtycke. Som tydligt framgår är Datainspektionen av motsatt uppfattning. Frågan avgörs av domstolen.

Vidare prövas om Art. 9.2g är ett giltigt undantag från det generella behandlingsförbudet. Detta då rättslig förpliktelse, Art. 6.1c, och allmänt intresse, Art. 6.1e, är de rättsliga grunder som Datainspektionen godkänt som behandlingsgrunder. Att dessa rättsliga grunder åberopas av en svensk myndighet gör att 3 kap 3§ dataskyddslagen[43] blir tillämplig. Ett grundligt och instruktivt resonemang förs på basis av lagens förarbeten.[44] Slutsatsen blir att närvarohantering är ett faktiskt handlande och ingen ärendehandläggning; att det är en omfattande och central uppgift i skolväsendet, som sker slentrianmässigt i den löpande verksamheten och att ansiktsigenkänning är en för integritetsingripande teknik för att lösa den uppgiften. Dessutom anses att sökningar på känsliga uppgifter måste göras för att själva identifieringen ska kunna genomföras, vilket uttryckligen strider mot 3 kap 3§ 2st i dataskyddslagen. Datainspektionen bedömer således Art. 9.2g som icke tillämplig. Därmed blir slutomdömet att gymnasienämnden saknat lagstöd för sin behandling av känsliga personuppgifter.[45]

---

[43] Lag med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:218), trädde ikraft samma dag som dataskyddsförordningen, d.v.s. 25 maj 2018. Om det inte hade handlat om en svensk myndighet hade 2 kap 2§ och 3§ i dataskyddslagen varit tillämpliga lagrum.

[44] Prop. 2017/18:105 Ny dataskyddslag.

[45] Datainspektionens resonemang är som nämnts mycket tydligt. Dess skärpa är en annan fråga. Även om argumentationen inte ska ifrågasättas här, så kan konstateras att gymnasienämnden inte utmanar den nämnvärt. Beträffande just 3 kap 3§ dataskyddslagen är ett flertal förvaltningsrättsliga begrepp centrala för den juridiska slutsatsen. Gymnasienämnden förefaller inte ha lagt ned särskilt mycket energi på att kunna använda dessa till

Konsekvensen av denna bedömning är också att behandlingen är otillåten från start.

7.3.3 Effektivitetsvinst blir uppsåt

En av bedömningspunkterna avseende om sanktionsavgifter ska påföras eller ej är huruvida överträdelsen av dataskyddsförordningens bestämmelser skett med uppsåt eller av oaktsamhet, Art. 83.2b. Datainspektionen är i detta fall av uppfattningen att det har skett uppsåtligen. Motiveringen[46] lyder:

"Behandlingarna har skett för att effektivisera verksamheten, behandlingen har således skett uppsåtligen. Dessa omständigheter är försvårande."

Formuleringen är besynnerlig. Frågan är ju om överträdelsen skett uppsåtligen. Kanske menas att eftersom ansiktsigenkänningstekniken medvetet valdes av högsta ledningen för att effektivisera närvarohanteringen, så utesluter det oaktsamhet. I så fall förefaller Datainspektionen anse att enbart det faktum att gymnasienämnden genom behandlingen ville effektivisera närvarohanteringen räcker för att fastslå uppsåtlig överträdelse. Då kan frågan ställas om oaktsamhet är möjlig i något fall. Av alla val som träffas i samband med personuppgiftsbehandlingar så torde de flesta grundas på önskan om förbättrade funktionella och ekonomiska resultat, d.v.s. någon form av effektivitetsvinst. Om behandlingen senare bedöms strida mot dataskyddsförordningen, är då den överträdelsen per definition uppsåtlig? Gymnasienämnden utmanar inte den korthuggna argumentationen, varför någon prövning av frågan inte är att vänta.

Om någon slutsats beträffande Datainspektionens syn på oaktsamhet och uppsåt vid överträdelse kan dras av denna formulering, så framstår antagandet rimligt, att uppsåt kommer anses föreligga i de flesta fall. Uppsåtligt handlande är alltid en försvårande omständighet, vilket också står i beslutet.

7.3.4 Kraven på konsekvensbedömning, Art. 35 och samråd, Art. 36

Reglerna om konsekvensbedömning avseende dataskydd återfinns i Art. 35. Artikeln är en av de längsta och mest svårgenomträngliga i hela förordningen. Förenklat och förkortat kan den sammanfattas med att om en behandling *"sannolikt leder till en hög risk för fysiska personers rättigheter och friheter"* så måste den personuppgiftsansvarige vara extra noggrann. Både avseende att behandlingen redan på planeringsstadiet faktiskt följer dataskyddsförordningen och att detta kan visas. Om en konsekvensbedömning krävs beror alltså av en riskbedömning. Det gör att regeln är ett tydligt uttryck för den riskbaserade metoden.

Förordningstexten anger tre olika fall:

- De generella fallen, Art. 35.1. Den personuppgiftsansvarige bedömer själv risken och beslutar.

stöd för sin uppfattning. De har heller inte försökt tillämpa något annat av undantagen i Art. 9.2. Nämnden har helt riktat in sig på att visa att samtycket är giltigt. Av flera potentiella grunder har de valt att lägga så gott som all argumentationskraft på en enda. Det framstår som riskabelt. Särskilt som många juridiska bedömare generellt sett anser samtycke vara den svåraste och mest arbetsamma rättsliga grunden att använda, oavsett fråga. Det generella rådet är att använda samtycke som sista utväg, när andra grunder inte kan användas. Om gymnasienämnden valt en klok väg återstår att se.

[46] S. 18 i tillsynsbeslutet.

- De särskilda fallen, Art. 35.3. Lagstiftaren har bestämt att i de fallen föreligger per definition en hög risk och därför krävs en konsekvensbedömning.
- Tillsynsmyndighetens lista, Art. 35.4. Datainspektionen har definierat nio kriterier och om en behandling uppfyller minst två av dessa anser de att en konsekvensbedömning krävs.[47]

Begreppet risk är svårdefinierat, vilket också tidigare har påpekats. Det är svårt att komma ifrån att olika människor har olika uppfattningar om vad som är riskabelt och inte. Enligt skäl 76 bör risken utvärderas på grundval av en objektiv bedömning. I skäl 75 anges ett antal möjliga skador som kan uppstå till följd av en personuppgiftsbehandling. Men förordningstexten tiger still angående exakt vad som ska bedömas objektivt för att dessa potentiella skador ska kunna undvikas. Den personuppgiftsansvarige framstår i slutändan som hänvisad till sitt eget omdöme avseende huruvida en behandling de facto sannolikt innebär en hög risk eller inte.

I det aktuella fallet anser Datainspektionen att gymnasienämndens riskbedömning saknar bedömning av de risker som de registrerades fri- och rättigheter utsätts för bara genom att själva behandlingen utförs, samt att redogörelse för proportionaliteten i att använda ansiktsigenkänning för närvarokontroll inte finns. Dessutom anser Datainspektionen att ett antal faktorer, bland annat användning av ny teknik och behandling av känsliga uppgifter om barn, gör att kravet på konsekvensbedömning är uppfyllt.

Vidare anser Datainspektionen att eftersom gymnasienämndens riskbedömning saknar bedömning av riskerna för de registrerades fri- och rättigheter, så saknas även redogörelse för hur dessa risker ska kunna minskas. Därför hade kravet på förhandssamråd enligt Art. 36 inträtt. Något förhandsamråd hade dock inte sökts. Här visar sig en stor konsekvens av ansvarsskyldighetsprincipens placering av bevisbördan. Datainspektionen underkänner gymnasienämndens resonemang på den grunden att det inte finns något. Datainspektionen behöver inte leda i bevis att kravet på förhandsråd hade inträtt. Det räcker med att de påstår att gymnasienämnden inte visar att det inte hade inträtt. Den praktiska betydelsen av denna juridiska teknikalitet är mycket stor.

Om förordningens krav på konsekvensbedömning respektive förhandssamråd inträtt eller ej är nu en fråga för domstolen. Det går att argumentera för bägge ståndpunkterna. Emellertid kan konstateras att Datainspektionen argumenterar utförligare för sin ståndpunkt än vad gymnasienämnden gör. Med tanke på att parterna till största delen själva ansvarar för att ta fram det material på vilket tvisten ska lösas, så talar detta till förmån för Datainspektionen.

[47]Varje nationell tillsynsmyndighet har ansvar för att en sådan förteckning publiceras. Enligt mekanismen för enhetlighet ska, genom Europeiska dataskyddstyrelsens överinseende, dessa förteckningar harmoniera med varandra. Länk till beslutet om förteckningen, diarienr. DI-2018-13200: https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-om--forteckning-enligt-artikel-354.pdf
Förteckningen bygger på den förteckning som Artikel 29-gruppen tagit fram, se: Riktlinjer om konsekvensbedömning avseende dataskydd, WP248 rev.01. Förteckningens rättskällestatus kan således diskuteras, vilket även vissa remissinstanser gjorde. Länk till själva förteckningen: https://www.datainspektionen.se/globalassets/dokument/beslut/forteckning---konsekvensbedomningar.pdf

7.4 Sammanfattning och slutsatser om beslut, resonemang och framtid

Många förvånades över att en gymnasienämnd i Skellefteå blev föremålet för den första sanktionsavgiften i Sverige. Enligt uppgift pågick då redan ett 30-tal tillsynsfall, däribland mot Spotify, Klarna och 1177-fallet. Alltså mot betydligt större aktörer. Detta visar på några saker:

- Datainspektionen har egen nyhetsbevakning. Ett inslag i SVT gav tillsynsuppslaget.
- Ansiktsigenkänning som teknik tilldrar sig Datainspektionens intresse.
- Behandling av känsliga uppgifter, särskilt minderårigas, uppmärksammas.
- Myndigheter har inget frikort från tillsyn.
- Den personuppgiftsansvariges storlek har ingen betydelse för tillsynsbeslutet. Det handlar om behandlingens förenlighet med dataskyddsförordningen.

Beträffande resonemangen kan noteras att de har tydlig legal förankring med utförlig argumentation. Därmed inte sagt att de är utan invändningar, men de är lätta att följa hela vägen från grund till slutsats.

De generella framtidsutsägelser som kan göras på basis av detta fall är framförallt att den personuppgiftsansvarige måste ha koll på sina behandlingar, deras ändamål och rättsliga grund. Därtill krävs en dokumenterad argumentation avseende behandlingens förenlighet med hela dataskyddsförordningen. Att effektiviteten ökar och att man själv bedömer behandlingen som rimlig är inte tillräckliga argument vid en granskning. Därtill gäller att ska man bege sig in i ett tekniskt nyland så behöver man ha både tekniken och juridiken klar för sig, samt hur man på en organisatorisk nivå ska få ihop det hela. Med tekniskt nyland menas både att tekniken i sig är ny och att tekniken används på ett nytt sätt i en ny kontext. Begreppet *ny* ska alltså tolkas brett. I det perspektivet är frågan om vad lagen enligt sin bokstav kräver underordnad frågan vilket underlag som bör finnas för en smidig och framgångsrik prövningsprocess. Den rättsliga argumentation som gymnasienämnden hittills har presterat kommer svårligen ta dem dit de vill.

8. Avslutning

Att praktiskt följa dataskyddsförordningen innebär att juridiska, tekniska och organisatoriska frågor måste hanteras samtidigt. Dessa frågor måste sedan få sin gemensamma lösning i konkreta åtgärder. Detta är lättare sagt än gjort. Några typexempel: en juridiskt korrekt lösning som inte kan förverkligas tekniskt är utan effekt. En teknisk lösning som inte är juridiskt korrekt är både olaglig och ett hot mot verksamheten. En lösning som fungerar både juridiskt och tekniskt, men inte passar in i organisationens arbetsmönster kommer inte att användas. Trots dessa tydliga utmaningar är just ett smidigt samspel mellan de tre områdena det krav som personuppgiftsbehandling nu och framöver måste leva upp till. För att bara nämna några praktiska konsekvenser av dataskyddsförordningen: tillsynen kommer succesivt att skärpas, förr eller senare introduceras automatiserade övervakningsprocesser. Aktivister kommer inse kraften i grupptalan. Företag kommer inse hur väl valda klagomål kan skapa stora problem för konkurrenter. Bolagspriset vid förvärv kommer påverkas av risker knutna till personuppgiftsbehandling. Listan kan göras mycket längre.

En presentation av dataskyddsförordningen har ingen inbyggd övre gräns för sin komplexitet. Denna informationsbroschyrs syfte är att lägga en gemensam kunskapsgrund för personalen på Sund Affärsbyrå och dess kunder. Som nämndes i inledningen begränsar den sig därför till vissa centrala delar av dataskyddsförordningen. Fokus har legat på övergripande förståelse, till främjande för en gemensam kunskapsbas. Med ökad förståelse ökar också insikten om vad man själv måste göra.

Den som har läst denna broschyr och har frågor eller synpunkter är varmt välkommen att höra av sig till mig.

Stefan Johansson
Dataskyddsombud
stefan@datakollen.se