Complior

Guide

GDPR version 1.0

Innehållsförteckning

Förord

Denna guide är tänkt som ett lättförståeligt, peda- gogiskt och omfattande hjälpmedel för dem som är ansvariga för sin organisations efterlevnad av den nya dataskyddsförordningen (GDPR). Denna guide kan självklart också vara till nytta för dem som har akademiska eller andra intressen. Då regelverket ännu inte tillämpats saknas praxis och det är ännu inte säkert hur den slutliga svenska lagen kommer att se ut. Det finns ändå mycket som organisationer måste lära sig och ta till sig redan idag för att hinna med att efter leva förordningen i tid.

Dataskyddsförordningen kommer att vara den viktigaste frågan för många styrelser och lednings- grupper år 2017/2018. Genom att läsa denna guide kommer du ha mycket mer än bara en grundläg- gande inblick i ämnet. Denna guide kommer med hjälp av konkreta exempel och lättförståeligt språk guida läsaren genom den jobbiga juridiska jargo- nen och de unika begreppen i förordningen.

Vid färdigskrivandet av denna guide kommer det att vara exakt ett år kvar tills förordningen ska tillämpas i svensk lag, och denna guide kommer att regelbundet uppdateras när mer information om förordningen offentliggörs. Vid nästkommande version av denna guide kommer följande avsnitt att läggas till: Profilering, Konsekvensbedömning, Överföring av personuppgifter till tredje land, Åt- komstkontroll, Logghantering för GDPR, Privacy by design och Rätt till dataportabilitet.

Jag önskar er lycka till med efterlevnaden.

Jonas Gharanfoli
säkerhetskonsult

1. Bakgrund till GDPR

Den 25 maj 2018 kommer den allmänna dataskyddsförordningen, på engelska General Data Protection Regulation (GDPR), att ersätta personuppgiftslagen och tillämpas i svensk lag. Förordningen omfattar alla organisationer som på något sätt behandlar personuppgifter såsom företag och myndigheter. Syftet med förordningen är att utöka och säkerställa den personliga integriteten hos alla EU/EES-medborgare. Om din organisation har exempelvis ett CRM-system eller ett register över anställda så kommer ni att behöva efterleva dataskyddsförordningen.

Vi har sedan länge haft svensk lagstiftning som PuL (personuppgiftslagen) och PDL (patientdatalagen) för att skydda den personliga integriteten hos fysiska personer, men det har saknats eftertryckliga konsekvenser för de som inte har efterlevt regelverken. PuL uppstod 1998 från den Europeiska kommissionens dataskyddsdirektiv som trädde i kraft 1995. Under 1995 var det inte så vanligt att personer ägde egna datorer och hade uppkoppling till internet, idag går nästan alla runt med en relativt stark dator med internetuppkoppling i fickan.

Den digitala värld vi idag lever i har ändrat förutsättningar för hur personuppgifter kan insamlas, spridas och analyseras. Utvecklingen av big data-analyser, marknadsföring samt införandet av tjänster som Facebook har förstärkt debatten om personlig integritet. Under januari 2012 kom den Europeiska kommissionen med förslaget att genomförligt reformera dataskyddsdirektivet. Följden av detta blev att dataskyddsdirektivet utökades och omvandlades till en förordning. Dataskyddsförordningen trädde i kraft den 24 maj 2016.

GDPR är en förordning och inte ett direktiv som PuL baseras på.

Både förordningar och direktiv kallas för rättsakter inom EU-rätt. Direktiv är mål som ges till medlemsländerna, det är sedan upp till varje enskilt medlemsland att bestämma hur målen ska uppnås genom att införliva direktivet i nya eller redan existerande lagar. Detta betyder att lagar som skapats från direktiv kan skilja sig väsentligt mellan medlemsländerna. Däremot så är förordningar i princip färdiga lagar som ska tillämpas direkt i sin helhet hos samtliga medlemsländer på ett förbestämt datum. Förordningar leder alltså till mycket starkare harmonisering inom EU/EES eftersom det ges mindre anpassningsutrymme på nationell nivå.

Då efterlevnadsbördan kommer att vara enorm för många organisationer finns det ändå ett positivt sätt att förhålla sig till GDPR. En organisation som förbereder sig i tid kan få en av- sevärd konkurrensfördel. Förutom förbättrat integritets- och dataskydd, så kommer många leverantörer och kunder kräva att din organisation efterlever GDPR eftersom det kan finnas risker för dem om ni inte gör det. Det är även så att medlems- stater och tillsynsmyndigheter uppmuntras av förordningen att införa certifikationsmekanismer för GDPR. Ungefär på samma sätt som organisationer kan certifiera sig för att visa sitt ansvar för miljön så kommer organisationer att kunna visa sitt ansvar för personlig integritet och att de tar informations- säkerhet på allvar.

Notera: Det är tyvärr väldigt vanligt att det står skrivet på företagshemsidor att GDPR kommer träda i kraft den 25 Maj 2018. Det är fel, den har redan trätt i kraft den 24 Maj 2016. Detta bety- der att förordningen är färdigskriven och att processen med att byta ut PuL och tillsätta GDPR till svensk lag har redan påbörjats. GDPR kommer alltså att tillämpas i svensk lag den 25 Maj 2018.

1.1 Vilka verksamheter berörs?

GDPR gäller för alla organisationer som ”behandlar” personuppgifter som tillhör EU/EES-medborgare, även om verksamheten befinner sig utanför EU/EES-området. Förordningen kommer att orsaka en stark global reaktion eftersom det finns många organisationer utanför EU/EES-gränser som behandlar personuppgifter om EU/EES-medborgare. Offentlig sektor kommer att beröras då myndigheter och offentliga organ också måste efterleva förordningen. Förordningen omfattar såväl de som styr behandlingen av personuppgifter (personuppgiftsansvariga) men även eventuella tjänsteleverantörer (personuppgiftsbiträden). Undantagna är brottsbekämpande myndigheter som polisen, de har fått ett eget direktiv från den Europeiska kommissionen.

1.2 Övergripande skillnader mellan GDPR och PUL

» GDPR sätter den registrerades rättigheter mer in fokus än tidigare.

» Tillsynsmyndighetens möjligheter till sanktioner stärks – max sanktionsavgift på 4% av den globala omsättningen av föregående år eller € 20.000.000, vilket som är större.

» Privacy by design – integritetsskydd ska finnas inbyggd i system redan från början och genomsyra hela livscykeln av systemet.

» Större krav på analyser, rutiner och dokumentation.

» Samtycket måste vara tydligare och krävs under fler omständigheter.

» Informationskravet till registrerade är hårdare.

» ”Rätten att bli glömd” kommer att lagfästas i GDPR. Detta innebär att organisationer måste under vissa omständigheter radera alla personuppgifter tillhörande registrerade ifall dessa registrerade kräver det.

» Behandling av barns uppgifter kommer att kräva samtycke från vårdnadshavare för informationssamhällets tjänster (ex. Facebook, Instagram).

» Nya förutsättningar inom marknadsföringen (profilering/ selektering).

» Din organisation måste under vissa omständigheter anlita ett dataskyddsombud.

» Leverantören (personuppgiftsbiträdet) blir tillsynsobjekt. Personuppgiftsbiträden, som inte kunde bli straffade genom PuL, kan nu få sanktionsavgifter om de bryter mot förordningen.

» Det ställs större krav på biträdesavtalen, de kommer att behö-va skrivas om.

» Missbruksregeln i PuL förvinner. Behandling av ostrukturerat material omfattas av hela lagen utan att det finns särskilda undantag.

2. Viktiga begrepp

Förordningen innehåller unika termer, definitioner och begrepp som läsaren måste ha kunskap om innan det går att förklara de mer komplicerade aspekterna av förordningen.

2.1 Vad är en personuppgift?

Enligt förordningen är en personuppgift:

”Varje upplysning som avser en identifierad eller identifierbar fysisk person 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, fysio- logiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.” (Artikel 4(1))

En identifierad eller identifierbar fysisk person betyder en levande människa i förordningen (det är upp till varje enskilt medlemsland att bestämma ifall det måste vara en levande människa eller om döda människors personuppgifter ska omfattas).

*” ...identifierbar fysisk person är en person som **direkt** eller **indirekt** kan identifieras...”*

Du kan direkt identifiera någon till exempel genom deras fulla namn eller personnummer. Om någon innehar ett väldigt sällsynt för-/efternamn räcker oftast detta för att direkt identifiera någon. Du kan indirekt identifiera någon genom att kombinera information som yrke, plats, fysiska egenskaper och sociala status. Exempelvis så är ”säkerhetskonsult + brunt hår + Frösunda” en personuppgift eftersom man med denna information indirekt kan koppla till ett väldigt fåtal identifierbara personer i Frösunda (ett litet område i Solna). Ett rättesnöre som brukar användas är att om informationen kan kopplas till mindre än sju personer så räknas det som en personuppgift.

”identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer...”

Onlineidentifikatorer som IP-adresser och cookies räknas även som personuppgifter. Lokaliseringsuppgifter som GPS-koordinater räknas som personuppgifter om de är kopplade till en person.

Räknas dynamiska IP-adresser som personuppgifter?

Idag är det väldigt vanligt att IP-adresser från webbplatsbesökare lagras av webbplatsinnehavare. En dynamisk IP-adress kan tillsammans med tidpunkt och internetleverantörens kundregister identifiera exakt vilken dator som besökt vilken webbsida vid en viss tidpunkt; alltså kan dessa uppgifter hänföras till en identifierbar fysisk person. Enligt en dom från EU-domstolen (Breyer-domen) anses dynamiska IP-adresser som personuppgifter ifall webbplatsinnehavaren ”förfogar över lagliga medel” för att begära ut övriga uppgifter från en tredje part, till exempel en internetleverantör, och det ska även inte vara ”omöjligt att genomföra i praktiken” för webbplatsinnehavaren.

2.2 Behandling

Begreppet behandling är ett väldigt brett definierat i förordning en, det innefattar i princip allt man kan tänkas göra med personuppgifter. Detta är den fulla definitionen från förordningen:

”En åtgärd eller kombination av åtgärder beträffande personupp- gifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organi- sering, strukturering, lagring, bearbetning eller ändring, framtag- ning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanföran- de, begränsning, radering eller förstöring.” (Artikel 4(2))

2.3 Tillsynsmyndighet

I varje medlemsland har det utsetts en tillsynsmyndighet vars funktion är att se till att dataskyddsförordningen följs.

I Sverige är tillsynsmyndigheten Datainspektionen. Varje tillsynsmyndighet kommer att bland annat ha följande roller och förpliktelser:

» Ska utföra granskningar

» Kan utfärda varningar

» Kan tillfälligt begränsa eller helt förbjuda behandling av personuppgifter

» Kan utfärda sanktionsavgifter

» Måste motta anmälningar under större personuppgifts-incidenter

» Kan utfärda certifieringar och återkalla certifieringar

» Ska framföra vägledande information till allmänheten om GDPR

Dataskyddsförordningens mål med tillsynsmyndigheterna är att organisationer bara ska svara under en överordnad tillsynsmyndighet, även om organisationen är verksam internationellt. Vilken tillsynsmyndighet som organisationen ska svara under beror på var organisationen har sin centrala förvaltning.

2.4 Personuppgiftsansvariga, personuppgiftsbiträden och biträdesavtal

Den nya dataskyddsförordningen ställer nya krav på personupp- giftsansvariga och personuppgiftsbiträden. Personuppgiftsan- svariga är den **juridiska person** (aktiebolag, myndighet, enskild firma, osv.) som styr ändamålet och vilka personuppgifter som behandlas. Personuppgiftsansvariga är inte en fysisk person som exempelvis CEO, CTO eller dataskyddsombud. Även om en an- ställd har inrätt ett olagligt register av personuppgifter kommer det vara själva organisation som betalar sanktionsavgiften. Självklart kan sedan organisationen åtala personen som har gjort fel. Håll i åtanke att den personuppgiftsansvarige har de största förpliktelserna i GDPR.

Ett personuppgiftsbiträde är oftast en juridisk person som behandlar personuppgifter åt personuppgiftsansvariges vägnar, alltså en leverantör. Behandling gäller inte bara lagring utan även åtkomst på distans för service, support, utveckling, underhåll och liknande. Ett personuppgiftsbiträde kan exempelvis vara en molntjänstleverantör. Det är nytt i GDPR att personuppgiftsbiträden blir tillsynsobjekt. Personuppgiftsbiträden, som inte kunde bli straffade genom PuL, kan genom GDPR bland annat råka ut för höga sanktionsavgifter.

Den stora frågan är, ifall personuppgiftsbiträden gör fel, kommer den personuppgiftsansvarige också att straffas och vice versa?

Denna fråga kan inte enkelt besvaras eftersom detta kommer att skilja sig åt från fall till fall. Det som är viktigt här är att följa ansvarsskyldighetsprincipen i förordningen. Att tydligt dokumentera exakt vilka förpliktelser den personuppgiftsansvarige har samt vilka förpliktelser som personuppgiftsbiträdet har. Detta måste styras genom ett biträdesavtal. Om ena parten inte följer avtalet så är det i princip den som kommer att straffas. Men avtalet kan självklart inte se ut hur som helst utan bör skapas med hjälp av en jurist och följa kraven på biträdesavtal som finns i artikel 28. Det finns även möjlighet att tillsynsmyndigheter kommer att skapa standardiserade avtal för att underlätta den här processen.

Notera: *Personuppgiftsbiträden är också i princip alltid en personuppgiftsansvarig. Detta är för att de har exempelvis egna anställda och leverantörer. Jag betonar att hela kedjan av leverantörer och underleverantörer är ansvarsskyldiga i GDPR. Detta medför att om en underleverantör gör fel kan det bli rättsliga påföljder för alla inom leverantörskedjan upp till den personuppgiftsansvarige.*

2.5 Särskilda kategorier av personuppgifter

Särskilda kategorier av personuppgifter eller känsliga kategorier av personuppgifter finns definierade i artikel 9(1), de kategorierna omfattar följande:

» Ras eller etniskt ursprung

» Politiska åsikter

» Religiös eller filosofisk övertygelse

» Medlemskap i fackförening

» Hälsa

» Sexualliv eller sexuell läggning

» Genetisk och biometrisk information

Det finns även fall där själva behandlingen av personuppgifter kan anses vara känslig. Det finns organisationer som kan behandla personuppgifter som i sig inte är känsliga, men med användning av olika typer av modeller och algoritmer kan urskilja känslig information. Det finns exempelvis företag som kan upptäcka ifall en person har benägenhet för diabe- tes bara genom att analysera handlingshistoriken av livsmedelsprodukter. Denna behandling är alltså känslig eftersom hälsorelaterad information anses tillhöra en särskild kategori av personuppgifter.

Notera: *Det är mycket svårare att få laglig grund för behandlingen av känsliga personuppgifter i förordningen. Om en organisation behandlar känsliga personuppgifter olagligt riskerar den at straffas med väldigt höga sanktionsavgifter. För laglig behandling av känsliga personuppgifter kommer extra skyddsåtgärder att behöva implementeras i de flesta fallen (exempelvis pseudonymisering).*

2.6 Extra skyddsvärda personuppgifter

Sedan har vi kategorier av personuppgifter som inte definieras som ”särskilda kategorier” i förordningen, men ändå kommer att behöva extra varsam behandling. Detta är på grund av att, likt de särskilda kategorierna, det finns stor risk att inskränka registrerades fri- och rättigheter. Behandlingen kan även leda till psykologisk- och/eller materiell skada ifall obehöriga individer får tag på uppgifterna. Jag har själv valt att kalla dessa personuppgifter för extra skyddsvärda personuppgifter.

Denna information omfattar bland annat:

» Sekretessbelagd information/tystnadsplikt (skyddade personuppgifter)

» Personnummer

» Passnummer

» Viss ekonomisk information (införsel)

» Annat som ligger nära privatlivet

» Information tillhörande barn

» Inloggningsuppgifter

» Kreditkortsdata

2.7 Brottsuppgifter

Artikel 10 i förordningen förbjuder uttryckligen behandling av personuppgifter som rör fällande domar i brottmål och överträdelser. Sådana uppgifter får endast behandlas under kontroll av en myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. I Sverige har vi nationell rätt som Skollagen. Den kräver kräver att innan ny personal kan anställas måste de visa ett registerutdrag från belastningsregistret som inte får vara mer än ett år gammalt. Detta betyder att för verksamheter inom exempelvis skola/barnomsorg så kommer det fortfarande vara lagligt att göra viss behandling av brottrelaterade uppgifter.

2.8 Strukturerat- och ostrukturerat material

Personuppgiftslagen gjorde stor skillnad på behandling av strukturerat material och ostrukturerat material, där behandling av ostrukturerat material fick mycket stora lättnader i PuL. Strukturerat material omfattar till exempel data som finns i traditionella dataregister, databaser och ärende- och dokumenthanteringssystem. Ostrukturerat material är data som inte finns i en strukturerad, lättsökbar och lättanalyserad datasamling; exempelvis personuppgifter i löpande text i ordbehandlingsprogram, löpande text på internet, ljud- och bildupptagningar och e-post.

Som sagt finns det stora lättnader i PuL med personuppgifter som behandlas i ostrukturerat material, detta kallas för Missbruksregeln. Missbruksregeln innebär att personuppgifter i ostrukturerat material kan behandlas i princip fritt så länge behandlingen inte kränker den registrerade. Detta undantag för ostrukturerat material finns inte i GDPR. Det är ett svenskt påhitt från PuL och finns inte i övriga Europa. Missbrukregeln kommer att försvinna och det spelar inte längre någon roll ifall personuppgifterna finns i strukturerat- eller ostrukturerat material.

2.9 Pseudonymisering och anonymisering

Pseudonymisering:

Innebär att personuppgifter byts ut mot icke-identifierande information. För att återskapa ursprungsinformationen krävs kompletterande uppgifter som förvaras separat. Exempelvis genom kryptering eller substitutionstekniker. Pseudonymiserade personuppgifter omfattas fortfarande av förordningen.

Anonymisering:

Personuppgifter byts ut mot icke-identifierande information. Till skillnad från pseudonymisering så finns det inga kompletterande uppgifter och det kommer aldrig att finnas ett sätt koppla information tillbaka till personen. Exempelvis om man raderar eller maskar ”nyckel-uppgifterna” som gör att informationen kan kopplas till en person. Anonymiserade personuppgifter omfattas inte längre av förordningen.

2.10 Dataskyddsombud

Dataskyddsombud var tidigare kallad personuppgiftsombud eller PuL-ombud. Dataskyddsombudets uppgifter finns uppradade i artikel 39(1). Sammanfattningsvis så ska dataskyddsombudet övervaka organisationens efterlevnad av GDPR, informera och ge råd till organisationen, samarbeta med- och vara kontaktpunkt för tillsynsmyndigheten. Det är väsentligt att det inte förekommer någon form av intressekonflikt, dataskyddsombudet får exempelvis inte vara CEO, CTO eller CIO.

Alla organisationer behöver inte anlita ett dataskyddsombud. De organisationer som möter följande kriterier i artikel 37(1) måste däremot anlita ett dataskyddsombud:

a) Behandlingen genomförs av en myndighet eller ett offentligt organ.

b) Organisationens kärnverksamhet består av behandling som innefattar regelbunden och systematisk övervakning av de registrerade i stor omfattning.

c) Organisationens kärnverksamhet består av behandling som innefattar särskilda kategorier av uppgifter i stor omfattning, samt personuppgifter som rör fällande domar i brottmål och överträdelser.

Artikel 37(5) kräver att organisationen anställer dataskyddsombudet på ”grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd”. Dataskyddsombudet bör med andra ord ha väldigt goda kunskaper om GDPR och dataskydd. Ett dataskyddsombud som saknar rätt kvalifikationer och missköter sina förpliktelser kan medföra förödande konsekvenser för hela organisationen. Artikel 37(6) tillåter den personuppgiftsansvarige eller personuppgiftsbiträdet att anställa någon från den egna personalen som dataskyddsombud, det kan vara en god idé att skicka denna anställda på någon form av utbildning för dataskyddsombud. Det är även tillåtet att anställa dataskyddsombudet utanför organisationen.

2.11 Personuppgiftsincident

Personuppgiftsincident eller ”breach” på engelska, har följande definition från förordningen:

”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”. (Artikel 4(12))

Detta kan exempelvis vara en hackerattack där personuppgifter har stulits för att sedan spridas på internet. Här gäller det att ha förberedda rutiner och processer på plats så att inte onödig tid förflyter för att de ansvariga inte har en aning om hur de ska reagera. En dataskyddspolicy bör införas där en incidenthanteringsprocess dokumenteras. Personuppgiftsbiträden är skyldiga att informera personuppgiftsansvariga ifall det har skett en personuppgiftsincident hos dem. Personuppgiftsansvariga kan i sin tur bli skyldiga att anmäla personuppgiftsincidenter till Datainspektionen och/eller berörda registrerade.

När behöver personuppgiftsansvariga anmäla personupp- giftsincidenter till Datainspektionen?

Personuppgiftsincidenten måste anmälas till Datainspektionen ifall det är sannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. De ansvariga i organisationen bör rådgöra med varandra direkt efter incidenten och avgöra ifall detta är fallet. Förordningen kräver dessutom i artikel 33(1) att den personuppgiftsansvarige anmäler incidenten till Datainspektionen ”utan onödigt dröjsmål” och, om så möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten. Anmälan måste innefatta en incidentrapport som ska innehålla informationen som beskrivs i artikel 33(3). Ifall exempelvis telefonnummer i registret över anställda raderas av misstag behöver detta inte anmälas till Datainspektionen.

När måste berörda personer (registrerade) bli informerade?

Berörda registrerade måste bli informerade ”utan onödigt dröjsmål” ifall incidenten sannolikt leder till en hög risk för berörda personers rättigheter och friheter. Förordningen säger i princip att för väldigt allvarliga incidenter måste en anmälan skickas till Datainspektionen samt att berörda individer informeras. För allvarliga incidenter kan det räcka med att bara skicka en anmälan till Datainspektionen. För personuppgiftsincidenter som är mindre allvarliga räcker det med dataskyddsombudet registrerar incidenten.

Artikel 34(3) innehåller villkor när berörda registrerade inte behöver informeras:

Ifall den personuppgiftsansvarige exempelvis har gjort de berörda uppgifterna ”*oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering*”, så behöver inte berörda registrerade bli informerade. Detta är en av de många fördelarna med att pseudonymera personuppgifter.

2.12 Administrativa sanktionsavgifter

Det har blivit en stor uppståndelse kring de notoriskt höga sanktionsavgifter som GDPR tillåter tillsynsmyndigheterna att utfärda. Många medier har varit snabba att påpeka att organisationer kan råka ut för sanktionsavgifter på €20,000,000 eller 4% av den globala omsättningen, vilket som är högre. Det bör förtydligas att detta är den maximala avgift som tillsynsmyndigheter tillåts att utfärda. I praktiken behöver organisationer i princip aldrig betala det absolut maximala sanktionsavgiftsbeloppet eftersom det finns väldigt många kriterier i förordningen som påverkar sanktionsavgiftens storlek, och då gäller det att organisationen har grovt försummat alla dessa kriterier. Artikel 83(2) radar upp dessa kriterier och tillsynsmyndigheten kommer exempelvis beakta: Överträdelsens karaktär, svårighetsgrad varaktighet, omfattning, skada skedd till berörda registrerade och ifall överträdelsen skett med uppsåt eller genom oaktsamhet för att nämna några.

En administrativ sanktionsavgift är inte detsamma som böter, att bryta mot en bestämmelse som är belagd med böter ses som en kriminell handling. Sanktionsavgifter går inte via polis, åklagare och domstol, utan Datainspektionen kan genom sin egen auktoritet utfärda sanktionsavgiften. Organisationen har rätt att motstå sanktionsavgiften i domstol efter att den har utfärdats, fast bevisbördan ligger då på organisationen.

Den administrativa sanktionsavgiften har tilldelats två olika nivåer:

Nivå 1: Maximal sanktionsavgift på €10 000 000 eller 2% av den globala omsättningen, vilket som är högre.

I regel så kommer överträdelser av personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter att ge sanktionsavgifter i den första nivån. Detta omfattar artiklarna 8, 11, 25–39, 42 och 43. Exempelvis så omfattar detta överträdelser gällan- de: Inbyggt dataskydd och dataskydd som standard, register över behandling, säkerhet i samband med behandlingen och anmälan av personuppgiftsincident.

Nivå 2: Maximal sanktionsavgift på €20 000 000 eller 4% av den globala omsättningen, vilket som är högre.

Den högsta nivån innefattar överträdelser gällande registrerades rättigheter (artikel 12–22), laglig grund (artikel 6), de grundläggande principerna (artikel 5), villkoren för samtycke (artikel 7), behandling av särskilda kategorier av personuppgifter (artikel 9), överföring av personuppgifter till tredjeland (44–49).

Om det skulle vara så att din organisation behöver betala en sanktionsavgift så behöver det inte sluta där. Förordningen ger berörda registrerade rätt att kräva skadestånd från organisationen för eventuellt lidande till följd av behandling som strider mot denna förordning. Ni kan med andra ord bli stämda. Förordningen nämner även att registrerade kan framföra en grupptalan, vilket betyder att en representant för en grupps talan inför domstol. På engelska heter detta ”class action lawsuit”.

2.13 Undantag

All behandling av personuppgifter omfattas inte av förordningen, här är undantagen:

Behandling av personuppgifter för privata ändamål:
All behandling av personuppgifter som görs inom den privata sfären omfattas inte av GDPR. En inbjudningslista till ett kalas som innehåller personuppgifter kommer inte omfattas av GDPR. Däremot så kommer ingenting som man gör inom ramen för sin yrkesroll att anses vara privat. En gråzon här är personalfester, kommer exempelvis bilder som tas under en personalfest att omfattas av förordningen? Svaret är ja ifall bilderna kommer att exempelvis läggas på företagshemsidan. Det kan vara bra att be om samtycke i sådana situationer: ”De som vill bli fotade står här, ni som inte vill det kan stå där borta”. Detta räcker för att få samtycke i dessa situationer och undviker att man av misstag fotar någon med skyddad identitet.

Behandling som täcks av grundlagen:
I Sverige har vi Tryckfrihetsförordningen som är en av Sveriges grundlagar, där lagfästs offentlighetsprincipen. Grundlagar gäller före dataskyddsförordningen och detta betyder att hemsidor som Merinfo.se och Ratsit.se kommer att kunna fortsätta existera efter GDPR tillämpas i svensk lag. Detta beror på att de upplyser om offentligt material, material som exempelvis kommer från skatteverket, och täcks av offentlighetsprincipen.

I artikel 85 fastställs det undantag från nästan hela förordningen (säkerhetsbestämmelserna måste fortfarande uppfyllas) för journalistiska ändamål och akademiskt, konstnärligt eller litterärt skapande.

3. Principer för behandling

Förordningen innefattar generella principer om hur personuppgifter ska behandlas i artikel 5. Budskapet från dessa principer genomsyrar hela förordningen och bör beaktas väl eftersom överträdelser av dessa principer kan leda till de hög- sta sanktionsavgifterna.

3.1 Laglighet, korrekthet och öppenhet

Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt.

Det kan tyckas självklart att personuppgifter ska behandlas lagligt. Detta syftar till att behandlingen har en laglig grund. Öppenhet innebär att organisationen måste vara öppen till intressenter med sin behandling. Det ska exempelvis stå klart och tydligt i en integritetspolicy vilka personuppgifter som behandlas, hur de behandlas och för vilka ändamål. Öppenhetsprincipen kräver att denna information måste vara lättillgänglig, koncis och att lättförståeligt språkbruk används.

3.2 Ändamålsbegränsning

Ändamålsbegränsningen innefattar två saker:

(1) Personuppgifter måste insamlas med särskilda, uttryckligt angivna och berättigade ändamål.

Särskilda och uttryckligt angivna innebär att ändamålet inte får vara för ospecifikt eller vagt uttryckt. Exempelvis så är meningen ”Vi samlar in uppgifterna för marknadsföringsskäl” inte tillräckligt specifikt eller uttryckligt angivet. Berättigade ändamål syftar till den lagliga grunden.

(2) De får inte vid senare tillfälle behandlas på ett sätt som är oförenligt med det ursprungliga syftet.

Om organisationen har insamlat personuppgifter för ett visst ändamål kan de inte under ett senare tillfälle behandla personuppgifter för ett annat ändamål som inte är förenligt med det ursprungliga ändamålet. Vad innebär ”förenligt” med det ursprungliga ändamålet?

I skäl (50) diskuteras detta. Sammanfattningsvis så ska dessa kriterier beaktas för att det nya ändamålet ska vara förenligt med det ursprungliga:

Koppling till ursprungsändamålet, sammanhang inom vilket personuppgifterna insamlats, registrerades rimliga förväntning- ar, behandlingens konsekvenser för de registrerade samt före- komsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

Personuppgifter kan även behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Men detta kräver att det finns skyddsåtgärder som pseudonymisering. (Artikel 89(1)).

3.3 Uppgiftsminimering

Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Denna princip innebär att personuppgifter inte ska behandlas om det ursprungliga ändamålet med behandlingen inte längre är relevant. Organisationer ska inte behandla mer personuppgifter än vad som är nödvändigt för att fullgöra ändamålet. Det är inte heller tillåtet att samla in personuppgifter för att de ”kan vara bra att ha” i en obestämd framtid.

3.4 Korrekthet

Personuppgifter måste vara korrekta och uppdaterade.

Det finns självklara risker för registrerade ifall okorrekta personuppgifter behandlas om dem. Exempelvis för ett försäkringsbolag kan detta innebära att kunden får felaktig försäkringspremie. Personuppgifter måste därför vara korrekta och hållas uppdaterade. Enligt artikel 5(1) måste ”alla rimliga åtgärder vidtas” för att inkorrekta personuppgifter antingen rättas eller tas bort.

3.5 Lagringsminimering

Personuppgifter får inte lagras längre än vad som är nödvändigt för behandlingens ändamål.

När personuppgifter inte längre behövs för det ursprungliga ändamålet ska personuppgifterna tas bort. Det ska finnas en rutinmässig process och granskning för att ta bort personupp- gifter. Det ska också fastställas, om möjligt, tidsperioder över hur länge personuppgifter kan bibehållas tills de ska tas bort. Som sagt finns det en möjlighet att arkivera personuppgifter för ex- empelvis statistiska ändamål om det införs skyddsåtgärder som pseudonymisering. Istället för att radera personuppgifterna kan dem även anonymiseras. Om ni har kvar personuppgifter från gamla kunder i systemen, där ändamålet med behandlingen inte längre är relevant, måste dessa tas bort.

3.6 Integritet och konfidentialitet

Dessa principer är två hörnpelare i informationssäkerhet. Integritet innebär att bara behöriga personer kan ändra personuppgifterna; write behörighet. Konfidentialitet innebär

att bara behöriga personer kan se personuppgifterna; read behörighet. Organisationen ska införa ”lämpliga tekniska eller organisatoriska åtgärder” mot ”obehörig eller otillåten behand- ling och mot förlust, förstöring eller skada genom olyckshändelse”.

För att följa denna princip bör organisationen införa skyddsmekanismer som bland annat åtkomstkontroll, loggning, fysisk säkerhet, brandväggar, antivirus, dataskyddspolicy och pseudonymisering.

3.7 Ansvarsskyldighet

Personuppgiftsansvarige måste kunna bevisa att ovannämnda principer följs vilket kräver omfattande analyser och dokumentation.

Den sista principen innebär att organisationer som behandlar personuppgifter ansvarar för att alla dessa principer följs. Detta har stora implikationer för organisationer eftersom

efterlevnadsbördan är väldigt stor samtidigt som efterlevnaden måste kunna bevisas. Organisationer kommer att behöva dokumentera mycket mer än vad de nödvändigtvis är vana vid. I artikel 30 finns det krav att uppföra ett register om organisationens personuppgiftsbehandling. Organisationen bör upprätta både externa och interna riktlinjer för behandlingen. En integritetspolicy är ett dokument som riktar sig till externa intressenter så att de får insyn i organisationens behandling. En dataskyddspolicy är ett internt dokument som alla inom organisationen ska följa. Vissa organisationer kommer även att behöva anlita ett dataskyddsombud som bidrar till organisationens efterlevnad av förordningen.

4. Laglig grund och samtycke

Innan organisationen kan behandla personuppgifter måste det finnas en laglig grund för behandlingen. Det finns mycket missförstånd kring detta, då många tror att det kommer att krävas samtycke till all behandling av personuppgifter. Detta är väldigt fel, då det finns många andra grunder att rättfärdiga sin behandling med. Nackdelen med samtycke är att den bara är giltig ifall den enskilde gör en aktiv handling, den kan återkallas när som helst och det får inte förekomma någon större maktobalans mellan de parter som ber om respektive ger samtycket (exempelvis mellan arbetsgivare och anställd). Samtycke bör som regel alltid övervägas sist av alla lagliga grunder. Många organisationer tenderar att använda samtycke i situationer där det egentligen inte behövs, och har blivit en typ av ”säkert kort” att förlita sig på. Att använda fel laglig grund, exempelvis samtycke, kan medföra att behandlingen blir olaglig.

Laglig grund beskrivs i Artikel 6 i GDPR. Följande avsnitt går igenom Artikel6(1) och förklara vad alla olika grunder innebär:

Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

Som sagt, ävenfast förordningen nämner samtycke först så bör denna lagliga grund beaktas sist. Det finns olika krav på samtycke. Först och främst måste enskilda utföra en aktiv handling, exempelvis bocka i en ruta där det står: ”Genom att bocka i denna ruta samtycker du till våra termer och har läst vår integritetspolicy (länk)”. Tystnad, inaktivitet eller föribockade rutor räknas inte som samtycke. Exemplet innan beskrev det förordningen kallar för **uttryckligt** samtycke, och det kan i vissa omständigheter rättfärdiga behandling av känsliga personuppgifter.

För behandling av icke-känsliga personuppgifter kan det räcka med att enskilda skriver in sina personuppgifter, exempelvis e-postadress, och det står bredvid fältet: ”Skriv in din e-postadress så att vi kan skicka nyhetsbrev om våra produkter till dig, mer information hittar du i vår integritetspolicy (länk)”. Tänk på att det alltid måste framgå tydligt vad enskilda samtycker till. Enskilda kan inte samtycka åt andra än till sig själv, undantag när vårdnadshavare ger samtycke åt omyndiga som inte kan ge ett lagligt samtycke. Det måste alltid finnas ett sätt att återkalla samtycket för att det ska vara giltigt.

b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

Ett typiskt exempel när ett avtal rättfärdigar behandlingen är ett anställningsavtal. En arbetsgivare får lagligt behandla personuppgifter om anställda som är nödvändiga för att fullgöra anställningsavtalet. När GDPR tillämpas i svensk lag behöver alltså inte arbetsgivare springa runt till alla sina anställda och be om samtycke.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

Företag är exempelvis skyldiga att följa bokföringslagen i Sverige och måste lagra personuppgifter en fastställd tid för detta ändamål. Företaget har alltså en rättslig förpliktelse att behandla sådana uppgifter och enskilda kan inte begära att få dessa uppgifter raderade innan organisationen har full- gjort denna rättsliga förpliktelse.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

Den här grunden handlar om nödsituationer, exempelvis om en person plötsligt blir svårt sjuk och personuppgifter behövs för att identifiera personen.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Tidigare så har svenska myndigheter förlitat sig på grunden ”berättigat intresse” när de fullgör sina uppgifter. Detta får de inte längre göra enligt artikel 6(1). Istället har denna grund tillkommit som ska användas av myndigheter. Det är upp till varje medlemsland att avgöra vad ”utföra en uppgift av allmänt intresse” kommer att innefatta.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättig- heter och friheter väger tyngre och kräver skydd av personupp- gifter, särskilt när den registrerade är ett barn.

Berättigat intresse innebär att det görs en intresseavvägning mellan nyttan av behandlingen och risken för enskildas grund- läggande rättigheter och friheter. Om risken för att registrerades fri- och rättigheter blir kränkta är större än den nytta personen och organisationen kommer att ha med behandlingen kan denna grund inte hävdas. Det står uttryckligen i skäl (47) i för- ordningen att direktmarknadsföring är ett berättigat intresse. Detta betyder att det fortfarande kommer att finnas möjlighet att använda direktmarknadsföring utan samtycke, men bara ifall nyttan väger högre än risken. Tänk på att ju känsligare behandlingen är desto svårare kommer det bli att hävda denna grund.

***Notera**: Datainspektionen har en broschyr där de utförligt förkla- rar berättigat intresse. Tyvärr så har de inte hunnit anpassa den till GDPR, utan den är i nuvarande stund bara anpassad till Pu*L.

5. De registrerades rättigheter

De registrerades rättigheter i förordningen måste respekteras om organisationen inte vill råka ut för höga sanktionsavgifter.

5.1 Informationsrättigheten

Personuppgiftsansvariga är skyldiga att informera berörda registrerade när de samlar in personuppgifter från dem. Artikel 13 radar upp allt som ska informeras; exempelvis identitet och kontaktuppgifter för den personuppgiftsansvarige, period som personuppgifter lagras, ändamålen med behandling och den rättsliga grunden som hävdas. Tänk på att informationskravet skiljer sig åt ifall den personuppgiftsansvarige samlar in personuppgifter direkt från den enskilda eller får dem indirekt från en tredje part. Informationskravet är fortfarande väldigt likt, men det tillkommer några extra informationskrav ifall den personuppgiftsansvariga får personuppgifterna indirekt, dessa finns i artikel 14.

5.2 Rätt till tillgång

Personuppgiftsansvariga är skyldiga att ge tillgång eller insyn över den behandling av personuppgifter som angår berörda registrerade. Registrerade kan alltså begära ut en kopia av informationen, under vissa omständigheter, som innehåller de personuppgifter som den personuppgiftsansvariga behandlar. Det innebär att det behövs processer för att lämna

ut information, men också för att säkerställa att det är rätt motpart som begärt att få ut uppgifterna. Den registrerade har i princip rätt att kunna se all fritext i noteringar som görs angående den registrerade. Det kan därför vara bra att införa en policy att saker som skrivs om kunder i systemen är sakliga och inte kränkande.

Artikel 15(1) kräver dessutom att ytterligare information ska medfölja kopian. Denna information ska bland annat innefatta:

» Ändamålen med behandlingen

» De kategorier av personuppgifter som behandlingen gäller

» De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.

» Om möjligt, den förutsedda period som personuppgifterna kommer att lagras

Om personuppgiftsansvariga lämnar ut personuppgifter till andra organisationer behöver inte den personuppgiftsansvarige rada upp namnet på alla organisationerna; istället räcker det med att säga vilka kategorier som dessa organisationer tillhör, exempelvis marknadsföringsbolag eller molntjänstleverantör. Den personuppgiftsansvarige kan inte kräva betalning från den registrerade för tillgång till kopian. Däremot kan den personuppgiftsansvarige begära betalning som är rimlig gentemot den administrativa kostnaden, ifall den registrerade repetitivt begär kopior och det inte är skäligt att ge kopian gratis.

5.3 Rätt till rättelse

Den enskilde har rätt att begära korrigering av felaktiga eller ofullständiga uppgifter. Denna rättighet ligger i nära anknytningen till rätten till tillgång. Om registrerade inte vet vilka uppgifter som behandlas kan de inte veta om de behöver korrigeras.

5.4 Rätt till radering (”rätten att bli bortglömd”)

Den registrerade har rätt att få sina personuppgifter raderade *”utan onödigt dröjsmål”* av den personuppgiftsansvariga på begäran. Detta är en av de mest kontroversiella delarna i förordningen och har fått smeknamnet ”delete-knappen”. Detta har skakat om IT-världen eftersom alla system inte är riktigt anpassade till att faktiskt kunna radera personuppgifter i större omfattning. Jag vill börja med att påpeka att organisationer inte behöver gå in sina backupper och radera personuppgifter i dem. Det finns en vittspridd missuppfattning att det räcker med att kryptera personuppgifterna och sedan radera nyckeln. Detta duger inte eftersom krypterade personuppgifter räknas som pseudonymiserade personuppgifter och dessa omfattas fortfarande av förordningen. Det finns ju en möjlighet att ”knäcka” krypterad information och återställa den till klartext med brute force-attacker. Däremot så fungerar det att anonymisera personuppgifterna och därmed uppfylla rätten att bli glömd. Personuppgiftsansvariga kan dessutom behålla personuppgifterna för arkivändamål.

Artikel 17 radar upp kriterier när personuppgiftsansvariga INTE behöver eller ska radera personuppgifterna även fast den registrerade begär det av dem:

a) För att utöva rätten till yttrande- och informationsfrihet.

b) För att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt.

c) För att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

d) För arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Exempelvis så kan det förekomma en fordran och en kund är skyldig organisationen pengar för obetalade fakturor. Då kan inte denna kund ringa och be om att få sina personuppgifter raderade. Bokföringslagen har också krav på att personuppgifter ska kvarstå en viss tidsperiod.

6 Checklista för efterlevnadsprojektet

Den nya förordningen kommer att kräva nya organisatoriska och tekniska åtgärder i din organisation. Ledningen bör initiera projektet för GDPR-efterlevnad och fördela ansvar och de nödvändiga resurserna. Det är nödvändigt att samarbete finns inom alla relevanta avdelningar i organisationen och att de eftersträvar samma mål. Detta är INTE bara ett IT-projekt som bara rör IT-avdelningen. Det finns två sidor av ett dataskyddsprojekt:

1. Den mjuka delen – Ledning, dokumentation, policy, utbildning, administration.

2. Den hårda delen – IT-säkerhet och rena systemkrav.

Mjuka krav:

1. Ett register kommer att behöva föras som omfattar bland annat kategorier av personuppgifter som behandlas, ändamål med behandlingen, biträden/ansvariga där det finns överföring av personuppgifter, osv. (artikel 30) Denna registerföring samt kartläggning av system är ett första steg till en åtgärdsplan.

2. Avgör den lagliga grunden för behandling av personuppgifter. Här bör samtycke alltid övervägas sist av alla möjliga grunder. (artikel 6)

3. Avgör ifall organisationen följer principerna i förordningen. (artikel 5)

4.Avgör ifall organisation kan tillförse de registrerade de rättigheter som finns i förordningen (rätten till radering, rätten till dataportabilitet, rätten till tillgång...)

5. Ta reda på ifall organisationen behöver anlita ett dataskyddsombud. (artikel 37)

6.Uppdatera biträdesavtalen – fastställ era förpliktelser inom GDPR gentemot era kunders/leverantörers förpliktelser. (artikel 28)

7. Framställ integritetspolicy. Det är dags att öppna sig till intressenter med vad/hur/varför personuppgifter behandlas i organisationen. Öppenhetsprincipen kräver att denna information ska vara lättillgänglig och att enkelt språkbruk används.

8.Framställ dataskyddspolicy, intern information där det bland annat finns en dokumenterad process för incident- hantering.

9.Avgör ifall organisationen behöver genomföra konsekvensbedömningar.

10.Om din organisation är verksam internationellt så måste det fastställas var organisationen har sin centrala förvalt- ning så att organisationen svarar under korrekt tillsynsmyn- dighet. I Sverige är tillsynsmyndigheten Datainspektionen.

Hårda krav:

1. Privacy by design – Överlag kommer system att behöva ett inbyggt dataskydd som genomsyrar hela livscykeln.

2. Pseudonymisering och kryptering – Behandling av känsliga/extra skyddsvärda personuppgifter kommer att kräva starkare integritetsskydd.

3. Gallring – Framställning av rutiner och tekniska lösningar för gallring av personuppgifter.

4. Behörighetskontroller – Bara personer med rätt behörighet ska ha åtkomst till personuppgifter. Fördela roller inom organisationen och gör så att anställda bara har tillgång till den information som är nödvändig för yrkesrollen.

5. Logghantering – Införande av loggar som ger adekvat spårbarhet. Vid en personuppgiftsincident är det väsentligt att det finns bevisunderlag och det kommer loggar att kunna bidra med.

6.Sårbarhetsanalyser – Penetrationstester och sårbarhetsskanning kan kartlägga sårbarheter i systemen.

7. Övriga tekniska åtgärder – SNTP, härdning av system, övervakningssystem, brandväggar och antivirus.


Complior