Företagen och dataskyddsförordningen

Nya regler för hantering av personuppgifter

Christina Wainikka och Carolina Brånby

Uppdaterad december 2017

SVENSKT NÄRINGSLIV

Företagen och dataskyddsförordningen

Nya regler för hantering av personuppgifter

Christina Wainikka och Carolina Brånby

Innehållsförteckning

Nya regler innebär nya krav

Teknikutvecklingen går snabbt framåt. Lagar och regler behöver ses över för att vara relevanta. Vad gäller personuppgiftsskydd har ambitionen varit att balansera integritetsskydd och innovationsmöjligheter. Med den nya lagstiftningen på plats kan vi konstatera att den uppgiften varit svår att lyckas med. Företagen har fått en omfattande läxa att göra för att leva upp till lagstiftarens förväntningar.

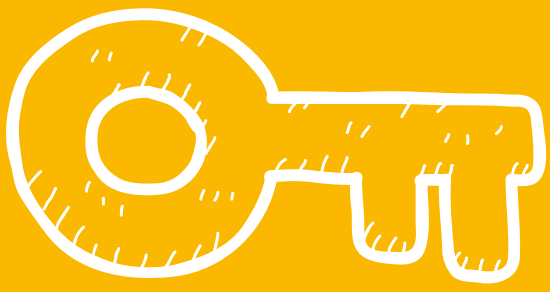
Från den 25 maj 2018 gäller dataskyddsförordningen i Sverige och övriga medlemsstater i EU. Förordningens fullständiga namn är *”Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning).”*

Dataskyddsförordningen ersätter personuppgiftslagen, PUL, och är en skärpning av personuppgiftsskyddet. Konsekvensen av de nya reglerna blir förändrade krav på hur personuppgifter måste, kan, får, och bör hanteras.

Syftet med den här skriften är att beskriva de nya reglerna och hur de påverkar företagens hantering av personuppgifter.

För att göra reglerna och deras tillämpning tydligare behöver de sättas in i sitt sammanhang. Personlig integritet är inte bara viktig inom ramen för regler om behandling av personuppgifter. För oss som individer handlar det också om exempelvis hur vi får omnämnas i traditionella medier och i olika sociala medier. Regler som gäller i sådana sammanhang behandlas därför också.

För många företag är det viktigt att i god tid se över hur organisationen och rutiner måste förändras för att verksamheten ska kunna följa de nya reglerna.



1. Bakgrund och motiv till regler om dataskydd

Den digitala tekniken för med sig många positiva saker. Tack vare big-data-analyser kan enskilda individer i allt större omfattning få relevant individualiserad utbildning, vård och kunderbjudanden. Genom digitalisering kan våra uppgifter ingå i kartläggningar som ger möjlighet till att nya produkter och tjänster utvecklas av företagen.

Men tekniken gör det också lätt att hitta information om fysiska personer på ett sätt som kan vara problematiskt. Aldrig har det varit så lätt att sprida uppgifter om personer som nu i den digitaliserade tid vi lever i.

För drygt tjugo år sedan kom det direktiv om automatiserad behandling och registerföring av personuppgifter som gav den personliga integriteten ett likartat skydd inom EU. Det hängde samman med ökad användning av digital teknik och att internet på allvar slog igenom.

Inom EU finns det två typer av rättsakter för regler som ska gälla inom unionen. Den ena är direktiv och den andra är förordningar. Direktiv måste omarbetas till nationell lagstiftning, såsom gjordes när PUL skapades i svensk rätt 1995. En förordning blir däremot direkt gällande i medlemsstaterna. Dataskyddsförordningen kommer från den 25 maj 2018 gälla i Sverige precis som om den varit en svensk lag som riksdagen fattat beslut om.

Bakgrund till förordningen: *"Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet."* (Skäl 1, dataskyddsförordningen)

Skyddet för människor *"bör, oavsett deras medborgarskap eller hemvist respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd för personuppgifter".* (Skäl 2, dataskyddsförordningen)

Svenska domstolar och myndigheter ska följa de tolkningar som görs på EU-nivå. Särskilt viktigt blir det därför att hålla koll på utvecklingen av praxis som sker hos EU-domstolen. Råd som tidigare lämnats från Datainspektionen kan bli överspelade i och med de nya reglerna. Dataskyddsmyndigheter från medlemsländerna kommer samverka i ett nytt samarbetsorgan, Europeiska dataskyddsstyrelsen, för att säkerställa likartad tillsyn och tolkning av dataskyddsförordningen inom unionen, se artikel 68, dataskyddsförordningen.

2. Vår rätt till oss själva

2.1 Regler som rör vår integritet

2.1.1 Många olika regler rör frågor om integritet

Ett antal regler styr hur vi får använda andras personuppgifter. Hur får vi till exempel nämna andras namn och använda bilder på andra? Reglerna är av väldigt olika slag och är skapade utifrån olika syften. I vissa fall är det den som personuppgiften handlar om som har störst rätt att bestämma hur personuppgiften används. I andra fall är det andra intressen som anses viktigare, vilket gör att personen uppgifterna handlar om då får begränsade möjligheter att protestera mot användandet.

2.1.2 Dataskyddsregler

Dataskyddsregler styr på vilket sätt personuppgifter får användas. Idag återfinns reglerna framför allt i PUL och de kommer ersättas av reglerna i dataskyddsförordningen. Fokus för de här reglerna är att skydda den personliga integriteten. Det gör att dessa regler tydligt begränsar hur vi får hantera personuppgifter.

Reglerna i både PUL och dataskyddsförordningen gäller dock inte för alla typer av behandling av personuppgifter. De gäller till exempel inte om behandlingen av personuppgifter sker för journalistiskt ändamål. I sådant fall kan det sägas att yttrandefrihetsskäl väger tyngre än skyddet för den personliga integriteten.

2.1.3 Yttrandefrihetsregler

Yttrandefriheten är grundlagsreglerad i Sverige genom både tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Utgångspunkten för dessa regler är att åsikter och information ska få flöda fritt. Rätten till personlig integritet är därmed begränsad i förhållande till friheten att sprida information.

Tryckfrihetsförordningen gäller för tryckta medier, såsom dagstidningar och veckotidningar. Yttrandefrihetsgrundlagen gäller för radio, tv, bio och i vissa fall för publiceringar på nätet. Inget av dessa regelverk gäller för kommersiella meddelanden.

Mer om yttrandefrihetsreglerna nedan.

2.1.4 Lagen om namn och bild i reklam

När personer ska vara med i reklamsammanhang måste de tillfrågas enligt lagen om namn och bild i reklam. Det gör att så fort det är fråga om kommersiella meddelanden, såsom reklamfilm eller en annons, kan personen i fråga stoppa användningen av bild eller nämnandet av namnet.

Lagen om namn och bild i reklam gäller även när personen i sig inte nämns vid sitt riktiga namn eller rent faktiskt är med på bild. Den gäller till exempel även när en imitatör används eller när ett smeknamn som förknippas med personen nämns.

Lagen gäller bara för levande personer vilket gör att det är tillåtet att i annonser och liknande hänvisa till avlidna personer.

2.1.5 Uppförandekoder och användarvillkor i sociala medier

Sociala medier såsom Facebook, Instagram, Snapchat och liknande, används av allt fler. När vi använder dessa medier måste vi som användare agera i enlighet med deras respektive användarvillkor. Medierna är till stora delar fria att själva bestämma sina användarvillkor vilket innebär att de i princip kan styra vad vi kan yttra om andra. Hur vi hänvisar till andra personer och delar bilder på sociala medier är således inte bara en fråga om regler från lagstiftaren utan även reglerat i de tjänster vi använder.

2.1.6 Upphovsrätt

En fotograf som tar bilder på en person får upphovsrätten till bilderna. Den som skriver en text där en person nämns kan få upphovsrätt till texten. Upphovsrätten innebär en ensamrätt att bestämma över hur det som är skyddat kan och får användas. Vill fotografen inte att bilden ska publiceras på nätet kan fotografen blockera sådan användning. I praktiken innebär det att fotografen i vissa fall har större möjligheter att hindra en publicering än personen på bilden har, särskilt om det gäller publicering i media.

2.2 Konsekvenser

2.2.1 Lapptäcke av regler som inte ger ett heltäckande skydd

Regelverket om när vi kan hindra andra från att skriva om oss eller att publicera bilder på oss är ett lapptäcke av en mängd olika regler. Dessa regler har ofta till syfte att skydda andra intressen än den personliga integriteten. Det kan handla om yttrandefrihet som bedöms som viktigare än den personliga integriteten i vissa fall. Det kan också handla om att upphovsmannens intresse väger över i förhållande till någon som förekommer i en text eller på en bild.

2.2.2 Behov av att hålla koll på vad som gäller i olika situationer

För att veta hur man får göra i en viss given situation måste man reda ut vilket regelverk det är som gäller. Detta är viktigt såväl för intern som extern kommunikation. Och inte minst viktigt är det när det gäller helt egna kanaler (såsom egna hemsidor) och när kommunikationen sker via sociala medier av olika slag.

3. Yttrande- och informationsfrihet

3.1 Reglering av yttrande- och informationsfriheten

Yttrandefrihet är en grundläggande mänsklig rättighet. Yttrandefriheten och informationsfriheten gör att vi får yttra oss och sprida information om andra, även om de kanske inte vill att informationen kommer ut.

Reglerna kring dessa friheter finns i såväl nationella grundlagar som i internationella konventioner och överenskommelser.

Eftersom reglerna i dataskyddsförordningens om skyddet av den personliga integriteten har ett annat syfte uppstår en konflikt mellan regelverken. Det som är tillåtet i ett sammanhang är det inte alls i ett annat. Att förstå de olika regelverkens hierarki är viktigt för att förstå när de olika reglerna gäller.

3.2 ”Gammelmedier”

Radio, tv och tryckta medier som tidningar och tidskrifter kallas ibland för ”gammelmedier”. Gemensamt för dessa medier är att de är grundlagsskyddade och att reglerna i dataskyddsförordningen inte gäller för dem.

”Gammelmedierna” har alltså lagligt stöd för att mer eller mindre fritt publicera uppgifter om enskilda personer. Gränsen går dock vid yttranden som kan utgöra förtal. Dessa medier är dessutom skyldiga till att följa olika pressetiska regler, vilket gör att de är återhållsamma med att publicera namn och bild på de som är misstänkta för brott. Medierna brukar, i enlighet med de pressetiska reglerna, avvakta med publicering till dess att dom har fallit.

3.3 Yttrandefrihet på nätet

3.3.1 Yttrandefrihetsgrundlagen (YGL)

Yttrandefrihetsgrundlagen gäller för vissa typer av publiceringar på nätet och omfattar till exempel de hemsidor som har ett utgivningsbevis från myndigheten för press, radio och tv. I praktiken är det väldigt enkelt att få ett utgivningsbevis, det är en ansökan som ska fyllas i och en avgift som ska betalas.

3.3.2 Relationen YGL och dataskyddsregler

För de hemsidor som har utgivningsbevis gäller YGL, vilket gör att det är i princip fritt att publicera personuppgifter. För hemsidor som inte har utgivningsbevis gäller reglerna i dataskyddsförordningen.

Konsekvensen för användarna är att olika regelverk för publicering kan gälla för snarlika hemsidor. Det som är tillåtet på en hemsida får inte publiceras på en annan.

3.3.3 Undantag – "journalistiskt ändamål"

I PUL finns ett undantag för behandling av personuppgifter som sker för journalistiskt ändamål. En motsvarande skrivning finns i dataskyddsförordningen för journalistiskt, akademiskt, konstnärligt eller litterärt skapande, se artikel 85. De undantagen gäller om de införs i svensk lag. Se Dataskyddsutredningens betänkande, maj 2017.

Det är oklart hur undantaget kommer att tolkas efter den 25 maj 2018. I svensk rättspraxis ligger fokus på just ändamålet med behandlingen av personuppgifterna för att publiceringen ska kunna anses vara journalistiskt. Personen som exempelvis publicerar en uppgift om någon behöver inte vara journalist och hemsidan som publicerar uppgiften behöver inte betraktas som till exempel en nättidning.

Oavsett hur införandet och tolkningen av journalistiskt ändamål kommer att ske framöver, finns all anledning att se över vilka regler som ska gälla för företagets hemsidor.

3.3.4 Andra regelverk som kan tillämpas

För de hemsidor som inte omfattas av grundlagsskydd finns ytterligare regler att ta hänsyn till. Dessa kan åberopas oavsett om dataskyddsförordningen är tillämplig eller inte.

Hit hör till exempel skadeståndslagen, som ger möjlighet att kräva skadestånd för kränkning. En kränkning kan det vara fråga om när det på en hemsida publiceras att någon gjort sig skyldig till brott eller fuskat i en sport.

Ett annat regelverk som har åberopats i vissa fall vid olika typer av nätpubliceringar är brottsbalken. Det finns exempel på fall där personer som skrivit kommentarer på Facebook har fällts för brott. Det har då handlat om att någon hängts ut som brottsling trots att detta inte stämt.

Ytterligare ett regelverk som kan aktualiseras är lagen om elektroniska anslagstavlor, den så kallade BBS-lagen. Den lagen gör att den som låter andra kommentera på sin hemsida har en skyldighet att rensa bort vissa typer av innehåll. Lagen tar främst sikte på innehåll såsom barnpornografi och sådant som utgör upphovsrättsintrång. Yttranden om andra, även om det utgör förtal, faller sällan in under lagens tillämpningsområde. I sådant fall är det snarare PUL som kan åberopas.

Checklista yttrande- och informationsfrihet

- ☑ Fatta beslut om företagets hemsida ska ha utgivningsbevis eller inte.
- ☑ Skapa riktlinjer och rutiner kring publicering på hemsidan som ligger i linje med de regelverk som gäller.
- ☑ Tänk på att olika regler gäller beroende på om publicering sker på egen hemsida eller via andra kanaler, såsom sociala medier.

4. Begreppet personuppgift

4.1 Rättslig definition av personuppgift

Dataskyddsförordningens regler gäller enbart för det som är personuppgifter.

Definition av begreppet personuppgift, artikel 4.1, dataskyddsförordningen:

”...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,”

Det är enbart uppgifter om fysiska personer som är personuppgifter. Uppgifter om företag och organisationer är som huvudregel inte personuppgifter. För juridiska personer är organisationsnumret inte en personuppgift. Det innebär att hanteringen av dessa nummer inte berörs av dataskyddsförordningen. För enskilda firmor utgörs organisationsnumret av innehavarens personnummer. Detta är alltså en personuppgift och måste hanteras som sådan.

Personuppgifter är alla uppgifter som handlar om oss som individer. Hit hör allt som direkt, eller indirekt, kan knytas till en levande fysisk person. Det innebär att inte bara uppgifter som namn, adress och personnummer är personuppgifter, utan även sådant som fotografier och vår dators IP-nummer. Hit hör också ”nicks” som används i ett datorspel eller liknande.

I de flesta fall är uppdelningen mellan vad som är uppgifter om juridiska och fysiska personer väldigt enkel att göra. Uppgifter om företaget är inte personuppgifter, men uppgifter om enskilda anställda eller styrelseledamöter är personuppgifter. Det finns dock en kategori av näringsidkare där denna uppdelning blir besvärlig. Det gäller alla som bedriver sin verksamhet i form av enskild firma. En enskild firma är helt kopplad till individen och organisationsnumret är detsamma som den fysiska personens personnummer. Det innebär att just de enskilda firmornas organisationsnummer faktiskt är en personuppgift.

Krypterade personuppgifter är enligt dataskyddsförordningen att se som personuppgifter även om den som har uppgifterna i krypterad form inte har tillgång till själva nyckeln för att få fram de faktiska personuppgifterna. Kryptering är alltså inte ett sätt att undvika regelverket, men väl en säkerhetsåtgärd.

4.2 Känsliga personuppgifter

Reglerna i dataskyddsförordningen gäller generellt för alla typer av personuppgifter, men det finns en del regler som tar sikte på särskilda kategorier av uppgifter, se artikel 9. Detta gäller särskilt det som kallas för känsliga personuppgifter, se skäl 51.

Till känsliga personuppgifter hör uppgifter som avslöjar politisk åskådning, religion, fackligt medlemskap eller etniskt ursprung. Behandling av genetiska och biometriska uppgifter för identifiering, uppgifter om hälsa, sexualliv och sexuell läggning är också känsliga uppgifter. Känsliga uppgifter får inte behandlas på samma sätt som andra personuppgifter eftersom deras behandling har särskild betydelse för individers integritet.

Utgångspunkten är att det råder förbud mot att behandla sådana personuppgifter, men det finns några undantag, bland annat inom arbetsrätten samt hälso- och sjukvården. Det kan också lämnas samtycke till behandling av sådana uppgifter. I samband med till exempel evenemang kan det behöva hanteras uppgifter om allergier och liknande.

En huvudregel för verksamheter kan vara att inte alls behandla känsliga personuppgifter. I viss mån måste kanske sådana uppgifter behandlas under en begränsad tid, men då ska det finnas tydliga rutiner om bortrensning av uppgifterna när de inte längre behövs.

4.3 Särskilt känsliga personuppgifter

En typ av uppgifter som är omgärdad av ytterligare begränsningar är uppgifter som rör fällande domar i brott och lagöverträdelser. Grundprincipen är att sådana uppgifter inte får behandlas, inte ens om samtycke inhämtas. Enligt artikel 10 får behandling utföras under kontroll av myndighet, enligt unionsrätten eller nationell rätt.

Det undantag som regleras i föreskrift från Datainspektionen, se DIFS 2010:1, ger arbetsgivare rätt att hantera enstaka uppgifter om brott och lagöverträdelser. Föreskriften torde göras om i och med ikraftträdandet av dataskyddsförordningen. Dessutom kan företag enligt 21 § PUL ansöka om tillstånd hos Datainspektionen att i annat fall behandla dessa uppgifter. Det är till exempel aktuellt för företag som behöver genomföra brottsregisterkontroll, så kallad screening, av sina medarbetare mot amerikanska myndigheters terrorlistor inför exporttillstånd. Den svenska Dataskyddsutredningen har i uppdrag att föreslå en ny reglering som utgår från bestämmelsen i PUL. Dataskyddsutredningen ska överlämna sitt betänkande till regeringen den 12 maj 2017.

Tänk på att:

- i princip alla uppgifter som kan kopplas till en fysisk person kan betraktas som personuppgifter
- även uppgifter om enskilda firmor är personuppgifter
- säkerhetsåtgärder behövs vid behandling av känsliga personuppgifter
- enstaka uppgifter om brott och lagöverträdelser får behandlas av arbetsgivare
- uppgifter om brott inte får behandlas utan tillstånd av Datainspektionen

5. Begreppet behandling

Syftet med reglerna om dataskydd är att skydda personers integritet. Personuppgifter får inte behandlas fritt. Det gör att ett viktigt begrepp i regleringen är ”behandling”.

Definition av begreppet behandling, artikel 4.2, dataskyddsförordningen:

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

Vid en första anblick kan det tyckas som att allt som kan göras med personuppgifter omfattas av begreppet. Det är dock några saker som faller utanför.

Att läsa en text, låt säga en blogg, där personuppgifter behandlas på fel sätt innebär inte att något fel begås. Att bara läsa eller ta del av någon annans behandling omfattas inte av begreppet behandling. Om man däremot utifrån dessa uppgifter börjar bygga upp adresslistor eller liknande är detta att klassa som behandling.

Det som omfattas av begreppet behandling är en mängd olika företeelser. Det kan handla om att samla in uppgifter om vissa personer för att senare kunna göra ett riktat utskick. Det kan handla om att spara kontaktuppgifter för att senare kunna kontakta en person hos en kund.

När något faller in under ”behandling av personuppgift” i regleringens mening måste man undersöka vilken rätt som finns för att göra den här behandlingen. Allt är inte förbjudet, men allt är inte heller tillåtet. Ska behandlingen göras bör man undersöka med vilken rätt man gör själva behandlingen.

6. Tillåten behandling av personuppgifter

6.1 Allmänt om när behandling är tillåten

Företaget har ansvar för och ska kunna visa att behandlingen sker på de sätt som anges i artikel 5.1. Varje behandling ska dessutom vara tillåten, ha lagligt stöd, enligt någon av de grunder som räknas upp i artikel 6.

Artikel 5.1 i dataskyddsförordningen anger de principer som gäller för behandling av personuppgifter:

”a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).

d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet). (...)

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. (...) (lagringsminimering).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).”

Varje enskild typ av behandling av personuppgifter måste ha regelstöd för att vara tillåten. Kan man inte hitta en sådan regel ska behandlingen av personuppgiften helt enkelt inte ske.

Artikel 6 i dataskyddsförordningen anger när behandling är tillåten:

”1. 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.

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.

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

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

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

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

Vid sidan om dessa punkter finns också ytterligare en anledning till att hantering av personuppgifter kan vara tillåten, nämligen att den faller helt utanför reglernas tillämpningsområde.

6.2 Vad omfattas inte?

Förordningen omfattar automatiserad behandling men även manuell behandling som medför att personuppgifter finns i ett register.

I dataskyddsförordningen, artikel 2, regleras i vilka sammanhang förordningen ska tillämpas.

”Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.”

Det gör att frågan uppkommer om vad som gäller utanför digitala system. Fokus för regleringen är det som görs i datorer, men begreppet omfattar även exempelvis kartotek och liknande som enkelt är sökbara. Handskrivna anteckningar som osorterat förs in i en papperskalender omfattas dock inte av begreppet behandling. Det gör att sådana anteckningar kan göras utan hänsyn till dataskyddsförordningen. Gränsdragningen kan dock i vissa fall vara svår att göra. Avgörande är om det kan ses som någon form av register, med sökbarhet.

I artikel 2.2 anges behandling som inte omfattas:

”Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.”

Här framkommer att sådan behandling som görs med hänvisning till rikets säkerhet, såsom behandling som görs inom försvaret, inte omfattas av reglerna. Allt sådant vi gör i hemmet, såsom listor över vilka släktingar som ska bjudas på bröllop, faller utanför reglernas tillämpningsområde. Här är det dock viktigt att komma ihåg att när vi rör oss i våra ”digitala vardagsrum”, som när vi skriver på en blogg, är det inte längre att anses som rent privat. Det gör att om vi har privata hemsidor som kan läsas öppet måste vi fundera över vilket regelverk det är som gäller. Se kapitel 3.3 om yttrandefrihet på nätet.

6.3 Samtycke

En av de centrala möjligheterna för att göra behandling av personuppgifter tillåten är att inhämta individens samtycke. Detta är reglerat på flera ställen i dataskyddsförordningen, artikel 4.11, 6.1a och 7. Frågan tas också upp i skäl 32, 42 och 43.

Frågan om samtycke är också central i PUL. I dataskyddsförordningen förändras dock de krav som ställas på samtycket och dess utformning.

Det är den personuppgiftsansvarige som ska kunna bevisa att samtycke har inhämtats. Det kräver i sig ingen särskild form, men samtycket måste inhämtas på ett sådant sätt att det går att bevisa i efterhand.

Idag är det till stora delar möjligt med ganska svepande formuleringar kring vad samtycket avser. Den som inhämtat samtycke har i allmänna ordalag kunnat beskriva vad det är som kommer hända med personuppgifterna.

De nya reglerna innebär att samtycket ska vara klart och tydligt samt kunna särskiljas från andra frågor. Samtycket ska alltså inte ske genom en öppen skrivning i form av att all typ av behandling av personuppgifter kan komma att ske. Alltför omfattande samtycken är ogiltiga. Till detta kommer att om behandlingen sker för flera olika syften ska samtycke inhämtas tydligt för varje syfte, inte i ett samlat samtycke.

Samtycket får inte göras ”tvingande” genom att exempelvis ha konstruktioner där avtal bara kan träffas om ett samtycke till behandling av personuppgifter också lämnas. Denna konstruktion är idag ganska vanlig i olika typer av webtjänster, men bör alltså ändras.

Ett samtycke ska alltid kunna återkallas. Den som har lämnat sitt samtycke till behandling av personuppgifter ska kunna ta tillbaka samtycket och därmed ta bort denna grund för att behandla personuppgifterna. Tanken är att återkallandet av samtycket ska kunna ske på ett lika enkelt sätt som det en gång var att lämna samtycket.

6.4 Fullgörande av avtal

I vissa fall kan en behandling av personuppgifter vara nödvändig för att en avtalspart ska kunna fullgöra sina åtaganden enligt avtalet. Sådan behandling är tillåten.

Det kan till exempel handla om en person som beställer en tjänst som ska utföras i dennes hem. För att tjänsten ska kunna utföras måste företaget som ska utföra tjänsten anteckna namn och adress till personen.

När behandling av personuppgifter görs med hänvisning till att det är nödvändigt för att kunna fullgöra ett avtal är det viktigt att bara den behandling som faktiskt krävs för detta sker. Om företaget önskar göra någon annan form av behandling, till exempel sparande av uppgifter för senare marknadsföring, måste en annan grund för behandlingen hittas. Det kan till exempel handla om att inhämta samtycke.

6.5 Fullgörande av rättslig förpliktelse

I vissa fall måste personuppgifter behandlas för att den personuppgiftsansvarige ska kunna fullgöra rättsliga förpliktelser. Det finns många olika lagregler som ställer krav på exempelvis arbetsgivare att de ska fullgöra skyldigheter gentemot olika myndigheter. Uppställs sådana rättsliga krav får denna typ av behandling av personuppgifter ske.

6.6 Skyddande av intressen

En anledning till att behandla personuppgifter kan vara att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person. När sådan behandling görs är den tillåten.

6.7 Allmänt intresse

Det är tillåtet att behandla personuppgifter om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. För företag är det framför allt frågan om utförande av en uppgift av allmänt intresse som skulle kunna aktualiseras.

6.8 Intresseavvägning

Intresseavvägning är en möjlig väg till att göra behandling av personuppgifter tillåten. Denna möjlighet finnas i artikel 6.1f (se även skäl 47 till 49). Intresseavvägningen innebär att om företaget (den personuppgiftsansvarige) har ett berättigat intresse av att behandla personuppgifter väger detta tyngre än den registrerade personens intresse av integritetsskydd och då får behandling ske.

Intresseavvägningen gör att det blir tillåtet att behandla personuppgifterna utan att personen ifråga har en avtalsrelation till den som behandlar uppgifterna eller att personen har lämnat sitt samtycke.

Det skulle kunna tolkas som att intresseavvägningen blir en slasktratt som det alltid går att åberopa. Risken är dock att om den avvägning man stödjer sig på inte anses vara korrekt gjord har behandlingen skett i strid med skyddsreglerna.

Intresseavvägningen kan helt klart vara en öppning för att behandla personuppgifter, men det är viktigt att göra avvägningen i varje enskilt fall. Görs ingen faktisk avvägning är risken att det bedöms som att personens intresse av skydd för sin integritet väger över.

I dataskyddsförordningen regleras också att den vars uppgifter behandlas med stöd av intresseavvägningen har rätt att invända mot behandlingen, se artikel 21. Det går dock att fortsätta hävda att den personuppgiftsansvariges intresse väger över.

När det gäller känsliga personuppgifter kan dessa inte behandlas med stöd av intresseavvägningen. För dessa krävs i princip att samtycke inhämtas.

Checklista tillåten behandling

- ☑ Analysera varför företaget behandlar personuppgifter i olika fall.
- ☑ Behandlas även känsliga uppgifter?
- ☑ Analysera därefter vilket lagligt stöd som finns för behandlingen av personuppgifterna. Det är bara om det finns ett lagligt stöd som behandlingen blir tillåten.
- ☑ Finns åtgärder som kan vidtas för att en viss behandling ska få lagligt stöd eller ska behandlingen upphöra?

7. Nyheterna i data-skyddsförordningen

7.1 En översikt

En stor del av de kommande reglerna är bekanta om man arbetat med PUL. Det gäller framför allt själva grundstrukturerna och en del av begreppen. Vid sidan av detta finns också viktiga nyheter.

De viktigaste nyheterna är:

– Högre krav på samtyckets utformning
– Tydligare krav på att informera
– Begränsning i rätten för individer i att få ut information
– Högre krav på radering av uppgifter
– Inbyggt dataskydd och dataskydd som standard
– Krav på att rapportera om dataintrång
– Krav på konsekvensbedömning för vissa typer av behandling
– Införande av dataskyddsombud
– Krav på möjlighet till dataportabilitet
– Möjlighet att använda sig av uppförandekoder
– Utökade möjligheter att agera för Datainspektionen
– Införande av ”avskräckande” sanktionsavgifter

7.2 Högre krav på samtyckets utformning

Samtycke är som huvudregel en grund som gör att företag får behandla personuppgifter, se kapitel 6.3. Frågan om samtycke är reglerad i artikel 7 i dataskyddsförordningen. Regleringen innebär några förändringar i förhållande till vad som gäller idag.

I likhet med vad som redan gäller enligt PUL måste information lämnas för att samtycket ska gälla. Den behandling som görs måste också vara inom ramen för det som man informerat om, så ett samtycke innebär inte att man får göra vad som helst med personuppgifterna.

Idag är det vanligt att frågan om samtycke bakas in i andra frågor. Det kan till exempel stå ”genom att anmäla dig till evenemanget samtycker du till att vi använder dina personuppgifter”. Såsom skrivningen i artikel 7.2 ser ut måste frågan om samtycke klart och tydligt kunna särskiljas från andra frågor.

Det är idag svårt att säga exakt hur högt kraven kommer att ställas. Skrivningen kan också tolkas som ett krav på att aktivt samtycke krävs för olika former av behandling som kan komma att ske av en och samma personuppgift.

Det ska vara lika lätt att återkalla ett samtycke till behandling som att ge det. Samtycket ska alltid kunna tas tillbaka. Det får inte heller vara så att samtycket får tvingas fram, det måste vara fullt ut frivilligt.

7.3 Tydligare krav på att informera

I dataskyddsförordningen finns i artikel 12 till 14 regler som innebär tydliga krav på att informera om den behandling av personuppgifter som sker. Den här informationen ska lämnas på ett tydligt sätt vilket bland annat innebär att den måste skrivas på ett lättfattligt sätt.

Informationen ska också kompletteras med kontaktuppgifter till den som är personuppgiftsansvarig och till dataskyddsombudet då de finns, så att personen vars uppgifter behandlas får veta vem som kan tillfrågas om det dyker upp frågor kring behandlingen av personuppgifter.

I förhållande till vad som gäller idag innebär dataskyddsförordningen en skärpning. Skärpningen består bland annat i att det ställs krav på att även informera om den rättsliga grunden för behandlingen och hur länge uppgiften kommer att sparas. Informationen ska också täcka hur man kan kontakta tillsynsmyndigheten.

Informationskravet hänger också samman med att om någon ska lämna samtycke till att personuppgifter får behandlas ska detta samtycke ha föregåtts av tillräcklig information så att den som lämnar samtycket faktiskt förstår vad det innebär.

Informera om:

- Kontaktuppgifter för frågor om behandlingen
- Vad informationen ska användas till
- Varför företaget har rätt att behandla personuppgiften (samtycke, avtal etc)
- Hur länge kommer informationen att sparas
- Kontaktuppgifter till Datainspektionen

7.4 Begränsad kostnadsfri information

Individer ska kunna begära ut information om vilka personuppgifter som behandlas av företaget, artikel 15, dataskyddsförordningen. Detta är en del av kraven som finns på att man ska informera. Enligt artikel 12.5 ska den här informationen lämnas ut kostnadsfritt.

För att förhindra missbruk av rätten till information införs begränsningar i vad som faktiskt kan begäras. Om begäran från en registrerad är uppenbart ogrundad eller orimlig får den personuppgiftsansvarige ta ut en rimlig avgift eller till och med vägra att tillmötesgå begäran.

Exakt var gränserna ska gå för vad som anses uppenbart ogrundat eller orimlig är svårt att säga innan detta har prövats av tillsynsmyndigheterna. Det finns en risk att ett företag tycker sig ha rätt att ta ut en avgift eller vägra lämna ut information men att Datainspektionen gör en annan bedömning. Företaget kan då drabbas av sanktioner.

7.5 Högre krav på radering av uppgifter

De höga krav på att uppgifter ska rensas bort när det inte längre finns lagligt stöd för att fortsätta ha dem kvar utökas i dataskyddsförordningen. En uttrycklig rätt införs för den registrerade att få sina personuppgifter raderade utan dröjsmål, den så kallade rätten att bli bortglömd. Den innebär att radering kan krävas om en person vill bli borttagen från att vara sökbar. Denna rätt är inte absolut. Behandling av personuppgifter kan få fortsätta om den till exempel är nödvändig för att utöva rätten till yttrande- och informationsfrihet, se kapitel 3.

I artikel 17 framgår att oavsett framförda krav ska personuppgifter raderas av den personuppgiftsansvarig när de inte längre är nödvändiga eller när den registrerade återkallar sitt samtycke som varit grunden för rätten att behandla personuppgifterna.

Kostnaderna för detta ska bäras av den personuppgiftsansvarige.

Denna rätt är dock inte utan undantag. Det kan till exempel vara nödvändigt att spara personuppgifter för att kunna göra gällande eller försvara rättsliga anspråk. Behövs till exempel uppgifterna för att kunna visa att en rekrytering gått rätt till i enlighet med diskrimineringslagstiftningens krav får uppgifterna sparas tills rättsliga anspråk inte längre kan göras.

Den som behandlar personuppgifter bör sätta upp rensningsrutiner utifrån preskriptionstiderna i olika regelverk. Strukturen för att hantera rensning och radering bör klargöras redan när beslut om att behandla vissa personuppgifter fattas. Detta inte minst eftersom informationskravet i dataskyddsförordningen även omfattar att informera om hur länge behandlingen förväntas ske.

Exempel på ett företags gallringsrutin:

Krav på att spara finns enligt:	Krav på att radera efter tidsgräns:
Bokföringslagens krav på underlag	7 år + innevarande år
Skattelagstiftningens krav på spara uppgift	7 år + innevarande år
Kamerainspelning, enligt tillståndskrav eller	60 dagar
Digitala fotografier på anställda	3 år (från avslutad anställning)
Besöksloggar i reception	60 dagar
Avtal med kunder	3 år från avtal upphört
Medlemskap i lojalitetsprogram	2 år efter avtal upphört
Kontrakt med anställda	10 år från anställning upphört

7.6 Inbyggt dataskydd och dataskydd som standard

Företaget ska säkerställa att dataskydd finns inbyggt i IT-strukturen. Både tekniska och organisatoriska åtgärder ska vidtas enligt artikel 25. Det kan till exempel handla om att personuppgifter pseudonymiseras eller krypteras, se artikel 4.5.

7.7 Krav på att rapportera om dataintrång

I dataskyddsförordningen finns helt nya krav på att informera om personuppgiftsincidenter. Med personuppgiftsincidenter avses till exempel dataintrång, vilket innebär att personuppgifter kan ha hamnat i orätta händer.

De nya reglerna innebär både krav i relation till tillsynsmyndigheten och i relation till de vars personuppgifter behandlas.

Enligt artikel 33 ska personuppgiftsincidenter rapporteras till tillsynsmyndigheten inom 72 timmar från att den personuppgiftsansvarige fått vetskap om incidenten. Enligt artikel 34 ska personuppgiftsincidenter anmälas till den registrerade om incidenten leder till en hög risk för personens rättigheter och friheter. Anmälan ska ske snabbt, men det finns inte en absolut tidsgräns såsom i relation till tillsynsmyndigheten. Det finns också här en möjlighet att informera allmänheten, enligt artikel 34.2 c. Detta gäller om kravet på att informera alla berörda skulle innebära en ”oproportionell ansträngning”.

7.8 Krav på konsekvensbedömning för ”hög risk” behandling

I artikel 35 ställs krav på att behandling som sannolikt leder till en hög risk för integritetsskyddet ska föregås av en konsekvensbedömning. Konsekvensbedömning är obligatoriskt om behandlingen avser till exempel profilering, känsliga personuppgifter eller övervakning av allmän plasts i stor omfattning. Enligt artikel 35.4 ska tillsynsmyndigheten ta fram en lista över vilka typer av behandling det är som ska omfattas av kravet. För de företag vars behandling kan komma att omfattas är det viktigt att hålla sig uppdaterad på riktlinjerna från Datainspektionen.

7.9 Krav på dataskyddsombud

Ett nytt begrepp i dataskyddsförordningen är dataskyddsombud. Med dataskyddsombud avses en person som utsetts för att vara ett stöd vid behandling av personuppgifter. På många sätt liknar det de personuppgiftsombud som finns i PUL, men inte fullt ut.

Det är inte alla organisationer som måste ha dataskyddsombud. I artikel 37.1 anges när det är obligatoriskt med dataskyddsombud:

– Myndigheter och andra offentliga organ,
– kärnverksamheten består av att behandla personuppgifter som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning eller
– kärnverksamheten består av behandling i stor omfattning av känsliga personuppgifter

Organisationer som ser en nytta med att ha ett dataskyddsombud kan utse ett på eget initiativ. För organisationer som ser att de behöver göra anpassningar av verksamheten för att klara av kraven i dataskyddsförordningen kan det vara bra att ha ett dataskyddsombud i verksamheten.

7.10 Krav på möjlighet till dataportabilitet

En nyhet i och med dataskyddsförordningen är att individer ska kunna ställa krav på dataportabilitet enligt artikel 20. Det här innebär att de registrerade ska ha rätt att få ut sina personuppgifter som har lämnats till en personuppgiftsansvarig för att sedan överföra dessa uppgifter till en annan personuppgiftsansvarig. Detta gäller dock bara om behandlingen sker automatiserat och om behandlingen bygger på samtycke eller fullgörande av avtal. Den personuppgiftsansvarige är skyldig att överföra uppgifterna direkt om den registrerade begär det och om det är tekniskt möjligt.

7.11 Möjlighet att använda sig av uppförandekoder

Dataskyddsförordningens olika regler ställer krav på dem som behandlar personuppgifter. Inom olika branscher används uppförandekoder och standarder för att säkerställa att man agerar på rätt sätt. De verktygen kan även användas för dataskydd. I artikel 24.3 anges att tillämpning av godkända uppförandekoder och certifieringar, sigill eller märkningar får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter. Se även artikel 40 och 42.

Uppförandekoder förbereds av branscher och sektorer för att företag ska kunna certifiera sig enligt dem. Tanken är att uppförandekoder och tillhörig certifiering kommer att kunna ske på likartade sätt som kring exempelvis ISO 9000-standarder. Datainspektionen kommer kunna godkänna uppförandekoder så snart som möjligt efter 25 maj 2018.

7.12 Utökade möjligheter att agera för Datainspektionen

Dataskyddsförordningen innebär att tillsynsmyndigheterna i medlemsstaterna får vissa utökade möjligheter att agera. En förändring är att medborgarna ska kunna vända sig till ”sin” tillsynsmyndighet även om deras klagomål rör ett företag i ett annat EU-land.

En annan förändring är att de nationella tillsynsmyndigheterna ska kunna döma ut en administrativ sanktionsavgift, se nedan 7.15. I och med att tillsynsmyndigheten kan döma ut den behövs alltså inte en domstolsprövning.

7.13 Behandling i annat EU-land

För de företag som har verksamhet i flera olika medlemsstater ska en tillsynsmyndighet vara behörig att agera som ansvarig för gränsöverskridande behandling, den så kallade one-stop-shopmekanismen i artikel 56. Tillsynsmyndigheten är den dataskyddsmyndighet som finns i det land där företaget har sitt huvudsakliga verksamhetsställe eller där företagets beslut om behandling fattas, se artikel 4.16.

Klagomål på hur en persons uppgifter hanteras ska kunna lämnas till tillsynsmyndigheten i det land där personen bor, arbetar eller där det påstådda intrånget begicks, artikel 77. Detta gäller alltså oavsett var företaget finns som gör behandlingen.

7.14 Undantaget om ostrukturerad information försvinner

Enligt 5a § PUL finns ett undantag beträffande behandling av personuppgifter som görs i ostrukturerad form, såsom löpande text i mejl eller mötesanteckningar. Det saknas ett liknande undantag i dataskyddsförordningen, vilket gör att även behandling som görs i ostrukturerad form från 2018 kräver lagligt stöd.

Dataskyddsförordningen gäller inte retroaktivt men den behandling av personuppgifter som sker genom att äldre dokument innehåller personuppgifter ska följa kraven i dataskyddsförordningen. Detta innebär att det kan behöva göras stora rensningar i gamla filer. Finns fortfarande stöd för behandlingen kan de gamla filerna ligga kvar, saknas stöd ska filerna rensas bort.

7.15 Förändrade sanktioner

De företag som agerar i strid med reglerna i dataskyddsförordningen riskerar flera olika sanktioner. Hit hör att den personuppgiftsansvarige eller personuppgiftsbiträdet har ett skadeståndsansvar gentemot den person som lidit materiell eller immateriell skada enligt artikel 82. Skadestånd döms ut av domstol i det land där den registrerade har sin hemvist eller där företaget är etablerat. Personuppgiftsansvarig och personuppgiftsbiträde kan vara solidariskt skadeståndsansvariga gentemot den registrerade, se artikel 82.

Den största förändringen i förhållande till vad som gäller idag är att det också införs något som kallas för administrativ sanktionsavgift enligt artikel 83. Den administrativa sanktionsavgiften kan uppgå till det högsta av 20 miljoner euro eller 4 procent av den globala årsomsättningen på koncernnivå.

Sanktionsavgiften kan påföras av tillsynsmyndigheten utöver eller i stället för de korrigerande åtgärderna i artikel 58.2, till exempel utfärdande av varning, reprimand eller föreläggande om rättelse och radering.

Sanktionsavgifter kan påföras en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte fullgör sina skyldigheter enligt förordningen.

De högsta beloppen utdöms för brott mot de grundläggande principerna för behandling såsom villkoren för samtycke, känsliga personuppgifter och de registrerades rättigheter som till exempel rätt till information, radering eller överflyttning (portabilitet) av uppgifter.

Små och medelstora företag, SME, med upp till 250 anställda är undantagna krav på registerföring enligt artikel 30.5 om behandlingen är tillfällig och inte riskfylld. I skäl 82 uppmanas tillsynsmyndigheterna att ta särskild hänsyn till SMEs särskilda behov vid tillämpning av dataskyddsförordningen. Än så länge finns ingen vägledning att tillgå som förklarar vad som närmre avses med dessa skrivningar.

8. Personuppgifter om personer utanför företaget

8.1 Kunder

En stor del av de kommande reglerna är bekanta om man arbetat med PUL. Det gäller framför allt själva grundstrukturerna och en del av begreppen. Vid sidan av detta finns också viktiga nyheter. Företag har ofta ett stort behov av att behandla personuppgifter i relation till sina kunder. De företag som främst riktar in sig på konsumenter kan behöva hantera kundlistor, kundklubbar och liknande.

För att behandla dessa personuppgifter krävs att det går att hitta ett stöd. När det gäller personuppgifter om befintliga kunder går det normalt att hänvisa till att behandlingen av personuppgifterna är nödvändigt för att företaget ska kunna fullfölja sin del av ett avtal. När det gäller kundklubbar och liknande kan behandlingen av personuppgifter ibland sträcka sig längre än vad som är nödvändigt för att fullfölja konkreta avtal. Behandlingen av personuppgifter kan då behöva stödja sig på ett samtycke. (Hänvisning till hur samtyckesreglerna ändras).

De företag som främst säljer till företag och myndigheter kan till viss del komma undan när det gäller behovet av att hitta stöd för att behandla uppgifter om kunderna. En kundlista kan då upprättas utan att behöva behandla personuppgifter. Det kan dock finnas behov av att behandla uppgifter om kontaktpersoner.

Stöd för att behandla kontaktpersoners personuppgifter kan finnas av flera skäl. Det kan vara nödvändigt att behandla personuppgifter för att företaget ska kunna fullgöra det som avtalet handlar om. Det kan till exempel handla om att det är kontaktpersonen som ska ta emot en viss leverans eller är den som samarbete ska ske med under ett uppdrag.

Ett annat skäl för att behandla uppgifter om kontaktpersoner är att samtycke inhämtas. Detta samtycke ska inhämtas från den person det faktiskt gäller och inte från dennes kollega eller chef.

Vissa verksamheter innebär en risk för att känsliga personuppgifter kan komma att behandlas. Det kan handla om att kunderna behöver dela med sig av till exempel information om sin hälsa. Då är det särskilt viktigt att det finns ett tydligt stöd för behandling av uppgifterna. Det går då inte att hänvisa till intresseavvägningen.

En annan typ av uppgifter som inte kan hanteras hur som helst gäller uppgifter om barn. Många gånger måste inhämtning av samtycke för att behandla barns personuppgifter inhämtas från föräldrarna.

Mycket av behandlingen av kunders personuppgifter stödjer sig på en pågående relation. När kundrelationen har upphört är det viktigt att stödet för behandling av personuppgifter omprövas. Argumentet att det är nödvändigt att behandla personuppgifterna för att fullfölja ett avtal gäller inte när själva avtalet är fullföljt. I praktiken innebär detta att det är viktigt att rensa bort personuppgifter från avslutade kundrelationer.

8.2 Potentiella kunder

Många företag arbetar aktivt med att hitta nya kunder. För att behandla personuppgifter om nya kunder (eller kontaktpersoner hos företag) går det inte att hitta stöd i att behandlingen sker för att fullfölja ett avtal. Det finns helt enkelt inget avtal än.

I vissa fall kan det hänvisas till intresseavvägningen som stöd för att behandla personuppgifter om potentiella kunder.

I dataskyddsförordningen finns en regel som gör att den vars personuppgifter behandlas kan göra en invändning mot att personuppgifterna behandlas för direkt marknadsföring, art. 21. Denna rätt är absolut, vilket innebär att om en sådan invändning görs får inte personuppgifterna längre behandlas, se art. 21.3.

Det som står i art. 21 om direkt marknadsföring gäller även för profilering.

Informationen om rätten att göra invändning mot behandlingen av personuppgifter ska lämnas av den som behandlar personuppgifterna. Denna information ska lämnas senast vid den första kommunikationen med personen. Kravet är, enligt art. 21.4, att informationen lämnas på ett tydligt sätt som är åtskilt från övrig information som lämnas. Detta är alltså inte något som ska döljas i en större textmassa eller i finstilt text.

8.3 Samarbetsparter

För många företag är samarbeten viktiga för att få verksamheten att fungera. När det gäller uppgifter om företag som man samarbetar med innebär inte detta nödvändigtvis att personuppgifter behandlas. Det är först när det sker anteckningar kring kontaktpersoner och liknande som det finns anledning att se om det finns stöd för behandlingen i dataskyddsreglerna.

Om det är nödvändigt att behandla uppgifter om en kontaktperson för att kunna fullfölja ett samarbetsavtal är det en giltig grund för att behandla personuppgifterna. Det kan också vara så att en intresseavvägning ger vid handen att det är intresset av att få behandla personuppgifterna som väger tyngre än personens intresse av personlig integritet.

Ett ytterligare skäl till att få behandla personuppgifter om kontaktpersoner hos samarbetspartners är att det kan inhämtas samtycke. Detta kan vara särskilt lämpligt när det gäller personer som inte direkt ingår i det direkta samarbetet men vars uppgifter man av olika skäl ändå ser ett behov av att ha kvar. Det kan till exempel handla om uppgifter till en kollega till kontaktpersonen eller till en person som kanske senare kan komma att bli en kontaktperson.

Samtycket ska, som alltid, vara informerat. Det är alltså viktigt att det tydligt informeras om att personuppgiften kommer att behandlas och vad denna behandling syftar till.

Vid organisationsförändringar hos en samarbetspartner kan kontaktpersoner försvinna som kontaktpersoner men ändå vara kvar hos samarbetspartnern. I sådana lägen är det viktigt att se över stödet för att fortsätta behandla personuppgiften. I många fall måste uppgiften rensas bort eller ett samtycke inhämtas för att fortsatta behandla uppgiften.

8.4 Leverantörer

Uppgifter om kontaktpersoner hos leverantörer kan ofta behöva behandlas för att säkerställa att leveranser sker, att de sker på rätt sätt och vid rätt tidpunkt. Behandlingen av uppgifter kring kontaktpersoner kan ofta hänvisas till att det är nödvändigt för att fullfölja åtaganden i avtal.

När det sker förändringar beträffande kontaktpersoner behöver rensning ske av personuppgifterna. Det finns då inte längre stöd att behandla uppgifterna genom att hänvisa till åtaganden i avtal.

Om det finns någon anledning att fortsätta behandla personuppgifter om en tidigare kontaktperson hos en leverantör bör samtycke inhämtas. Det kan visserligen vara så att intresseavvägningen ger vid handen att en fortsatt behandling har rättsligt stöd, men detta kan vara svagt. Det är därför ofta bättre att inhämta ett uttryckligt samtycke.

8.5 Hemsida

Nästan alla verksamheter har idag egna hemsidor. På hemsidorna publiceras ibland olika typer av personuppgifter. Det kan handla om en kund som uttalar sig om en vara eller tjänst. Det kan också handla om andra personer som av någon anledning är intressanta att ha med på hemsidan.

Om hemsidan har ett utgivningsbevis från Myndigheten för press, radio och tv behöver inte reglerna om dataskydd tillämpas. Det är då möjligt att publicera namn, bild och liknande för olika personer. Detta helt utan att fråga dem om tillstånd.

Om hemsidan inte har ett utgivningsbevis kan reglerna om dataskydd behöva beaktas. I vissa fall kan publicering av personuppgifter på hemsidan ändå vara tillåten, med hänvisning till att publiceringen sker av journalistiskt ändamål.

För publicering på hemsidor kan det vara särskilt viktigt att tänka på de känsliga uppgifterna. Uppgifter om till exempel hälsa och politisk åskådning bör hållas borta från hemsidespublicering. Finns det en önskan om att publicera uppgifterna bör uttryckliga samtycken inhämtas.

8.6 Evenemang

I samband med evenemang av olika slag, såsom mässor eller konferenser, kan det vara lockande att spara uppgifter om deltagarna för att senare kunna kontakta dem av olika skäl.

När det gäller en aktuell aktivitet är det självklart att behandling av personuppgifter får ske för att administrera den. Behandlingen kan behöva ske för att skapa en deltagarlista och kanske skicka en faktura i efterhand. Det finns då en relation som medför rätt att behandla personuppgifter för att fullfölja ett åtagande.

Det är dock inte tillåtet att rakt av ta personuppgifter från deltagarlistor och använda dem för andra ändamål. Det är alltså viktigt att rensa ut personuppgifter efter att aktiviteter genomförts. Om det finns önskemål om att använda personuppgifterna för andra ändamål måste samtycke inhämtas. För att samtycke ska kunna lämnas krävs att den det gäller får tillräcklig information om vad syftet bakom behandlingen av personuppgifterna är.

Vid evenemang kan många gånger så kallade känsliga uppgifter komma att behandlas. De känsliga uppgifter som kan komma att hanteras i samband med evenemang är särskilt uppgifter om hälsa och religiös tillhörighet. I samband med evenemang bjuds kanske på något att äta eller dricka. Då ska ett informerat samtycke inhämtas från deltagaren i anmälan där grunden för behandlingen anges som ”samtycke”.

I anmälningsformuläret finnas då ofta möjlighet att tala om ifall man lider av någon allergi eller av annat skäl inte äter allt. Sådan information är känsliga uppgifter, eftersom det av uppgifterna kan framgå religiös tillhörighet och/eller hälsotillstånd.

Det är tillåtet att hantera uppgifterna i samband med genomförandet av evenemanget. Det är också nödvändigt att behandla uppgifterna för att kunna fullfölja åtaganden i samband med själva evenemanget. Efter genomförda evenemang bör dock den här typen av uppgifter snarast rensas bort. Känsliga personuppgifter ska inte finnas med på till exempel deltagarlistor.

9. Personuppgifter inom företaget

9.1 Anställda

En arbetsgivare kan ha många skäl till att behandla personuppgifter om de anställda. Många av dessa skäl ligger i linje med de regler kring stöd för behandling som finns såväl i PUL som i dataskyddsförordningen.

Centralt är att arbetsgivaren ofta behöver behandla personuppgifter som ett led i själva avtalsrelationen. Det kan handla om att behandla personuppgifter i lönesystemet för att kunna betala ut lön. Det kan också handla om att behandla personuppgifter i inpasseringssystem eller liknande för att rätt lön ska kunna betalas ut.

I vissa fall kan det finnas anledning att fundera särskilt på vilket stöd som finns för behandlingen. Det kan till exempel gälla önskemål om att publicera namn och bild på de anställda på hemsidan. Har hemsidan utgivningsbevis behöver inte samtycke inhämtas. I annat fall kan det ofta vara lämpligt att inhämta samtycke även om det kanske kan finnas stöd i gällande rätt för att behandla personuppgifter på hemsidan.

Enligt PUL kan stöd för att behandla uppgifter om de anställda på en hemsida ofta hämtas från den så kallade missbruksregeln i 5a § PUL. Den innebär att behandling som sker i ostrukturerat material är tillåten. Detta undantag försvinner i och med att dataskyddsförordningen träder i kraft.

I vissa fall kan det i anställningsrelationen uppkomma behov av att behandla känsliga personuppgifter. I en del fall kan stöd finnas för att behandla dessa uppgifter eftersom det kan vara nödvändigt för att till exempel uppfylla skyldigheter och rättigheter inom arbetsrätten. Det kan till exempel handla om krav som ställs i samband med rehabilitering.

9.2 Rekrytering

I samband med rekrytering får företag in många personers uppgifter. Under själva rekryteringsprocessen är det tillåtet att behandla uppgifterna, men när rekryteringsprocessen är avslutad ska uppgifterna rensas.

Denna rensning kan dock behöva avvaktas något om det finns anledning att anta att någon gör en invändning mot hur rekryteringen gått till. Finns till exempel en risk att någon hävdar att urvalet baseras på diskriminering måste uppgifterna finnas kvar för att kunna bemöta sådana påståenden. Rensningen måste alltså då sättas i relation till preskriptionsreglerna i diskrimineringslagen.

9.3 Före detta anställda

När anställningar har avslutats ska personuppgifterna rensas bort eftersom de skäl som finns för behandling av personuppgifterna inte längre finns kvar. Uppgifterna behöver inte rensas ut omedelbart utan först när alla åtaganden upphört. Behandling som sker av skatterättsliga skäl måste till exempel fortsätta tills dessa skäl upphört.

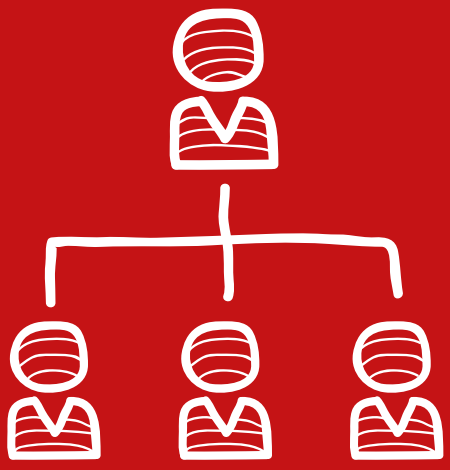
Hos en del arbetsgivare finns olika former av alumninätverk som till exempel pensionärsklubbar. Behandlingen av personuppgifter i de sammanhangen kan med fördel hanteras genom att samtycke inhämtas. Blir personerna medlemmar får uppgifterna hanteras med hänvisning till att det behövs för medlemskapets skull.

9.4 Sanktioner

Den arbetsgivare som bryter mot reglerna om skydd för personuppgifter i relation till personer inom företaget riskerar flera olika sanktioner. Förutom sanktionsavgift vid tillsyn av datainspektionen och skadestånd till enskild som lidit skada kan skadeståndsreglerna inom arbetsrätten bli tillämpliga.

Inventera hur uppgifter om anställda hanteras

- rekryteringsunderlag
- anställningsavtal
- utvärderingar och analyser



10. Ansvars-struktur

Den som är ansvarig för behandlingen av personuppgifterna inom en verksamhet är normalt sett den juridiska personen som därmed är den personuppgiftsansvariga. Det innebär att det är den egna organisationen som är ansvarig. Det faktum att det är en anställd i organisationen som fattat beslutet om behandlingen innebär inte att den individen blir personuppgiftsansvarig.

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning är ett personuppgiftsbiträde. Ett personuppgiftsbiträde finns utanför den personuppgiftsansvariges organisation och får bara behandla personuppgifter enligt givna instruktioner.

Mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska det finnas ett skriftligt avtal. I avtalet ska anges att personuppgiftsbiträdet bara får behandla personuppgifterna i enlighet med instruktionerna samt att biträdet måste vidta lämpliga åtgärder för att skydda personuppgifterna.

Ett företag som är personuppgiftsbiträdet har eget ansvar för registerföring, artikel 30, tillräckliga säkerhetsåtgärder, artikel 32, och att utse dataskyddsombud, artikel 37. Företaget har skadeståndsansvar och kan ådömas sanktionsavgifter, se artikel 82 och 83.

Den personuppgiftsansvarige har ett tydligt ansvar för att kontrollera att personuppgiftsbiträdet inte agerar i strid med avtal och fastlagda rutiner, se artikel 28.3h. Den personuppgiftsansvarige kan göra inspektioner hos personuppgiftsbiträdet som då har skyldighet att tillhandahålla all information som krävs för att fastställa att personuppgiftsbiträdet agerat korrekt enligt artikel 28.

Glöm inte:

- Utbilda företagets personal i dataskydd
- Undersök om företaget har skyldighet att tillsätta ett dataskyddsombud
- Skapa rutiner för löpande uppföljning och utvärdering

11. Åtgärder att vidta inför de nya reglerna

11.1 Betydelsen av att börja direkt

Dataskyddsförordningen ska tillämpas från den 25 maj. Med tanke på att de nya reglerna kan medföra ett behov av att se över organisation, rutiner och IT-system kan det dock vara klokt att börja anpassningen till de nya reglerna redan nu.

Fram till att dataskyddsförordningen träder i kraft kommer olika typer av riktlinjer publiceras och Datainspektionen kommer att ha ett stort informationsansvar. Datainspektionen håller bland annat utbildningar runt om i landet. Information om det nya regelverket finns på: datainspektionen.se/dataskyddsreformen.

Det är fortfarande oklart hur tolkningen av förordningen ska ske i en del avseenden. Dataskyddsmyndigheterna kommer att presentera fler riktlinjer under året genom sitt samverkansorgan artikel 29-gruppen. I maj kommer den svenska dataskyddsutredningen med sitt betänkande om dataskyddsförordningen och ett nytt svenskt regelverk.

För att inte missa information är det bra att utse en person i organisationen som är ansvarig för att bevaka utvecklingen. Den personen kan också ha ansvar för att se över vilka åtgärder som behöver göras för att följa dataskyddsförordningen.

11.2 Några saker som kan behöva göras

En av de viktigaste sakerna att börja med är att skapa en samsyn i organisationen kring hur frågan om anpassning till dataskyddsförordningen ska gå till. För att kunna skapa denna samsyn behövs också en insikt i organisationen om betydelsen av att hantera personuppgifter korrekt.

11.3 Inventering

Ett första steg i en anpassning till de nya reglerna kan vara att göra en inventering av vad som faktiskt sker i organisationen idag.

Inventeringen kan göras med utgångspunkt i följande frågor:

– Vilka personuppgifter hanteras i organisationen?
– I vilka system behandlas personuppgifter?
– Vem/vilka är processägare?
– Vilket rättsligt stöd finns för den behandling som görs?
– I vilken mån förändras detta rättsliga stöd i och med dataskydds-förordningen? (T ex genom att missbruksregeln försvinner.)
– Vilka avtal och överenskommelser finns idag beträffande behandling av personuppgifter?
– Hur ser rutinerna ut för inhämtning av samtycke? Hur fungerar det i praktiken?
– Hur ser rutinerna ut för radering och gallring av personuppgifter? Hur fungerar det i praktiken?

11.4 Beslut om organisation

Utifrån resultatet av inventeringen behöver beslut fattas om hur själva organisationen kring hanteringen av dataskyddsfrågor ska se ut. Såsom dataskyddsförordningen är konstruerad ställs krav på att organisationen kan hantera vissa frågor på ett skyndsamt sätt. Det är därför nödvändigt att se till att organisationen kan hantera exempelvis rapportering om personuppgiftsincidenter.

11.5 Anpassning av IT-system

Datainspektionen menar att många av de krav som ställs i dataskydds-förordningen kan hanteras genom ”privacy by design”. Med detta avses att IT-systemen utformas på ett sådant sätt att lagens krav har beaktats. Det kan förväntas att tydligare riktlinjer för detta kommer att utvecklas under tiden fram till den 25 maj 2018. Detta sker bland annat via den hänvisning som kommer kunna göras till uppförandekoder såsom är reglerat i art. 41.

Checklista åtgärder att vidta

- ☑ Finns en samsyn i organisationen på vad som behöver göras?
- ☑ Har ni kontroll över de personuppgifter ni behandlar och på vilket sätt?
- ☑ Se över organisationen, beslutsstrukturer och rutiner.
- ☑ Säkerställ att IT-systemen uppfyller nuvarande och kommande krav.

Form & produktion: Herlin Widerberg Tryck: Arkitektkopia

Från den 25 maj 2018 gäller dataskyddsförordningen i Sverige och övriga medlemsstater i EU. Den ersätter då personuppgiftslagen, PUL. Teknikutvecklingen går snabbt framåt. Lagar och regler behöver ses över för att vara relevanta. Vad gäller personuppgiftsskydd har ambitionen varit att balansera integritetsskydd och innovationsmöjligheter. Med den nya lagstiftningen på plats kan vi konstatera att den uppgiften varit svår att lyckas med. Företagen har fått en omfattande läxa att göra för att leva upp till lagstiftarens förväntningar. Syftet med den här skriften är att beskriva de nya reglerna och hur de påverkar företagens hantering av personuppgifter.

Lagtext och mer information finns på
www.datainspektionen.se/dataskydd

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

SVENSKT NÄRINGSLIV