GDPR-guide

CloudPro

EN DEL AV COMBINED EXCELLENCE

Innehåll

1. Inledning

Kärt barn har många namn och i Sverige har den nya europeiska dataskyddsregleringen inte mindre än tre stycken: General Data Protection Regulation, dataskyddsförordningen och GDPR. Du har säkert hört dem alla förut, men om du inte har det är den här guiden en bra plats att börja.

Dataskyddsförordningen är, precis som namnet antyder, en europeisk förordning som reglerar skydd av data inom EU. Den träder i kraft den 25 maj 2018 och ersätter då personuppgiftslagen (PUL). Efter det datumet förväntas det att alla som berörs av förordningen lever upp till dess krav. Men det är långt ifrån solklart exakt vilka krav det rör sig om, eftersom det kommer att komma tolkningar från EU-domstolen och Integritetsskyddsmyndigheten (ISM) från dagen för ikraftträdande och under flera år framöver. Dessa tolkningar kommer att precisera innebörden i GDPR:s bestämmelser. Men det betyder inte att du och din organisation är fria från ansvar. Så vad ska du göra?

Den här guiden innehåller information, tips och hjälp som du kan använda dig av när din organisation arbetar för att anpassa sin verksamhet till GDPR. Den hjälper dig med vad som är viktigast att hinna med innan den 25 maj 2018 och vad du kan avvakta med i väntan på preciseringar. Tanken med guiden är att den ska ge en översiktlig men klar och tydlig bild av de viktigaste delarna av GDPR – så att din tolkning av själva förordningen ska bli betydligt mindre trögflytande.

Genom att läsa den här guiden kommer du att lära dig:

- Vad GDPR är, vad den innebär i praktiken och vilka som kommer att behöva följa den.
- Vad personuppgifter är för något.
- Vad som menas med ”laglig grund” och vad varje sådan grund innebär.
- Vilka krav som ställs på ett giltigt samtycke enligt GDPR.
- Vad känsliga personuppgifter är för något och när sådana får behandlas.
- Vilka rättigheter individer har till sina personuppgifter.
- Vad en personuppgiftsincident är för något och hur man ska agera när en sådan inträffar.
- Vad ett dataskyddsombud är för något och när ett sådant ska anlitas.
- Vad en konsekvensbedömning är för något och när en sådan ska göras.
- Vad som menas med behandlingsregister, *privacy by design* och ”tekniska och organisatoriska säkerhetsåtgärder”.
- Vad som gäller för små och medelstora företag under GDPR.
- Vad som gäller särskilt enligt svensk lag.
- Hur du håller dig uppdaterad om GDPR och relaterade bestämmelser.
- Vilka övergripande steg som behöver tas för att anpassa sig till GDPR, samt tips på hur detta kan göras.
- Hur CloudPro kan hjälpa dig med ditt anpassningsarbete.

2. GDPR – dataskyddsförordningen

2.1 Vad är det för något?

Syftet med GDPR är att uppnå en enhetlig dataskyddslagstiftning i EU och på så sätt stärka individers rättigheter. Många av GDPR:s regler liknar de som idag finns i PUL. De största förändringarna jämfört med PUL är att de registrerades (personerna vars uppgifter behandlas av en personuppgiftsansvarig) rättigheter utökas, att sanktioner som drabbar sådana personuppgiftsansvariga vars personuppgiftsbehandling inte följer lagen blir hårdare och att kraven på personuppgiftsansvariga i övrigt skärps.

GDPR träder i kraft den 25 maj 2018 och kommer då att vara direkt gällande som svensk lag. I Sverige kommer även en kompletterande dataskyddslag att träda i kraft samma datum.

2.2 Vilka berörs?

GDPR kommer att påverka:

a) all verksamhet som inte är av rent privat natur,
b) som innebär behandling av personuppgifter (se Grundläggande definitioner),
c) vilken sker automatiserat eller, om ett sökbart register förs över uppgifterna, manuellt (se Gäller GDPR för all personuppgiftsbehandling?),
d) och som har en koppling till EU på något av följande sätt:
    a. den personuppgiftsansvarige eller personuppgiftsbiträdet (se Grundläggande definitioner) är etablerad inom EU;
    b. behandlingen av personuppgifter avser registrerade som befinner sig inom EU och har anknytning till utbjudande av varor eller tjänster eller till övervakning av de registrerades beteende; eller
    c. den personuppgiftsansvarige är etablerad på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

Verksamheter som inte omfattas av EU-rätten eller som utförs inom ramen för den gemensamma utrikes- och säkerhetspolitiken täcks dock inte av GDPR, förutom vid tillämpningen av den föreslagna dataskyddslagens bestämmelser (se Den svenska dataskyddslagen).

Det vida tillämpningsområdet innebär att i princip alla företag, myndigheter, kommuner, föreningar och enskilda som har en anknytning till EU måste följa dataskyddsförordningens regler. Rent privat behandling av personuppgifter, t.ex. upprättande av en privat lista över vänners telefonnummer, täcks dock inte.

2.3 Vad innebär det?

Om din verksamhet berörs av GDPR innebär det att du måste förbereda dig inför ikraftträdandet. Den 25 maj 2018 vill du åtminstone ha koll på:

- vilka behandlingar som utförs inom din verksamhet;
- att alla dessa behandlingar har berättigade ändamål och bygger på lagliga grunder;
- att du har tillräckliga processer och rutiner på plats för att kunna vidta åtgärder på begäran från en registrerad; och
- att du i övrigt har inrättat processer och rutiner för bl.a. incidenthanteringar och riskanalyser.

Du måste också se till att alla anställda får en tillräcklig utbildning om hur GDPR påverkar deras arbete – utan kompetenta människor finns det inte någon särskilt stor mening med rutiner.

2.4 Vad är personuppgifter?

Med personuppgifter menas all information (”varje upplysning”) som direkt eller indirekt går att koppla till en identifierbar levande person, särskilt med hänvisning till en identifierare såsom namn, personnummer, lokaliseringsuppgifter eller onlineidentifikatorer eller faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Mailadresser, telefonnummer och bilder är några vanliga exempel på personuppgifter.

Elektroniska identiteter kan räknas som personuppgifter om de går att koppla till levande personer. Exempel är IP-nummer och så kallade ”cookies” som lagrar information om en användares besök på en webbplats. Även uppgifter som är krypterade, anonymiserade eller på annat sätt avidentifierade är personuppgifter om de med hjälp av kompletterande information (och utan ett allt för omfattande arbete) kan kopplas till en fysisk levande person.

2.5 Grundläggande definitioner

Här är några andra begrepp som är bra att ha koll på i läsningen av denna guide.

Artikel 29-gruppen

Denna grupp kom till 1996 genom dataskyddsdirektivets artikel 29 (därav namnet). Den består av en företrädare för varje nationell tillsynsmyndighet i EU-medlemsstaterna, en företrä-

	dare för EU-kommissionen samt den europeiska datatillsynsmannen. En av gruppens uppgifter är att ge vägledning gällande tolkningen av europeisk dataskyddslagstiftning.
Behandling	Alla åtgärder som vidtas i fråga om personuppgifter, t.ex. insamling, lagring och bearbetning.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Alla som kommer åt eller kan komma åt personuppgifter är personuppgiftsbiträden, t.ex. leverantörer av system innehållande personuppgifter.
Registrerade	De fysiska, levande personer vars personuppgifter behandlas.
Tillsynsmyndighet	Den nationella myndighet som ska övervaka att GDPR efterlevs i landet. I Sverige är det Integritetsskyddsmyndigheten (ISM) som kommer att vara tillsynsmyndighet enligt GDPR (se Grundläggande definitioner). På ISM:s hemsida (www.Integritetsskyddsmyndigheten.se) läggs kontinuerligt ut information om dataskyddsreformen samt om hur GDPR ska tolkas och efterlevas.

2.6 Gäller GDPR för all personuppgiftsbehandling?

All behandling av personuppgifter täcks inte, även om verksamheten har en koppling till EU. GDPR gäller för två olika typer av behandlingar:

a) helt eller delvis **automatiserad** behandling, och
b) manuell behandling som ingår i eller kommer att ingå i ett **register.**

Med automatiserad behandling menas att personuppgifterna behandlas elektroniskt i någon form av system. Det spelar här ingen roll om personuppgifterna lagras i löpande text eller i register. Härmed upphävs alltså den så kallade ”Missbruksregeln” som infördes genom PUL.

Vad gäller manuell behandling ingår dock inte personuppgifter som behandlas på lösa pappersark eller som inte går att söka igenom på ett enkelt sätt – det måste röra sig om register som exempelvis

förvaras i en pärm och i vilket man kan söka på en personuppgift för att hitta en specifik post. Behandling som inte listas i ett register ska följa GDPR:s regler om tanken är att uppgifterna kommer att föras in i ett sådant register.

2.7 Grundläggande principer

GDPR har sex grundläggande principer för personuppgiftsbehandling:

1. **Laglighet, korrekthet och öppenhet.** Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt gentemot den registrerade.

2. **Ändamålsbegränsning.** Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får senare inte behandlas på ett sätt som går emot dessa ändamål.

3. **Uppgiftsminimering.** Personuppgifter ska vara adekvata, relevanta och inte för omfattande för behandlingens ändamål.

4. **Korrekthet.** Personuppgifter ska vara korrekta och uppdateras vid behov.

5. **Lagringsminimering.** Personuppgifter får inte lagras på ett sådant sätt att de kan användas för att identifiera en registrerad under en längre period än vad behandlingsändamålen kräver.

6. **Integritet och konfidentialitet.** Lämplig säkerhet ska säkerställas för personuppgifter som behandlas, så att obehörig eller otillåten behandling, förlust, förstöring eller skada genom olyckshändelse kan undvikas.

En nyhet jämfört med PUL är en sjunde princip, nämligen principen om **ansvarsskyldighet** som innebär att den personuppgiftsansvarige ansvarar för att ovanstående principer efterlevs i all personuppgiftsbehandling som utförs under dennes ansvar och ska kunna visa att GDPR följs. I övrigt motsvarar GDPR:s principer de som redan finns i PUL.

2.8 Konsekvenser av att inte uppfylla GDPR:s krav

Till skillnad från vad som gäller enligt PUL, kommer GDPR inte att medföra någon risk för böter eller fängelse vid olaglig personuppgiftsbehandling. Däremot introduceras höga så kallade sanktionsavgifter som kan komma i fråga för personuppgiftsansvariga företag som bryter mot GDPR:s bestämmelser. Dessa sanktionsavgifter, som har ett tak på 20 miljoner euro eller 4% av den globala årsomsättningen (beroende på vilket som är högst), har utan tvekan en potential att bringa företag i konkurs. I Sverige

har det dessutom föreslagits att även myndigheter ska kunna drabbas av sanktionsavgifter, dock endast upp till ett tak på 20 miljoner SEK.

Sanktionsavgifter är dock inte det enda personuppgiftsansvariga behöver oroa sig för – fysiska personer som har ”lidit materiell eller immateriell skada till följd av en överträdelse av [GDPR]” kan begära skadestånd från den personuppgiftsansvarige eller personuppgiftsbiträdet. I praktiken är detta troligtvis den största risken, eftersom Integritetsskyddsmyndigheten i nuläget har långt ifrån de resurser som skulle krävas för att se så att GDPR följs.

2.9 Fördelar och möjligheter

För personuppgiftsansvariga kan det kännas som ett enda stort måste-arbete att anpassa sig till den nya dataskyddslagstiftningen, men det är viktigt att komma ihåg att förändringen innebär en större trygghet för individer och dessutom en bra möjlighet för din organisation att gå igenom och förbättra interna processer, rutiner och dokumentation.

De personuppgiftsansvariga som sköter sin personuppgiftsbehandling i enlighet med GDPR kommer dessutom med all sannolikhet att belönas med konkurrensfördelar jämfört med de som släntrar efter. Om din organisation kan visa att den hanterar kunddata på ett sätt som respekterar de registrerades integritet, kommer det att ge ett kännbart resultat.

3. Lagliga grunder

3.1 Sju lagliga grunder

För att få behandla personuppgifter måste behandlingen vila på dels ett berättigat ändamål (se Grundläggande principer), dels minst en av de lagliga grunder som räknas upp i GDPR. Genom att bygga på en laglig grund uppfylls även den första dataskyddsprincipen – att personuppgifterna behandlas på ett lagligt sätt.

- **Samtycke.** Den registrerade har lämnat entydigt, frivilligt och specifikt samtycke.
- **Avtal.** Behandlingen är nödvändig för att fullgöra eller ingå ett avtal.
- **Rättslig förpliktelse.** Behandlingen är nödvändig för att kunna fullgöra en rättslig förpliktelse.
- **Grundläggande intressen.** Behandlingen är nödvändig för att skydda en fysisk persons grundläggande intressen.
- **Allmänt intresse.** Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.
- **Myndighetsutövning.** Behandlingen är nödvändig som ett led i myndighetsutövning.
- **Berättigat intresse.** Behandlingen är nödvändig för ett berättigat intresse hos den personuppgiftsansvarige eller en tredje part, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre.

När personuppgifter samlas in ska den registrerade få information om bland annat vilken laglig grund behandlingen av hens personuppgifter vilar på (se De två informationsrättigheterna). Det måste därför säkerställas redan innan uppgifterna samlas in vilken laglig grund som är aktuell.

Det räcker dock inte att det finns en laglig grund för behandlingen – den måste fortfarande uppfylla resten av kraven som ställs upp i GDPR, såsom de grundläggande principerna.

3.2 Samtycke

*"Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett **frivilligt**, **specifikt**, **informerat** och **otvetydigt** medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring."* (Skäl 32, GDPR)

Samtycke är en laglig grund som kan användas för att få utföra en personuppgiftsbehandling som inte är nödvändig av något annat skäl (det vill säga, som inte har en annan laglig grund).

Kravet på samtycke enligt GDPR är detsamma som enligt PUL, även om formuleringarna skiljer sig något åt. Ett samtycke måste vara frivilligt och otvetydigt, röra ett specifikt ändamål och ges efter att den registrerade har informerats om detta ändamål samt vissa andra detaljer. Även om en person samtycker till att få sina personuppgifter behandlade, är samtycket inte giltigt – och behandlingen därför olaglig – om det inte lever upp till de här kraven.

Även sådana behandlingar som idag bygger på samtycke enligt PUL bör ses över för att kontrollera att samtycket fortfarande är giltigt – inte bara för att säkerställa att GDPR:s krav är uppfyllda, utan också för att undersöka om gamla samtycken behöver förnyas för att de är föråldrade. Ett samtycke håller nämligen inte för evigt och beroende på omständigheterna kan det behöva förnyas med jämna mellanrum.

3.2.1 Frivilligt

För att ett samtycke ska anses ha lämnats frivilligt ska den registrerade ha haft en genuin och fri valmöjlighet i sitt beslut och hen ska kunna vägra eller ta tillbaka samtycket när som helst. Samtycket måste vara avskilt, det vill säga det anses inte ha lämnats frivilligt om till exempel ingåendet av ett avtal kräver att den registrerade samtycker även till annan behandling.

Enligt Artikel 29-gruppen, som tillhandahåller vägledningar gällande tolkningen av europeisk dataskyddslagstiftning, kan arbetstagare i princip aldrig ge ett giltigt samtycke med hänsyn till beroendeställningen mellan hen och arbetsgivaren. För att en arbetstagares samtycke ska vara giltigt måste det ha getts under exceptionella omständigheter, när inga konsekvenser överhuvudtaget är kopplade till en vägran att samtycka.

Utöver att samtycket ska vara frivilligt måste det även lämnas aktivt, vilket innebär att till exempel på förhand ikryssade rutor inte får användas.

3.2.2 Specifikt och informerat

Den registrerade ska vara informerad om vad hen samtycker till och samtycket ska gälla behandling för ett specifikt ändamål.

När samtycke begärs ska den registrerade därför, för att samtycket ska anses giltigt, informeras om:

- Vad samtycket gäller,

- Hur långt samtycket sträcker sig,
- Den personuppgiftsansvariges identitet,
- Eventuellt personuppgiftbiträdes identitet,
- Syftet med behandlingen som samtycket avser, och
- Rätten att ta tillbaka sitt samtycke samt hur hen ska gå tillväga för att utöva den.

Informationen som lämnas ska vara tydlig och otvetydig, så det lönar sig att ge den registrerade så mycket information som möjligt. När samtycke begärs i samband med att personuppgifter samlas in, ska information kopplad till insamlingen också lämnas (se De två informationsrättigheterna).

3.2.3 Otvetydigt

Det ska vara tydligt att den registrerade har samtyckt till en specifik behandling för specifika ändamål och den personuppgiftsansvarige ska kunna bevisa att så är fallet. Exempel på sätt att inhämta giltiga samtycken är:

- Kryssrutor (dock inte på förhand ikryssade sådana, se Frivilligt).
- Underskrift eller digital signering av samtyckesdokument.
- Muntlig förklaring (en skriftlig bekräftelse rekommenderas dock).
- Manuell ändring av tekniska standardinställningar.

3.2.4 Att bevisa samtycke

"Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter." (Art. 7(1), GDPR)

Den personuppgiftsansvarige måste kunna bevisa att samtycke inhämtats och att personen som samtyckt är den registrerade. För att uppfylla det förstnämnda kravet bör varje system innehålla dokumentation över inhämtade samtycken. Bra dokumentation innehåller information om följande:

- Vem som samtyckte;
- Hur hens identitet bekräftades;

- När samtycket inhämtades;
- Vilken information som lämnades vid inhämtande av samtycket;
- Hur samtycket inhämtades;
- Om samtycket har tagits tillbaka och i så fall när; och
- När samtycket bör förnyas.

Ett sätt att bekräfta identiteten på den som samtycker är att kräva ”dubbelt” samtycke, genom att först begära samtycke genom exempelvis en kryssruta på en hemsida och därefter skicka ett mail med en länk som den registrerade måste klicka på för att slutföra processen. Vissa företag har infört en funktion som skickar ett kvitto till den registrerade på att hen har samtyckt, vad hen samtyckt till, hur hens personuppgifter kommer att behandlas, datum, hur länge samtycket är giltigt samt namnet på den personuppgiftsansvarige.

3.2.5 Barns samtycke i sociala nätverk

Särskilda regler gäller för barns användning av vad som i GDPR kallas för ”informationssamhällets tjänster”, det vill säga till exempel sociala nätverkstjänster. För att samtycke till behandling av personuppgifter i ett sådant sammanhang ska vara tillåtet, måste den registrerade enligt GDPR vara minst 16 år gammal. Om den registrerade är yngre än 16 år måste hens vårdnadshavare samtycka till behandlingen.

I Sverige har det föreslagits att åldersgränsen ska sänkas till 13 år.

3.3 Avtal

”Behandling bör vara laglig när den är nödvändig i samband med avtal eller när det finns en avsikt att ingå ett avtal.” (Skäl 44, GDPR)

Avtal som laglig grund gäller bara när den registrerade är, eller avser att bli, part i avtalet i fråga. Enligt ISM är kund- och personaladministrativa system för fakturering eller löneberäkning exempel på sådan personuppgiftsbehandling som kan vila på denna grund.

3.4 Rättslig förpliktelse

Personuppgiftsbehandling får ske om den är nödvändig för att den personuppgiftsansvarige ska kunna efterleva en rättslig förpliktelse. Den rättsliga förpliktelsen behöver inte bygga på en lag, utan kan också framgå av förelägganden, myndighetsbeslut eller domar. I Sverige har GDPR tolkats på så sätt att även avtal, inklusive kollektivavtal, kan innebära rättsliga förpliktelser. Om den registrerade är part i avtalet i fråga är det dock den lagliga grunden för avtal som blir aktuell (se Avtal).

För att en rättslig förpliktelse ska kunna läggas till grund för personuppgiftsbehandling krävs att syftet med behandlingen framgår i författningen eller avtalet eller kan utläsas av beslutet i vilket förpliktelsen finns.

3.5 Grundläggande intressen

"Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv." (Skäl 46, GDPR)

Med grundläggande intressen menas i GDPR sådana intressen som är av avgörande betydelse för en fysisk persons liv. Ett tydligt exempel på en situation där den här grunden kan bli aktuell är när personuppgiftsbehandling är nödvändig för livsavgörande vård i en akut situation och den registrerade inte kan lämna sitt samtycke.

Grundläggande intressen för en annan person än den registrerade bör bara användas som laglig grund om det är uppenbart att ingen annan laglig grund kan användas.

3.6 Allmänt intresse och myndighetsutövning

Enligt dessa lagliga grunder får personuppgifter behandlas om det är nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. I båda fallen ska uppgiften eller myndighetsutövningen grundas på EU-rätt eller svensk rätt.

Den personuppgiftsansvarige måste inte nödvändigtvis vara en myndighet för att kunna använda sig av den här grunden – inte ens vad gäller myndighetsutövningen, eftersom sådan utövning i vissa fall kan utföras även av privata aktörer.

I Sverige regleras personuppgiftsbehandling vid myndighetsutövning ofta i så kallade registerförfattningar, till exempel patientdatalagen, polisdatalagen eller lagen om behandling av personuppgifter inom socialtjänsten. Registerförfattningar går alltid före generella dataskyddsbestämmelser.

3.7 Berättigat intresse

Den sista lagliga grunden innebär att en intresseavvägning görs mellan den personuppgiftsansvariges intresse av att behandla personuppgifter och den registrerades intresse av att skydda sina personuppgifter. Om den avvägningen resulterar i bedömningen att den personuppgiftsansvariges berättigade intresse väger tyngre, får behandlingen utföras.

Ett berättigat intresse kan som exempel finnas när det finns ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige, såsom när den registrerade är kund hos eller arbetar för den ansvarige.

Andra exempel på möjliga berättigade intressen är:

- Att utföra sådan personuppgiftsbehandling som är absolut nödvändig för att förhindra bedrägerier.
- Att behandla personuppgifter för direktmarknadsföring.
- Att överföra personuppgifter inom en koncern för interna administrativa ändamål.
- Att utföra sådan personuppgiftsbehandling som är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet.

Om den registrerade inte rimligen kan förvänta sig någon ytterligare behandling, väger hens intressen troligtvis tyngre än den personuppgiftsansvariges.

4. Känsliga personuppgifter

Känsliga personuppgifter är sådana uppgifter som avslöjar:

a) ras eller etniskt ursprung,
b) sexualliv eller sexuell läggning,
c) politiska åsikter,
d) religiös eller filosofisk övertygelse eller medlemskap i fackförening,
e) genetiska eller biometriska uppgifter, eller
f) uppgifter om hälsa.

Huvudregeln är att behandling av sådana personuppgifter är förbjuden. Det finns dock vissa undantag:

- **Uttryckligt samtycke.** Den registrerade har lämnat uttryckligt samtycke.
- **Berättigad, icke vinstdrivande verksamhet med lämpliga skyddsåtgärder.** Behandlingen utförs inom ramen för sådan verksamhet.
- **Offentliggjorda uppgifter.** Behandlingen rör personuppgifter som offentliggjorts av den registrerade.
- **Arbetsrätten, social trygghet och socialt skydd.** Behandlingen är nödvändig för att skyldigheter ska kunna fullgöras eller rättigheter utövas inom något av dessa områden.
- **Grundläggande intressen.** Behandlingen är nödvändig för att skydda en fysisk persons grundläggande intressen och hen är inkapabel att ge samtycke.
- **Rättsliga anspråk.** Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk.
- **Viktigt allmänt intresse.** Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse.
- **Hälsa och social omsorg.** Behandlingen är nödvändig för hälsa och social omsorg samt sker under ansvar av en yrkesutövare som omfattas av tystnadsplikt.
- **Folkhälsa.** Behandlingen är nödvändig av hänsyn till allmänt intresse på folkhälsoområdet.
- **Arkiv, vetenskap, historia och statistik.** Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Dessa undantag liknar de lagliga grunder som ställs upp för all personuppgiftsbehandling, men det är viktigt att komma ihåg att behandlingen av känsliga personuppgifter *både* måste vila på en laglig grund och falla under ett giltigt undantag från förbudet. Att så är fallet har bekräftats av ISM.

5. Den registrerades rättigheter

5.1 Åtta rättigheter

De flesta rättigheter är sig lika från PUL:s tid, men det finns vissa skillnader. Dessa är de rättigheter som listas för registrerade i GDPR:

1. Rätten till information.
2. Rätten till tillgång.
3. Rätten till rättelse.
4. Rätten till radering.
5. Rätten till begränsning.
6. Rätten till dataportabilitet.
7. Rätten att invända.
8. Rätten att inte bli utsatt för automatiserat beslutsfattande, inklusive profilering.

Alla begäranden som grundas på ovan rättigheter ska som huvudregel besvaras inom en månad efter att de mottogs. Om en begäran är komplicerad eller om den ansvarige har fått en stor mängd begäranden får perioden dock förlängas till tre månader som mest. I ett sådant fall ska den registrerade meddelas om anledningen till förseningen inom den första månaden.

Det finns vissa undantag från den registrerades rättigheter, bland annat vad gäller begäranden som är uppenbart ogrundade eller orimliga, särskilt repetitiva sådana. Sådana begäranden får antingen nekas helt eller beviljas mot en administrativ avgift. Om en begäran nekas helt måste den personuppgiftsansvarige kunna visa att den var uppenbart ogrundad eller orimlig.

Om det inte går att identifiera den registrerade får en begäran om tillgång, rättelse, radering, begränsning eller dataportabilitet vägras såvida inte den registrerade kan lämna in information som bekräftar hens identitet.

5.2 De två informationsrättigheterna

Den registrerades rätt till information innebär att den personuppgiftsansvarige ska lämna information om vad personuppgifterna kommer att användas till. Detta görs vid insamlingen om uppgifterna samlas in från den registrerade själv och inom en månad om uppgifterna härstammar från en annan källa.

Den andra rättigheten, rätten till tillgång, innebär en rätt att få viss information på begäran under behandlingens gång, i samband med ett utdrag av den registrerades personuppgifter. Rätten att få ett utdrag av sina personuppgifter medför att den personuppgiftsansvarige måste kunna lämna ut en kopia av de uppgifter som denne behandlar.

All information till den registrerade ska lämnas kostnadsfritt i en koncis, lättillgänglig, skriftlig (exempelvis elektronisk) form och med användande av ett tydligt och enkelt språk.

Information som ska lämnas	Vid insamling från den registrerade	Vid insamling från annan källa	På begäran under behandlingens gång
Personuppgiftsansvarigs identitet och kontaktuppgifter	X	X	
Dataskyddsombuds identitet och kontaktuppgifter	X	X	
Ändamål	X	X	X
Laglig grund	X	X	
Kategorier av personuppgifter		X	X
Ev. berättigat intresse till grund för intresseavvägning	X	X	
Mottagare av uppgifter	X	X	X
Överföring av uppgifter till tredje land	X	X	X
Lagringstid	X	X	X
Den registrerades rättigheter	X	X	X
Rätten att ta tillbaka ett samtycke	X	X	
Rätten att lämna klagomål till Integritetsskyddsmyndigheten	X	X	X
Skyldighet att lämna uppgifterna enligt avtal eller lag	X		
Automatiserat beslutsfattande	X	X	X
Källa varifrån uppgifterna har hämtats		X	X
Behandling för annat ändamål än det ursprungliga	X	X	

5.3 Rätten till rättelse

Om den registrerades personuppgifter är felaktiga eller ofullständiga har hen en rätt att få uppgifterna rättade respektive kompletterade om de är relevanta för behandlingens ändamål. I det fall den personuppgiftsansvarige har lämnat ut personuppgifterna till någon annan ska mottagaren meddelas om att uppgifterna har rättats eller kompletterats, om det inte visar sig omöjligt eller alltför betungande.

5.4 Rätten till radering

Den här rättigheten kallas även för ”rätten att bli bortglömd” (på engelska, *the right to be forgotten*) och innebär att en registrerad har rätt att få sina personuppgifter raderade om något av följande gäller:

a) Uppgifterna är inte längre nödvändiga för behandlingens ändamål;

b) Den registrerade återkallar sitt samtycke eller invänder mot behandlingen;

c) Uppgifterna har behandlats på ett olagligt sätt;

d) Uppgifterna måste raderas för att uppfylla en rättslig förpliktelse; eller

e) Uppgifterna har samlats in i samband med att ett barn har skapat en profil i ett socialt nätverk.

Även om någon av ovan punkter är tillämplig, finns det ändå flera undantag till rättigheten. Om behandlingen av personuppgifterna är fortsatt nödvändig, till exempel för att en rättslig förpliktelse ska kunna uppfyllas eller för arkivändamål av allmänt intresse, ska uppgifterna inte raderas.

Om rättigheten ändå gäller och om den som ansvarar för personuppgiftsbehandlingen har offentliggjort uppgifterna ska (med hänsyn till tillgänglig teknik och kostnaden för åtgärderna) andra fysiska eller juridiska personer som behandlar uppgifterna underrättas om att den registrerade begärt en radering av eventuella länkar till eller kopior/reproduktioner av uppgifterna. Den personuppgiftsansvarige ska även underrätta de mottagare till vilka personuppgifterna har lämnats ut om att radering har gjorts, såvida det inte visar sig vara omöjligt eller innebära en oproportionerlig ansträngning.

Observera dock att det inte nödvändigtvis betyder att uppgifterna raderas totalt. Om en av platserna där uppgifterna finns täcks av lagstiftning som undantas från GDPR:s regler, t.ex. tryckfrihetsförordningen, är den som äger sidan inte skyldig att radera uppgifterna. Detta gäller exempelvis insändare på en nyhetssida.

Med andra ord är rätten till radering invecklad och fylld med undantag och det finns därmed ingen garanterad rätt att bli fullkomligt ”bortglömd”.

5.5 Rätten till begränsning

Med att en personuppgiftsbehandling begränsas menas att personuppgifterna i framtiden bara får behandlas under vissa omständigheter, till exempel med hänsyn till ett viktigt allmänintresse eller för att skydda en fysisk eller juridisk persons rättigheter. I övrigt får uppgifterna bara lagras.

Den registrerade kan begära att hens personuppgifter begränsas enligt följande villkor:

a) Om uppgifternas korrekthet bestrids av den registrerade begränsas behandlingen under den tid som behövs för att den personuppgiftsansvarige ska kunna kontrollera korrektheten.

b) Om behandlingen är olaglig kan den registrerade begära begränsning istället för radering.

c) Om den personuppgiftsansvarige inte längre behöver personuppgifterna för att uppfylla ändamålen med behandlingen, men den registrerade behöver dem för att fastställa, göra gällande eller försvara rättsliga anspråk, kan en begränsning göras.

d) Om den registrerade invänder mot en behandling som grundar sig på ett berättigat intresse för den personuppgiftsansvarige (se Berättigat intresse) begränsas behandlingen i väntan på en intresseavvägning.

Den personuppgiftsansvarige är skyldig att underrätta eventuella mottagare om att en begränsning har skett om det inte visar sig omöjligt eller oproportionerligt ansträngande. Innan en begränsning upphör ska den registrerade meddelas om detta.

5.6 Rätten till dataportabilitet

Dataportabilitet är en nyhet som introduceras genom GDPR. Genom denna rättighet kan en registrerad få ut och använda sina personuppgifter på annat håll genom att lämna dem till en annan personuppgiftsansvarig. Uppgifterna ska lämnas ut i ett strukturerat, allmänt använt, maskinläsbart och interoperabelt format, exempelvis .xml eller .csv (om inget annat format anses lämpligare). Om det är tekniskt möjligt ska den personuppgiftsansvarige på begäran från den registrerade överföra personuppgifter direkt till en annan part.

Rätten till dataportabilitet gäller bara om personuppgiftsbehandlingen sker automatiserat och om den lagliga grunden för behandlingen är samtycke eller avtal. Dessutom gäller den bara för sådana personuppgifter som den registrerade själv har lämnat.

Tänk på att om din organisation tar emot personuppgifter från en annan part genom att en registrerad utövar sin rätt till dataportabilitet, får ni inte behandla dessa uppgifter på ett sätt som strider mot de ursprungliga ändamålen. Därför måste ändamålen säkerställas innan uppgifterna tas emot.

I många fall behandlas information som innehåller personuppgifter tillhörande flera olika personer. Om en registrerad begär utlämnande eller överföring av sådan information, underlättar det om samtycke kan inhämtas från de tredje parterna (det kan ju hända att även de vill överföra sina uppgifter). Det får dock bedömas från fall till fall om det är lämpligt att begära samtycke eftersom det inte är strikt nödvändigt.

5.7 Rätten att invända

Det finns tre situationer i vilka en registrerad har en rätt att göra invändningar mot en personuppgiftsbehandling:

- Behandlingen grundas på någon av följande lagliga grunder: Allmänt intresse, Myndighetsutövning eller Berättigat intresse;
- Behandlingen har ett samband med direkt marknadsföring; eller
- Behandlingen utförs för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Om en invändning görs får personuppgifterna bara behandlas under vissa förutsättningar.

5.8 Rätten att inte bli utsatt för automatiserat beslutsfattande och profilering

Med automatiserat beslutsfattande menas i det här sammanhanget beslut som fattas gällande den registrerade utan mänsklig inblandning. Exempelvis täcks ett automatiserat avslag på en kreditansökan på internet av definitionen för automatiserat beslutsfattande. Om ett sådant beslut påverkar den registrerade i betydande grad, exempelvis genom att innebära rättsliga konsekvenser för den registrerade, är huvudregeln att hen har en rätt att inte utsättas för behandlingen i fråga.

Det finns dock vissa undantag från den här rättigheten, nämligen om beslutet:

a) Baseras på *uttryckligt samtycke* från den registrerade;

b) Är nödvändigt för ingåendet eller fullgörandet av ett avtal mellan den registrerade och den personuppgiftsansvarige; eller

c) Tillåts enligt en tillämplig lag som fastställer lämpliga skyddsåtgärder.

Även om automatiserat beslutsfattande är tillåtet ska den registrerade ha en rätt att komma i personlig kontakt med den personuppgiftsansvarige för att kunna uttrycka sin åsikt och bestrida beslutet.

Profilering är en form av automatiserad behandling genom vilken personliga egenskaper hos den registrerade bedöms, exempelvis i syfte att analysera eller förutsäga hens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar. Profilering täcks av rätten att inte bli utsatt för automatiserat beslutsfattande.

Ett automatiserat beslut får inte baseras på känsliga personuppgifter såvida inte uttryckligt samtycke har givits eller behandlingen är nödvändig av hänsyn till ett allmänt intresse.

6. Personuppgiftsincidenter

Det är lätt att tänka att ett starkt personuppgiftsskydd handlar om teknologi och därför landar på IT-avdelningens bord, men faktum är att de flesta informationssäkerhetsincidenter sker tack vare den mänskliga faktorn. Med tanke på den korta tidsfristen inom vilken en inträffad personuppgiftsincident ska rapporteras till ISM (se nedan) är det av oerhörd vikt att alla anställda i en organisation har koll på hur de ska agera i händelse av en incident.

En personuppgiftsincident är 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. Om det bedöms sannolikt att en sådan incident medför en risk för fysiska personers rättigheter och friheter ska incidenten rapporteras till ISM inom 72 timmar, vilket är en nyhet introducerad av GDPR. Anmäls inte incidenten i tid kan resultatet bli en avgift på upp till 10 miljoner euro eller 2% av den totala globala årsomsättningen.

Utöver anmälan till ISM ska, om det är sannolikt att incidenten medför en *hög* risk för fysiska personers rättigheter och friheter (exempelvis en risk att utsättas för diskriminering, ID-stölder, bedrägerier eller finansiella stölder), även berörda registrerade informeras om incidenten utan onödigt dröjsmål. Detta behöver dock inte göras om lämpliga skyddsåtgärder vidtagits eller om det skulle innebära en oproportionerlig ansträngning.

Information som ska lämnas	Integritetsskydds-myndigheten	Berörda registrerade
En klar och tydlig beskrivning av den inträffade incidenten	X	X
Ungefärligt antal registrerade som berörts	X	
Vilken kategori av personuppgifter som berörts	X	
Ungefärligt antal personuppgiftsposter som berörts	X	
Namn på kontaktperson där mer information kan fås	X	X
En beskrivning av sannolika konsekvenser	X	X
En beskrivning av åtgärder som vidtagits eller föreslagits i respons	X	X

7. Dataskyddsombud

Ett så kallat dataskyddsombud (tidigare PUL-ombud) har till uppgift att kontrollera att GDPR följs inom organisationen och kan anlitas antingen externt eller internt. Det är bra att ha ett dataskyddsombud, men endast obligatoriskt att utnämna ett i tre fall:

a) När behandlingen genomförs av en myndighet eller ett offentligt organ, dock inte i en domstols dömande verksamhet;

b) När kärnverksamheten består av behandling som kräver regelbunden och systematisk övervakning av registrerade i stor omfattning; eller

c) När kärnverksamheten består av behandling i stor omfattning av känsliga uppgifter (se Känsliga personuppgifter) eller uppgifter som rör fällande domar i brottmål och överträdelser.

Dataskyddsombudet ska informera och ge råd till organisationen gällande GDPR och dataskydd i övrigt, övervaka organisationens ansträngningar samt fungera som kontaktpunkt för ISM och de registrerade. Ett ombud ska utses på basis av yrkesmässiga kvalifikationer, kunskap om dataskyddslagstiftning och -praxis samt hens förmåga att fullgöra sina uppgifter. Kontaktuppgifter till dataskyddsombudet ska offentliggöras och meddelas till ISM.

Den som utnämnt ombudet (den personuppgiftsansvarige eller ett personuppgiftsbiträde) ska se till att hen har de resurser som krävs för att kunna utföra sina uppgifter, inklusive tillgång till personuppgifter och behandlingsförfaranden. Ombudet skyddas i GDPR genom att hen inte får avsättas eller bli föremål för sanktioner på grund av utförandet av sina uppgifter som dataskyddsombud. I Sverige har det föreslagits att dataskyddsombud ska vara bundna av tystnadsplikt.

Om din organisation ingår i en koncern behöver bara ett dataskyddsombud utses för alla bolag inom koncernen, så länge det är enkelt att nå ombudet på varje etableringsort.

En person som är PUL-ombud går inte automatiskt över till att bli dataskyddsombud den 25 maj 2018 – ombudets kontaktuppgifter måste lämnas till ISM.

8. Konsekvensbedömning

Om någon typ av personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska en konsekvensbedömning göras innan behandlingen inleds. En sådan bedömning ska innehålla åtminstone:

- En systematisk beskrivning av den planerade behandlingen och dess syften;
- När den lagliga grunden är ett berättigat intresse, en beskrivning av det intresset (se Berättigat intresse);
- En bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till dess syften;
- En bedömning av riskerna för de registrerades rättigheter och friheter; och
- Vilka åtgärder som planerats för att hantera riskerna.

Så vad anses då utgöra en hög risk? I GDPR finns en lista över behandlingar som *kräver* en konsekvensbedömning:

- Automatiserad behandling som innebär en systematisk och omfattande bedömning av individers personliga egenskaper och resulterar i ett beslut som i betydande grad påverkar dessa individer.
- Behandling i stor omfattning av känsliga personuppgifter eller personuppgifter som rör fällande domar i brottmål och överträdelser.
- Behandling som innebär att en allmän plats övervakas systematiskt och i stor omfattning.

Det är dock aldrig fel att göra en konsekvensbedömning, eftersom den är ett användbart verktyg som kan underlätta efterlevnaden av GDPR. Är det osäkert om en konsekvensbedömning behöver göras eller inte rekommenderas därför att man ändå gör en bedömning. Konsekvensbedömningen kan sedan användas som en sorts mall för hur behandlingen ska genomföras.

Visar konsekvensbedömningen att en viss behandling skulle leda till en hög risk om inte särskilda åtgärder vidtas för att minska risken, ska den personuppgiftsansvarige genomföra ett så kallat förhandssamråd med ISM. Om ISM anser att behandlingen strider mot GDPR, ska myndigheten ge den personuppgiftsansvarige skriftliga råd inom åtta veckor.

9. Övriga skyldigheter

9.1 Behandlingsregister

Personuppgiftsansvariga och personuppgiftsbiträden ska föra register över de behandlingar som utförs. Undantaget är för företag som har färre än 250 anställda – om så är fallet behöver ett register endast föras om behandlingen:

- Inte är tillfällig;
- Sannolikt kommer att innebära en risk för registrerades rättigheter och friheter;
- Omfattar känsliga personuppgifter; eller
- Omfattar personuppgifter om fällande domar i brottmål samt överträdelser.

Att register ska föras över alla behandlingar som inte är tillfälliga, även för små företag, innebär i praktiken att i princip alla som behandlar personuppgifter är skyldiga att föra register – alla som har en anställd eller kund behandlar ju dennes personuppgifter mer än endast tillfälligt!

Behandlingsregistret ska på begäran göras tillgängligt för ISM.

Registrets innehåll	Personuppgiftsansvariga	Personuppgiftsbiträden
Kontaktuppgifter till den personuppgiftsansvarige	X	X
Kontaktuppgifter till ev. dataskyddsombud	X	X
Kontaktuppgifter till personuppgiftsbiträdet		X
Kontaktuppgifter till ev. underbiträden		X
Kontaktuppgifter till ev. företrädare för den ansvarige	X	X
Kontaktuppgifter till ev. företrädare för biträdet		X
Ändamål	X	
Kategori av behandling		X

Kategorier av registrerade	X	
Kategorier av personuppgifter	X	
Kategorier av mottagare	X	
Överföringar till tredje land samt ev. skyddsåtgärder	X	X
Tidsfrister för radering	X	
Tekniska och organisatoriska säkerhetsåtgärder	X	X

9.2 Inbyggt dataskydd och dataskydd som standard

Med inbyggt dataskydd (*privacy by design*) menas att man redan vid utformandet av system och rutiner tar hänsyn till GDPR:s grundläggande principer (se Grundläggande principer) och övriga dataskyddsregler. Exempelvis bör de system som används till personuppgiftsbehandling ha funktioner genom vilka personuppgifter kan raderas (gärna automatiskt), krypteras, begränsas till endast lagring och korrigeras vid behov.

Dataskydd som standard (*privacy by default*) innebär att personuppgifter i normalfallet endast behandlas om det är nödvändigt. Med det menas inte att behandlingen ska vara absolut nödvändig, utan det räcker med att den skulle resultera i effektivitetsvinster. Ett exempel på dataskydd som standard är att anpassa standardinställningarna i en tjänst för sociala media så att inte mer information än nödvändigt samlas in av den registrerade eller visas på hens profil. Vill den registrerade dela med sig av fler uppgifter utöver vad standardinställningarna tillåter är det då upp till hen att ändra inställningarna manuellt.

Nedan följer ett antal förslag på åtgärder som kan vidtas för att uppfylla GDPR:s krav i detta hänseende.

- **Undvik fritextfält.** Genom att ta kontroll över vilka personuppgifter som kan samlas in och registreras minskas risken för att information samlas in som inte är nödvändig för ändamålet.

- **Begränsa till det som är tillåtet.** Spärra funktioner och begränsa möjligheter så att personuppgifter inte kan användas på ett sätt som går emot lagstiftningen.

- **Underlätta inhämtande och återtagande av samtycke.** Om en viss behandling grundas på samtycke bör funktioner byggas in i systemet som underlättar både inhämtande och återtagande av samtycke.

- **Inför automatisk gallring.** Funktioner som automatiskt rensar bort vissa personuppgifter efter en bestämd tidsperiod minskar både mängden manuellt arbete och risken för att personuppgifter behandlas längre än vad som är nödvändigt.

- **Möjliggör insyn för registrerade.** I vissa typer av system, exempelvis sociala medier, kan det vara lämpligt att göra det möjligt för registrerade att själva ha direkt insyn i personuppgiftsbehandlingen, genom till exempel en funktion för att enkelt och automatiskt begära ett utdrag.

- **Begränsa åtkomst.** Anpassa behörighetsstyrningen efter vilka som faktiskt behöver ha tillgång till personuppgifterna för att kunna utföra sina arbetsuppgifter.

- **Implementera tekniska säkerhetsåtgärder.** Exempelvis tvåfaktorsautentisering, kryptering och säkerhetskopiering.

9.3 Säkerhet för personuppgifter

Den som behandlar personuppgifter ska vidta lämpliga tekniska och organisatoriska åtgärder för att se till att behandlingen har en lämplig säkerhetsnivå. Vilken säkerhetsnivå som är lämplig beror på vilka uppgifter som behandlas, vilka risker behandlingen medför, vilka tekniska möjligheter som finns och kostnaderna för åtgärderna.

I GDPR föreslås pseudonymisering och kryptering som möjliga säkerhetsåtgärder. Pseudonymisering innebär att uppgifterna inte kan kopplas till en specifik individ utan kompletterande information. Den kompletterande informationen måste hållas avskild från uppgifterna för att pseudonymiseringen ska ha någon verkan. Krypterade personuppgifter kan fortfarande kopplas till en individ, men det krävs en ”nyckel” för att kunna dekryptera dem så att de går att tyda. Lösenord brukar vanligen vara krypterade.

I övrigt finns det en mängd olika säkerhetsåtgärder som kan vidtas och som har sin grund i informationssäkerhet. Nedan följer en lista över några av de åtgärder som bör övervägas och som med fördel kan införas i en informationssäkerhetspolicy.

Tekniskt

- Automatisk utloggning eller skärmsläckare med lösenord när användaren lämnar sin arbetsplats.
- Kryptering av personuppgifter.
- Automatisk säkerhetskopiering och loggning av säkerhetskopieringen.
- Kartläggning av ingångar till datorsystem och införande av åtgärder för att upptäcka och skydda mot virusattacker eller skadliga program.

Organisatoriskt

- En säkerhetspolicy innehållande organisationens säkerhetsstrategi, ansvarsfördelning och övergripande säkerhetsmål.
- Tydliga rutiner och processer som gör det lätt för medarbetare att tänka säkerhetsmedvetet.
- Relevant säkerhetsutbildning för all personal.
- Rutiner för säkerhetskopiering (backup) av personuppgifter.
- Säkerhetsrutiner för besök samt för avveckling av användarkonton och liknande när en anställd slutar.
- Lämpliga identifikationsmetoder såsom passerkort, personliga lösenord osv.

Fysiskt

- Fysiskt skydd (exempelvis lås, larm och brandskydd) för IT-utrustning som används för person-uppgiftsbehandling.
- Redundans för att skydda vid exempelvis strömavbrott eller fel.
- Begränsning av åtkomst till IT-utrustning.

Övrigt

- Säker förstöring av lagringsmedia samt säker utplåning av personuppgifter som inte längre är nödvändiga.
- Reparation och service som sker på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga.
- Regelbundna kontroller av säkerheten.

Det blir enklare att komma på lämpliga säkerhetsåtgärder om man har en riskanalys i botten. Därför kan det vara bra att göra sådana analyser, även utöver de konsekvensbedömningar som GDPR reglerar (se Konsekvensbedömning).

10. Den svenska dataskyddslagen

GDPR är direkt gällande i hela EU den dag den träder i kraft, men EU:s medlemsländer har ändå getts både möjligheter och skyldigheter till nationella kompletteringar. Därför kommer i Sverige en dataskyddslag med kompletterande bestämmelser till EU:s dataskyddsförordning att träda i kraft samma datum som GDPR, det vill säga den 25 maj 2018. I maj 2017 publicerades den officiella utredningen inför dataskyddslagen, SOU 2017:39. Lagen är inte slutgiltigt utformad än, men det kan ändå vara värdefullt att redan nu ta upp ett par viktiga delar av förslaget.

Följande är några viktiga punkter som har föreslagits ska stadgas i den svenska dataskyddslagen:

- Utvidgat tillämpningsområde (se Vilka berörs?) så att även verksamhet som inte omfattas av unionsrätten samt verksamhet som utförs inom ramen för den gemensamma utrikes- och säkerhetspolitiken ska falla under GDPR:s regler – dock endast vid tillämpningen av dataskyddslagen.

- Den lagliga grunden rättslig förpliktelse (se Rättslig förpliktelse) kan även syfta till förpliktelser i avtal, till exempel kollektivavtal.

- Personnummer och samordningsnummer (identitetsbeteckning för någon som aldrig folkbokförts i Sverige) får bara behandlas utan samtycke om det är ”klart motiverat” med hänsyn till behandlingens ändamål, vikten av en säker identifiering eller något annat beaktansvärt skäl.

- Rätten till information och tillgång (se De två informationsrättigheterna) gäller inte för uppgifter som omfattas av sekretess. Rätten till tillgång gäller inte heller för uppgifter som behandlas i löpande text som utgör utkast eller minnesanteckning.

- Åldersgränsen för när giltigt samtycke kan lämnas till personuppgiftsbehandling i samband med att en profil skapas i ett socialt nätverk ska vara 13 år, till skillnad från GDPR:s gräns på 16 år (se Barns samtycke i sociala nätverk).

- Tystnadsplikt ska gälla för dataskyddsombud (se Dataskyddsombud) vad gäller sådant som ombudet har fått veta om enskilds personliga eller ekonomiska förhållanden.

- Sanktionsavgifter får tas ut av statliga och kommunala myndigheter till ett maxbelopp av 20 miljoner SEK (se Konsekvenser av att inte uppfylla GDPR:s krav).

Dataskyddsutredningen kan läsas i sin helhet på 9te.ch/SOU-2017-39.

11. Användbara resurser

Den här guiden har gått igenom GDPR:s viktigaste områden, men den skrapar fortfarande bara på ytan. Med tanke på att GDPR:s tolkning och tillämpning kommer att preciseras närmare under flera år efter dess ikraftträdande, är det viktigt att din organisation håller sig uppdaterad. Här följer ett par resurser som är bra att känna till.

11.1 Lagtext

För att kunna följa en lag behöver man självklart ha tillgång till den. Du kan läsa GDPR på svenska eller engelska med hjälp av länkarna nedan. Båda språkversionerna är officiella, men vid tolkningssvårigheter kan det hjälpa att jämföra dem med varandra.

GDPR på svenska: 9te.ch/GDPR-sv

GDPR på engelska: 9te.ch/GDPR-en

Den svenska dataskyddslagen med kompletterande bestämmelser till EU:s dataskyddsförordning har ännu inte fått sin slutgiltiga utformning, men kommer att träda i kraft samma datum som GDPR, det vill säga den 25 maj 2018. Den kommer då att vara sökbar på www.riksdagen.se/sv/dokument-lagar.

11.2 Praxis

EU-domstolen kommer att komma med löpande tolkningar av GDPR allt eftersom mål kommer upp till prövning under förordningens levnadstid. Alla domstolens domar är sökbara på www.curia.europa.eu.

11.3 Vägledningar och annan information

Särskilt innan GDPR trätt i kraft samt under dess första tid kommer diverse vägledningar att komma för hur GDPR ska tolkas närmare. Den främsta källan är Artikel 29-gruppen, som hittills publicerat vägledningar gällande dataportabilitet, dataskyddsombud och tillsynsmyndigheter. Du hittar de senaste av gruppens vägledningar på 9te.ch/art-29-wp.

Integritetsskyddsmyndigheten har en hemsida med matnyttig information om dataskyddsreformen. På den sidan kan du även läsa de två vägledningar som publicerats av ISM hittills, gällande hur personuppgiftsansvariga och personuppgiftsbiträden kan förbereda sig inför GDPR:s ikraftträdande: www.Integritetsskyddsmyndigheten.se/dataskyddsreformen. Om du vill gå ett steg längre håller ISM även i diverse utbildningar om GDPR. Platserna till dessa brukar ta slut kort tid efter att de släppts. Läs mer om ISM:s utbildningar på www.Integritetsskyddsmyndigheten.se/utbildning.

12. Checklistor

I det här avsnittet finns checklistor för några av de olika områden som täcks av GDPR. De är inte uttömmande, men kan fungera som en översikt över vad som behöver göras för att uppfylla kraven i den nya lagstiftningen.

12.1 Generell checklista

Den här checklistan kan hjälpa dig som inte vet var du ska börja för att komma igång med din verksamhets anpassningsarbete.

- **Börja med att kartlägga och dokumentera vilka behandlingar ni utför.** Det kan vara allt från ett sökbart register i en pärm som listar vilka nycklar som lämnats ut till vilka anställda, till en stor databas fylld med uppgifter om användare i ett system. Tänk att allt som innehåller personuppgifter – både fysiska register och digitala filer (se Gäller GDPR för all personuppgiftsbehandling?) – ska föras in i ett behandlingsregister. När du har koll på var personuppgifterna finns, blir det betydligt lättare att besvara begäranden från registrerade i framtiden. (Dessutom är det ett uttryckligt krav i GDPR att föra behandlingsregister.)

- **När alla behandlingar är kartlagda, fundera över om de lever upp till GDPR:s krav.** Behandlas personuppgifterna för berättigade ändamål snarare än för att ”de kan vara bra att ha”? Bygger behandlingen på en laglig grund, t.ex. avtal, rättsligt krav eller samtycke? Behandlas några extra känsliga personuppgifter (t.ex. uppgifter om religion, hälsa eller sexualitet) och i så fall, skyddas de på ett lämpligt sätt? Utförs några extra riskfyllda behandlingar (t.ex. en systematisk bedömning av individers personliga egenskaper) och i så fall, har det gjorts någon riskanalys?

- **Fundera över om era säkerhetsåtgärder är tillräckliga, eller om det behövs fler.** Kanske kan fler uppgifter krypteras, eller så kan den där pärmen med uppgifter om anställda låsas in i ett skåp som bara ett begränsat antal personer har nyckel till.

- **Börja integritetssäkra nya system som utvecklas och se över så att nuvarande system redan är säkrade.** Dataskyddsförordningen kräver att IT-system integritetssäkras redan från början, dvs. de ska utformas (och vid behov ändras) med de grundläggande dataskyddsprinciperna i åtanke (se Grundläggande principer och Inbyggt dataskydd och dataskydd som standard). Kan rättigheter beviljas på ett smidigt sätt, till exempel? Under den här punkten ingår också att ta kontakt med systemleverantörer för att ta reda på hur deras system lever upp till GDPR:s krav – behöver avtal omförhandlas?

- **Se över behörigheter.** Vem kan t.ex. besluta om rättelse av personuppgifter? Var i organisationen ligger ansvaret för dataskyddsfrågor? Vilka roller har tillgång till behandlade personuppgifter? Vilka andra roller och ansvarsområden har utsetts och behöver de förändras? Vilka personer har vilka roller?

- **Kartlägg vilka externa parter som har eller kan få tillgång till de personuppgifter ni behandlar.** Det kan röra sig om allt från städbolag till systemleverantörer. Alla dessa parter är personuppgiftsbiträden och därför måste ni skriva särskilda avtal med dem för att säkerställa att den behandling de utför åt er sker på ett lagligt och korrekt sätt. Om ni redan har sådana avtal, se över dem en gång till så att de överensstämmer med de nya lagkraven.

- **Utforma och implementera rutiner för att besvara individers begäranden om hanteringen av deras personuppgifter.** De personer vars uppgifter du behandlar har vissa rättigheter, t.ex. till utdrag, rättelse och – i vissa fall – radering av uppgifterna. För att begäranden om åtgärder ska kunna ske på ett snabbt och smidigt sätt behövs tydliga rutiner för hur ansvarig personal ska gå tillväga.

- **Ta fram diverse standardtexter.** För att kunna säkerställa att dataskyddsförordningens krav efterlevs bör standardtexter tas fram bl.a. vad gäller samtycke och utlämnande av information till registrerade. Det finns en rad formkrav på dessa sorters texter i GDPR.

- **Se till att personalen har den utbildning som behövs.** Rutiner och processer är bara till hjälp om det finns människor bakom som ser till att allt fungerar. Grundläggande information kan vara bra att ge till alla anställda, men de som kommer att arbeta med t.ex. att besvara rättighetsbegäranden behöver en mer grundlig utbildning.

12.2 Checklista för lagliga grunder

All personuppgiftsbehandling måste vila på en laglig grund, exempelvis samtycke eller avtal. Här är några tips på steg att ta för att uppfylla detta krav.

- **Börja med att utreda om all behandling som utförs bygger på berättigat ändamål och lagliga grunder.** Det här är det självklara stället att börja på. Om en laglig grund angetts för den behandling som redan utförs, är den fortfarande tillämplig? Om ingen laglig grund angetts, kan det finnas någon? Om inte, måste behandlingen upphöra.

- **Ta reda på om just din verksamhet har särskilda lagkrav på sig som kräver behandling.** Den lagliga grunden ”rättslig förpliktelse” (se Rättslig förpliktelse) blir då aktuell. Detta gäller

exempelvis för myndigheter, som enligt arkivlagen måste spara vissa personuppgifter även efter att den ursprungliga lagliga grunden upphört för att de ska kunna lämna ut allmänna handlingar. Arbetsrättslig lagstiftning innebär vidare att uppgifter om anställda ska sparas även efter att anställningen upphört. Vidare ställer bokföringslagen krav på bevarande av bokföringsunderlag.

- **Säkerställ att de registrerade informeras om vilken laglig grund behandlingen bygger på när uppgifterna samlas in.** Att de registrerade ska ha tillgång till tydlig och klar information om hur deras personuppgifter behandlas är ett uttryckligt krav i GDPR. Beroende på hur uppgifterna samlas in kan det finnas olika sätt att informera på, men ett standardtips som vanligen är lämpligt är att ha en dedikerad sida på sin webbplats där all information finns att finna. (Se De två informationsrättigheterna.)

- **Säkerställ att alla samtycken som inhämtas dokumenteras i bevissyfte.** För att kunna bevisa att ett samtycke har givits samt att det givits under de förutsättningar som GDPR kräver, behöver det dokumenteras. (Se Att bevisa samtycke.) Ett sätt att göra detta på kan vara att ha automatisk loggning över lämnade samtycken. Om det inte går att bevisa att ett samtycke lämnats, måste det inhämtas på nytt.

12.3 Checklista för känsliga personuppgifter

Kraven för att få behandla känsliga personuppgifter (se Känsliga personuppgifter) är särskilt höga. Här är några saker du behöver tänka på.

- **Se till att särskild justifikation finns där det behövs.** *Utöver* berättigat ändamål och laglig grund kräver behandlingen av känsliga personuppgifter även en extra grund för behandlingen (se Känsliga personuppgifter). Några av dessa är *uttryckligt* samtycke, ett viktigt allmänt intresse eller att uppgifterna har offentliggjorts av den registrerade. Behandling av känsliga personuppgifter får inte utföras om det inte finns en särskild grund.

- **Implementera tillfredsställande säkerhetsåtgärder för känsliga personuppgifter.** Sådana uppgifter behöver skyddas särskilt. Överväg därför extra höga säkerhetsåtgärder för behandling av känsliga personuppgifter.

- **Om behandlingen av känsliga uppgifter utförs i stor omfattning – gör en konsekvensbedömning och utse dataskyddsombud.** Ett dataskyddsombud ska alltid utses och en konsekvensbedömning alltid göras innan en sådan behandling inleds. Se Dataskyddsombud respektive Konsekvensbedömning.

12.4 Checklista för rättigheter

En av de viktigaste delarna av GDPR är den som stadgar de registrerades olika rättigheter. Följ den här checklistan för att få en övergripande bild av huruvida din verksamhet lever upp till kraven.

- **Identifiera var alla personuppgifter finns någonstans och implementera effektiva sök-funktioner.** Om en begäran om radering kommer vill ni veta var alla den registrerades person-uppgifter finns – glöms uppgifter bort någonstans kan det leda till skadestånd eller i värsta fall sanktionsavgifter. Det är ännu oklart exakt vad som kommer gälla för personuppgifter i mail och dylikt, men tills vidare – i väntan på förtydliganden från EU:s sida – kan man avvakta med den frågan. Enligt GDPR ska en begäran kunna nekas om den är uppenbart orimlig, vilket skulle kunna inkludera uppgifter som är mycket svåra att söka efter. I helt nyutvecklade system re-kommenderas dock att funktioner för enkel sökning implementeras. Det bästa är om en enda sökning kan ge resultat i alla system som används.

- **Upprätta dataskyddspolicyer som informerar de registrerade om hur deras personupp-gifter behandlas och vad de har för rättigheter.** Det är ett uttryckligt krav enligt GDPR (se De två informationsrättigheterna, även Checklista för lagliga grunder) att de registrerade ska informeras när deras personuppgifter samlas in. Denna information ska vara skriven med ett klart och tydligt språk och vara lätt att ta del av.

- **Implementera en funktion som registrerade kan använda sig av för att kommunicera med er om dataskyddsfrågor.** En egen sida på webbplatsen exempelvis, där registrerade kan skicka in begäranden kopplade till deras personuppgifter eller ställa frågor. En funktion för begäran-den måste kunna kontrollera identitet (och, om barns personuppgifter behandlas, ålder) och bör även låta den registrerade spåra sin begäran. Definierade svarstider bör finnas på sidan.

- **Säkerställ att det finns funktioner i system och rutiner för personal så att begäranden från registrerade kan beviljas.** Uppgifter ska kunna raderas, rättas/kompletteras och lämnas ut till den registrerade i ett allmänt använt och maskinläsbart format. Alla typer av behandlingar ska kunna begränsas (pausas) eller avslutas helt. Alla dessa åtgärder ska kunna vidtas inom en rimlig tid och i vissa fall måste en bedömning göras för att säkerställa att det verkligen finns en grund för åtgärden (se Den registrerades rättigheter). Relevant personal behöver därför även ha en grundläggande utbildning angående hur de ska hantera rättighetsbegäranden.

12.5 Checklista för säkerhet och incidenter

Säkerhet för personuppgifter är viktigt, för att undvika incidenter som kan leda till dyra kostnader och renommeskador. Här är en grundläggande checklista över saker att tänka på.

- **Utforma en plan för utveckling och inköp av nya system och ställ krav på systemleverantörer.** Som nämnts i Inbyggt dataskydd och dataskydd som standard ska system integritetssäkras, det vill säga de ska bland annat innehålla funktioner som höjer säkerhetsnivån för behandlade personuppgifter. Din verksamhet behöver lägga upp en plan för hur det här ska åstadkommas.

- **Kartlägg vilka risker som finns i er verksamhet.** En rekommendation är att föra ett riskregister som innehåller information om bland annat risknivåer, potentiella konsekvenser och åtgärdsförslag. Utifrån detta riskregister kan ni sedan avgöra vilka åtgärder som behöver tas för att skydda personuppgifter.

- **Avgör om personuppgifter bör krypteras.** Lösenord ska alltid vara krypterade, men även andra känsliga uppgifter kan behöva kryptering, exempelvis personnummer och kontonummer. Vidare kan kryptering behövas om personuppgifter samlas in genom fritextfält, eftersom det inte går att förutse vilka uppgifter en person kan tänkas ange.

- **Överväg ytterligare säkerhetsåtgärder.** Exempelvis daglig säkerhetskopiering, fysiska skydd såsom larm och bommar eller dubbel autentisering för vissa funktioner – se fler exempel i Säkerhet för personuppgifter. Inför även en process för att testa säkerhetsåtgärderna.

- **Avgör om en konsekvensbedömning behöver göras för någon behandling.** Se Konsekvensbedömning för mer information.

- **Skriv personuppgiftsbiträdesavtal med leverantörer och andra som har tillgång till de personuppgifter ni behandlar.** Eftersom en personuppgiftsansvarig alltid har det yttersta ansvaret för att personuppgifterna behandlas lagenligt, måste avtal skrivas med biträden för att ställa krav på att de följer dataskyddslagstiftningen. (Se även Generell checklista.)

- **Om personuppgifter överförs till mottagare utanför EU, se till att överföringen är godkänd enligt GDPR.** Om EU-kommissionen har godkänt det specifika mottagarlandet (se 9te.ch/godkanda-lander) kan överföring ske. I övriga fall måste en bedömning göras av jurist.

- **Utforma en incidenthanteringsplan.** Se till att det går att upptäcka personuppgiftsincidenter på ett tidigt stadium och att det finns en process för dokumentation och mätning av inträffade incidenter. Vilken information som ska lämnas i samband med att en personuppgiftsincident inträffar och när den ska lämnas framgår av Personuppgiftsincidenter.

12.6 Checklista för HR

Något som alla verksamheter har gemensamt är de anställda – alla de som arbetar för att få verksamheten att gå runt. Därför är HR och behandling av anställdas personuppgifter något som alla verksamheter kommer att behöva tänka på. Den här checklistan syftar till att ge tips och hjälp gällande vad som gäller för anställdas personuppgifter.

- **Spara inte sådan information som inte är nödvändig.** I enlighet med principerna om ändamålsbegränsning och uppgiftsminimering får man inte samla in fler personuppgifter än vad som verkligen behövs. Under exempelvis en anställningsintervju kan det komma upp mycket information, särskilt om personliga förhållanden – utan ett tydligt berättigat syfte får sådana uppgifter inte antecknas och sparas.

- **Tänk på att samtycke måste vara frivilligt.** I en anställnings- eller rekryteringssituation är det svårt att be om samtycke, eftersom beroendeförhållandet mellan arbetsgivaren och arbetstagaren kan göra att arbetstagaren känner sig tvingad att lämna samtycke till viss behandling. Ett samtycke är inte giltigt om det inte är lämnat frivilligt och utan press, så var extra noggrann när det är dags att begära samtycke från en blivande eller nuvarande anställd. Be inte om samtycke i en rekryteringsprocess om det i praktiken är så att sökande som inte lämnar sitt samtycke blir bortsorterade direkt.

- **Uppgifter kan inte samlas in hur som helst från sociala medier.** Att kolla upp en sökande på internet är tillåtet; om den sökande själv har lagt upp viss information på sociala medier ses det som publicering. Detsamma gäller om informationen lagts upp av någon annan (även om det krävs ett visst mått av källkritik). Det är däremot inte tillåtet att kopiera och spara inlägg som den sökande publicerat utan att först be om tillstånd från den sökande själv. I denna aspekt är det viktigt att även reflektera kring diskrimineringslagstiftningen. För även om det är tillåtet att ta reda uppgifter om sökande, kan det bli aktuellt att kunna visa att vissa uppgifter inte legat till grund för ett nekande.

- **Automatiserat beslutsfattande kan användas i rekryteringsprocessen under vissa förutsättningar.** Användningen av sådant beslutsfattande (se Rätten att inte bli utsatt för automatiserat beslutsfattande och profilering) för att göra urval i en rekryteringsprocess är tillåtet under förutsättning att det är nödvändigt för att anställningsavtalet ska kunna ingås. Om det inte är nödvändigt krävs den arbetssökandes uttryckliga samtycke. Samtycke måste dock återigen vara frivilligt – om ett uteblivet samtycke direkt sorterar bort den sökande ur processen, finns ingen faktisk frivillighet. Även om automatiserat beslutsfattande är tillåtet ska den sökande dessutom alltid ha rätt att bestrida det resulterande beslutet.

13. Behöver du hjälp?

CloudPros säkerhetsavdelning är experter på GDPR. Med juridisk och affärsmässig kompetens kan vi hjälpa dig och din verksamhet i den utsträckning det behövs. Kanske vill ni enbart ha en föreläsning, eller utbildning för relevant personal, men göra resten av arbetet själv? Kanske är ni i behov av löpande rådgivning som stöd medan ni anpassar er verksamhet till GDPR? Eller kanske vill ni anlita någon som går in och sköter hela arbetet åt er? Vi erbjuder tjänster på alla nivåer och skräddarsyr våra offertförslag efter vad just *ni* behöver.

För mer information om våra tjänster, gå in på www.cloudpro.se.