Delphi

Dataskyddsförordningen (”GDPR”)

Agnes Hammarstrand

Advokatfirman Delphi

23 mars 2018

Agenda

- Grundläggande om lagen
- Vem ansvarar?
- De grundläggande principerna och hur får personuppgifter behandlas
- Samtycke
- Registerförteckningen och rutiner för att visa att lagen följs
- Den registrerades rättigheter
- Överföring av personuppgifter
- Vem ansvarar och arbetar med frågorna internt – dataskyddsombud
- Säkerhet och IT-krav
- Andra krav
- Konsekvenser och hur ska vi arbeta med lagen?

Grundläggande om lagen

Idag: Personuppgiftslagen (”PuL”)

- Syfte att skydda mot att personlig integritet kränks genom behandling av personuppgifter
- I praktiken få sanktioner vid brott mot lagen
  - Många bryter idag mot lagen
- Nationell lag baserad på EU-direktiv
- Annan lagstiftning gäller före

Ny EU-förordning

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 (”GDPR”)
- Direkt gällande förordning som ersätter PuL och motsvarande lagar i hela EU (EES)
- Syfte
  - Möta teknikens förändringar
  - Stärka integritetsskyddet
  - Harmonisering, underlätta handel/fritt flöde inom EU
- De nya reglerna gäller från och med den **25 maj 2018**

Förordningen i korthet

- Principerna bygger på nuvarande lag, men också ett stort antal nyheter
- På vissa områden kan Sverige avvika i speciallag
  - Journalistiska ändamål
  - Akademiskt, konstnärligt eller litterärt skapande
  - Offentlighetsprincipen
  - Personnummer
  - Arbetsrätt
  - Forskningsändamål eller statistiska ändamål

Obs! Kompletterande lagstiftning

- Förordningen kompletteras av nationella regler
- Flera utredningar tillsatta i Sverige
  - Målsättning: Bevara så mycket som möjligt av tidigare bestämmelser – många regler kommer därför förbli som innan
- Dessutom finns kompletterande lag som får stor betydelse på enskilda områden i praktiken, t.ex. inom arbetsrätt
- Många konkreta frågor kommer därför ändå kräva bedömning utanför förordningen

Prop. 2017/18:105 – Ny dataskyddslag

- Utredningen föreslår en nya dataskyddslag
- Målsättning: Bevara så mycket som möjligt av tidigare bestämmelser
- Preciserar vad som ska gälla för svenska förhållanden

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 15 februari 2018

Stefan Löfven

Morgan Johansson
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

Regeringen föreslår att personuppgiftslagen upphävs och att en ny lag med kompletterande bestämmelser till EU:s dataskyddsförordning införs. Vidare föreslås att vissa bestämmelser i offentlighets- och sekretesslagen ändras.

Den föreslagna lagen innehåller bl.a. bestämmelser om att dataskydds-förordningen med vissa undantag ska gälla även utanför sitt egentliga tillämpningsområde, t.ex. i verksamhet som rör nationell säkerhet. Lagen ska dock vara subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i s.k. registerförfattningar. Lagförslaget förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen. Regeringen föreslår bl.a. att ett barn som är minst 13 år ska kunna samtycka till behandling av personuppgifter i samband med användning av informationssamhällets tjänster, t.ex. sociala medier. Vidare föreslås att sanktionsavgifter ska kunna tas ut även då en myndighet bryter mot dataskyddsförordningen. Förslaget till ny lag innehåller också vissa bestämmelser om begränsning av de registrerades rättigheter samt om skadestånd och överklagande av bl.a. tillsynsmyndighetens beslut.

Slutligen anges att dataskyddsförordningen och den nya lagen inte ska tillämpas i den utsträckning det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Lagändringarna föreslås träda i kraft den 25 maj 2018.

Förhållandet till offentlighetsprincipen

- PuL inskränker inte en kommuns skyldighet att lämna ut personuppgifter enligt 2 kap. tryckfrihetsförordningen
  - Skyldigheten att lämna ut uppgifter gäller efter att en medborgare begärt ett sådant utlämnande
  - När skyldighet att lämna ut information inte finns (t.ex. elektroniskt) måste kommunen pröva noga om det är möjligt att lämna ut med hänsyn till PuL
- Inga förändringar vad gäller offentlighets- och sekretesslagstiftningen föreslås

Exempel på utredningar och förslag till speciallag

- *Dataskydd inom Socialdepartementets verksamhetsområde (Prop. 2017/18:171)*
  - Förslag till ändringar i patientdatalagen och i socialförsäkringsbalken
  - Övergripande syftet är att behålla allt så likt exempelvis patientdatalagen och socialtjänstlagen idag som möjligt
- *Så stärker vi den personliga integriteten* (S*OU 2017:52 -)*
  - Föreslår upprättande av uppförandekoder inom skolan och hälso- och sjukvården, speciellt inom patientdatalagens område
  - Kompletterande bestämmelser till patientdatalagen föreslås, t.ex. för att konkretisera några av de krav som ställs på ett informationssystem som har den typen av uppgifter

Exempel på utredningar och förslag till speciallag forts.

- *En ny kamerabevakningslag (SOU 2017:55)*
  - Förslag att det ska bli enklare för kommuner att få tillstånd för kameraövervakning på offentliga platser
  - Möjligheterna att få tillstånd för kameraövervakning inom hälso- och sjukvården föreslås förbättras
- *Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)*
  - En ny lag om en hög gemensam nivå av säkerhet i nätverk och informationssystem föreslås
- *EU:s dataskyddsförordning och utbildningsområdet (SOU 2017:49)*
  - *Specificerar tolkning inom utbildningsområdet*

Patientdatalagen idag

- Gäller alla vårdgivare
- Ramlagstidning för informationshantering om patienter inom hälso- och sjukvård
- Utöver regler om journalföring även regler om patientdata
- Ansvar för verksamhetschef
- Regler om direktåtkomst, sammanhållen journalföring m.m.

Lagen om behandling av personuppgifter inom Socialtjänsten idag

- Gäller all verksamhet inom socialtjänsten och verksamhet som i annat fall enligt lag handhas av socialnämnd
- Personuppgiftsansvarig är den som behandlar personuppgifter inom sin socialtjänstverksamhet
- Särskilda regler om sammanställningar av personuppgifter, sekretess m.m.

När gäller GDPR?

- *Gäller för ansvarig eller biträde **etablerad i unionen**, oavsett om behandlingen utförs i unionen eller inte*
- Även om inte etablerade i unionen
  - Avser registrerade som befinner sig i unionen; och
  - Behandlingen har anknytning till utbjudande av varor eller tjänster till sådana registrerade i unionen
- Ej privat natur
- Gäller all *behandling* av *personuppgifter*

Vad är en personuppgift?

- ***Personuppgifter*** – varje uppgift varigenom en fysisk person *direkt eller indirekt* kan identifieras
- Är detta en personuppgift?
  - Agnes.hammarstand@delphi.se
  - 83.248.106.125 (en IP-adress)
  - En adressuppgift
  - Ett bilregistreringsnummer eller bostadsadress
  - En bild:

Vad är en behandling?

- Definitionen av behandling är vid och omfattar **alla åtgärder** som vidtas i fråga om personuppgifter
- Exempel
  - Insamling
  - Registrering
  - Lagring
  - Spridning
  - Samkörning
  - Radering
- Undantag för bl.a. rent personligt bruk

Undantaget för ostrukturerat material är borttaget

- Enligt PuL fanns ett undantag för uppgifter som inte ”strukturerats för att påtagligt underlätta sökning”
- Nu omfattas även ostrukturerat material (i digital form)
- Lagen omfattar all behandling som
  - *”helt eller delvis företas på automatisk väg”; och*
  - annan behandling som *”ingår i eller kommer ingå i ett register”*
- Påverkar t.ex. löpande text i ordbehandlingsprogram, text eller e-mail, inlägg på sociala medier

I praktiken...

- Register
  - Alla olika register över registrerade medborgare
  - Register med leverantörer och samarbetspartners
  - Anställningsregister
  - Kandidater (för anställningar)
  - Anhörigregister
- Eventuella andra registrerade, t.ex. nyhetsbrev
- Annan behandling – t.ex. GPS-övervakning, digitala tjänster, molntjänster, appar, dokument, whistleblowingsystem, passersystem, sociala medier och hemsidan
- Även ostrukturerad data, t.ex. mejl och dokument

Sanktioner

- Rätt för individer att kräva skadestånd och straff
- Varning, reprimand eller ”beordran”
- Begränsning eller förbud
- Administrativa böter (”böter”)
- Medlemsstaterna ska fastställa sanktioner för de överträdelser som inte är föremål för böter och säkerställa att sanktionerna genomförs

Böter för en kommun (enligt förslaget prop. 2017/18:105)

- 1: Upp till det högre beloppet av 5 000 000 kr
  - Mindre allvarliga överträdelser
- 2: Upp till det högre beloppet av 10 000 000 kr
  - Allvarliga överträdelser
  - Underlåtenhet att följa förlägganden och beslut av tillsynsmyndigheten
  - Underlåtenhet att bistå tillsynsmyndigheten
- Vid bestämmandet av avgiftens storlek i det enskilda fallet ska dataskyddsförordningens bestämmelser tillämpas

Administrativa böter – Hur?

- Administrativa böter ska *beroende på omständigheterna i det enskilda fallet* åläggas utöver eller i stället för andra åtgärder
- Böterna ska vara *effektiva, proportionella* och *avskräckande*
- Harmoniserade bötesnivåer
- Hänsyn till ett antal faktorer, t.ex.
  - Överträdelsens natur, svårighetsgrad och varaktighet
  - De åtgärder som vidtagits för att lindra skada
  - Graden samarbete med myndigheterna/egen anmälan
  - Genomförda säkerhetsåtgärder

Tillsyn

- Nationell tillsynsmyndighet
  - Datainspektionen som föreslås byta namn till ”Integritetsskyddsmyndigheten”
- Europeisk dataskyddstyrelse
  - Består av chefen för en tillsynsmyndighet per medlemsstat och Europeiska datatillsynsmannen

Konsekvenser av lagen

- Dataskydd blir en ledningsfråga
- Viktigare att följa lagen
- Integritetsfrågorna får mer uppmärksamhet och kräver resurser, organisation och budget
- Ökat fokus på förebyggande åtgärder och dokumentation
- System och databaser kan bli olagliga

Vem ansvarar?

Personuppgiftsansvarig

- *”En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra **bestämmer ändamålen och medlen för behandlingen** av personuppgifter*”
- Ansvarar alltid självständigt för att lagen uppfylls och ska kunna **visa** att lagen följs
- Det är alltså ni som ansvarar för att t.ex. era IT-system uppfyller lagens krav (inte leverantören)
- Ska genomföra lämpliga organisatoriska och tekniska åtgärder för att följa lagen – när lämpligt anta policyer.
- Jfr. personuppgiftsombud (nu dataskyddsombud) – en fysisk person

Särskilt om vårdgivare

- I lag kan förskrivas att någon är personuppgiftsansvarig
- Exempel: Vårdgivare är alltid personuppgiftsansvarig enligt Patientdatalagen
- ”Vårdgivare” och ”vårdenheter”
- Socialdataskyddsutredningen (SOU 2017:66)
- Inga förändringar vad gäller *ansvar* för behandling av personuppgifter om patienter inom hälso- och sjukvården föreslås

Personuppgiftsansvarig i kommunen

- I en kommun är typiskt sätt både kommunstyrelsen och de kommunala nämnderna personuppgiftsansvariga för sina egna behandlingar
- Självständig nämnd = egen förvaltningsmyndighet = eget personuppgiftsansvar
- Om olika nämnder är olika juridiska personer – då kan inte uppgifter föras ut mellan nämnderna hur som helst
- Inga förändringar föreslagna

Gemensamt personuppgiftsansvar

- *”Om två eller flera personuppgiftsansvariga **gemensamt** fastställer ändamålen med och medlen för behandlingen av personuppgifter”*
- Ska gemensamt fastställa sitt respektive ansvar avseende den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla information
- Delge väsentliga drag i arrangemanget för registrerade
- Den registrerade kan utöva sina rättigheter mot var och en av de personuppgiftsansvariga

Personuppgiftsbiträde

- *”En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som **behandlar personuppgifter för den personuppgiftsansvariges räkning**”*
- Finns alltid utanför den personuppgiftsansvariges organisation
- Utökade direkta skyldigheter
- Tillsynsobjekt - kan också åläggas sanktionsavgift

→Vem är personuppgiftsansvarig?

- Vem är personuppgiftsansvarig för vilka uppgifter?
- Är ni gemensamt personuppgiftsansvariga?
- Vilka biträden har ni?

Hur avgöra vem som är personuppgiftsansvarig?

- Vem bestämmer syftena med behandlingen?
- Vem bestämmer hur behandlingen ska ske?
  - T.ex. vilka uppgifter ska behandlas, vilka ska få tillgång till dem och när ska uppgifter raderas
- Den som enbart har tillgång till ett system är normalt inte ansvarig (om denne inte bestämmer någonting)

De grundläggande principerna och hur får personuppgifter behandlas?

Vad innebär reglerna i korthet?

- Identifiera varje behandling och lista dessa i en registerförteckning
- Varje behandling (och varje register) ska vara laglig
- Uppgifter får inte behandlas (t.ex. lagras) om ni inte har ett lagligt stöd för det – inga onödiga uppgifter
- Ha olika rutiner, dokumentation och policys på plats för att följa reglerna
- Arbeta aktivt med lagen, skapa medvetenhet m.m.

“Accountability”

- Kommuner ska kunna **visa** att lagen följs
- Den allmänna anmälningsskyldigheten försvinner – i stället får ni större eget ansvar
- Krav på att
  - Varje behandling ska vara laglig
  - Krav på att ha olika rutiner, dokumentation och policyer på plats för att följa reglerna
  - Ordning och reda, policyer och rutiner
  - Krav att arbeta aktivt med lagen, skapa medvetenhet m.m.
- Skyldighet för personuppgiftsansvariga (och biträden) att föra register över behandlingen ”Registerförteckning” (se vidare nedan)

Grundläggande principer

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
  - Uppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål
  - Får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål
- Uppgiftsminimering
  - Uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen
- Korrekthet
  - Uppgifter ska vara korrekta och om nödvändigt uppdaterade, annars raderas eller rättas
- Lagringsminimering
  - Uppgifter får inte sparas längre tid än nödvändigt för ändamålen
- Integritet och konfidentialitet
  - Krav på säkerhet, inbegripet skydd mot obehörig/otillåten behandling och mot förlust

”Integritetstrappan” – vilka regler gäller enligt lagen (exempel)?

Är behandlingen laglig?

Grundläggande principer att följa, t.ex. gallring, tid

Speciella krav för känsliga uppgifter

Information till registrerade (personuppgifts-policy)

Säkerhet, rutiner för dataportabilitet, etc.

Avtal, dokumentation, rutiner, m.m.

Förbud att flytta uppgifter utanför EU

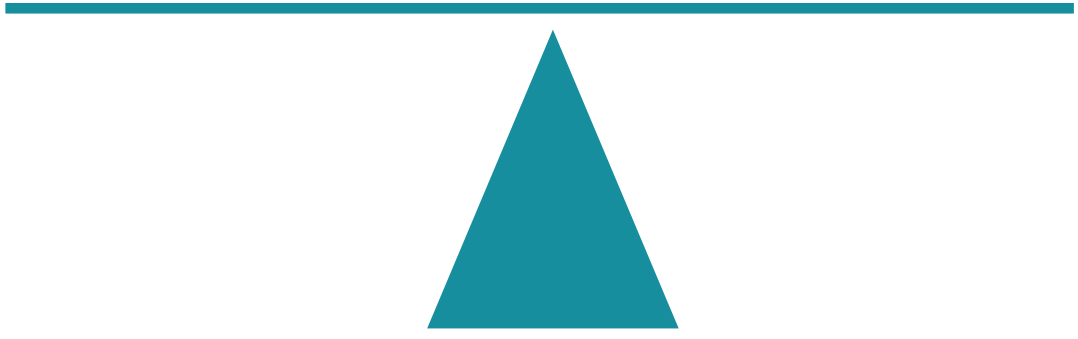
När är behandling tillåten?

- Samtycke från den registrerade
- Nödvändig för att ett avtal med den registrerade ska kunna fullgöras
- Nödvändig för att fullgöra rättslig förpliktelse
- Nödvändig för att skydda intressen av grundläggande betydelse för registrerade eller annan fysisk person
- Nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning
- Intresseavvägning

Intresseavvägning

Den registrerades intressen eller grundläggande rättigheter och friheter

Personuppgiftsansvariges *berättigade* intresse



Intresseavvägning

→ Vilka behandlingar och register har ni? Laglig grund?

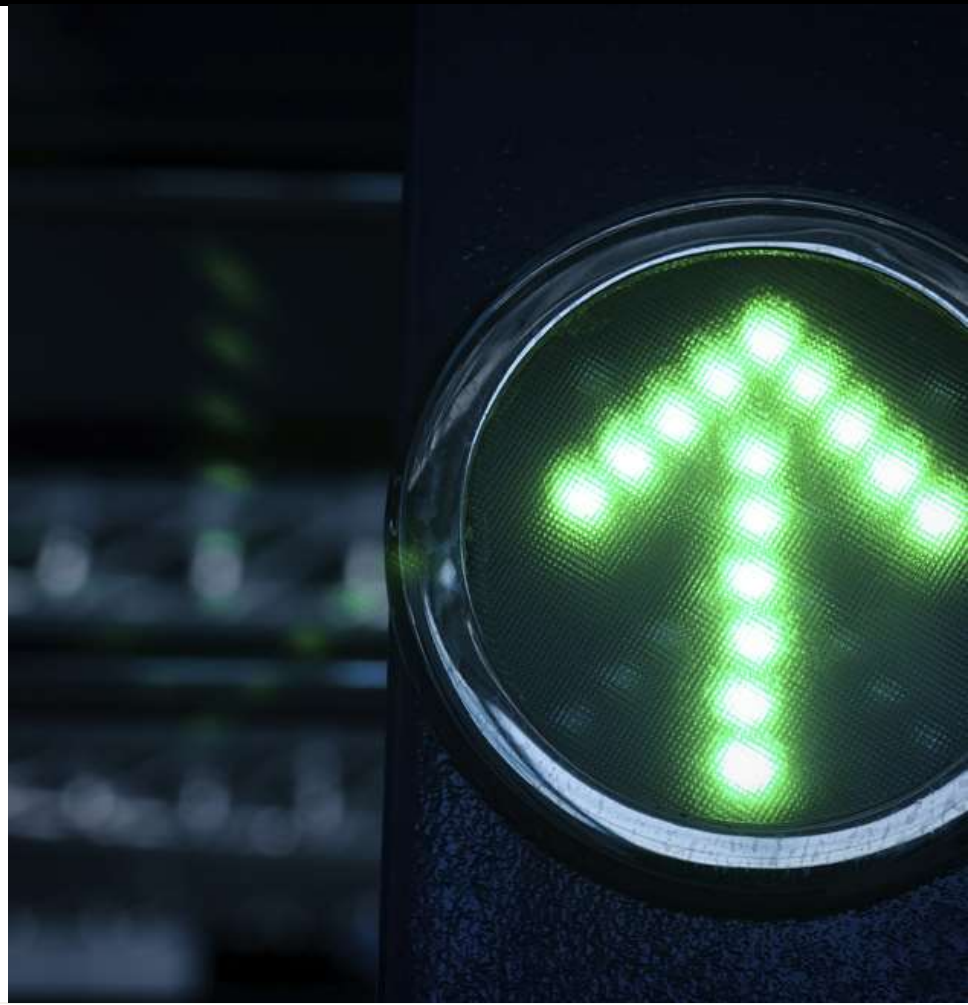
- Hur kan vi börja identifiera dessa?
- Olika register
  - Era register om olika kategorier medborgare
  - Register med leverantörer och samarbetspartners
  - Anställningsregister
  - Kandidater (för anställningar)
- Eventuella andra registrerade, t.ex. nyhetsbrev
- Annan behandling – t.ex. GPS-övervakning, digitala tjänster, molntjänster, appar, dokument, whistleblowingsystem, passersystem, sociala medier och hemsidan
- Även ostrukturerad data, t.ex. mejl och dokument

Samtycke

- *”Varje slag av **frivillig, specifik, informerad, och otvetydig viljeyttring**, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande behandling, godtar behandling av personuppgifter”*
- Informerat samtycke – information först
- Kan vara muntligt eller skriftligt

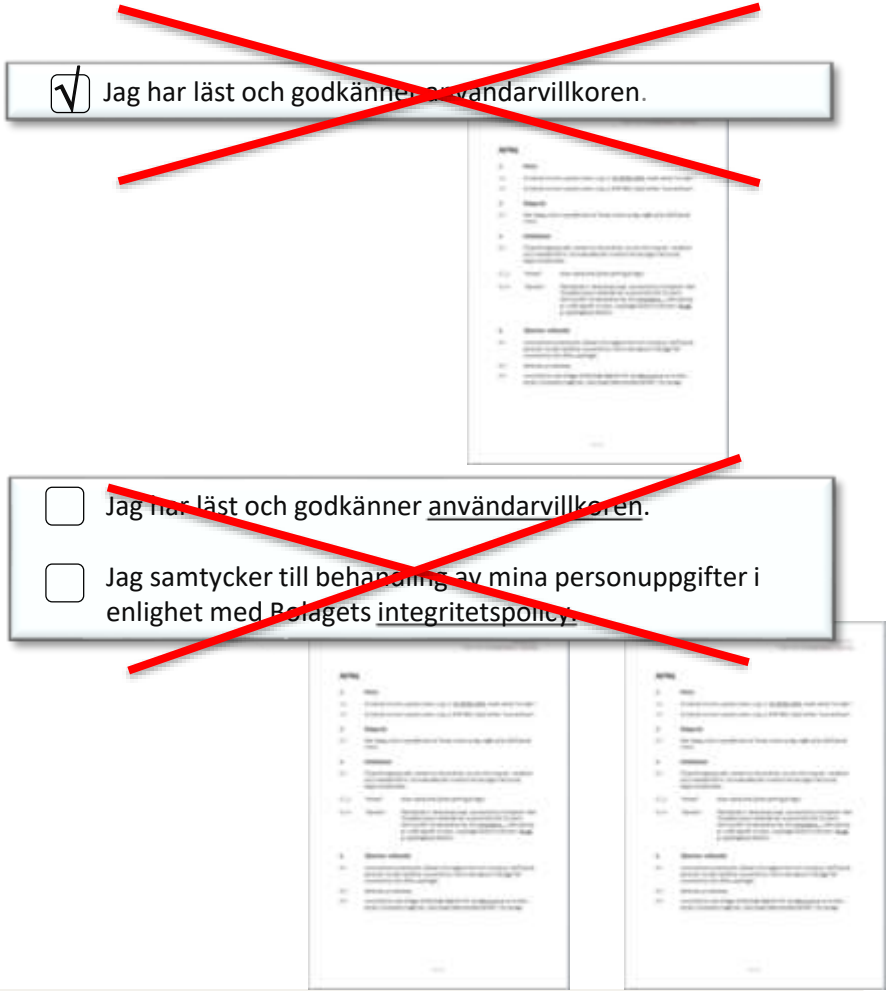
Frivilligt

- Största hänsyn ska tas till om ett avtal villkorats av samtycke trots att detta inte är nödvändigt för genomförandet av avtalet
- Det får inte råda betydande ojämlikhet mellan parterna (anställningsförhållande)
- Fri valmöjlighet eller inte?
- Det ska vara lika lätt att återkalla sitt samtycke som att lämna det
- Separata samtycken för olika behandlingar



Skriftligt samtycke

- Begriplig och lättillgänglig form
- Klart och tydligt språk
- Ej oskäliga villkor
- Kunna särskiljas från andra frågor i en ”begriplig och lättillgänglig form”
- Bör vara separat text och separat text



Inhämta nytt samtycke?

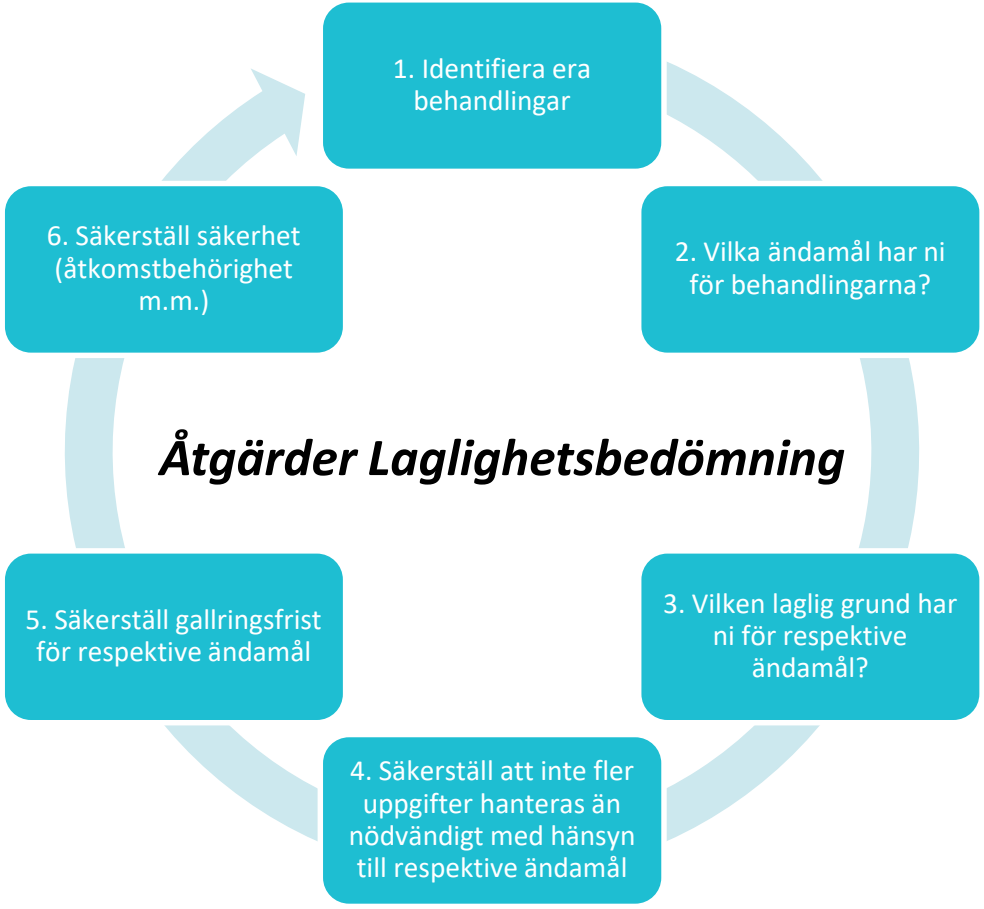
- När förordningen börjar tillämpas upphävs det direktiv som PuL grundas på
- Alla samtycken behöver då följa nya lagen
- Om behandlingen grundar sig på samtycke enligt direktivet är det inte nödvändigt att inhämta samtycke på nytt för att behandlingen ska kunna fortsätta efter att förordningen börjar tillämpas
  - ”Om det sätt på vilket samtycket gavs överens-stämmer med förordningens bestämmelser”

→ *Åtgärder samtycke*

- *Använder ni samtycke idag?*
- *Vilka samtycken vill ni/behöver ni ha?*
- *Se över om gamla samtycken är giltiga*
  - *Kan information behöva raderas?*
  - *Behöver nya samtycken inhämtas?*
- *Kan vi finna alternativ laglig grund istället för samtycke?*
- *Skriv nya samtyckestexter och utvärdera hur många samtycken som behövs i visst fall*?

Laglighetsbedömning

- Vad är ändamålet med en viss behandling?
- Finns laglig grund enligt förordningen?
  - Nödvändigt p.g.a. avtal med den registrerade
  - Laglig skyldighet att utföra behandling, t.ex. bokföringslag, arbetsmiljölag, osv.
  - Intresseavvägning
- Annars behövs samtycke!
  - Är samtycke en rimlig och proportionell åtgärd eller ska vi låta bli att utföra behandlingen?
  - Hur samlar vi in samtycket?


1. Identifiera era behandlingar
2. Vilka ändamål har ni för behandlingarna?
3. Vilken laglig grund har ni för respektive ändamål?
4. Säkerställ att inte fler uppgifter hanteras än nödvändigt med hänsyn till respektive ändamål
5. Säkerställ gallringsfrist för respektive ändamål
6. Säkerställ säkerhet (åtkomstbehörighet m.m.)
Åtgärder Laglighetsbedömning

Förslag till nya ePrivacy-regler

- Förslag till förordning om integritet och elektronisk kommunikation (COM (2017) 10 final)
- Kompletterar dataskyddsförordningen
  - Speciallag
  - Samma regler i hela EU
  - Även många andra nyheter för operatörer
- Risk för böter upp till 4 % av omsättningen
- *Förslag till nya regler för cookies*
- *Liknande regler som idag rörande direktmarknadsföring – men hårdare sanktioner och europeisk lika regler*
- *Förslag: Antas senast den 25 maj 2018 (?)*

ePrivacy

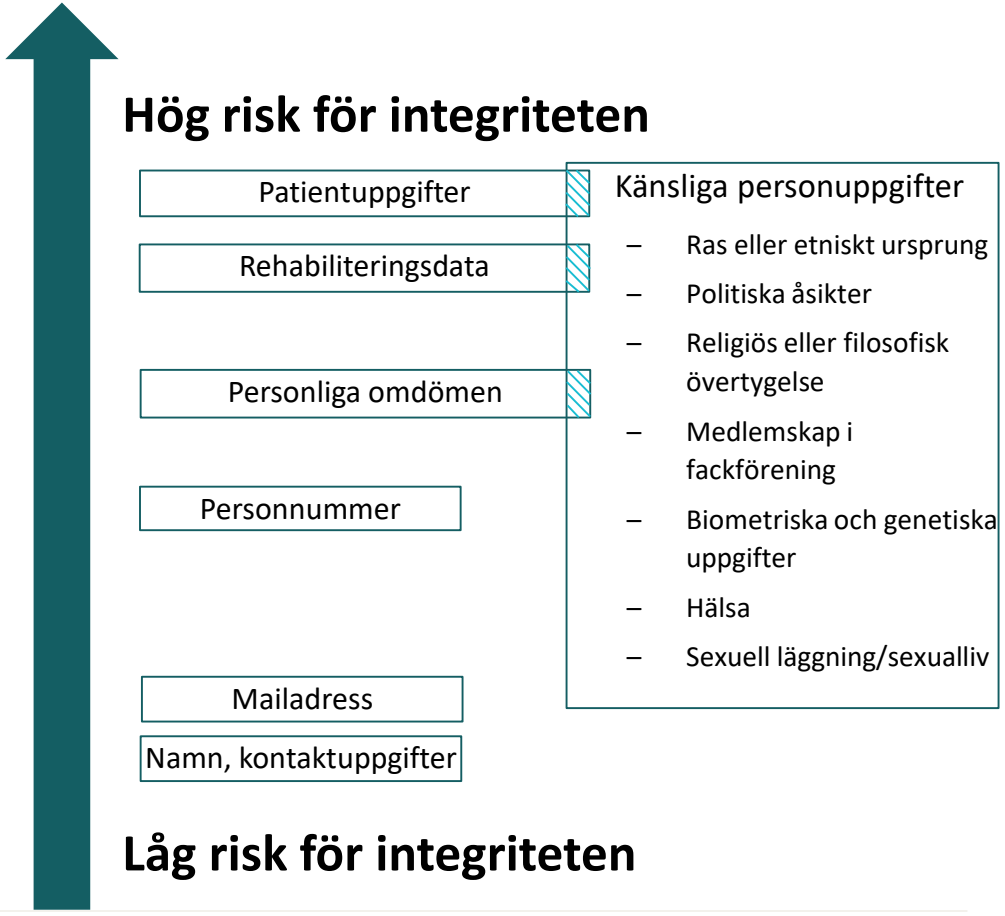
- Samtycke ska ej behövas om nödvändigt för att
  - Tillhandahålla tjänst användaren begärt, t.ex. titta på en hemsida, spara varukorg, tillhandahålla en onlinetjänst
  - Mäta antalet webbplatsbesökare
- Undantagen från samtycke gäller inte 3:e parts cookies
  - Vid användning av Google Analytics, bannerreklam, m.m. bör alltid samtycke krävas
  - Viktigare att ha koll på tilläggstjänster m.m.
- Krav på webbläsare att kunna ge samtycke eller förbud mot cookies vid installation samt möjlighet blockera cookies
- Slutet på vanliga cookie-banners?

Känsliga personuppgifter

- Känsliga personuppgifter (”en särskild kategori uppgifter”)
  - Ras eller etniskt ursprung
  - Politiska åsikter
  - Religiös eller filosofisk övertygelse
  - Medlemskap i fackförening
  - Biometriska och genetiska uppgifter
  - Hälsa
  - Sexuell läggning/sexualliv
- Får fortfarande bara behandlas i undantagsfall, exempelvis
  - Uttryckligt samtycke
  - *Nödvändig* behandling för vissa syften inom arbetsrätten och angivna syften enligt nationell lag, t.ex. omsorg, socialt skydd

Desto mer känsliga uppgifter – ju hårdare tolkas principerna

- Ju högre risk för integritetskränkning ju viktigare är principerna
- Behöver inte alltid bero på kategoriseringen av data



Förslag till undantag för hantering av känsliga uppgifter (prop. 2017/18:105)

- Kommuner ska få behandla känsliga personuppgifter
  - I löpande text om uppgifterna lämnats i ett ärende eller är nödvändiga för handläggning av ett ärende
  - Om uppgifterna lämnats till kommunen och behandlingen krävs enligt lag
  - I enstaka fall om det är absolut nödvändigt för ändamålet med behandlingen och den inte innebär otillbörligt intrång i den registrerades rättigheter
- OBS! Sökbegrepp som avslöjar känsliga uppgifter får ej användas

Särskilt om vissa andra personuppgifter

- Förslag enligt prop. 2017/18:105
- Specialregel om personnummer föreslagen. Får behandlas utan samtycke endast när det är klart motiverat med hänsyn
  - till ändamålet med behandlingen
  - vikten av en säker identifiering
  - något annat beaktansvärt skäl
- Förbjudet att hantera uppgifter om fällande domar och överträdelser (tidigare brott) förutom i undantagsfall t.ex. för att anmäla brott

→ Känsliga personuppgifter - åtgärder

- *Åtgärd: Hur behandlar ni känsliga personuppgifter?*
- *Är behandlingen strikt nödvändig för att uppfylla vår skyldighet enligt lag?*
- *Kan ni mappa känsliga personuppgifter?*

→ Möjlighet anonymisera?

- Kan informationen anonymiseras och presenteras på ett generellt plan?
  - Då gäller inte personuppgiftslagen
- Sammanställning av data för t.ex. statistik
- *Åtgärd: Vilken data behöver ni för ändamål där ni kan ha den anonymt?*

Individens rättigheter

Information som ska lämnas självmant

- ”Privacy policy”, ”Information om behandling av personuppgifter”, ”Integritetspolicy”
- Information ska lämnas självmant till alla registrerade
- Mer omfattande information än enligt PuL
- Olika krav beroende på om uppgifterna samlats in från den registrerade själv eller ej

Undantag från informationsskyldigheten

- Kravet på att självmant lämna information gäller inte om uppgifterna enligt lag eller författning inte får lämnas ut (både för det fall uppgifterna kommer från den registrerade själv eller från annan)
- Om uppgifterna inte har samlats in från den registrerade själv finns ytterligare undantag
  - Sekretesslag eller tystnadsplikt
  - Erhållande eller utelämnande uttryckligen föreskrivs i lag som även fastställer lämpliga åtgärder för att skydda den registrerades intressen
  - Omöjlig under vissa omständigheter, bl.a. allmänt intresse

Utökade informationskrav enligt patientdatalagen

- Kraven på information till den registrerade utökas om behandlingen omfattas av patientdatalagen. Då ska den registrerade även informeras om
  - Vilken uppgiftsskyldighet som följer av lag eller förordning
  - Vilka sekretess- och säkerhetsbestämmelser som gäller för uppgifterna och behandlingen
  - Rätten att begära att vissa uppgifter spärras
  - Rätten att få information om vilken direktåtkomst eller elektronisk åtkomst som har förekommit
  - Rätten till skadestånd
  - Vad som gäller för sökbegreppet, direktåtkomst och utlämnande av uppgifter med automatiserad behandling
  - Information som ska lämnas innan journal görs tillgänglig för annan vårdgivare

Information som ska lämnas självmant

- *→ Åtgärd: Ta fram eller uppdatera informationshandlingar och integritetspolicyer*
  - *Anställda och kandidater*
  - *Medborgare av olika kategorier*
  - *Övriga registrerade*

Information på begäran - registerutdrag

- Registrerade har rätt att begära ut information om t.ex. kategorier av uppgifter som behandlas, mottagare, period, m.m.
- Även rätt att få en kopia på uppgifterna
- Ska lämnas utan onödigt dröjsmål och senast inom en månad efter begäran
- Perioden får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden

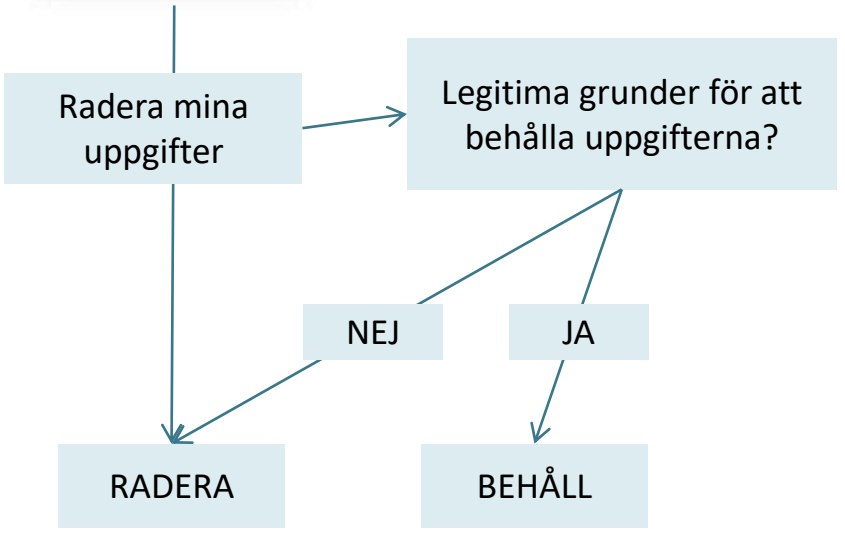
Information på begäran - registerutdrag

- Kravet på att lämna information på begäran gäller inte om uppgifterna enligt lag eller författning inte får lämnas ut
- Registerutdrag behöver som huvudregel inte innefatta information från löpande text som inte har färdigställts eller som är minnesanteckningar eller liknande
- Registerutdrag som lämnas från socialnämnden behöver inte heller innehålla information som den registrerade redan har fått, exempelvis eftersom denne har informerats enligt förvaltningslagen. Men den registrerade ska informeras om vilka handlingar som finns i ärendet
- *→ Åtgärd: Kan ni hantera registerutdrag? Se över rutinerna för registerutdrag! Vem hanterar? E-mailadress/kontaktperson*

Rätten att ”bli bortglömd”

Minimera volymen av sparade personuppgifter

Krav på att radera - om ingen legitim grund för fortsatt behandling finns



→ *Åtgärd: Säkerställ att det är möjligt att bli glömd*

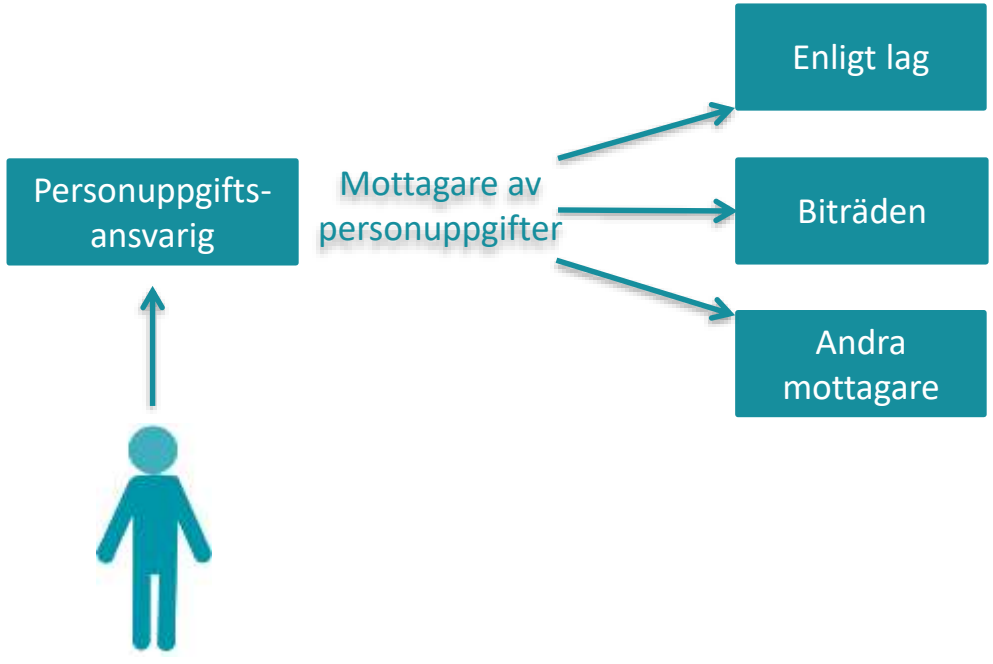
Rätt till rättelse och begränsning

- Den registrerade har rätt att kräva att uppgifterna rättas, raderas eller begränsas
- Vid rättelse, begränsning eller radering: Viktigt meddela personuppgiftsbiträden/mottagare av uppgifter att också rätta, begränsa och radera!
- → *Åtgärd*: *Se över rutiner för att säkerställa rättning, radering och begränsning*

Överföring av personuppgifter

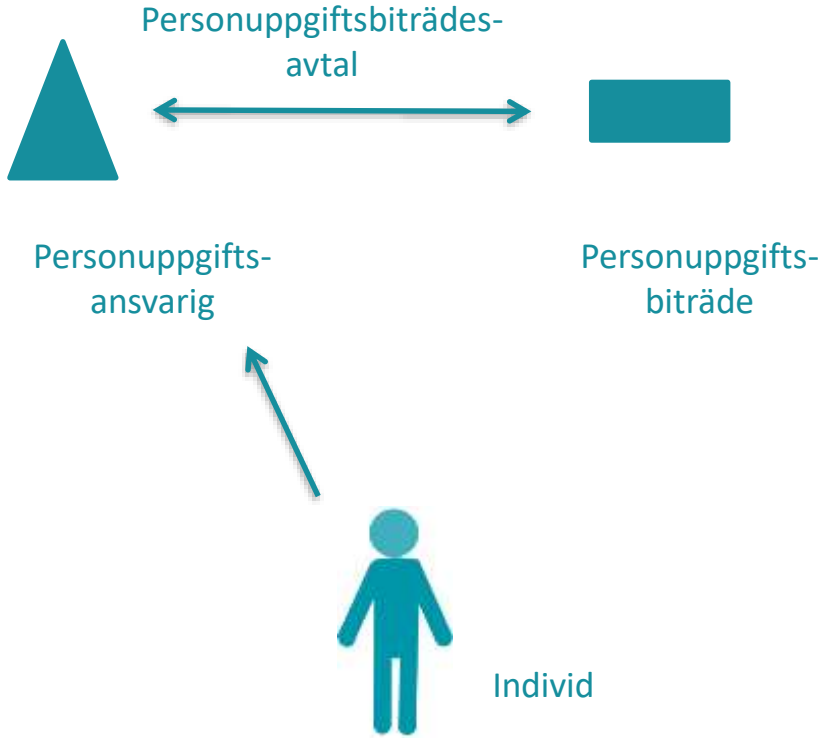
Delning av personuppgifter

- Fundera över vilka ni delar personuppgifter med
- Biträden – behandlar för er räkning
- Övriga: Vilket lagligt stöd har ni för att dela uppgifterna?
- Informera i er policy till registrerade

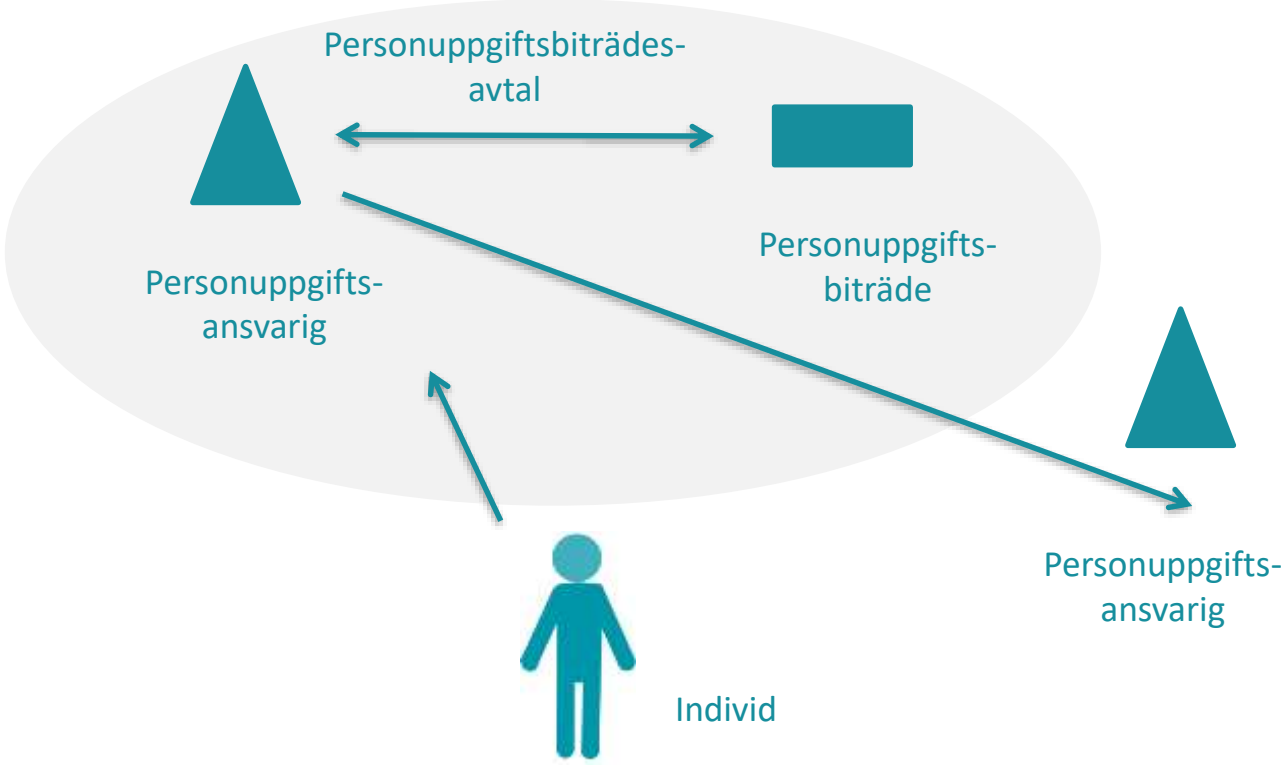


Krav på personuppgiftsbiträdesavtal

- Biträdesavtal ska finnas med alla biträden
- Utökade krav på biträden
- Inte längre ett standardavtal – viktigt anpassa till situationen – förhandla



Vem är biträde resp. ansvarig



Dokumenterade instruktioner

- I avtalet ska särskilt förskrivas att biträdet endast får agera enligt ansvariges *dokumenterade* instruktioner
- Instruktionerna behöver anpassas till vilken detaljnivå som biträdet ska hantera uppgifter på
  - Informationssäkerhet OCH praktiska rutiner
  - Vilka uppgifter, hur länge, osv.
- Kan t.ex. vara en bilaga till biträdesavtalet

Att tänka på vad gäller biträdesavtal

- Två delar

  1. Det juridiska avtalet

  2. Dokumenterade instruktioner - i avtalet ska särskilt förskrivas att biträdet endast får agera enligt ansvariges *dokumenterade* instruktioner

- Svårt ha en mall – men försök skapa malldokument för olika typsituationer!
- Hur säkerställs bra rutiner för hur ni kan arbeta med avtal? När anlita jurist? När klara själv?

→ *Åtgärder biträdesavtal*

- Vilka biträden har ni?
- Vem för förteckning över dessa?
- Ta fram mallar till personuppgiftsbiträdesavtal eller uppdatera gamla personuppgiftsbiträdesavtal
  - Vilka olika mallar behövs?
- Hur säkerställer ni att avtal ingås?
- Var lagras avtalen?
- Hur säkerställs bra rutiner för hur ni kan arbeta med avtal? När anlita dataskyddsjurist? När klara själv?

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3, Allmänna dataskyddsförordningen EU 2016/679[1]

Detta Personuppgiftsbiträdesavtal är träffat (2018-00-00) mellan:

(nedan kallad "Personuppgiftsansvarig"), organisationsnummer #, med adress # och,
(nedan kallad "Personuppgiftsbiträde"), organisationsnummer #, med adress # (gemensamt benämnda "Parterna") har denna dag träffat följande Personuppgiftsbiträdesavtal.

1 BAKGRUND OCH SYFTE

1.1 Detta Personuppgiftsbiträdesavtal är en del av ett huvudavtal om tillhandahållandet av tjänster som ingåtts mellan Kommunen/Landstinget/Regionen och leverantören och ska läsas och förstås mot bakgrund av detta. Personuppgiftsbiträdesavtalet reglerar Personuppgiftsbiträdets behandling av Personuppgifter för Personuppgiftsansvarigs räkning samt den integritetsnivå som ska uppnås vid Behandlingen (nedan kallad behandling/en).

1.2 Detta Personuppgiftsbiträdesavtal syftar till att säkerställa de registrerades fri- och rättigheter

Viktiga förhandlingspunkter

- Ansvarsfördelning
- Hur biträdet får överföra utanför EES-området
- Hur biträdet får anlita underbiträden
  - Särskilt förhandstillstånd
  - Allmänt förhandstillstånd
- De dokumenterade instruktionerna
- Ersättning
- Vad ska ske efter avslutat behandling?
  - Återlämna
  - Radera

Överföring av personuppgifter

- Huvudregeln är ett **förbud mot överföring av personuppgifter utanför EU**
- Lagstiftningen ska inte kunna kringgås genom att flytta ut data
- Behöver ha koll på var data behandlas
- Räcker att någon ges tillgång till data t.ex. för support
- Viktigt att ha koll på leverantörer – lovar de att bara behandla personuppgifter inom EU?

Tillåten överföring

- Kommissionen kan besluta att ett land eller en internationell organisation *”säkerställer en adekvat skyddsnivå”* = överföring kräver då inget särskilt tillstånd
- Ett flertal listade länder, t.ex. EES-länderna
- Inte Kina, USA, Indien

Lämpliga skyddsåtgärder

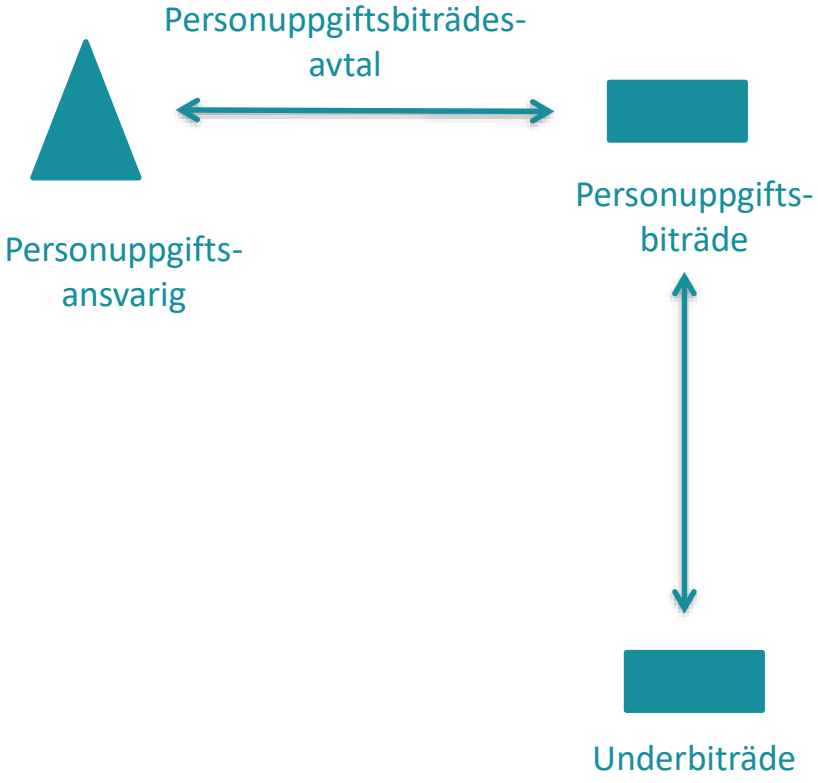
- Ett rättsligt bindande och verkställbart instrument
- Bindande företagsbestämmelser *(”Binding Corporate Rules”*)
- Standardiserade dataskyddsbestämmelser som antas/godkänns av tillsynsmyndighet och kommissionen
- Godkänd uppförandekod/certifieringsmekanism
- Avtalsklausuler (*”Standard Contractual Clauses”, även kallade (”Modellklausulerna”)*)
- Vissa undantag i enskilda fall

Lämpliga skyddsåtgärder i praktiken

- Modellklausulsavtal - standardavtal
  - Använd dessa!
- Binding Corporate Rules (BCR)
  - Tillsynsmyndigheten godkänner bindande företagsbestämmelser
  - Företagsintern policy
- Privacy Shield (USA)
  - En form av certifiering för amerikanska företag
  - Ett ramverk som ska göra det möjligt att överföra personuppgifter från Europa till USA

Hur ingå modellklausuler och biträdesavtal praktiskt?

- Säkerställ kontroll – ni måste i avtal ha en rättighet att få reda på vilka underbiträden personuppgiftsbiträdet har
- Informationsskyldighet till ansvarige om underbiträden
- Samma villkor måste gälla för underbiträden som för personuppgiftsbiträdet
- Modellklausulerna får inte ändras eller sättas ur spel genom annat avtal
- Ange tillämplig lag – (om behandling i Sverige så ska svensk rätt anges)



Åtgärder: Hur göra i praktiken?

- Vet ni var era biträden behandlar uppgifter?
- Utbilda organisationen om t.ex. cloudtjänster och andra varningsklockor
- För enstaka avtal: Använd modellklausulerna
- Säkerställ att biträdesavtalen innehåller praktiska möjligheter att kontrollera var behandling sker och av vem – exempelvis genom krav på informationsskyldighet, audits, biträdets anlitande av underbiträden etc.

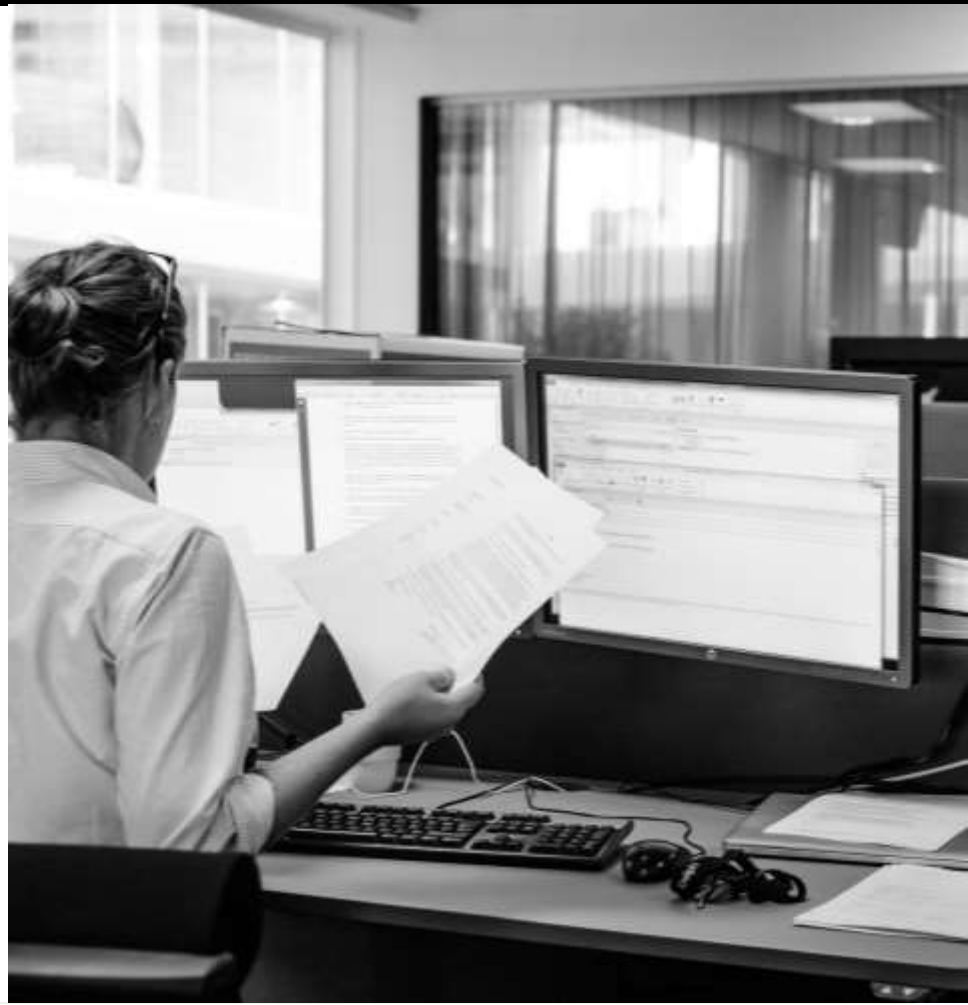
Upphandling av IT-tjänster och molntjänster

- Så snart personuppgifter ska behandlas: Viktigt hur upphandlingen görs
  - Privacy-krav på systemet eller tjänsten - Privacy by design
  - Risk- och sårbarhetsanalys (teknik)
  - Krav på personuppgiftsbiträdesavtal (och avtalet i övrigt)
  - Krav på dokumenterade instruktioner
  - Laglig grund om överföring till tredje land (t.ex. modellklausulerna) alt. löfte i avtal att ej överföra till tredje land
  - Speciallag
- Vid molntjänster och outsourcing: Extra krav för att bl.a. säkerställa att lagarna inte kringgås
  - Svårigheter kring kontroll av underbiträden
- *Åtgärd: Säkerställ att rutiner följs vid upphandlingar*

Vem ansvarar internt? Dataskyddsombud m.m.

Vem ansvarar internt?

- Tidigare: Personuppgiftsombud, nu dataskyddsombud
- Måste utses av alla offentliga organ
- Förändrad roll
- Tydligare regler och krav för dataskyddsombudet



Krav på dataskyddsombud

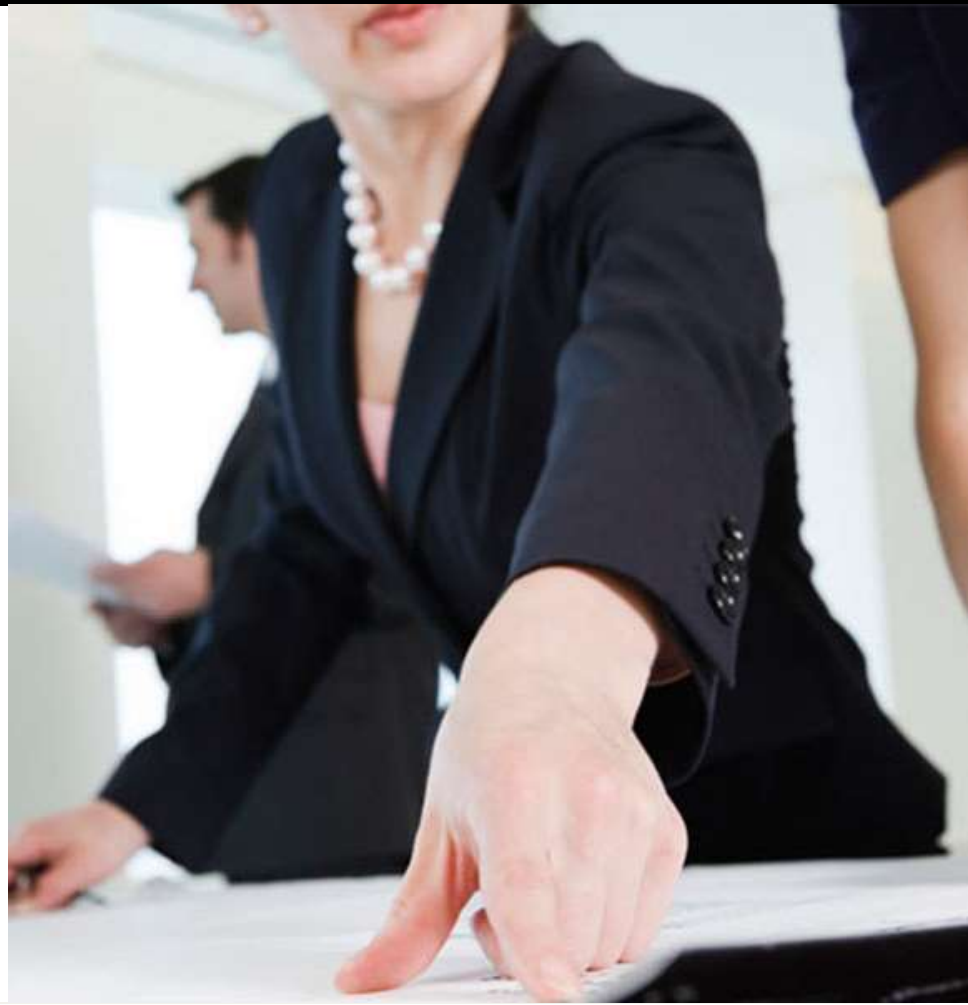
- Speciell anställd eller konsult med ansvar för personuppgiftshantering
  - Skapa medvetenhet, övervaka efterlevnad m.m.
- Kriterier för utnämnande
  - Yrkesmässiga kvalifikationer
  - Sakkunskap om lagstiftning och praxis om dataskydd
  - Förmågan att fullgöra sina uppgifter
- Dataskyddsombudets kontaktuppgifter ska offentliggöras och meddelas till Datainspektionen
- Dataskyddsombudet ska vara kontaktbar för de registrerade

Dataskyddsombudets ställning

- Ska *”på ett korrekt sätt och i god tid”* delta i alla frågor som rör skyddet av personuppgifter
- Ska erhålla stöd från personuppgiftsansvarig vid utförandet av sina arbetsuppgifter
- Ska få tillräckliga resurser, tillgång till personuppgifter och behandlingsförfaranden och upprätthållande av kunskap
- Får inte motta instruktioner som gäller utförandet av arbetsuppgifterna
- Får inte avsättas eller bli föremål för sanktioner
- Ska rapportera direkt till högsta förvaltningsnivå
- Får ha andra uppgifter och uppdrag, men den registeransvarige ska *”se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt”*
- *Åtgärder: Utvärdera om ni behöver anställa, vidareutbilda eller anlita en utomstående uppdragstagare!*

Vem utser ni?

- Kan vara anställd eller konsult
- Ska anmälas till Datainspektionen
- Ett dataskyddsombud kan utses för flera personuppgiftsansvariga eller offentliga organ *”med hänsyn till deras organisationsstruktur och storlek”*
- Samma dataskyddsombud för flera nämnder inom en kommun? Samarbete mellan mindre kommuner och myndigheter?



Registerförteckning, inventering och rutiner för att visa att lagen följs

Registerförteckning

- Krav på att föra ett register över alla behandlingar
- Registret ska innehålla
  - namn och kontaktuppgifter för den personuppgiftsansvariga och dataskyddsombudet
  - ändamålen med behandlingen
  - beskrivning av kategorierna av registrerade och personuppgifter
  - kategorier av mottagare
  - ev. överföringar till tredjeland eller internationella organisationer
  - förutsedda tidsfrister för radering
  - allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder
- *Åtgärd: Säkerställ rutiner för att föra och löpande uppdatera er registerförteckning*

Vad mer kan vara bra att ha i en registerförteckning?

- Namn på behandling
- Laglig grund
- Applikationer/system där behandlingen sker
- Lagras personuppgifter i en molntjänst?
- Har information lämnats?
- Kommentar

Hur kan en registerförteckning se ut?

- Inga formkrav
- En förteckning per behandling eller flera behandlingar i varje förteckning?
- Word eller Excel?
- Köpt applikation eller system?

Behandling av personuppgifter

Uppgifter till förteckning enligt 39 § Personuppgiftslagen

Förteckningen skall förvaras av personuppgiftsombudet. OBS Den skall inte sändas in till Datainspektionen. Detta är ett exempel på hur förteckningen kan se ut. Det är tillåtet att utforma den på annat sätt. Uppgifterna i fält markerade med * är dock obligatoriska.

Personuppgiftsansvarig	Namn (t.ex. myndighet eller juridisk person) *		Organisationsnummer *
	Postutdelningsadress *		
	Postnummer *	Ort/namn *	Telefonnummer *
Registret/behandlingen	Uppgifterna nedan är: ☐ Uppgifter om ny behandling ☐ Ändring av eller tillägg till tidigare anmälan ☐ Avanmälan		
	Registrets/behandlingens namn:		
	Ändamålet/ändamålen med behandlingen: *①		
	Övriga kategorier (grupper) av personer som berörs av behandlingen: *②		

	Behandlingens namn	Kategorier av registrerade	Avdelningen med behandlingen	Kategorier av personuppgifter	Laglig grund	Applikationsvyer av vår behandlingsmiljö	Lagrar personuppgifter i tredjeland?	Kategorier av mottagare	Sker överföring av personuppgifter utanför EU/EES eller till en internationell organisation? (Ja/Nej)	Det är [illegible]
2	Kontonummer	Anställda	Betala ut löner	Kontonummer	anställningsavtalet					
3	Anställningsdata	Anställda	Anställningsförhållanden, att anställda ska kunna fullgöra sina arbetsuppgifter	Kontaktuppgifter som namn, telefonnummer, e-mail	Nödvändigt för anställningsavtalet					
4	Anställningsdata	Anställda	Anställningsförhållandet, att anställda ska kunna fullgöra sina arbetsuppgifter	Användaruppgifter, e-mailadress	Nödvändigt för anställningsavtalet					
5	Anhöriguppgifter	Anhöriga till anställda	Kontakta anhörig om någon blir sjuk, dör, misshandlas eller försvinner	Namn, telefonnummer	Intresseavvägning eller samtycke?					
6	Kontaktpersoner hos leverantörer och samarbetspartners	Kontaktpersoner hos leverantörer och samarbetspartners	Administrera leverantörsavtalen	Kontaktuppgifter, e-mail, namn, telefonnummer	Intresseavvägning					
7	Kontaktuppgifter till kunder	Kunder	Administrera avtalsförhållandet, marknadsföring	Kontaktuppgifter, e-mail, namn, telefonnummer, inloggningsuppgifter	Nödvändig för avtalet. Intresseavvägning.					
8	Kunddata	Kunder	Administrera kundförhållanden, marknadsföring	Kunddata, köphistorik	Nödvändig för avtalet					
9	Kunddata	Kunder	Administrera kundförhållandet	Kontaktuppgifter som namn, telefonnummer, e-mail	Nödvändigt för avtalet. Intresseavvägning.					
10	Köphistorik	Kunder	Administrera kundförhållandet?	Köphistorik, personalrabatterna etc.	Nödvändigt för avtalet.					
11	Brott mot användaravtalet	Kunder	Kunna säkerställa om någon bryter mot användarvillkoren	Typ av brott mot användarvillkoren	Intresseavvägning					
12	Bokföring	Kunder	Följa bokföringslagen		Följa lagstiftning					
13										
14										
15										

→ Registerförteckning – hur gör ni?

- Hur vill ni föra ert register?
  - Excelark, köpt applikation eller egenutvecklad applikation?
  - Tänk på hur många som behöver access
  - Hur förvaltar ni registret på sikt? Var sparas registret? Hur uppdateras det?
- Påbörja registerförteckningen så tidigt som möjligt för att undvika dubbelarbete
- Vem ansvarar?

Inventering

- Hur inleder vi inventeringen?
- Hur kan insamlingen ske?
- Hur många personuppgiftsansvariga har ni?
- Vilka behandlingar har ni för respektive ansvarig?

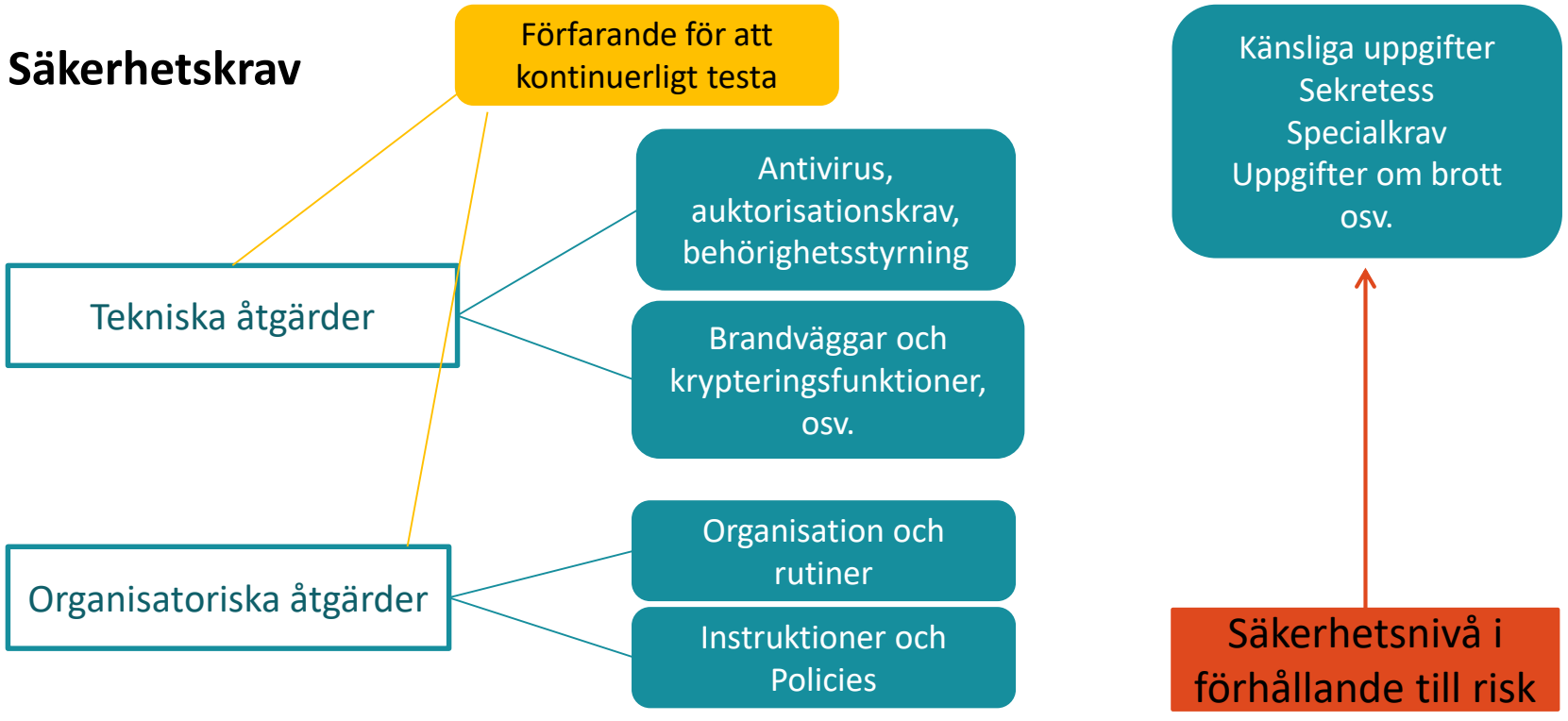
→ Hur bevisar vi att vi följer lagen?

- Var sparar vi alla biträdesavtal och avtal?
- Hur kan vi spara ev. samtycken?
- Hur kan vi i övrigt skapa rutiner för att visa att vi följer lagens alla krav?

Säkerhet och IT-krav

Utökade säkerhetskrav

- Ska ”*vidta **lämpliga tekniska och organisatoriska åtgärder** för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken”*
- Kan inbegripa t.ex.
  - Pseudonymisering och kryptering av personuppgifter
  - Fortlöpande kontroll av de system som behandlar uppgifterna och
  - System för att testa effektiviteten hos åtgärder som ska säkerställa behandlingens säkerhet
- Att följa en uppförandekod eller en standard kan användas för att visa att följer kraven
- Uttryckliga krav på att skydda personuppgifter från att förstöras och röjas



Åtgärder: Säkerställ att IT- och säkerhetsansvariga har kompetens och resurser för att arbeta med dataskydd. Se över era säkerhetsrutiner (såväl teknisk som organisatorisk, t.ex. NDA). Hur kan ni arbeta med säkerhetskraven?

Informationskrav vid person-uppgiftsincident

- Informera om *”personuppgiftsincident*” utan *oskäligt dröjsmål*
- Informera tillsynsmyndigheten
  - Som huvudregel: **Inom 72 timmar** efter vetskap om intrånget
- Informera varje registrerad individ
  - Om sannolikt leder till hög risk för enskildas rättigheter
  - Undantag, t.ex. om system finns för att bevisa att de ”förlorade” uppgifterna gjorts oläsbara för utomstående, t.ex. kryptering
  - Oproportionerlig ansträngning: Istället informera allmänheten
- Biträden ska underrätta ansvarig utan onödigt dröjsmål efter vetskap om incident

Informationskrav vid person-uppgiftsincident

- Anmälan till tillsynsmyndigheten ska åtminstone beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet personuppgifter som berörs
  - Förmedla namn och kontaktuppgifter på dataskyddsombud eller andra kontaktpunkter där mer information kan erhållas
  - Beskriva de sannolika konsekvenserna av personuppgiftsincidenten och
  - Beskriva de åtgärder som den ansvarige har vidtagit eller föreslagit för att åtgärda incidenten, inbegripet, när så är möjligt, åtgärder för att mildra dess potentiella effekter
- Alla incidenter, dess effekter och åtgärderna som vidtagits ska dokumenteras
- *Åtgärder: Se över/stärk era säkerhetsåtgärder och inför rutiner för att meddela registrerade individer*

Privacy by design

- ”Inbyggd integritet”
- Säkerhets- och integritetsaspekter ska tas hänsyn till redan vid planering och utveckling av IT-system
- De grundläggande principerna, t.ex. undvika fritextfält, behörighet, standardinställningar för lagring, m.m.
- Den som är personuppgiftsansvarig ska ställa kraven
- Anpassa systemen efter vilka dataskyddskrav som gäller för just er kommun och varje situation
- Kommissionen får fastställa förordningar om *tolkningen* samt *tekniska standarder*
- *Åtgärder: Inför rutiner för att ställa krav vid IT-upphandlingar samt utbilda eventuella arkitekter*

Privacy by design – exempel

- Behörighet
- Uppgiftsminimering
- Anonymisera om möjligt, undvik peka ut individer
- Begränsa åtkomsten till uppgifterna
- Hög säkerhet
  - Möjligheter till kryptering, säkerhetskopiering och loggar, säker utplåning
- Funktioner för autentisering
- Enkel möjlighet till gallring, automatisk och enkel radering av uppgifter som inte behövs
- Möjliggöra utelämnande av information till registrerade
- Minimera fritextfält

Privacy by design för applikationer

- Spåra laglig grund av uppgifterna
- Klassificera registrerad utifrån kategori (medborgare, leverantör, etc.)
- Standardinställningar för lagringsfrister och gallringstid
- Enkelt att helt radera
- Säkerhet
- Möjlighet till registerutdrag
- Behörighetsstyrning – begränsa åtkomst
- Om fritextfält – möjlighet att varna användaren

Andra krav på en leverantör

- Varierar beroende på onlinetjänst (Cloud) eller licens (on premise)
- Personuppgiftsbiträdesavtal
- Dokumenterade instruktioner
  - Säkerhet, sekretess, personal
- Krav på lagring i EES eller annan laglig grund för överföring

Krav enligt Socialstyrelsens föreskrifter för patientdata

- Speciella IT-säkerhetskrav enligt Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40)
- Loggar
  - Dokumentation och systematisk kontroll av åtkomst till patientdata. Patientens rätt att ta del av loggarna
  - Loggar ska sparas i fem år
- Strikt behörighetskontroll
  - Individuell behörighet per användare
  - Behörighet ska föregås av behovs- och riskanalys
  - Rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna och säkerställa att behörigheter är riktiga och aktuella
- Sammanhållen journalföring
  - Patientens rätt att motsätta sig vårdgivares direktåtkomst
- Säkerhetskopior: Krav på fastställd periodicitet och på förvaring på ett säkert sätt väl åtskilda från original

Krav enligt Socialstyrelsens föreskrifter forts.

- Vid utveckling av nya IT-system som används för behandling av personuppgifter
  - Vårdgivare ska säkerställa att personuppgifternas tillgänglighet, riktighet, sekretess och spårbarhet inte riskeras
  - Krav på att testa nya system innan de tas i drift
  - Krav på att upphandlad utvecklare uppfyller HSLF-FS 2016:40
- Behandling i öppna nät
  - Särskilda skyddsåtgärder, så inte obehöriga kan ta del av överförda uppgifter
  - Elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering, dvs. kontroll av identitet på två olika sätt
  - Enskildas direktåtkomst tillåts endast efter att den enskildes identitet har säkerställts genom stark autentisering

→ Hur hanterar ni säkerhetskrav?

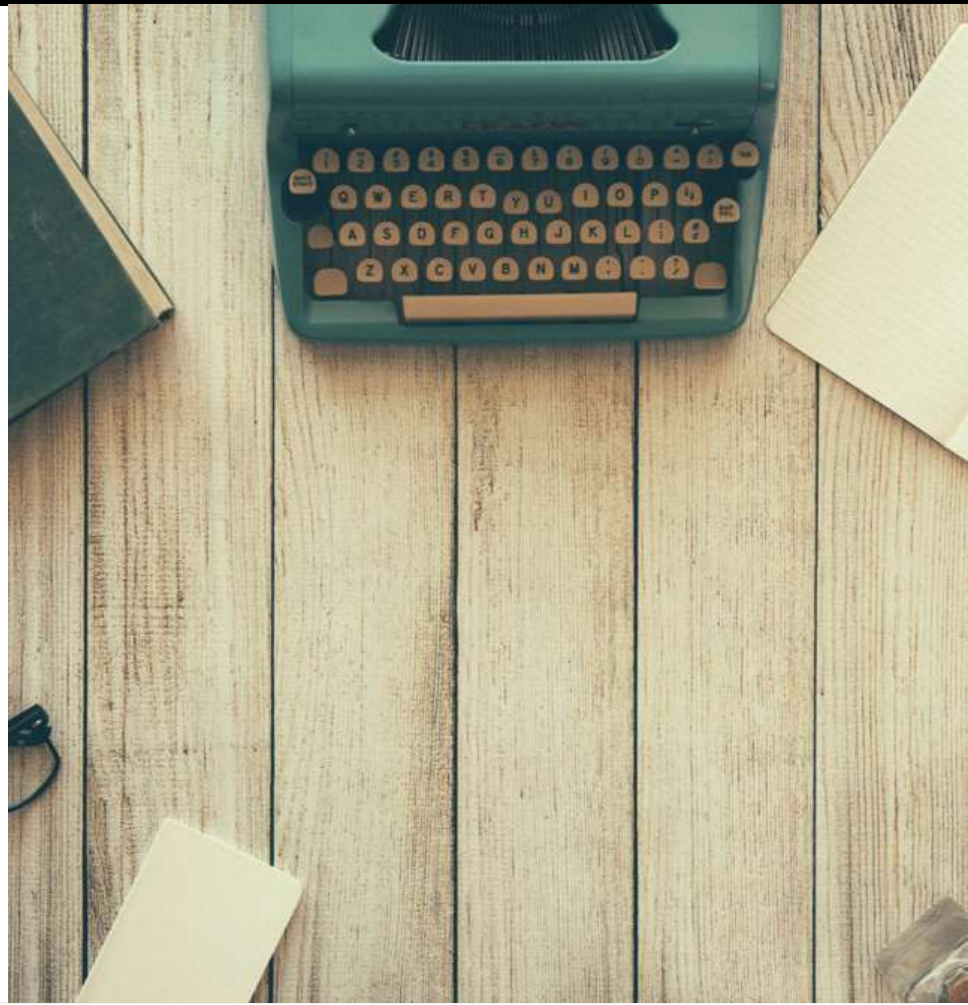
- Vem ansvarar?
- Vilken kompetens har ni internt?
- Rutiner för personuppgiftsincident?
- Vad kan göras för att undvika incidenter?

→ Era IT-system

- Vilka system har ni?
- Hur uppfyller ni kraven i era egna system?
- Vilka leverantörer behöver ni kravställa mot?
- Hur kan vi uppfylla de grundläggande kraven i våra system?

→Hur kan ni uppfylla de grundläggande kriterierna?

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet – åtkomstkontroll
- De registrerades rättigheter
  - Rätt bli raderad
  - Rätt få registerutdrag
  - Rätt till rättelse



Konsekvensbedömningar

Konsekvensbedömning (”PIA”)

- Nytt krav på att göra en ”konsekvensbedömning” *(Data Protection Impact Assessment)* och dokumentera grunderna för beslutet
- När? *”Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål,* ***sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”***

När ska en konsekvensbedömning avseende dataskydd göras?

- Konsekvensbedömning krävs särskilt i följande fall

a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer

b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10

c) Systematisk övervakning av en allmän plats i stor omfattning

Vilken vägledning finns att få?

- Bedömningen ska göras i förväg
- Konsekvensbedömning *bör* göras för personuppgiftsbehandling som påbörjas redan innan GDPR träder ikraft
- En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker
- Förhandssamråd med tillsynsmyndigheten om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk
- *Artikel 29-gruppens vägledning för konsekvensbedömningar avseende dataskydd*
- Datainspektionen ***ska*** upprätta en förteckning
- *Åtgärd: Inför rutiner för konsekvensbedömningar samt en ev. mall för dessa*

Exempel på när PIA bör göras – om fler än två av nedan gäller

- Behandlingen innehåller element av bedömning eller värderingar
- Behandlingen syftar till att fatta automatiserade beslut med rättsliga följder eller liknande för den registrerade
- Behandlingen innefattar systematisk övervakning
- Behandlingen omfattar känsliga personuppgifter
- Behandlingen innebär att personuppgifter behandlas i stor skala
- Behandlingen innefattar samkörning av uppgifter mellan olika register
- Behandlingen omfattar personuppgifter om särskilt utsatta eller skyddsvärda typer av registrerade
- Personuppgifterna behandlas på ett innovativt sätt
- Personuppgifter ska föras över till ett land utanför EES
- Personuppgiftsbehandlingen i sig förhindrar registrerade från att utöva en rättighet eller att använda en tjänst eller ett avtal

Andra regler

”Dataportabilitet” – underlätta att flytta uppgifter mellan olika leverantörer

- Individer ska lättare kunna få ut och överföra uppgifter från en personuppgiftsansvarig till en annan (från en organisation till en annan)
- Gäller när grunden för behandlingen är samtycke eller avtal och behandlingen sker automatiserat
- Den ansvarige ska tillhandahålla uppgifterna i *” i ett strukturerat, allmänt använt och maskinläsbart format”*
- → *Åtgärd: Kommer ni rent praktiskt sannolikt träffas av denna skyldighet? Hur säkerställer vi i sådant fall rutiner?*

Uppförandekoder och certifiering

- Möjlighet till certifiering tre år i taget
  - Finns ej praktiskt idag
- Lagen uppmuntrar utarbetandet av uppförandekoder
  - Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder som ges in till tillsynsmyndigheten

Det vidare projektet – hur göra?

Juridisk genomgång	• Är behandlingen laglig, hur görs idag? Laglig grund/ändamål för den behandling som görs (register som finns)? Dokumentation över behandling, osv.
Juridiska dokument/ policyer	• Personuppgiftsbiträdesavtal, information till registrerade (personuppgiftspolicy), eventuella samtyckestexter, interna policyer för behandling, dokumentation över konsekvensbedömning, dokumentation/avtal för överföring till tredje land, osv.
Tekniska åtgärder	• Säkerhetskrav, inbyggd integritet (privacy by design), gallring, behörighetsstyrning, autentisering, osv.
Organisation	• Dataskyddsombud, ansvar över system och rutiner, rapportordning, osv.
Organisatoriska åtgärder - rutiner	• Utelämnande av information, dokumentera samtycken, checklistor, register över behandling, rutiner för anmälan av personuppgiftsincident, konsekvensbedömning vid ny behandling, rutiner vid upphandlingar, osv.

Skapa medvetenhet och acceptens för att ni behöver arbeta med lagen

- Säkerställ att ledning är med och sätter ambitionsnivå
- Bestäm nivå av compliance – er egna ambitionsnivå
- Vilken är er ambitionsnivå? Budget?
- Inse att
  - GDPR kräver olika typer av kompetens
  - Ni behöver inleda ett projekt för att förbereda er
  - Arbetet är inte slut med projektet
  - Det kommer kräva tid och resurser

Hur kan vi förbereda oss?

- Skapa medvetande internt om de nya reglerna och den nya rollen – informera och utbilda
- Ett projekt för att följa lagen behövs
  - Gör en nulägesanalys
  - Efterlevnadsprojekt

Tips för ett lyckat efterlevnadsprojekt

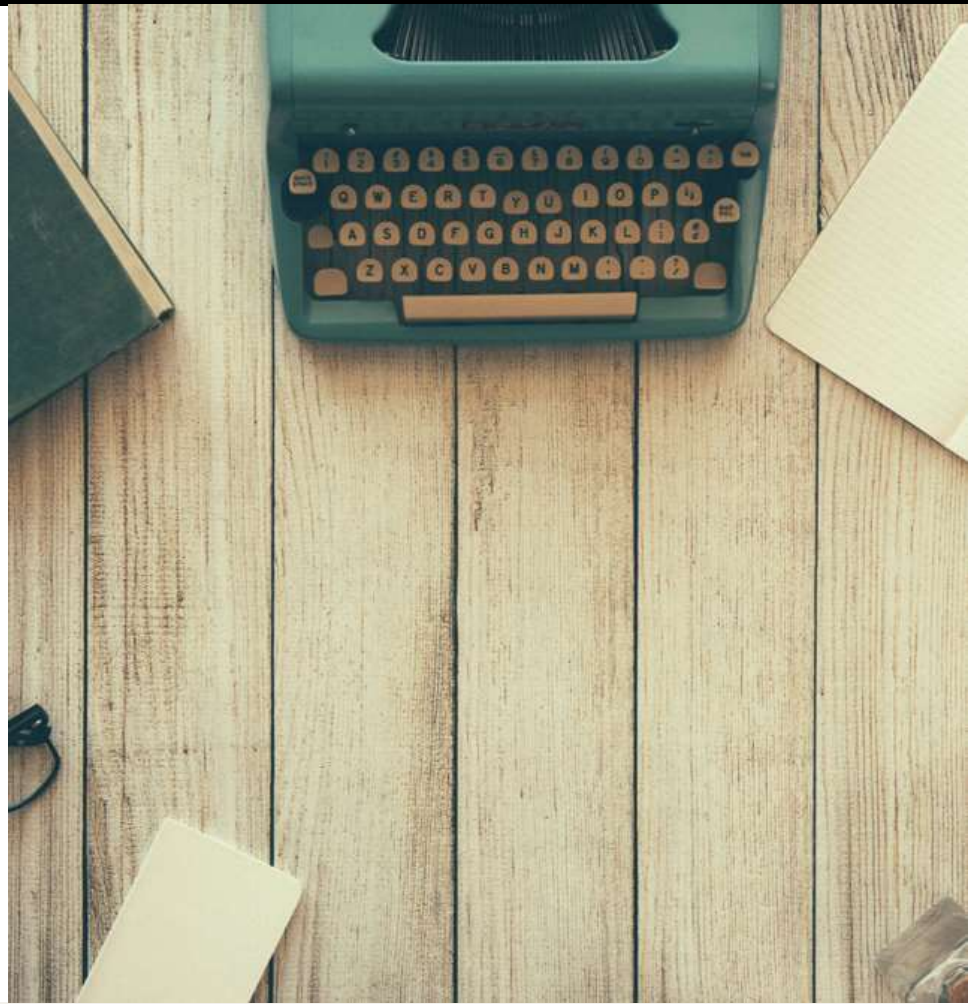
- Budgetera och avsätt resurser noga
- Ha en intern projektledare och ev. även en inhyrd
- Lägg mycket tid i början på att identifiera rätt personer som ska delta
- Lägg stor vikt vid planeringsstadiet
- Diskutera ambitionsnivå av compliance – riskapproach

Nulägesanalys

- Identifiera behandlingar och system
  - Laglig grund för behandlingen
- Identifiera tredjeparter
- Mappa när ni är personuppgiftsansvariga (och biträden)
- Vilka juridiska dokument, rutiner och samtycken finns idag?
- Vilka särskilda frågor har ni att titta på?
- *Identifiera brister och områden att hantera inför att förordningen träder i kraft*

Var står ni idag?

- Följer ni PuL?
- Har ni koll på era behandlingar? Registerförteckning, osv?
- Om ni inte arbetat med PuL så mycket innan: Lägg inte för mycket tid på att analysera var ni står idag…
- Köp inga dyra rapporter för att konstatera att ni inte har ett bra nuläge om ni redan vet det



Starta upp projektet

- Vilka ska delta i projektgruppen?
  - Juridik
  - IT
  - HR
  - Ekonomi
  - Sälj/kund/marknad
  - Andra som har bra koll på hur personuppgifter hanteras
  - En projektledare ”Ordning och reda- person”
- Ha en intern projektledare och ev. även en inhyrd

Efterlevnadsprojekt

- Hur säkerställa ett effektivt efterlevnadssystem
  - Säkerställ att behandlingen är laglig
  - Sätt ansvar och organisation
  - Uppdatera juridiska dokument, avtal, samtycken och policyer
  - IT- och säkerhetsåtgärder
  - Organisatoriska åtgärder och rutiner – accountability

Juridisk dokumentation/policyer – behöver ha

- Interna policyer för behandlingen, lagrings- och gallringsrutiner (ej formellt krav)
  - Personuppgiftspolicy inkl. gallringspolicy
  - IT-policy
- Personuppgiftsbiträdesavtal och ev. underbiträdesavtal
- Information till registrerade (personuppgiftspolicy)
  - Anställda
  - Kandidater
  - Kontaktpersoner hos leverantörer och samarbetspartners
  - Kunder/kontakter hos kunder
  - Ev. andra registrerade – nyhetsbrev, kundklubb, m.m.

Juridisk dokumentation – bör ha eller behövs ibland

- Samtyckestexter
- Villkor för lojalitetsprogram eller kundklubb
- Avtal om gemensamt personuppgiftsansvar
- Mall och checklista för konsekvensbedömning
- Avtal om överföring till tredje land
- Dokumentation och checklista för incidenthantering
- Checklista inför upphandling och avtals ingående

IT- och säkerhetsåtgärder (exempel)

- Säkerhetskrav – är de tillräckliga utifrån de krav som ställs i lag och med hänsyn till vilka uppgifter det rör sig om?
- Börja tillämpa inbyggd integritet (privacy by design) vid egen utveckling
- Tekniska rutiner för gallring, behörighetsstyrning, autentisering
- Tekniska rutiner för att undvika personuppgiftsincidenter

Organisatoriska åtgärder och rutiner

- Utbildningsrutiner (och rutiner för att övervaka att utbildning genomförts)
- Utelämnande av information
- Dokumentationsrutiner
- Samtycken checklistor
- Register över behandling
- Rutiner för anmälan av personuppgiftsincident
- Konsekvensbedömning vid ny behandling
- Rutiner vid upphandlingar
- Contract management
- Sekretessavtal
- Med mera..

Agnes Hammarstrand / Partner, Lawyer
Mobile phone: +46 (0)730-83 50 70
agnes.hammarstrand@delphi.se

@IT_advokaten

Advokatfirman Delphi / Östra Hamngatan 29 / 411 10 Göteborg / Sweden
Phone: + 46 (0)31 10 72 00 / Fax: +46 (0)31 13 94 69 / delphi.se


Delphi