GDPR och ansvarsrollerna

Peter Nordbeck, Advokat/Partner

Ängla Eklund, Associate

Agenda

- Ansvarsrollerna
  - Personuppgiftsansvarig
  - Personuppgiftsbiträde
  - Gemensamt personuppgiftsansvar
- Molntjänster och ansvar
- Tidigare vägledningar
- Lagreglerade fall av personuppgiftsansvar
- Praktiska exempel

Delphi

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*”
- Personuppgiftsansvarig ansvarar alltid självständigt för att lagen följs
- Ansvaret är typiskt sett företagets, inte en persons

Personuppgiftsansvarig i praktiken

- Ni är ansvariga för all personuppgiftsbehandling som ni är personuppgiftsansvarig för
- Detta gäller oavsett vem som gör behandlingen.
- Det är alltså ni som ansvarar för att t.ex. er IT-miljö och IT-system uppfyller lagens krav (inte en IT-leverantör)

Delphi

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

Gemensamt personuppgiftsansvar

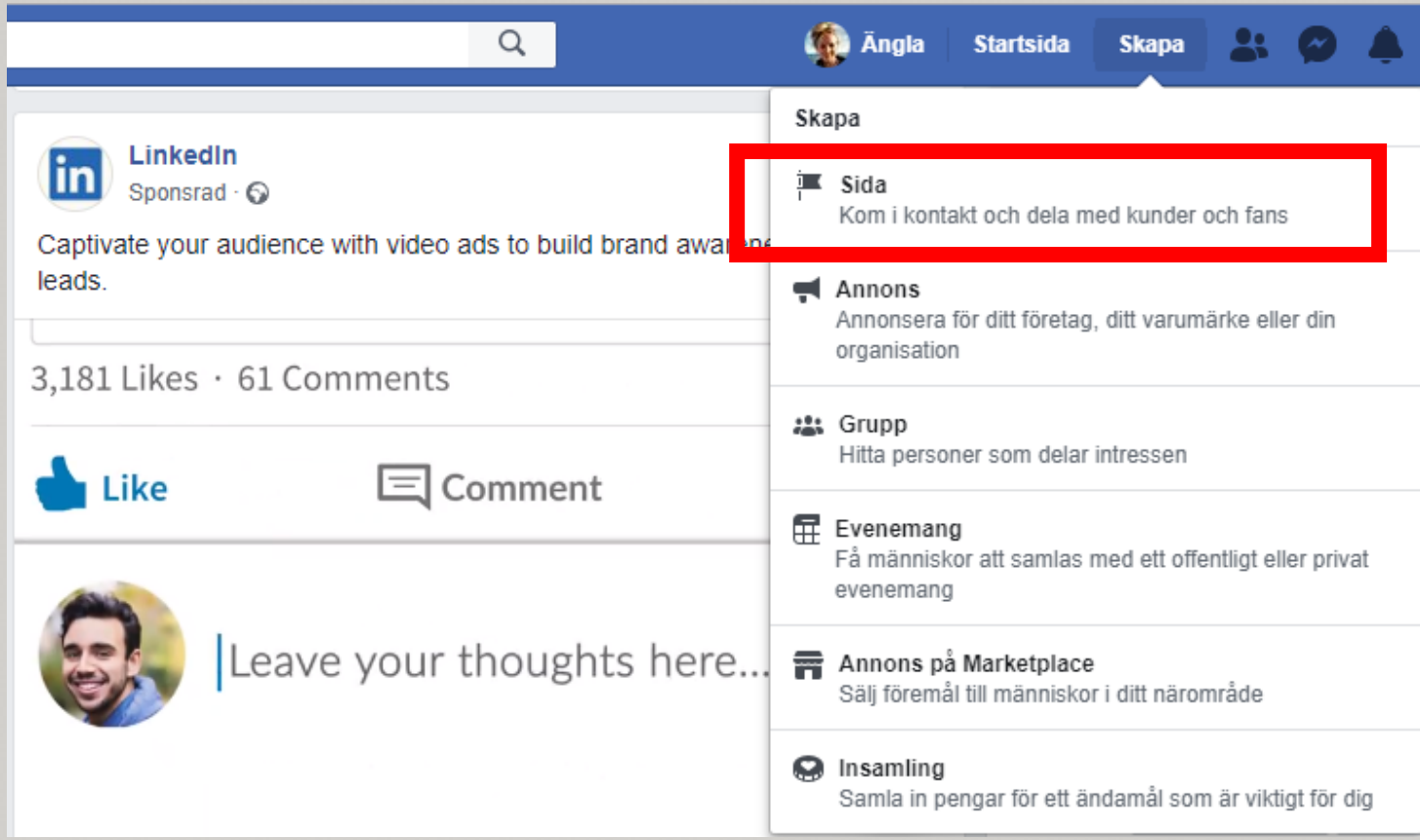
- *”Om två eller flera personuppgiftsansvariga **gemensamt** fastställer ändamålen med och medlen för behandlingen av personuppgifter”*
- Ett gemensamt ansvar får ett antal konsekvenser:
  - Ska gemensamt fastställa sitt respektive ansvar avseende den registrerades rättigheter och sina respektive skyldigheter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

Domen om Jehovas vittnen

- Bakgrund
- En fysisk eller juridisk person som i eget syfte påverkar behandlingen av personuppgifter, och därigenom bidrar till att bestämma ändamål och medel för behandlingen, kan däremot anses vara registeransvarig.
- För att flera aktörer ska anses ha ett gemensamt ansvar för samma behandling krävs dessutom inte att var och en av dessa har tillgång till de aktuella personuppgifterna.

C-210/16 – Fansidor

- Kan administratören av en ”fanpage” hållas ansvarig för överträdelser av dataskyddsregler?
- Ingår särskilt avtal.
- Facebook placerar genom sidan kakor hos besökaren, även hos sådana som inte har Facebookkonto.
- Statistik om besökare.
- Gemensamt ansvar
  - Gemensamt enligt GDPR?



Fashion ID.

- Kan en webbsideägare som installerat tredjepartspixlar hållas gemensamt ansvarig för personuppgiftsbehandlingen?
- Fashion ID har möjliggjort för Facebook att samla in personuppgifter genom att inkorporera Facebooks plugin på sin hemsida.
- Denna plugin har tillåtit Fashion ID att optimera sin marknadsföring genom synliggörande på Facebook.
- Det faktum att Fashion ID inte utfört den relevanta personuppgiftsbehandlingen eller haft tillgång till de aktuella personuppgifterna utesluter inte ett gemensamt personuppgiftsansvar.

Delphi

Vad är viktigt att beakta?

- Biträdesavtal finnas på plats.
  - Sanktioner vid överträdelser.
  - Olika uppfattningar avseende möjligheten att fördela skyldigheter genom avtal.
- Att om uppdragstagaren är personuppgiftsansvarig har uppdragstagaren större möjligheter att använda personuppgifterna för egna ändamål.
- Måste ett inbördes arrangemang inrättas där parterna fördelar skyldigheter mellan sig
- Man måste också tänka på risken för att den registrerade kan vända sig mot vem som helst av de gemensamt personuppgiftsansvariga.
  - Detta gäller även vid biträdessituationer.

HFD 2015 ref 3

- Bakgrund
- ”Det är bolaget som har utarbetat metoden för vilka uppgifter som ska samlas in för detta ändamål och varifrån de ska hämtas samt hur det ska ske. Den av bolaget utarbetade arbetsmetoden bör rimligen utgöra skälet till att uppdragsgivarna anlitar bolaget för utförande av uppdraget. Även om uppdragsgivarna tillhandahåller grundinformation och har möjlighet att skräddarsy omfattningen av personuppgiftsbehandlingen, innebär det sagda att bolaget har en sådan självständig ställning och kan bestämma ändamålen med och medlen för behandlingen av personuppgifter på ett sådant sätt att bolaget är att betrakta som personuppgiftsansvarigt för tjänsten screening.”

Molntjänster och personuppgiftslagen

Allt fler kommuner, myndigheter och företag använder sig av så kallade molntjänster. Molntjänster innebär att exempelvis processorkraft, lagring och funktioner tillhandahålls av leverantörer som tjänster över internet.

Den som använder en molntjänst för lagring av personuppgifter, till exempel i ett löneregister, förlorar den faktiska kontrollen över de personuppgifter som lagras. Till detta kommer att molnleverantörer ofta använder sig av standardavtal, det vill säga i förväg definierade användarvillkor, och anlitar underleverantörer. Det är därför viktigt att den som tänker använda en molntjänst i sin verksamhet är medveten om de krav som ställs enligt personuppgiftslagen.

Den som anlitar en molnleverantör är alltid personuppgiftsansvarig

Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av molntjänstleverantören eller dess underleverantörer. Leverantören, och alla dess underleverantörer som anlitas för behandlingen, är den personuppgiftsansvariges personuppgiftsbiträden. Det är den personuppgiftsansvarige som ansvarar för att personuppgiftslagen och andra lagar följs, till exempel myndighetsspecifika registerförfattningar och offentlighets- och sekretesslagen.

Men vänta nu....

Molntjänster och personuppgiftslagen

Allt fler kommuner, myndigheter och företag använder sig av så kallade molntjänster. Molntjänster innebär att exempelvis processorkraft, lagring och funktioner tillhandahålls av leverantörer som tjänster över internet.

Den som använder en molntjänst för lagring av personuppgifter, till exempel i ett löneregister, förlorar den faktiska kontrollen över de personuppgifter som lagras. Till detta kommer att molnleverantörer ofta använder sig av standardavtal, det vill säga i förväg definierade användarvillkor, och anlitar underleverantörer. Det är därför viktigt att den som tänker använda en molntjänst i sin verksamhet är medveten om de krav som ställs enligt personuppgiftslagen.

Den som anlitar en molnleverantör är alltid personuppgiftsansvarig

Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av molntjänstleverantören eller dess underleverantörer. Leverantören, och alla dess underleverantörer som anlitas för behandlingen, är den personuppgiftsansvariges personuppgiftsbiträden. Det är den personuppgiftsansvarige som ansvarar för att personuppgiftslagen och andra lagar följs, till exempel myndighetsspecifika registerförfattningar och offentlighets- och sekretesslagen.

Bolaget erbjuder sig inom ramen för tjäns[illegible]eening att verifiera olika uppgifter som lämnas till uppdra[illegible]aren från arbetssökande. Det är bolaget som har utarbetat metode[illegible] vilka uppgifter som ska samlas in för detta ändamål och varifr[illegible]ska hämtas samt hur det ska ske. Den av bolaget utarbetade arb[illegible]oden bör rimligen utgöra skälet till att uppdragsgivarna anlitar [illegible] för utförande av uppdraget. Även om uppdragsgivarna [illegible]ndahåller grundinformation och har möjlighet att skräddarsy [illegible]nfattningen av personuppgiftsbehandlingen, innebär det sagda att [illegible]olaget har en sådan självständig ställning och kan bestämma ändamålen [illegible]med och medlen för behandlingen av personuppgifter på ett sådant sätt att bolaget är att betrakta som personuppgiftsansvarigt för tjänsten [illegible]creening.

Vägledning Artikel 29-gruppen

- Registeransvarig
  - Förmågan att ”bestämma ändamålen och medlen …” kan vara ett resultat av:
    - Uppdrag eller en plikt att samla in och behandla vissa uppgifter,
    - gemensamma rättsliga bestämmelser,
    - befintliga traditionella roller som normalt innebär ett visst ansvar inom vissa organisationer,
    - faktiska omständigheter; och
    - andra faktorer (t.ex. avtalsförhållanden, faktisk kontroll hos en part, synlighet i förhållande till de registrerade etc.).
  - Det är den som bestämmer ”ändamålet” för behandlingen som (i praktiken) betraktas som registeransvarig. Beslutet om ”medlen” för behandlingen får däremot delegeras av den registeransvarige i fråga om tekniska och organisatoriska frågor.

- Registerförare
  - Två grundvillkor:
    - separat rättslig enhet i förhållande till den registeransvarige, och
    - behandlar personuppgifter på den registeransvariges vägnar.

Delphi

Exempel 23: Revisorer

Hur revisorer ska betraktas varierar beroende på sammanhanget. När revisorer tillhandahåller tjänster till allmänheten och småföretagare på grundval av mycket övergripande instruktioner (”deklarera åt mig”) är det – precis som för juridiska ombud som agerar under liknande omständigheter och av liknande anledningar – revisorn som är registeransvarig. Men om en revisor anlitas av ett företag och har fått detaljerade instruktioner av företagets egen revisor, kanske för att göra en ingående revision, ska den revisorn i allmänhet – om han inte är en vanlig anställd – betraktas som registerförare, på grund av de tydliga instruktionerna och det begränsade utrymmet för egna beslut. Här finns dock ett viktigt förbehåll, nämligen att när en revisor anser sig ha upptäckt oegentligheter som måste rapporteras, agerar denne som en oberoende registeransvarig, eftersom han eller hon uppfyller sina yrkesmässiga skyldigheter.

Exempel 22: Webbplats för efterlysningar

En webbplats för efterlysningar framställdes som en ren registerförare, eftersom det var de som annonserade efter förlorade föremål som skulle avgöra innehållet och alltså ändamålet på mikronivå (t.ex. hitta ett borttappat smycke, en försvunnen papegoja osv.). En dataskyddsmyndighet avvisade det argumentet. Webbplatsen skapades i syfte att tjäna pengar på annonsering efter försvunna saker och det faktum att de inte bestämde vilka specifika saker det annonserades efter (i motsats till att bestämma annonskategorier) var inte lika avgörande, eftersom definitionen av ”registeransvarig” inte uttryckligen omfattar beslut om innehållet. Webbplatsen beslutar i fråga om införing osv. och har ansvar för att innehållet är lämpligt.

Exempel 20: Teletjänstcentraler

En registeransvarig lägger ut en del av sina åtgärder på entreprenad till en teletjänstcentral och instruerar teletjänstcentralen att presentera sig med den registeransvariges identitet när de ringer upp den registeransvariges kunder. I det här fallet leder kundernas förväntningar och det sätt som den registeransvarige presenterar sig för dem via teletjänstcentralen till slutsatsen att teletjänstcentralen fungerar som registerförare för den registeransvarige (för dennes räkning).

Exempel 21: Advokater

En advokat företräder sin klient i domstol och behandlar, beroende på uppdrag, personuppgifter i samband med klientens ärende. Den rättsliga grunden för att använda den information som krävs utgörs av uppdraget från klienten. Men detta uppdrag handlar inte om uppgiftsbehandling utan om att bli företrädd i domstol, vilket är en verksamhet som jurister traditionellt har sin egen rättsliga grund för. Dessa yrken måste därför betraktas som oberoende ”registeransvariga” när de behandlar uppgifter i samband med att de företräder sina klienter.

Kriterier för att bedöma ansvar

- Synligheten av uppdragstagaren i förhållande till de registrerade.
- Den uppfattning som de registrerade får.
- Nivån på förhandsinstruktioner från den personuppgiftsansvarige.
- Att den personuppgiftsansvarige har en kontinuerlig och noggrann övervakning för att förvissa sig om att personuppgiftsbiträdet följer instruktioner och avtalsvillkor ordentligt.
- Vem som bestämmer vilken information som ska inhämtas från de registrerade.
- Vem som bestämmer det sätt som behandlingen ska utföras på.
- Vem som ansvarar för resultatet av uppdraget.
- Det finns legala krav som uppdragstagaren måste förhålla sig till vid utförandet.
- Uppdragstagaren har sina egna villkor som gäller direkt mot de registrerade.
- Uppdragstagaren är fri att använda sin expertis inom det område som uppdraget avser.
- Uppdragstagaren använder verktyg som utgör uppdragstagarens affärshemligheter vid utförande av uppdraget.

Delphi

Möjlighet att ”outsourca” till biträdet

- Artikel 29-gruppen anger att det finns en möjlighet att outsourca medlen till ett biträde.
- Från ICO:s vägledning:
  - Within the terms of the agreement with the data controller, and its contract, a data processor may decide:
    - What IT systems or other methods to use to collect personal data;
    - how to store the personal data;
    - the detail of the security surrounding the personal data;
    - the means used to transfer the personal data from one organisation to another;
    - the means used to retrieve personal data about certain individuals;
    - the method for ensuring a retention schedule is adhered to; and
    - the means used to delete or dispose of the data.

Fort. att ”outsourca” till biträdet

- Den franska dataskyddsmyndigheten (CNIL) anser att molntjänstleverantören och kunden i vissa fall, och för vissa behandlingar, kan vara gemensamt personuppgiftsansvarig för behandlingen.
  - Skäl för detta är att:
    - erbjuder högt standardiserade tjänster,
    - standardiserade villkor, dvs. tjänster som inte är anpassade till enskilda molntjänstkunder, och
    - ej förhandlingsbara villkor.

Uppdragstagaren = ansvarig?

- Tidigare: om uppdragstagaren omfattades av vissa regulatoriska krav enligt lag eller god sed tyder detta på att det rör sig ett ökat ansvar.
- Denna omständighet har beaktats i GDPR.

”Den personuppgiftsansvarige får endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt. Det innebär att det inte finns någon motsägelse mellan att vara personuppgiftsbiträde och ha eget regulatoriskt ansvar för vilket man är personuppgiftsansvarig.”

Delphi

Ny vägledning kommer

- Datainspektionens uppdrag att ta fram nya EU-riktlinjer för tolkning av begreppen.

Lagreglerade fall av personuppgiftsansvar

- Några lagreglerade fall av personuppgiftsansvar
  - Vårdgivare enligt patientdatalagen
    - En vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför.
  - Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten
    - En juridisk eller fysisk person som ansvarar för privat verksamhet är personuppgiftsansvarig för den behandling som görs i dess verksamhet.

Svårigheter med särskilt reglerat ansvar

- Upphandlar hemtjänst-tjänster
  - Ska biträdesavtal vara med i upphandlingen?
  - Kommunen ställer krav som ska vara uppfyllda i upphandlingsunderlaget.
  - Leverantören är som huvudregel personuppgiftsansvarig för behandlingen.
  - Exempel:
    - Om kommunen anvisar ett IT-system där leverantören ska redovisa utförda tjänster, är då kommunen att anse som personuppgiftsbiträde till leverantören? Trots att kommunen är uppdragsgivare och leverantören är uppdragstagare…
- Med tech
  - Avancerade ansvarskedjor

Praktiska exempel

- Men hur gör man då?
- Att uppdragstagaren inte samlar in personuppgifter själv, utan får dem från uppdragsgivaren kan vara en indikation på att uppdragstagaren är biträde.
- Omvänt om uppdragstagaren får uppgifterna direkt från den registrerade
  - Ex. ett företag har ramavtal med ett taxibolag om att de anställda får utnyttja taxibolagets tjänster till rabatterat pris. Taxibolaget får personuppgifter direkt från de anställda. Taxibolaget är personuppgiftsansvarig.
- Resebyrå anser sig själva vara personuppgiftsansvariga och Datainspektionen har hållit med i ett tidigare samrådsyttrande.
- Rekryteringsbolag får anses vara personuppgiftsansvariga när de samlar i uppgifter om kandidater och överför dessa uppgifter till ett företag som anlitar dem.
- Det finns en uppfattning om att ”Uppdraget gäller ju inte behandling av personuppgifter”… så därför är uppdragstagaren personuppgiftsansvarig. Vad säger vi om den? Hur många uppdrag avser just personuppgiftsbehandling?

Delphi team

Peter Nordbeck

Advokat/Partner

- +46 709 25 25 01
- peter.nordbeck@delphi.se

Ängla Eklund

Associate

- +46 767 72 00 18
- angla.eklund@delphi.se