



Myndigheter, företag och andra organisationers ansvar för

Personuppgifter i sociala medier

Allt fler kommuner, myndigheter och företag använder sig av Facebook, Twitter, bloggar och andra typer av sociala medier som kommunikationskanaler. Användningen av dessa medier kan innebära att personuppgifter behandlas, vilket i sin tur innebär att organisationerna måste se till att följa reglerna i personuppgiftslagen och, i vissa fall, särskild registerlagstiftning.

I det här informationsbladet får du veta mer om vad detta kan innebära för din organisation. Informationen riktas till myndigheter, kommuner och andra organisationer och rör endast behandling av personuppgifter.

Observera att en organisations ansvar för personuppgifter som publiceras via ett visst socialt media är beroende av utformningen av den sociala medietjänst som används och att de sociala medierna är under ständig förändring och utveckling.

Dessa regler gäller enligt personuppgiftslagen

I personuppgiftslagen gäller olika regler beroende på om de personuppgifter som behandlas är strukturerade eller inte. I normalfallet när organisationer skapar en Facebook-sida, en blogg eller använder sig av Twitter är personuppgifterna som organisationen behandlar och har tillgång till inte strukturerade i personuppgiftslagens mening. När personuppgifterna är ostrukturerade är publiceringen tillåten så länge uppgifterna inte är kränkande (5 a § personuppgiftslagen) och organisationen uppfyller vissa krav på säkerhet (31–32 §§ personuppgiftslagen).



Datainspektionen

Personuppgiftslagen gäller dock inte:

- när det finns avvikande bestämmelser i andra lagar eller förordningar
- då personuppgifter behandlas för privata ändamål (organisationer kan dock aldrig behandla personuppgifter för privata ändamål)
- om det strider mot bestämmelserna om tryck- och yttrandefrihet
- om publiceringen av personuppgifter kan bedömas ske för ett uteslutande journalistiskt ändamål, det vill säga om syftet är att informera, utöva kritik och väcka debatt om samhällsfrågor av betydelse för allmänheten. I så fall gäller endast bestämmelserna om säkerhet.

Vem har ansvar för vad?

Ansvaret för behandling av personuppgifter via sociala medier kan delas in i ansvaret för organisationens egna inlägg och publiceringar och ansvaret för inlägg som publiceras av besökare. Några exempel:

- Facebook och bloggar: Organisationen är ansvarig för personuppgifter som publiceras på organisationens Facebook-sida och/eller blogg. Ansvaret omfattar både personuppgifter som organisationen själv publicerar och personuppgifter som publiceras av andra i till exempel en kommentar på sidan. Även den besökare som skrivit en kommentar kan ha ett ansvar för vad den själv skrivit.
- Twitter: Organisationen ansvarar endast för personuppgifter som organisationen själv publicerat, inte personuppgifter som andra twittrande lämnar. Det beror på att organisationen inte kan påverka publiceringen av andras twitter-inlägg.

För andra sociala medier måste organisationen göra en egen bedömning av vilket ansvar den har för andras publiceringar. Kan organisationen påverka det som besökaren publicerar och därmed bestämma över ändamålen och medlen för den behandling av personuppgifter som andra utför (som för Facebook och bloggar)? Eller kan den det inte (som på Twitter)? Svaret påverkar organisationens ansvar.



Organisationens ansvar

Organisationen har ett ansvar för att personuppgifter på dess Facebook-sida, blogg, Twitter-konto och liknande inte behandlas på ett sådant sätt att de kränker enskildas personliga integritet. Ett företag, kommun, myndighet eller annan organisation som använder sociala medier:

- får inte publicera kränkande personuppgifter
- ska hålla uppsikt över besökares kommentarer för att upptäcka kränkande personuppgifter
- ska ta bort kränkande personuppgifter
- kan bli skadeståndsskyldig för kränkande personuppgifter.

Organisationen är dessutom skyldig att vidta lämpliga säkerhetsåtgärder. Det kan bland annat innebära att:

- De som arbetar med sociala medier för organisationens räkning bör informeras om ändamålen med den behandling av personuppgifter som kan förekomma och att användning som är oförenlig med dessa ändamål är förbjuden. Det är därför bra om organisationen utformar en intern policy som beskriver hur organisationen ska använda de sociala medierna och hur personuppgifter på dessa ska hanteras.
- Kraven på lämpliga säkerhetsåtgärder blir större ju större risken är för att känsliga uppgifter kan förekomma. Exempelvis kan det vara nödvändigt att ha en noggrannare uppsikt över besökares kommentarer om det har förekommit många kränkande kommentarer på sidan.



WORDPRESS



Det här bör organisationen tänka på

För att minska risken för kränkningar av enskildas personliga integritet och för att minska risken för att bli skadeståndsskyldig, bör organisationen vidta åtgärder i förebyggande syfte.

- Organisationen bör informera om syftet med Facebook-sidan, bloggen eller liknande samt för vilka ändamål kommentarsfunktionen är tänkt att användas, vilka typer av kommentarer som inte får förekomma och vad som kan hända om enskilda inte följer anvisningarna.
- Organisationen bör uppmana besökare att rapportera kränkande innehåll och ha rutiner för att hantera klagomål. Om det är lämpligt kan organisationen även hänvisa till exempelvis Facebooks eller bloggverktygets egen klagomålsfunktion.

Tänk också på att:

- Utforma sidan så att det tydligt framgår att det är organisationen som står bakom den.
- Det kan finnas andra bestämmelser, utöver personuppgiftslagen, som har betydelse för vad som är tillåtet och inte, som exempelvis bestämmelser i register-

författningar, bestämmelser om allmänna handlingar, sekretess och arkivering samt lagen om ansvar för elektroniska anslagstavlor.

- Informationen i det här informationsbladet utgår ifrån förutsättningen att organisationen inte behandlar eller kommer att behandla personuppgifterna i ett register, ärendehanteringssystem eller annan databas, på ett strukturerat sätt. I så fall gäller personuppgiftslagen i sin helhet.

BAKGRUND

Detta informationsblad grundas på slutsatser som Datainspektionen kommit fram till efter att ha granskat hur en statlig myndighet, en kommun och ett företag använder Facebook, bloggar och Twitter. Besluten från inspektionerna finns tillgängliga på www.datainspektionen.se/sociala-medier

Mer information

På www.datainspektionen.se kan du läsa mer om personuppgiftslagen. Där hittar du mer information om bland annat reglerna för strukturerade och ostrukturerade personuppgifter och it-säkerhet.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.



Datainspektionen