



Myndigheter, företag och andra organisationers ansvar för

Personuppgifter i sociala medier

Allt fler organisationer använder sig av sociala medier, som exempelvis Facebook, Instagram, Youtube, LinkedIn, Google Plus, Flickr, Pinterest, Twitter, bloggar och diskussionsforum. Denna användning 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 en organisation som är aktiv på sociala medier ska tänka på för att leva upp till personuppgiftslagen.

Dessa regler gäller enligt personuppgiftslagen

Olika regler i personuppgiftslagen gäller beroende på om de personuppgifter som behandlas är strukturerade eller inte. I normalfallet när organisationer skapar en profil i ett socialt medium (till exempel en Facebookprofil) är personuppgifterna som organisationen behandlar och har tillgång till ostrukturerade i lagens mening. När uppgifterna är ostrukturerade är publicering tillåten så länge uppgifterna inte är kränkande (5 a § personuppgiftslagen) och under förutsättning att organisationen uppfyller vissa krav på säkerhet (30–31 §§ personuppgiftslagen).

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.

Organisationens ansvar för egna och andras publiceringar

En organisation som använder sociala medier har ett ansvar för publiceringar (av kommentarer, bilder, filmklipp med mera) som görs av anställda och andra som publicerar inlägg för organisationens räkning i de sociala medierna. För att organisationen även ska anses ha ett ansvar för publiceringar som görs av användare som inte agerar på uppdrag av organisationen, krävs att organisationen har möjlighet att påverka och därmed bestämma över användares inlägg. En omständighet som medför att organisationen blir personuppgiftsansvarig är om organisationen har möjlighet att ta bort användares publiceringar. Det kan också ha betydelse om organisationen har möjlighet att stänga av kommentarsfunktionen, samt om det är organisationen själv som tillhandahåller det sociala mediet. Några exempel:

- Facebook, Youtube, Instagram, LinkedIn, Google Plus, Flickr, Pinterest och bloggar: Organisationen är ansvarig för personuppgifter som publiceras på organisationens profil. Ansvaret omfattar både personuppgifter som organisationen själv publicerar och personuppgifter som publiceras av andra, i till exempel en kommentar på profilen. Observera att även den användare 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 inlägg på Twitter.



Organisationen måste göra en egen bedömning av vilket ansvar den har för publiceringar i olika sociala medier, genom att utvärdera om organisationen kan påverka det som användare publicerar, som på exempelvis Facebook.

Observera att en organisations ansvar för personuppgifter som publiceras i ett visst socialt medium alltså är beroende av utformningen av den sociala medietjänst som används. Förändringar av tjänsten kan därför leda till att en organisations ansvar förändras. Därför är det viktigt att vara uppmärksam på sådana förändringar i funktioner och inställningar.

Vad innebär organisationens ansvar?

Vid publicering i sociala medier har organisationen ett ansvar för att personuppgifter, som omfattas av organisationens personuppgiftsansvar, behandlas på ett sätt som inte är kränkande enligt personuppgiftslagen. Ansvaret gäller publiceringar som görs för organisationens räkning i de sociala medierna. I många sociala medier (såsom Facebook, Youtube, Instagram, LinkedIn, Google Plus, Flickr, Pinterest och bloggar) gäller ansvaret som sagt även användares publiceringar, exempelvis användarkommentarer, på organisationens profiler.

Ansvaret innebär att organisationen:

- inte får publicera kränkande personuppgifter
- ska hålla regelbunden uppsikt över publiceringar för att upptäcka kränkande personuppgifter
- skyndsamt ska ta bort kränkande personuppgifter.

Hur ofta organisationen behöver ha uppsikt kan variera mellan olika utrymmen i de sociala medierna. Beroende på personuppgiftsbehandlings karaktär kan man behöva ställa olika höga krav på uppsiktens omfattning. Om det exempelvis på en Facebookprofil inte tidigare har förekommit användarkommentarer, kan kraven på uppsikt anses vara lägre än om det förekommer många användarkommentarer. Om det tidigare har förekommit kränkande kommentarer är uppsikt särskilt viktigt.

Organisationen är dessutom skyldig att vidta lämpliga säkerhetsåtgärder. Det innebär bland annat att organisationen ska ge instruktioner till de som arbetar med sociala medier för organisationens räkning, anställda och andra som agerar på uppdrag av organisationen. Det kan till exempel göras genom en intern policy eller handledning som beskriver hur organisationen ska använda de sociala medierna.



WORDPRESS



Det här bör organisationen tänka på

För att minska risken för kränkningar av enskildas personliga integritet bör organisationen vidta åtgärder i förebyggande syfte. Organisationen bör till exempel:

- informera om för vilka ändamål som kommentarsfunktionen är tänkt att användas, vilka typer av kommentarer som inte får förekomma och att publiceringar kan komma att plockas bort
- uppmana användare att rapportera kränkande innehåll till organisationen och ha rutiner för att hantera klagomål.

Tänk också på att:

- Utforma profilen i det sociala mediet 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 registerförfattningar, 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 organisationer använder olika 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.