



GDPR och maillistor. Hur ska en Arbetsmarknadsgrupp göra?

GDPR handlar om hur man samlar in och behandlar persondata. Det finns till för att skydda personer på olika sätt och därför är det viktigt att vi som organisation behandlar vår persondata på rätt sätt. En anpassning till denna nya lag som har varit särskilt omständigt för Chalmers studentkårs organisation är hanteringen av maillistor. I detta dokument hoppas vi i kårledningen kunna förtydliga de aktuella riktlinjerna som gäller när ni som arbetsmarknadsgrupp ska spara, använda och radera maillistor.

Insamling av maillistor

Med maillistor syftar vi på maillistor bestående av antingen personliga eller studentmail för kårens medlemmar. Dessa definieras som personuppgifter och faller därför under särskilt skydd likt vilken ägodel som helst. Precis som det finns krav på att hur valuta hanteras har man nu satt spelregler för hur persondata ska hanteras.

När vi gör mailutskick på olika listor så är det första du ska tänka på vems maillistorna är. Är det din sektionens maillista som ni samlat in själva eller är det listor ni har fått från till exempel högskolan/kåren? Den som äger maillistorna har nämligen en skyldighet att personuppgifterna som finns i maillistorna är insamlade och lagrade på rätt sätt. Vad är då rätt sätt?

När man samlar in listorna så måste den som lämnar personuppgifterna aktivt godkänna vad de ska användas till. Om man vill använda till exempel maillistor för att marknadsföra företag eller andra event så behöver de som lämnat uppgifterna godkänt att de vill ha den typen av mail. Annars har du använt personuppgifterna felaktigt jämfört med vad du bett om tillåtelse för. Man kan aldrig heller samla in en uppgift "tills vidare" utan behöver tidsavgränsning som faller i linje med syftet man beskrivet. Sedan ska personen som lämnar över sin information alltid ha möjlighet att begära sina uppgifter raderade om ingen högre lag säger annat. Detta gör man genom att alltid ange företagets fullständiga namn så de har möjlighet att söka upp er i det scenariot då de önskar få ett utdrag. Denna process underlättas även markant om ni har ett uppdaterat personuppgiftsregister inom er organisation.

Många andra parter på Chalmers har tillgång till olika maillistor som är i ert intresse att använda. Oavsett om det handlar om högskolan, kåren eller annat företag så har det skapat sina register efter villkor med de ingående personerna. För att ni ska kunna få tillgång till maillistor från ett annat företag är det viktigt att ni tecknar ett utförligt kontrakt med dem som innefattar det godkända användandet enligt GDPR och syftet som beskrivits till personen. Ansvar för att denna lista sköts på rätt sätt ligger hos den organisation som samlat in den, men om ni ser till att läsa på om GDPR och vilka villkor som gäller för just den listan kommer förhandlingen om listorna att gå mycket smidigare för alla involverade.

En fråga som ofta dyker upp i näringslivssammanhang är huruvida insamling av företagsmail räknas som ett personuppgiftsregister. Detta beror på hur mailadressen är strukturerad. En postmail som cio@companyone.com som ligger publikt är fritt att spara. Men företaget har en struktur som gör att mailet innehåller personuppgifter som johan.svensson@companyone.com så är det per definition en personuppgift. Företaget har högst troligt avtalat med sina anställda att deras personuppgifter kommer finnas publikt tillgängliga, men det vet inte vi som samlar in mailen. I dessa fall är det bäst att kolla först om det är okej att lägga till mailadressen på en lista.



När får vi använda oss av maillistor?

Självklart regleras användandet av maillistor ni har tillgång till via avtalen ni tecknar antingen med individer eller andra företag. Vi vill dock ange några ramar och tumregler ni bör förhålla er till när ni tar fram avtal eller funderar på inför ett enskilt utskick via listan.

I grunden handlar mailutskick om att ha en bra relation med mottagaren. De måste uppleva att de är rättvist behandlade och att de har kontroll över hur sina uppgifter. Vi är därför restriktiva med frekvensen av massutskick för att undvika att meddelandet verkar som spam.

Innehållet i dessa utskick är också avgörande för huruvida man har laglig grund för att använda sig av registret. Alla på listan ska vara relevanta för informationen. Du kan inte skicka ut ett meddelande till en hel lista där bara en bråkdel har anledning till att få informationen. Exempel på sådana situationer handlar oftast om osorterade maillistor, som om du har en osorterad lista på alla som går ett visst program så är det inte relevant för alla att få mail om event för nollan under mottagningen eller exempelvis exjobbserbjudanden.

Hur länge får man spara uppgifterna, undantag och vad man gör sedan?

I de flesta fallen får ni endast spara insamlade personuppgifter så länge som ni avtalat med de inblandade personerna. Undantag gäller för till exempel bokföringssyften (du är skyldig att spara uppgifter som är relevant för att kunna utföra en korrekt bokföring under 7 års tid och däribland personuppgifter) eller säkerhetsfrågor (svartlistor och liknande register där det sker intressekonflikt). När datumet är nått då ni är skyldiga att ta bort personuppgifterna från samtliga av era system. I många fall utgår syftet med att ha kvar personuppgifterna innan avtalat datum och då är det alltid bäst att ta bort dem redan då. I era personuppgiftsregister bör ni ha förtecknat vilka olika system som maillistor och liknande har sparats i och hur länge det får vara där. Oftast kan man aldrig ta bort data som laddas upp på internet helt och hållet. När man t.ex. laddar upp en fil på Google's moln kommer det alltid finnas spår av datan kvar någonstans i världen. Det viktigaste är dock att ni gör datan otillgänglig för er. Sedan är det en bra praktik att upprätthålla händelseloggar för era register så ni vet när persondata förändras eller raderas.

Vad händer om vi inte följer GDPR? Egentligen?

Primära syftet med GDPR var att ge tillbaka rättigheter till EUs medborgare. Därmed är det upp till medborgarna att anmäla när deras rättigheter har blivit kränkta. När någon upplever att ett företag inte agerar korrekt i behandlingen av deras personuppgifter kan de anmäla detta till [datainspektionen](#). Detta granskas sedan av datainspektionen som avgör om klagomålet beror på systematiska, enstaka/generella fel eller allvarligheten av felet. Detta kan resultera i sanktioner mot företaget upp till 20 miljoner euro eller 4 procent av företagets globala årsomsättning. Detta är dock för extrema fall som förs upp till europeiska domstolen. De fall som fällt i Sverige hittills har legat på ca 100 000-200 000 kr. Med de allvarliga konsekvenserna för att missköta denna nya förordning så har kåren valt att prioritera översynen av hanteringen av personuppgifter. Det som kan hända om en del av Chalmers blir inspekterade av datainspektionen kommer troligtvis alla delar bli granskade då omvärlden inte ser någon skillnad på Chalmers, kåren, sektioner osv.



Kårens riktlinjer och rekommendationer

Nu när ni förhoppningsvis gjort er införstådda i vad GDPR är och hur förordningen påverkar oss kommer en del riktlinjer för vilka krav som gäller för kårens maillistor som ni har tillgång till via era styren. Vi har även formulerat ett par rekommendationer för de vanligaste problemen med att samla in maillistor och sälja reklam via dem till företag.

Kårens maillistor

Teknologsektionerna har i början av verksamhetsåret 19/20 fått tillgång till kompletta medlemslistor med mail och namn. Villkoren för att få använda dess finns deklarerade i sektionsavtalen som skrivs halvårsvis. I detta avtal står vid fastställandet av detta dokument följande villkor för användandet av listorna:

- Sektionen ansvarar för att praktisera säker hantering av sina medlemmars kontaktuppgifter genom att uppfylla gällande lagstiftning rörande behandling av personuppgifter (GDPR)
- Sektionen ansvarar för att sina medlemmars kontaktuppgifter inte utnyttjas i något som helst kommersiellt syfte eller lämna vidare uppgifter till tredje part utan godkännande från kåren.
- Sektioner ansvarar för att vid uppdatering av sina medlemmars kontaktuppgifter omedelbart radera de gamla uppgifterna.

Något som visade sig otydligt i detta avtal var under vilka villkor som kåren kommer godkänna kommersiellt bruk av våra listor. Det är alltså i ytterst få fall då vi kommer kunna ge ett godkännande. I och med att listorna inte är sorterade per klass utan bara efter sektionstillhörighetottagaren kan listan inte användas när bara en särskild klass eller grupp är målgruppen. Exempel på detta är exjobbserbjudanden som bara är relevanta för masters åren eller om ett företag inom en viss bransch bara är relevant för en viss inriktning på programmet.

Vår rekommendation är alltså att ni **avstår** från att erbjuda mailutskick via kårens maillistor som en säljpunkt till företag. Ni bör istället erbjuda denna typen av tjänst efter att ni kollat med oss först om ett sådant utbyte är möjligt.

Passiv reklam.

Genom att vara ett officiellt organ är ni fria att marknadsföra er själva och er verksamhet till kårmedlemmar via våra listor. Detta innebär alltså att ni kan göra reklam för ett event som ni arrangerar för ett företag, t.ex. lunchföreläsningar, mässor, afterwork osv. För att det ska vara möjligt måste huvudsyftet med informationen ni skickar ut tydligt vara ert arrangemang och inte det sponsrande företaget.



Hur man skapar en regelrätt maillista med kårens verktyg.

Det viktigaste med den uppdaterade personuppgiftsförordningen är att individer ska ha kontroll över sina personuppgifter. För att det ska vara möjligt måste man kunna välja när man ger ut ansvar för sina personuppgifter till företag och under vilka villkor den transaktionen sker under. Därmed begär man alltid medgivande när man samlar in personuppgifter med utförlig information om hur de kommer behandlas av företaget i fråga. Ni som arbetsmarknadsgrupp har möjlighet att utföra denna typen av insamling via våra listor. Vårt råd till er som arbetsmarknadsgrupp är att skapa en "Näringslivs maillista". Skapa ett formulär där studenter kan skicka in sina kontaktuppgifter i syfte att få reklam och erbjudanden från företag som via er vill marknadsföra sig till studenter vid er utbildning. I detta formulär kan ni göra studenten medveten om att ni kommer sälja uppgifterna vidare till relevanta och intresserade företag. I informationen måste ni uppfylla följande kriterier i informationen till studenten för att insamlingen ska vara laglig:

- Syftet med att spara datan ska vara tydligt
- Datan får bara sparas under en angiven tid
- Det ska vara tydligt vem som sparar datan och hur man får tag i ansvarige som kan radera ens uppgifter
- Om och hur datan kommer hanteras av en eventuell tredje part

För att sammanfatta vår rekommenderade handlingsplan för att möjliggöra mailutskick för företagskunder:

1. Få tillgång till kårens maillista via sektionsstyrelsen.
2. Skapa ett formulär där man får ange sina personuppgifter och godkänna utgivandet av dessa till externa företag.
3. Skicka ut formuläret via kårens maillista och upprätta ett register över hur länge den insamlade persondatan får sparas.
4. Marknadsför denna lista till företag som ett smidigt sätt att nå ut till studenter.
5. Utför önskade mailutskick åt företag eller lämna ut listan beroende på vad medlemmarna godkände i punkt 2.