

Q&A – SÄRSKILDA FRÅGOR SOM UPPKOMMIT VID FRUKOSTMÖTE		
Nr.	Fråga	Svar
1.	Vad gäller för personuppgifter som vi samlat in innan GDPR börjar tillämpas? Behöver vi exempelvis inhämta förnyade samtycken?	<p>Strukturen i GDPR är i huvudsak densamma som i det nuvarande dataskyddsdirektivet och den svenska personuppgiftslagen (PuL). Det innebär bland annat att GDPR, likt dagens regler, kommer att kräva en laglig grund för behandling av personuppgifter och att behandlingen måste följa vissa grundläggande principer, såsom att det måste finnas ett berättigat ändamål, att personuppgifterna ska vara relevanta och inte för omfattande samt att uppgifterna ska behandlas på ett korrekt och öppet sätt etc.</p> <p>Om ni följer dagens lagstiftning bör detta alltså redan finnas på plats för behandlingen av de personuppgifter ni samlat in sedan tidigare. Behandlingen av personuppgifterna är då godtagbar under förutsättning att ni anpassar den till de nya krav som ställs enligt GDPR, t.ex. avseende de registrerades rättigheter och utökade informationskrav.</p> <p>En viktig nyhet i GDPR är att den som är personuppgiftsansvarig måste kunna visa att reglerna följs. Ni bör därför kartlägga och dokumentera vad ni gör, både för att säkerställa att ni gör rätt och för att kunna visa att ni gör rätt.</p> <p>Även när det gäller samtycke är det grundläggande konceptet detsamma som enligt dagens regler, dvs. att samtycke kan användas som laglig grund och måste för att vara giltigt vara frivilligt, specifikt, informerat och otvetydigt. Om ni har inhämtat samtycken som är godkända enligt nuvarande regler behöver ni sannolikt inte inhämta nya samtycken.</p>

		<p>De ändringar som GDPR medför när det gäller samtycke kommer då istället främst att handla om hur ni hanterar samtycken. Ändringarna speglar ett mer dynamiskt sätt att se på samtycke som ett pågående och aktivt val istället för en engångshändelse genom ikryssande av en ruta. Ni behöver därför tydliga och granulära opt in-metoder, register över inhämtade samtycken och lättillgängliga sätt för de registrerade att återkalla sitt samtycke.</p> <p>Sammanfattningsvis innebär det sagda att ett övergripande svar som gäller för alla situationer inte kan lämnas utan ni måste avgöra i det enskilda fallet.</p>
2.	<p>Vad gäller för samtycken till utskick av nyhetsbrev till prenumeranter som fått prenumeration till följd av medlemskap i en organisation?</p>	<p>Samma krav ställs på samtycket i denna situation som i andra situationer där samtycke samlas in. Samtycket måste för att vara giltigt vara frivilligt, specifikt, informerat och otvetydigt. Den registrerade ska också ha rätt att återkalla samtycket.</p> <p>När det gäller nyhetsbrev är det dock inte säkert att ni behöver stödja behandlingen på samtycke.</p> <p>Om prenumerationen automatiskt ingår i organisationsmedlemskapet kan ni inte stödja er på avtalet med medlemmen eftersom den registrerade inte är part. Istället bör ni använda er av berättigat intresse (intresseavvägning) som laglig grund. Både ni och organisationen har ett berättigat intresse av att informera prenumeranterna om viktiga ändringar av betydelse för prenumerationen. Med hänsyn till att intrånget i prenumerantens integritet är mycket litet väger ert och organisationens intressen tyngre. Om nyhetsbrev utgör marknadsföring måste den registrerade kunna motsätta sig att ta emot marknadsföringen.</p>
3.	<p>Hur ska vi hantera personuppgifter i t.ex. adresslistor, som samlas in av någon annan och bara "mellanlandar" hos oss innan de går till tryckeriet?</p>	<p>Här är det värt att notera det materiella tillämpningsområdet för GDPR. Förordningen gäller för sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Om behandlingen är manuell omfattas den alltså bara om personuppgifterna ingår i ett register.</p> <p>Med register avses en sammanställning av personuppgifter som</p>

		<p>är ordnad enligt särskilda kriterier, t.ex. akter med dokument sorterade kronologiskt och alfabetiskt såsom fysiska patientregister inom sjukvården.</p> <p>Om personuppgifter endast ”mellanlandar” hos er för vidarebefordran och ni inte lägger in dem i era system eller register genomför ni ingen personuppgiftsbehandling. GDPR är då inte tillämpligt.</p> <p>Om ni däremot sparar uppgifterna eller på annat sätt använder dem kommer GDPR att vara tillämpligt för er behandling. Hur situationen då bör hanteras beror på vem som bestämmer ändamål och medel för behandlingen av de aktuella personuppgifterna. Om ni bestämmer är ni personuppgiftsansvariga och måste följa de regler som gäller för personuppgiftsansvariga; om ni behandlar uppgifterna för annans räkning är ni personuppgiftsbiträde och måste följa de regler som gäller för biträden.</p>
4.	<p>Vad gäller för gåvoprenumerationer? Hur ska vi praktiskt hantera gåvor i fråga om information till gåvomottagaren och laglig grund? Behöver vi samtycke från mottagaren för att behandla dennes uppgifter? Kan ansvar skjutas över på givaren?</p>	<p>När en prenumeration ges i gåva måste ni registrera adress- och kontaktuppgifter om mottagaren för att kunna administrera prenumerationen och leverera produkten. Frågan blir då med vilken laglig grund ni behandlar personuppgifterna om mottagaren, som inte känner till behandlingen, och hur ni kan informera mottagaren om behandlingen utan att förstöra överraskningen från givaren.</p> <p>Eftersom den registrerade, dvs. mottagaren, inte är part i avtalet om prenumerationen kan ni inte stödja er på avtalet. Samtycke är inte heller lämpligt att inhämta eftersom det skulle förstöra överraskningen. Den lämpligaste lagliga grunden för gåvoprenumerationer är er eller tredje parts berättigade intressen (intresseavvägning). Ni har ett berättigat intresse av att leverera en beställd och betald produkt och givaren har ett berättigat intresse att mottagaren får gåvan. Med hänsyn till att intrånget i mottagaren integritet är mycket litet väger ert och givarens intressen tyngre.</p> <p>När det gäller information till mottagaren om att ni behandlar dennes personuppgifter så behöver informationen inte lämnas</p>

		<p>omedelbart. Den kan lämnas inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas, eller, om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade.</p> <p>För gåvoprenumerationer bör därför information lämnas till mottagaren inom en månad från att ni fick uppgifterna.</p>
5.	<p>Vad gäller för källskyddat material enligt GDPR?</p>	<p>Med "källskyddat material" avses material som skyddas av den rätt till anonymitet som framgår av både tryckfrihetsförordningen och yttrandefrihetsgrundlagen.</p> <p>GDPR medger att nationell rätt får föreskriva om undantag till vissa av förordningens artiklar (för bl.a. tryck- och yttrandefrihet och journalistiska ändamål). I det nuvarande förslaget till sådan lagstiftning i Sverige framgår att GDPR inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet. Regler om källskyddat material (rätt till anonymitet) går således före reglerna om dataskydd i GDPR.</p> <p>I förslaget framgår att <i>"Det får inte råda någon osäkerhet kring detta, eftersom det skulle kunna få påverkan på vitala och mycket känsliga delar av den opinionsskapande verksamheten, såsom meddelarfrihet och källskydd. Vi föreslår därför en upplysningsbestämmelse som tydliggör att bestämmelserna i dataskyddsförordningen och i dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet."</i></p> <p>Förslaget till den svenska lagen medger även utanför det grundlagsskyddade området undantag för behandling av personuppgifter som sker för journalistiska ändamål.</p>

6.	<p>Vad behöver man tänka på när det gäller retargeting/remarketing vid användandet av pixelinformation?</p>	<p>Eftersom vi inte känner till hur medlemmarnas retargeting/remarketing går till så är det svårt att ge ett exakt svar på denna fråga.</p> <p>Generellt kan sägas att ni bör försöka ta reda på om och i så fall vilka personuppgifter som kan komma att föras över genom ert användande av pixeln. Det kan t.ex. vara IP-adress, unique user ID m.m.</p> <p>Om ni använder er av en extern part som levererar ”remarketinglösningen” så måste ni utreda om leverantören är personuppgiftsansvarig eller biträde. Om det är ett biträde så behöver ett personuppgiftsbiträdesavtal upprättas.</p> <p>Om leverantören är ansvarig så behövs en legal grund till stöd för att lämna informationen till den ansvarige. Den legala grunden för denna typ av marknadsföring är vanligen intresseavvägning. När ni stödjer er på en intresseavvägning måste ert berättigade intresse för behandlingen anges och ni måste motivera varför detta intresse väger tyngre än den registrerades intressen och rättigheter.</p> <p>Ni är även skyldiga att tillhandahålla information om behandlingen till den registrerade vilken bland annat måste innehålla information om vad ni gör och varför samt vilka rättigheter den registrerade har.</p>
7.	<p>Hur länge får man spara exempelvis mejladresser och adresser från prenumeranter som avslutat sin prenumeration? Får man göra ett utskick med erbjudande om rabatterad prenumeration till dem?</p>	<p>Hur länge personuppgifter får sparas beror på ändamålet med behandlingen. Det går därför inte att ge ett generellt svar som gäller för alla situationer.</p> <p>När det gäller direktmarknadsföring genom utskick av erbjudanden om rabatterad prenumeration får ni skicka reklam till kunden om det finns ett kundförhållande mellan er (personuppgiftsansvarig) och kunden, under förutsättning att kunden inte har motsatt sig det. Kunden har nämligen rätt att motsätta sig att ta emot obeställd reklam enligt både GDPR och marknadsföringslagen. Under förutsättning att ni erbjuder möjlighet att motsätta sig får ni alltså göra reklamutskick så länge kundförhållandet pågår.</p>

		<p>Datainspektionen har uttalat att i normala fall får personuppgifter om en tidigare kund användas för marknadsföringsändamål under ett års tid efter det att kundförhållandet har upphört, dvs. efter det att varan eller tjänsten är levererad och betald samt att eventuell garantitid har löpt ut. Kunden har dock rätt att begära att dennes uppgifter tas bort tidigare.</p>
8.	<p>Vad gäller för bilder och bilddatabaser? Vilka bilder räknas som personuppgifter? Måste en redaktion före register över sina bilder och fotografier?</p>	<p>Dataskyddsförordningen är tillämplig på i princip all behandling av personuppgifter som görs på elektronisk väg (automatiserad behandling) och i vissa fall även på manuell behandling. Personuppgifter innefattar alla uppgifter eller upplysningar som avser en identifierad eller identifierbar fysisk person. GDPR gäller på samma sätt för personuppgifter i bild som i text.</p> <p>Det avgörande för om bilder omfattas av GDPR är därmed om det är möjligt att identifiera en levande person på bilden eller om bilden föreställer något som kan kopplas till en person – exempelvis en bil med registreringsnummer, tatueringar, klädsel, eller hårfärg. Kan bilden, direkt eller indirekt, knytas till en fysisk person är bilden en personuppgift och GDPR är då tillämplig.</p> <p>Varje personuppgiftsansvarig (den som bestämmer ändamål och medel för behandlingen) ska föra ett register över behandling som utförts under dess ansvar. Registret ska innehålla kontaktuppgifter till personuppgiftsansvarig, behandlingens ändamål, kategorierna av registrerade och av personuppgifter, till vilka personuppgifterna har lämnats ut, tidsfrister för radering och information om säkerhetsåtgärder. Även varje personuppgiftsbiträde ska föra ett liknande register, med vissa undantag. Register ska göras tillgängligt för Datainspektionen, på begäran.</p> <p>Däremot tillåter GDPR att undantag görs i nationell rätt för tryck- och yttrandefrihet och journalistiska ändamål. I förslaget till dataskyddslagen framgår att GDPR inte tillämpas då den strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen (se även fråga 5 om källskyddat material). Dessutom ska enligt förslaget många artiklar i GDPR inte tillämpas vid behandling av personuppgifter som sker för journalistiska ändamål, däribland kravet på registerföring (art. 30). En redaktion som har bilder i</p>

		bilddatabaser för journalistiska ändamål behöver därför inte föra register över denna behandling.
9.	Är Dropbox GDPR-säkrat?	<p>Dropbox har uttalat att de uppfyller många av kraven i GDPR redan nu och att de kommer att uppnå fullständig efterlevnad före 25 maj 2018. Om Dropbox faktiskt kommer att göra det är svårt för oss att säga i dagsläget.</p> <p>Även om Dropbox uppnår fullständig efterlevnad måste ni som personuppgiftsansvariga se till att relationen mellan er och Dropbox uppfyller GDPR:s krav när ni anlitar Dropbox som biträde. Ni måste bl.a. se till att ett personuppgiftsbiträdesavtal som är förenligt med GDPR upprättas.</p>