Kort vägledning om legal behandling av personuppgifter - i sociala medier, annan marknadsföring eller när de behövs för att fullgöra ett avtal

Efter att GDPR (Dataskyddsförordningen) trädde i kraft för två år sedan kommer nya domar och uppdateringar om hur personuppgifter ska hanteras. Det är både svårtolkat och förvirrande att navigera i flödet om vad som ska gälla så några korta riktlinjer kan vara bra att ha för handen.

Personuppgifter

För det första är det viktigt att ha klart för sig vad som är personuppgifter. Personuppgifter är all typ av information **som kan kopplas till en specifik person (levande), t.ex.**

- namn, adress och personnummer
- foto
- ljudinspelningar
- m.fl

För **ALL** personuppgiftsbehandling krävs att man har stöd i lag. Sådant stöd i lag är antingen att uppgifterna behövs för att

1. fullgöra ett avtal eller
2. fullgöra en rättslig förpliktelse t.ex. att en arbetsgivare är skyldig att redovisa skatter och sociala avgifter för de anställda) eller
3. skydda intressen som är av grundläggande betydelse för den registrerade (t.ex. i vårdsammanhang när personens liva är i fara) eller
4. utföra en uppgift av allmänt intresse eller som följd av myndighetsutövning (t.ex. privat hälso- och sjukvård, skolverksamhet, kollektivtrafik) eller
5. ändamål som rör den personuppgiftsansvariges eller 3e parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre (t.ex. i en företagskoncern med flera personuppgiftsansvariga kan dessa ha ett berättigat intresse av att överföra personuppgifter inom koncernen för interna administrativa ändamål)
6. **Om man inte kan stödja sin behandling av uppgifterna på någon punkt ovan behövs ett frivilligt och tydligt samtycke från den registrerade**

Personuppgifter i sociala medier eller marknadsföring utan att man har någon legal grund (1-6 ovan) att stödja sig på är inte tillåtet!!

Om man haft en kundrelation kan man marknadsföra sig mot kund med stöd av punkt 5 (man kan anta att kund fortsatt är intresserad av företagets tjänster) eller punkt 6. Då ska det **ALLTID** finnas en möjlighet att tacka nej till fortsatta utskick.

Har man **inte haft någon kundrelation** utan vill väcka ett intresse hos en potentiell framtida kund, bör man ha tydligt visa hur man fått sina kontaktuppgifter (vilken källa) och ALDRIG

maila till en kund som inte själv lämnat sin mailadress utan då gäller endast postalt utskick. Om en person lämnat sina uppgifter för att få nyhetsbrev har personen självmant lämnat sina uppgifter för ett specifikt syfte = nyhetsbrev och det får anses som ett aktivt samtycke enligt ovan punkt 6.

Foton på personer i sociala medier eller på webb-sidor

Se till att alltid tydligt informera om att bilder kan komma att användas på webb-sida eller i sociala medier. Har man inte gjort det eller är man det minsta osäker bör bilderna göras så pass otydliga att det inte är möjligt att identifiera personerna på bilderna.

Var hanteras bilder eller andra personuppgifter på sociala medier eller webb-plats, inom eller utanför EU/EES?

Eftersom det som grundregel är FÖRBJUDET att överföra personuppgifter till tredje land (alla länder utanför EU/EES), måste man veta var personuppgifterna behandlas rent geografiskt. Bara för att man ingått avtal med en leverantör i Sverige betyder det inte att uppgifterna stannar i Sverige. De kan behandlas på en server utanför EU/EES, i en molntjänst eller som t.ex. för amerikanska bolag som Facebook, i USA.

OM uppgifter behandlas inom EU/EES, omfattas alla dessa länder av GDPR och alla företag, organisationer, myndigheter mm ska självmant leva upp till kraven som finns i GDPR.

För att kunna få överföra personuppgifter till länder utanför EU/EES gäller att man grundar överföringen på ett undantag i GDPR. Dessa undantag återfinns i artiklarna 45-50, men för mindre företag inom besöksnäringen är det f.n. endast undantagen i artikel 49 som är relevant:

a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.
b) Överföringen är nödvändig för att fullgöra ett avtal mellan den *registrerade och den personuppgiftsansvarige* eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.
c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den *personuppgiftsansvarige och en annan fysisk eller juridisk person* i den registrerades intresse.
--
e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Något som nyligen diskuterats är en dom från EU-domstolen (Schrems II) som kom juli -20 och betyder att USA INTE når upp till ”adekvat skyddsnivå” i sina tidigare **generella överenskommelser** (tidigare Safe Harbour-bestämmelsen och nu senast Privacy Shield).”Adekvat skyddsnivå” är ett av de andra undantagen man kan grunda sin överföring till tredje land på. Detta senaste avgörande i EU-domstolen och underkännandet av USA:s

skyddsnivå för personuppgifter spelar dock ingen roll om man kan hitta stöd i någon bestämmelse i artikel 49, se ovan.

När det är fråga om överföring till ett tredje land har man dessutom en långtgående undersökningsplikt och ett ansvar; både i att ta reda på vilket skydd personuppgifterna i praktiken har i tredjelandet, hur lagstiftningen ser ut där och att informera de registrerade om skydd och risker!

Vad behöver man göra?

Som alltid - oavsett var personuppgifter hanteras – behöver man

- kartlägga vilken behandling av personuppgifter som sker – både rörande kunder, anställda och ev. leverantörer
- göra en gedigen konsekvensbedömning.
- Se till att ovan finns dokumenterat och lättillgängligt!
- Kontrollera och uppdatera kontinuerligt

Om man blir anmäld måste man kunna visa vad man grundar behandlingen på, vilka överväganden man gjort, hur uppgifterna skyddas, sin skriftliga konsekvensanalys och eventuella undantag man stödjer sig på.

Du hittar mer information på hemsidan för Integritetsskyddsmyndigheten (IMY) *(Tidigare Datainspektionen)*

Oktober 2020, (uppdaterad feb 2021)