Enkla grunder i dataskydd

Nästa år får Sverige och övriga EU en ny gemensam lagstiftning som reglerar hur bland annat företag får behandla personuppgifter. En nyhet i denna dataskyddsförordning är kännbara sanktionsavgifter om man bryter mot reglerna, något som har fått många företag att fundera över hur de hanterar och skyddar personuppgifter. Här följer en enkel grundkurs i dataskydd med fokus på mindre företag.

Dataskydd på 5 röda

Samla inte in fler personuppgifter än nödvändigt och enbart för ett visst, i förväg bestämt ändamål. Spara inte uppgifterna längre än nödvändigt. Se till att ni har stöd i lagen för att samla in uppgifterna.

Vad är egentligen en personuppgift?

Personuppgifter är all slags information som kan knytas till en fysisk person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Ja, till och med ljudinspelningar som lagras elektroniskt kan vara personuppgifter även om det inte nämns några namn i inspelningen. Ett bolagsnummer är ofta inte en personuppgift men är det om det handlar om en enskild näringsverksamhet. Registreringsnumret på en bil kan vara en personuppgift om det går att knyta till en fysisk person medan registreringsnumret på en firmabil som används av flera, kanske inte är en personuppgift.

ÄVEN KÄND SOM GDPR

Dataskyddsförordningen kallas ibland kort för GDPR vilket står för General Data Protection Regulation. Förordningen börjar tillämpas i maj 2018 och ersätter då den svenska personuppgiftslagen.

Sexualliv och religion

I dataskyddsförordningen skiljer man mellan ”vanliga” personuppgifter och känsliga personuppgifter. Känsliga uppgifter är sådana som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv. Uppgifter om hälsa kan till exempel vara sjukfrånvaro, graviditet och läkarbesök. Normalt är det förbjudet att hantera sådana personuppgifter men det finns undantag från förbudet. Känsliga uppgifter måste också skyddas mer än andra uppgifter.

NYTT I FÖRORDNINGEN

Med dataskyddsförordningen kommer även genetiska uppgifter räknas som känsliga personuppgifter. Samma sak gäller biometriska uppgifter som används för identifiera en fysisk person.

Men är det verkligen så nytt?

Att vi nästa år får en ny lag som reglerar hur man samlar in och använder personuppgifter har väckt stor uppmärksamhet. Men faktum är att vi i Sverige har haft sådan lagstiftning ända sedan 1973 då datalagen trädde i kraft. Det var dessutom världens första nationella datalag. I grunden innehåller förordningen samma regler och principer som dagens lagstiftning men det finns nyheter.

När får personuppgifter samlas in?

Personuppgifter får bara samlas in för ”särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål”, säger förordningen. Alltså, uppgifter som samlas in för ett visst syfte, får inte sedan användas för helt andra syften. Ett företag kan till exempel utrusta sina bilar med speciell gps-utrustning som används för elektroniska körjournaler för att förenkla redovisningen till Skatteverket. Men, arbetsgivare får inte använda uppgifterna som gps:en samlar in för att kontrollera hur långa raster de anställda tar.
Man måste också ha stöd i förordningen för att hantera personuppgifter. Det finns ett par olika ”rättsliga grunder” som företag kan använda. De viktigaste är:

RÄTTSLIG FÖRPLIKTELSE

I vissa fall är företag skyldiga att registrera personuppgifter, som exempelvis för att uppfylla bokföringsskyldigheten i bokföringslagen.

AVTAL

Anställningsavtal, kundavtal och leverantörsavtal är exempel på avtal som innebär att företag måste registrera och hantera personuppgifter (men bara de uppgifter som behövs för att uppfylla avtalet).

SAMTYCKE

Ett annat alternativ är att be personen ifråga att få registrera uppgifter om honom/henne. Det kallas för att få personens samtycke. Ett samtycke är enligt förordningen ”varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne”.

På litet enklare svenska: man måste få tydlig information om vilka uppgifter som samlas in och vad de ska användas till, för att man sedan ska kunna ge sitt godkännande.

INTRESSEAVVÄGNING

Det är också möjligt att hantera personuppgifter efter en så kallad intresseavvägning om företaget kan visa att dess intresse av att hantera uppgifterna väger tyngre än den enskildes rätt till privatliv. Enligt personuppgiftslagen, som gäller i skrivande stund, kan företag i många fall använda intresseavvägning som grund för att hantera personuppgifter som används vid marknadsföring och direktreklam. OBS! Man får inte skicka direktreklam till någon som sagt nej till det.

EXEMPEL PÅ RÄTTSLIGA GRUNDER

Lönesystem	Avtal
Kundregister	Avtal. För vissa uppgifter krävs samtycke
Register med potentiella kunder	Intresseavvägning
Webbplatsen	Samtycke eller intresseavvägning

Informera mera...

När ni samlar in uppgifter om en person så måste ni informera personen i fråga. I förordningen finns en lång lista över vilken information som ska ges, men mycket kort ska ni tala om att ni samlar in personuppgifter, vilka uppgifter det handlar om och varför ni gör det. Kommer ni att lämna uppgifterna vidare till andra, måste ni tala om det.

... och spara mindre

En viktig regel i förordningen är att man inte får spara personuppgifter för länge. När de inte längre behövs för det syfte som de en gång samlades in för, så ska de tas bort. För ett företag innebär det till exempel att uppgifter om personer som inte längre är kunder (eller leverantörer) måste tas bort från it-systemen. Nu, när personuppgiftslagen gäller, är praxis att personuppgifter om en tidigare kund i normala fall får användas för marknadsföringsändamål under ett års tid efter att kundrelationen har upphört. Om säljaren ska kunna fullgöra eventuella garantiåtaganden kan det motivera att vissa personuppgifter bevaras tills garantin har gått ut.

TÄNK OCKSÅ PÅ DETTA!

Det kan finnas krav i annan lagstiftning som innebär att uppgifterna måste sparas en viss tid, till exempel för bokförings- och arkivändamål.

Se över säkerheten!

Tänk på att skydda personuppgifterna som ni hanterar, så att de inte stjäls eller oavsiktligt raderas eller ändras. Ett nytt krav i förordningen är att om ni råkar ut för en "personuppgiftsincident" så måste ni rapportera det till Datainspektionen. En sådan incident kan till exempel vara ett usb-minne med personuppgifter som tappats bort, ett dataintrång på en av företagets servrar eller att någon anställd obehörigt tagit del av personuppgifter. Ett tips är att se över skyddet av personuppgifterna i era it-system så att incidenter inte inträffar.

Får man spara uppgifter om sina kunders intressen?

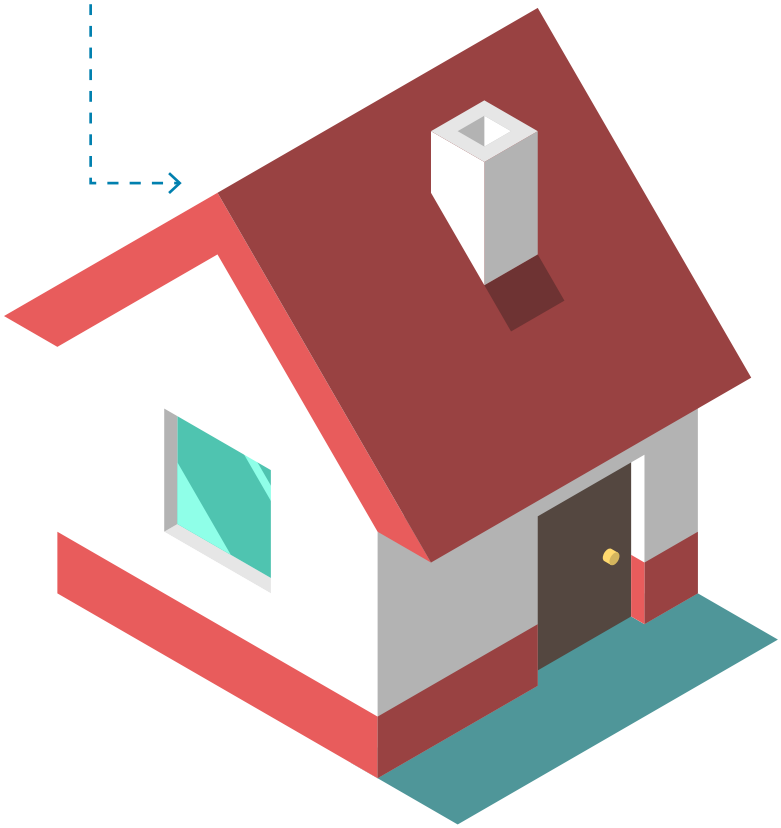
I ett CRM-system för kundvård vill man kanske registrera fler uppgifter om kunderna än de som behövs för att uppfylla avtalet med kunden. Spelar kunden golf? Hur många barn har kunden? Har kunden allergier som kan vara bra att känna till innan affärslunchen? För att få registrera den typen av uppgifter krävs normalt att kunden ger sitt samtycke, det vill säga att kunden först får information om att ni kommer att spara den typen av uppgifter och varför, och sedan godkänner att ni gör det. Men, man måste också se till att uppgifterna är relevanta för kundrelationen. Annars får de inte registreras.

Ordning på torpet!

Alla företag (och andra organisationer) är enligt förordningen skyldiga att ha ett register som beskriver de olika sätt som man hanterar personuppgifter på. Vem internt är ansvarig för ett visst register eller it-system, vad används det till, vilka typer av personer förekommer i det, vilka typer av uppgifter och med vilken rättslig grund hanteras uppgifterna?

Miljonböter om ni inte sköter er

En nyhet i dataskyddsförordningen är att Datainspektionen kan besluta att ett företag som inte följer reglerna i förordningen ska betala en administrativ sanktionsavgift, vilket är en form av böter. Sanktionsavgiften kan vara upp till 20 miljoner euro eller fyra procent av den globala årsomsättningen.



Risken för kännbara böter har gjort att företag och andra organisationer tar skyddet av personuppgifter på större allvar. Det är positivt.

ELISABETH JILDERYD, DATAINSPEKTIONEN

LÄS MER OM DATASKYDD

I den här artikeln tar vi upp några av de viktigaste grunderna i dataskydd. Men, vi tar inte upp alla krav och bedömningar som kan bli aktuella då personuppgifter samlas in och hanteras. Ett bra ställe att fortsätta inläsningen på den kommande förordningen är: www.datainspektionen.se/dataskyddsreformen