FOYEN

Det var ett väldigt tjat om det där med GDPR!

Den 25 maj har nu kommit och gått, och himlen trillade inte ner över våra huvuden. Våra mejlkorgar svämmade dock över av e-postmeddelanden från alla håll, alla med samma budskap. ”Du är viktig för oss, och här ser du hur vi behandlar dina personuppgifter”. Men är allt som vanligt nu igen?

Många företag och myndigheter har arbetat hårt det senaste året (eller till och med åren) för att vara klara den 25 maj, och uppfylla kraven i den nya personuppgiftslagstiftningen. Långt ifrån alla är klara, och det finns många som inte ens börjat. Men GDPR har kommit för att stanna (tills vidare åtminstone) och man ska i sin verksamhet hela tiden leva efter de nya bestämmelserna. Är man inte klar nu, så ska man se till att bli klar och att ha en plan för hur man ska bedriva sin verksamhet på ett sätt som följer gällande lagstiftning.

Mycket är dock förvirrande, och många felaktiga föreställningar florerar kring hur man ska agera.

Alla de e-postbrev som skickats ut, har skickats ut eftersom man har en skyldighet att berätta för dem vars uppgifter man behandlar att man behandlar uppgifter och hur man behandlar uppgifter. Vad informationen ska innehålla bestäms av lagstiftningen, och det är ganska omfattande uppgifter.

Men sedan blir det mer förvirrande. En del informerar bara, och andra begär samtycke också. Varför då?

Jo, för att få behandla personuppgifter måste man ha en laglig grund. En sådan grund kan vara samtycke. Ett samtycke ska vara informerat och frivilligt – och man ska när som helst kunna återkalla samtycket. Om den registrerade återkallar samtycket, ska man upphöra med behandlingen. Man ska också kunna bevisa att man har fått samtycke, vilket riskerar att leda till viss administration. En hel del av de brev man har fått har således dels varit information, dels har de begärt samtycke till behandlingen. Har man inte gett samtycket, så ska de upphöra med behandlingen.

Den andra kategorin e-postbrev man har sett har istället bara varit information. Då grundar man behandlingen på något annat än samtycke, till exempel avtal. Om avtal inte finns, är det sannolikt intresseavvägning som är den lagliga grunden för behandling.

Intresseavvägning innebär att den som behandlar personuppgifter har ett berättigat intresse som väger tyngre än den enskildes intresse av att inte bli behandlad. Ofta handlar det om nyhetsbrev eller annan marknadsföring. Det anses i regel vara en berättigad grund för behandling. Som registrerad har man dock alltid rätt att vägra detta, enklast genom en ”un-subscribe”-knapp i slutet av marknadsföringsbrevet man får.

Inte sällan sammanblandas dessa två grunder för behandlingen.

Det finns fler grunder för behandling – och man måste titta på varje behandling för sig. Är man arbetsgivare behandlar man de anställdas personuppgifter för att uppfylla sina förpliktelser enligt anställningsavtalet, till exempel betala ut lön. Man behandlar dock också de anställdas personuppgifter när man skickar dem till Skatteverket i form av kontrolluppgift. Detta gör man på grund av en rättslig förpliktelse, en annan laglig grund för behandling.

När man väl har kommit fram till vilken grund för behandling man har i varje enskilt fall, ska man se till att man behandlar personuppgifterna på ett lagligt sätt. Inte för länge, inte fler än nödvändigt och att man exempelvis ser till att rätta felaktiga uppgifter.

Har man väl kommit fram till detta, ska det dokumenteras. En inventering av vilka personuppgifter man har och varför man behandlar dem, samt hur man behandlar dem och dokumentering av denna inventering är således det som behöver göras för att man ska agera i enlighet med lagen. Har man inte gjort detta än, så ska man börja nu.

Som leverantör av olika tjänster och produkter, kan man räkna med att krav kommer att ställas från köpare av dessa att man behandlar personuppgifter i enlighet med GDPR. Man kan dessutom vara pro-aktiv och i sin marknadsföring skryta om att man hanterar personuppgifter korrekt. I offentliga upphandlingar kommer man att se ökade krav på detta område, eftersom myndigheter också måste följa GDPR, och således måste ställa krav på hur detta görs. Att ha koll på sina personuppgiftsbehandlingar kan också innebära att man lättare kan utveckla en ny affärsidé, eller att man äntligen storstädar i sina register och får en aktuell, korrekt och relevant kundlista.

Så förutom att GDPR är en tvingande lagstiftning, som inte lämnar utrymme för ”skolk”, så är det också en lagstiftning som man kan dra nytta av i sin verksamhet genom att man inför effektivare och säkrare processer. Dessa i sin tur medför att man faktiskt behandlar personuppgifter på ett korrekt sätt som gör kunder och kontakter nöjda. Inte minst så är det en fördel i en säljprocess, att man med säkerhet kan säga att: ”Javisst, såklart vi följer GDPR” till en framtida kund.

Det är alltså inte försent att kontrollera era processer och system, det är inte försent att skicka ut information till era anställda, kunder och kontakter och andra vars uppgifter ni behandlar. Det är inte försent att säkerställa att ni idag och framöver följer GDPR.

Sara Malmgren, advokat och ansvarig för avdelningen IT och nya teknologier på Foyen Advokatfirma
sara.malmgren@foyen.se

Som medlem i SBR har du tillgång till 15 minuters fri rådgivning hos Foyen Advokatfirma. Rådgivningen når du på 08-506 184 00.