Så får du kontroll över företagets personuppgifter

Den 25 maj 2018 träder den nya europeiska dataskyddsförordningen ”The General Data Protection Regulation” (GDPR) i kraft.

Företag som inte efterlever den nya förordningen kan få böter på upp till det högsta av 20 miljoner euro eller 4 % av den globala omsättningen.

Som ett led i att uppfylla GDPR-reglerna är det viktigt att kartlägga hur och för vilka syften alla personuppgifter inom hela verksamheten behandlas.

Du behöver veta och dokumentera var uppgifterna kommer från, var och hur personuppgifterna lagras samt hur personuppgifterna används.

Personuppgifter är alla uppgifter som kan härledas till en individ och kan till exempel omfatta namn, kontaktuppgifter, IP-adresser, geografiska platser, kön, inkomst, intressen och besök på webbplatser.

Checklista för personuppgifter

Använd denna lista med frågor som hjälp för att analysera personuppgifterna som finns sparade i era system.

1 Vilka personuppgifter samlas in?

Beskriv vilken kategori personuppgifter som samlas in, till exempel namn, adress, e-postadress, telefonnummer. Om det även förekommer andra typer av personuppgifter såsom födelsedatum, personnummer, fotografier etc som kan identifiera en person ska dessa beskrivas.

2 Vad är syftet med att behandla en viss kategori personuppgifter?

Förklara varför du behandlar de personuppgifter som du gör. Om du till exempel verkligen behöver lagra födelsedatum, så måste du kunna förklara varför och vad ni använder det till.

3 Vilken är den lagliga grunden?

Förklara företagets lagliga grund för behandlingen av den aktuella kategorin personuppgifter.

4 Varifrån kommer personuppgifterna?

Beskriv hur du samlar in personuppgifterna. Får du uppgifterna via webbformulär, visitkort som samlas in vid olika sammanhang, via integrationer med andra system o.s.v.

5 Vilken klassificering är aktuell?

Klassificeringar av personuppgifter kan vara konfidentiella, anonyma, känsliga o.s.v. Till exempel kan känsliga uppgifter vara information om hälsa eller facklig tillhörighet. Observera att alla personuppgifter som kan vara känsliga eller konfidentiella kräver extra säkerhetsåtgärder.

6 Hur länge sparas personuppgifterna?

Ange hur länge den aktuella kategorin av personuppgifter kommer sparas. Personuppgifter får inte sparas längre tid än nödvändigt med hänsyn till ändamålet med uppgifterna. Vad som är nödvändigt med hänsyn till ändamålet kan bero på vad annan lagstiftning, t ex bokföringslag eller arbetsrättslig lagstiftning anger eller vad som följer av gällande praxis och vägledningar.

7 Vem ska ha tillgång till personuppgifterna?

Beskriv vem som har tillgång till personuppgifterna och säkerställ att uppgifter inte hanteras av fler personer än nödvändigt. Till exempel har medarbetarna på löneavdelningen tillgång till lönesystemet, HR-avdelningen till HR-information och säljavdelningen till kundinformation. Ibland kan åtkomst behöva begränsas mer än så.

8 Överförs personuppgifter till andra länder?

Personuppgifter ska som huvudregel endast behandlas inom EU.
När överföring av personuppgifter sker måste du ha vidtagit lämpliga skyddsåtgärder, t.ex. ingått ett speciellt avtal om överföringen och dokumentera detta.

9 Vilket system lagras informationen i?

Du har med största sannolikhet separata system för hantering av löner och kundinformation. Du behöver se över och dokumentera i vilka system ni på olika sätt behandlar respektive kategori personuppgifter

10 Har uttryckligt samtycke givits för användning av uppgifterna?

I vissa fall kan behandling av personuppgifter kräva samtycke. Redogör för om personen frivilligt har gett sitt samtycke till att du kan använda personuppgifterna i marknadsföringssyfte. Klart och tydligt samtycke krävs t ex som huvudregel om du behandlar personuppgifter om personer som du inte har en aktiv kundrelation med.

11 Har den berörda personen informerats om att ni behandlar personuppgifter?

Enligt lagen krävs att du informerar de registrerade om hur ni behandlar dess personuppgifter. Det finns flera krav på vad denna information ska innehålla och du bör anlita en jurist för att ta fram informationshandlingar. Denna typ av information tillhandahålls som regel i kundkontakten, vid ett uppstartsmöte och/eller i integritetspolicyn på er webbplats.

12 Delas personuppgifterna med tredje part och varför?

Om personuppgifter delas med andra, bör du beskriva vilken typ av personuppgifter som sprids vidare, med vilken tredje part, vilka personuppgifter samt till vilket syfte.

Enligt GDPR ska även ett uppgiftsbiträdesavtal upprättas som reglerar ett antal olika punkter enligt lag, t ex säkerheten hos mottagaren samt fördelning av ansvaret mellan er och tredje part.

13 Hur garanteras säkerheten för personuppgifterna?

Beskriv säkerhetsåtgärderna som används för att skydda personuppgifterna. Detta är extra viktigt om du har känsliga uppgifter lagrade.

Nästa steg

När du har besvarat frågorna i checklistan kommer den att hjälpa dig att fastställa vilka uppgifter ni önskar behandla. Du bör inte spara mer information än nödvändigt och du bör radera uppgifter som inte används.

Om ditt företag samlar in mycket uppgifter utan något relevant syfte eller nytta kan ni inte fortsätta med det.

Kartläggningen av företagets uppgifter och fast-ställandet av vilka uppgifter ni behöver behandla och ert lagliga stöd för detta är några av de första viktiga stegen som krävs för att ni ska kunna efterleva GDPR. Det finns även många andra åtgärder du behöver vidta för att följa lagstiftningen.

Säkerställ att era systemlösningar hjälper er att på ett effektivt sätt följa lagstiftningen, genom t ex automatisk radering av uppgifter som ej ska sparas, funktioner för information och rättelse samt dokumentation av lagligt stöd för behandling.

Om du har frågor om hur SuperOffice CRM kan ge dig stöd under er GDPR-resa, kontakta oss på +46 8 522 33 800