Svenskt Näringsliv svarar på vanliga frågor om nya dataskyddsförordningen

Fråga: Vad är en personuppgift?

Svar: Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Som exempel kan nämnas namn, personnummer, telefonnummer, adress eller e-postadress. Även bilder och ljudupptagningar av personer kan vara personuppgifter. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas också som personuppgifter om de kan kopplas till fysiska personer. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel som rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. Om det således existerar en ”nyckel” som gör det möjligt att koppla en viss uppgift till en fysisk person, så är uppgiften en personuppgift, även om uppgiften och ”nyckeln” finns hos olika parter. Skäl 28: Så kallad pseudonymisering utesluter inte krav på andra åtgärder för dataskydd.

Fråga: Vad är personuppgiftsskyddet?

Svar: Med personuppgiftsskyddet avses för närvarande personuppgiftslagen (1998:204). Personuppgiftslagen innehåller regler som ska skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Personuppgiftslagen bygger på ett EG-direktiv och varje EU-land har varit tvungen att införa nationell lag baserad på direktivet. Från och med 25 maj 2018 kommer personuppgiftslagen att ersättas av dataskyddsförordningen. Dataskyddsförordningen gäller som lag direkt och på samma sätt i alla EU:s medlemsstater. Dataskyddsförordningen kommer att innebära dels att rättigheterna stärks för enskilda personer, dels att det införs nya krav för bolag, myndigheter och andra organisationer som samlar in personuppgifter. Dataskyddsförordningen innehåller även nya bestämmelser om stränga sanktioner vid överträdelse av Dataskyddsförordningen. Tillsynsmyndigheten, som i Sveriges fall utgörs av Datainspektionen, kan besluta om en administrativ sanktionsavgift på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen, beroende på vilket belopp som är högst.

Fråga: Vilken är den minsta gemensamma nämnaren för personskyddsdata? Om jag har ditt namn och din mailadress, är det personskyddsdata eller inte?

Svar: Både namn och e-postadress är personuppgifter som omfattas av Dataskyddsförordningens regler.

Fråga: Vad händer om företaget hanterat personuppgifter felaktigt?

Svar: De påföljder som kan komma i fråga vid brott mot Dataskyddsförordningen är (i) skadestånd till den registrerade samt (ii) en administrativ sanktionsavgift på upp till det högsta av 20 000 000 EUR eller 4% av den totala globala årsomsättningen. Därutöver gäller att varje EU-medlemsstat har möjlighet att besluta om även andra sanktioner för överträdelse av Dataskyddsförordningen.

Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Den personuppgiftsansvarige är skadeståndsskyldig i förhållande till den registrerade för behandling av personuppgifter som sker i strid med bestämmelserna i Dataskyddsförordningen.

Personuppgiftsbiträde är någon som behandlar personuppgifter för den personuppgiftsansvariges räkning. Enligt Dataskyddsförordningen är även ett personuppgiftsbiträde skadeståndsskyldig i förhållande till den registrerade om personuppgiftsbiträdet bryter mot sina åtaganden enligt Dataskyddsförordningen eller den personuppgiftsansvariges anvisningar.

Fråga: Är mitt kundregister en integritetsfråga?

Svar: Om kundregistret innehåller uppgifter om fysiska personer, så omfattas kundregistret av Dataskyddsförordningen och dess bestämmelser. De rättsliga grunderna, för när behandling av personuppgifter är tillåten, är i stort sett oförändrade i förhållande till personuppgiftslagen. Som tidigare gäller således att behandling av personuppgifter får ske, bland annat om det föreligger ett samtycke. Dataskyddsförordningen ställer dock strängare krav på tydighet när det gäller lämnade av samtycken. Om behandlingen är nödvändig för att fullgöra ett avtal eller så kan behandlingen anses tillåten efter en intresseavvägning. Personuppgifter får nämligen behandlas utan den registrerades samtycke om behandlingen är nödvändig för att ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige ska kunna tillgodoses – om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten, så kallad intresseavvägning. Behandling av personuppgifter t ex för direktmarknadsföring anges i skälen till dataskyddsförordningen kunna vara ett sådant berättigat intresse.

Fråga: Vilka delar av mitt kundregister måste vara krypterat?

Svar: Av Dataskyddsförordningen följer bland annat att den som är personuppgiftsansvarig ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Generellt gäller att ju känsligare personuppgifterna är eller ju fler personuppgifter som hanteras, desto mer omfattande bör säkerhetsåtgärderna vara.

Uppgifter som normalt ingår i ett kundregister, d v s namn, telefonnummer, adress och e-postadress, har tidigare betraktas som förhållandevis harmlösa uppgifter och har därför normalt inte behövt vara krypterade. Det gäller sannolikt även enligt en tillämpning av Dataskyddsförordningen.

I det fall behandlingen innefattar behandling av särskilt integritetskänsliga uppgifter, såsom ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter som rör hälsa eller sexualliv eller av annan anledning kan anses riskfylld, så blir bedömningen sannolikt den motsatta. Notera i sammanhanget att behandling av sådana särskilt integritetskänsliga uppgifter endast är tillåten i vissa särskilt begränsade fall.

Fråga: Om vi gör en Excel fil som innehåller potentiella kunder som vi ska ringa, kan den göra så vi får böter?

Svar: Förutsatt att listan innehåller uppgifter avseende fysiska personer så är Dataskyddsförordningen tillämplig. Enligt nuvarande personuppgiftslagen finns förenklade regler när det gäller behandling av personuppgifter i ostrukturerat material, t ex såsom personuppgifter i en Excel fil. Den förenklade regleringen innebär att vardaglig ostrukturerad behandling i princip får utföras fritt så länge man inte kränker den uppgifterna avser. Dessa förenklade regler gäller inte efter 24 maj 2018 då dataskyddsförordningen börjar tillämpas, varför frågan måste bedömas med beaktande av samtliga bestämmelser i dataskyddsförordningen.
Det är då nödvändigt att avgöra om det föreligger någon laglig grund för bolagets behandling av de potentiella kunderna.

Inledningsvis har man då att först beakta vissa grundläggande principer för behandling av personuppgifter. Av dessa regler följer bland annat att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifterna får sedan inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna ursprungligen samlades in. De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Vidare gäller att personuppgifter som behandlas ska vara korrekta, och om nödvändigt, uppdaterade. Personuppgifterna får inte heller bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

I likhet med vad som tidigare gällt enligt personuppgiftslagen, följer av dessa bestämmelser att bolaget inte får spara uppgifterna om de potentiella kunderna utan begränsning i tiden utan att uppgifterna måste gallras efter viss tid.

Vidare måste bolagets behandling ha något lagligt stöd. Enligt huvudregeln krävs den enskildes samtycke för att det ska vara tillåtet att behandla personuppgifter. Undantag har dock gjorts för behandlingar som är nödvändiga för vissa i lagen angivna ändamål.

Finns inte något samtycke eller något annat uttryckligt stöd för behandlingen i Dataskyddsförordningen, så kan behandlingen ändå anses tillåten efter en intresseavvägning. Personuppgifter får nämligen behandlas utan den registrerades samtycke om behandlingen är nödvändig för ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige ska kunna tillgodoses – om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten (”intresseavvägning”).

Som angivits ovan är intresset av att marknadsföra produkter och tjänster ofta ett sådant berättigat intresse som enligt dataskyddsförordningen ger rätt att behandla personuppgifter med stöd av en intresseavvägning. Den registrerade har som tidigare rätt att motsätta sig bland annat behandling för direkt marknadsföring, varvid sådan behandling inte längre är tillåten. Vid sidan av nämnda undantag för behandling för direkt marknadsföring, så finns mer omfattande regler till stöd för den registrerade att motsätta sig behandling av personuppgifter.
Ytterst finns en risk att bolaget, om det felaktigt behandlar uppgifter om potentiella kunder, riskerar såväl skadeståndsskyldighet i förhållande till den registrerade som administrativa sanktionsavgifter. Bolaget har därför all anledning att säkerställa att all personuppgiftsbehandling följer de regler som framgår av dataskyddsförordningen.