Regionledningskontoret
Ekonomi och finans

Känslig information i fakturor och/eller fakturaunderlag till och ifrån Region Stockholm

Allmänt

För att kunna behandla personuppgifter på ett lagligt och korrekt sätt finns bestämmelser i dataskyddsförordningen (GDPR). En av de viktigaste bestämmelserna är artikel 6 GDPR om rättslig grund som stöd för behandlingen. Alla behandlingar av personuppgifter ska ha en rättslig grund som stöd för behandlingen. I artikel 6 anges: ”Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt”. Av de grunder som finns stödjer vi oss normalt på dessa två vid faktura-hantering:

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse (moms, bokföringslag) som åvilar den personuppgiftsansvarige.
e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse (till exempel betala fakturor för just våra medborgares räkning) eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Tänk på att namn, personnummer/samordningsnummer som kopplas ihop med uppgift om hälsa/sjukdom för en fysisk person (den registrerade) är en känslig personuppgift. För att behandla känsliga personuppgifter finns ytterligare krav i GDPR.

Det finns inget uttryckligt förbud att ha personnummer i en faktura/e-faktura, men en bedömning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras. För att få använda personnummer vid fakturering krävs stöd i 3 kap. 10 dataskyddslagen (2018:218). Om man inte har samtycke från den det berör (den registrerade) får man behandla personnummer/samordningsnummer enbart av följande skäl:

A. Om det utifrån ändamålet med behandlingen, dvs. skälet till varför man behöver behandla personnummer/samordningsnummer motiverar att uppgifterna behandlas.
B. Om det behövs för att säkert identifiera en fysisk person.
C. Om det finns något annat beaktansvärt skäl.

När det gäller en faktura kan personnummer behövas för en exakt identifierande uppgift vid fakturaadministrationen och för att uppfylla lagkrav kring redovisning och skatt. Då kan man hänvisa till punkten A eller B ovan.

Inblandade systems säkerhetsklassning ska beaktas och gällande GDPR-krav (det ska finnas register över innehållet i personuppgiftsbehandlingen där fakturorna ingår, dokumenterat ändamål och rättslig grund) ska vara korrekt dokumenterade. Ett riskbaserat arbetssätt ska också finnas.

(Dokumentet framtaget i samråd med Avdelning för juridik hos Sveriges Kommuner och Regioner samt Strategisk IT på Regionledningskontoret, Region Stockholm dec 2019-maj 2020)

Inkommande fakturor (leverantörsfakturor)

Region Stockholm skiljer inte på hur fakturor med eller utan känslig information ska adresseras utan rekommenderar alla leverantörer att skicka e-faktura i PEPPOL-format. Utväxling av e-handelsdokument genom PEPPOL skiljer sig inte så mycket jämfört med hur det fungerat tidigare med VAN-operatörer. Skillnaden är att PEPPOL ställer krav på att all trafik måste vara krypterad och signerad. (I Norge överväger man att sända betalningar via PEPPOL:s kommunikation.)

Utgående fakturor (kundfakturor)

Elektroniska fakturor och bilagor rekommenderas. Skicka till kundens PEPPOL-id eller be denne skaffa sådant.

Ett brev skyddas av sitt kuvert. Det är också bara en begränsad krets som har tillgång till brevet under transporten. Risken för förlust och förseningar under transport är dock betydande. Och mottagandebekräftelse uteblir.

Vanlig e-post är att jämföra med vykort. Det finns vissa saker man inte skriver på vykort och dem skriver man inte heller i ett vanligt mail t.ex. personnummer och/eller uppgifter om någons hälsa. Om man krypterar innehållet innan man skickar det får man ett godtagbart skydd.

(Dokumentet framtaget i samråd med Avdelning för juridik hos Sveriges Kommuner och Regioner samt Strategisk IT på Regionledningskontoret, Region Stockholm dec 2019-maj 2020)