



Grundläggande principer för personuppgiftsbehandling hos KPMG

Laglighet, korrekthet och öppenhet

Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt så att den registrerade förstår hur hans eller hennes uppgifter behandlas och varför.

Förutsättningar för en laglig och korrekt behandling av personuppgifter är att KPMG:s medarbetare har kunskap om vilka krav som gäller, stöd genom vägledande dokumentation och tillgång till medarbetare med kunskap avseende regleringen av personuppgiftsbehandling för besvarande av frågor.

KPMG:s vägledningar innefattar rekommendationer till medarbetarna avseende laglighet och korrekthet vid olika slags behandling av personuppgifter, bland annat i uppdragsverksamheten samt vid användning av e-post.

Principen om öppenhet innebär att de registrerade har tillgång till information om hur och varför deras personuppgifter behandlas. KPMG:s medarbetare ska också via företagets intranät ha tillgång till information om hur företaget behandlar personuppgifter.

Ändamålsbegränsning

Principen om ändamålsbegränsning innebär att personuppgifter endast får behandlas för tydligt angivna ändamål och att de inte i ett senare skede får behandlas för något annat oförenligt ändamål.

Utgångspunkten för KPMG:s efterlevnad av ändamålsbegränsningar är att medarbetarna vid behandling av personuppgifter har kunskap om ändamålen för behandling av personuppgifter och förbudet mot att behandla personuppgifter för oförenliga ändamål samt att dessa ändamål dokumenteras. Härigenom ges medarbetarna möjlighet att efterleva samt verka för att principen om ändamålsbegränsning efterlevs vid behandlingen av personuppgifter.

Uppgiftsminimering

Principen om uppgiftsminimering innebär att fler eller känsligare personuppgifter än vad som behövs för att uppfylla ändamålet inte får behandlas.

Utgångspunkten för KPMG:s efterlevnad avseende uppgiftsminimering är att medarbetarna har kunskap om principen om uppgiftsminimering. Härigenom ges medarbetarna möjlighet att begränsa KPMG:s användning av personuppgifter för att inte avse annat än vad som behövs för att uppfylla ändamålet med behandlingen av personuppgifterna.

Härtill innefattar KPMG:s vägledningar rekommendationer till medarbetarna avseende minimering av personuppgifter, till exempel vid användande av e-post och vid bevarande av uppdragsdokumentation.



Korrekthet

Principen om korrekthet innebär att de personuppgifter som företaget behandlar ska vara korrekta och om nödvändigt uppdaterade.

Utgångspunkten för KPMG:s efterlevnad av principen om korrekthet är att medarbetarna har kunskap om principen om kravet på korrekthet och möjlighet att korrigera eventuella felaktigheter eller verka för att eventuella felaktigheter korrigeras genom företagets rutiner.

Det framgår av KPMG:s vägledningar och rutiner att medarbetare som upptäcker felaktigheter i personuppgifter ska rätta dessa eller verka för att företaget ges möjlighet att rätta felaktigheterna. KPMG har en rutin för medarbetare att anmäla eventuella felaktigheter i de personuppgifter som KPMG behandlar.

Härigenom ges medarbetarna kunskap om att eventuellt felaktiga personuppgifter ska korrigeras och tillgång till en rutin för att verka för KPMG:s korrigerings av eventuellt felaktiga personuppgifter.

Lagringsminimering

Principen om lagringsminimering innebär att personuppgifter inte får sparas i identifierbart skick under en längre tid än vad som är nödvändigt för ändamålet med behandlingen.

KPMG:s efterlevnad av principen om lagringsminimering sker genom fastställande av interna regler för lagring, vilka bland annat innefattar tidsfrister för radering på olika områden.

Integritet och konfidentialitet

Principen om integritet och konfidentialitet innebär att personuppgifterna ska skyddas med lämpliga tekniska och organisatoriska åtgärder så att de inte blir åtkomliga för obehöriga, förstörs eller oavsiktligt raderas.

KPMG:s efterlevnad av principen om integritet och konfidentialitet sker genom fastställande av interna regler för informationssäkerhet och reglering av tystnadsplikt med samtliga anställda och underkonsulter.

Ansvarsskyldighet

Principen om ansvarsskyldighet innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att principerna för personuppgiftsbehandling efterlevs.

KPMG visar att de grundläggande principerna om personuppgiftsbehandling genom att bland annat

- Internt och externt informera om företagets regler och rutiner för hantering av personuppgifter
- Fastställa och uppdatera strategi för dataskydd (riskpolicy)
- Dokumentera rutiner för dataskydd
- Genomföra konsekvensbedömningar vid behov



- Utse dataskyddsbud

Inbyggt dataskydd och dataskydd som standard

Härtill gäller att företagets vägledningar och rutiner baseras på "inbyggt dataskydd" samt "dataskydd som standard".

"Inbyggt dataskydd" innebär att

- Företaget före och vid behandling av personuppgifter vidtar lämpliga åtgärder som främjar uppfyllandet av dataskyddsprinciperna och integrerar nödvändiga säkerhetsåtgärder och
- Företaget vid behandling av personuppgifter använder tekniska och organisatoriska åtgärder med beaktande av den senaste tekniska utvecklingen, kostnader, behandlingens art, omfattning, sammanhang och ändamål samt riskerna med personuppgiftsbehandlingen.

"Dataskydd som standard" innebär att

- Företaget verkar för att medarbetarna ska hantera personuppgifter på ett integritetssäkert sätt och
- Företaget vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa att endast uppgifter som är nödvändiga för ändamålet behandlas med beaktande av mängden uppgifter, behandlingens omfattning, lagringstid och tillgänglighet.