

# GDPR som tjänstepaket

## Innehåll

<b>1</b>	<b>DPO / DSO som tjänst.....</b>	<b>1</b>
<b>2</b>	<b>Combitech GDPR tjänster .....</b>	<b>2</b>
2.1	GDPR tjänst 1: Kartläggning av personuppgiftsbehandlingar .....	2
2.2	GDPR tjänst 2: DPIA, analys av risker och konsekvenser.....	2
2.3	GDPR tjänst: Registerförteckning .....	3
2.4	GDPR tjänst 4: Gap eller mognads analys.....	3
2.5	GDPR tjänst 5: Utvärdering vid företagsförvärv.....	4
<b>3</b>	<b>Fler GDPR tjänster .....</b>	<b>4</b>
3.1	Exempel på andra integritetstjänster som vi erbjuder.....	4

## 1 DPO / DSO som tjänst

Våra erfarna konsulter är redo att kliva in i er organisation och agera som organisationens dataskyddsbud utefter organisationens unika behov. Oavsett om ni har en komplett implementerad efterlevnad av dataskyddsförordningen och behöver stöd av ett dataskyddsbud i frågor, eller om ni behöver stöd i att skapa systematiskt och löpande efterlevnad, så har våra experter erfarenhet att stötta både privata och offentliga organisationer.

Vi hjälper även våra kunder med personuppgiftsincidenthantering, återkommande kontroller, utvärderingar för nya eller ändrade behandlingar av personuppgifter, samt stöd vid exempelvis upprättande och utvärdering av personuppgiftsbiträdesavtal.

Vid uppköp av annat bolag kan olika frågor behöva beaktas, kostnadsdrivande efterlevnadsskillnader, det juridiska ansvaret som övergår dag 1. Det kan vara av betydelse att beaktat dessa frågor före uppköpet så att man slipper oväntade problem och risker.

## 2 Combitech GDPR tjänster

Alla våra tjänster är baserade på dataskyddsförordningens krav på företag och organisationer. Vi har ett metodiskt arbetssätt för värdering av efterlevnad av kraven, och introducerar begreppet "efterlevnadsområden". Vår erfarenhet visar att detta ger er som kund ett effektivt och strukturerat angreppssätt till efterlevnad av GDPR.

På detta sätt har vi även definierat grundläggande områden som bör adresseras först, för att effektivt komma vidare inom övriga efterlevnadsområden. Dessa grundläggande aktiviteter har vi definierat som tjänstepaket 1, 2 och 3

Våra erfarna experter kan ge er det stöd som ni behöver för att möta alla krav för efterlevnad av GDPR. Vi hjälper er att uppnå den nivå för efterlevnad som är lämplig för just er verksamhet, sett utifrån vilka personuppgifter och behandlingar som just ni utför.

Idag efterlever de flesta organisationer dataskyddsförordningen, men många kanske inte fullt ut jobbar med uppföljningsarbetet och förbättringsarbetet som också är GDPR-krav. Här kan mognadsanalys ge en tydlig bild på vilka områden som behöver förbättras och vilka som redan är bra, se tjänst nr 4. Vårt verktyg för mognadsanalys kan ge er grafisk presentation över status vilket förenklar för ledningen att prioritera och planera. Även den detaljerade informationen dokumenteras.

Vi erbjuder anpassad paketering av GDPR tjänster, vilka kan beställas separat eller i kombination.

### 2.1 GDPR tjänst 1: Kartläggning av personuppgiftsbehandlingar

GDPR kravställning av organisationer att kartlägga behandlingarna av personuppgifter är att betrakta som första steget mot att efterleva GDPR. Själva kravet att kartlägga behandlingarna innefattar att behandlingen är förstådd och att potentiella risker och konsekvenser av behandlingen är väldokumenterad, och att riskminimering är implementerad.

Våra konsulter är erfarna i att identifiera och analysera risker och konsekvenser och kan stötta er organisation i att identifiera lämpliga minimeringsåtgärder. På Combitech

Under kartläggningsarbetet utgår vi från en enklare riskvärderingsmodell, och när det verkligen behövs kan en mer djupgående analys göras.

Omfattningen på kartläggningsarbetet står i proportion med antalet behandlingar som görs i organisationen.

### 2.2 GDPR tjänst 2: DPIA, analys av risker och konsekvenser

I arbetet med att efterleva GDPR så är det nödvändigt att identifiera och analysera risker och konsekvenser med behandlingarna. På Combitech har vi mångårig erfarenhet att genomföra risk och konsekvensanalys, och applicerar denna erfarenhet för att optimera resultatet för er organisation.

För effektivt arbete där er kunskap om er egen verksamhet tillvaratas har vi två arbetsmodeller, en där vår expert i samarbete med er områdesexpert genomför analys och bedömning. När behandlingarna är mer komplexa rekommenderar vi att jobba i

workshop-form en halv dag där tre till fem representanter från er organisation med lämplig expertis deltar.

Vi vägleder er organisation för att säkerställa att använd tid och arbetsinsats kommer till nytta och används där det behövs, och undvika kostnadsdrivande och tidskrävande aktiviteter som inte behövs för att driva arbetet framåt.

## 2.3 GDPR tjänst: Registerförteckning

Det är lagkrav på att de behandlingar av personuppgifter som görs i organisationen skall dokumenteras, och även vilken information som skall ingå. Denna dokumentation är också bevis på att kartläggning av behandlingar av personuppgifter har blivit genomförd. Registerförteckningsarbetet kan med fördel genomföras som en direkt fortsättning på kartläggningsarbetet.

Vi använder metoder som formats från vår långa erfarenhet av att hjälpa våra kunder att uppnå och förbättra sin efterlevnad av dataskyddslagen. Våra drivkrafter är att leverera effektiva resultat med mätbar kvalitet.

Vissa kunder vill kombinera den insamlade informationen om behandlingar med annan information för fler användningsområden. Vi kan anpassa våra mallar och metoder för att passa för just era behov.

Det finns olika metoder för att dokumentera behandlingar av personuppgifter, som alla möter de legala kraven. Dock är det så att en del metoder som är enklare att upprätta och innehåller enbart kravställd information kanske inte är helt optimalt för att stötta det långsiktiga arbetet med att upprätthålla efterlevnaden. Medan andra metoder kan å andra sidan stötta det långsiktiga arbetet men kräva betydande arbete för att föra in informationen om behandlingarna.

## 2.4 GDPR tjänst 4: Gap eller mognads analys

GDPR innefattar krav inom flera olika områden. Vår använda arbetsmodell kategoriserar dessa områden, för att ge organisationen en klar och tydlig bild på status på efterlevnaden av GDPR. Samma arbetsmodell ger er förståelse för analysens grunder och adderar värde till organisationen säkerhetsstrategi.

Analysen ger organisationen värdefull förståelse på kartläggningen på behandlingarna av personuppgifter. Resultatet presenteras i översiktliga diagram som visar efterlevnadsnivå som varje efterlevnadsområde har. Det finns även detaljerad status på kravnivå.

Genom att tydliggöra status på detta sätt så ges personuppgiftsansvarig kvalificerad information på organisationens status. Vilket ger värdefullt stöd för prioritering och planering av investeringar och förbättringsarbete av säkerhetsorganisationen.

## 2.5 GDPR tjänst 5: Utvärdering vid företagsförvärv

För företag som växer med hjälp av företagsförvärv är skillnader i IT-miljön och efterlevnadsstatus gällande GDPR av stor betydelse. När förvärvet har genomförts juridisk så blir det övertagande företaget från första stund dag juridisk ansvarig för alla eventuella brister som förvärvet i sin efterlevnad gentemot dataskyddsförordningen. Långt ifrån alla företag har lämpliga utvärderingsmodeller för att kunna värdera förvärvets status med avseende på efterlevnad gentemot GDPR, och därmed kostnadsdrivande skillnader som behöver adresseras. Ofta förvärvas yngre bolag där efterlevnad av dataskyddsförordningen kanske inte har implementerats alls eller fullt ut.

Som regel genomförs omfattande värderingar på förvärvets affärspotential, finansiella risker, skillnader i IT-miljö, där också förändringskostnader efter förvärvet kartläggs. Medan liten eller obefintlig ges åt efterlevnaden av dataskyddsförordningen, och vilka kostnader och risker som kan uppstå inom detta område. Ett annat vanligt misstag är att helt fokusera på kundernas personuppgifter och helt glömma att de anställdas personuppgifter måste kartläggas på samma sätt, och där finns dessutom alltid känsligt data.

Våra experter har erfarenheten att kartlägga skillnader i efterlevnad mellan bolag och tillhandahålla värdeuppskattningar till stöd vid analyserna av förvärvets potential. Denna information bidrar till att ge en mer komplett bild av faktiska förvärvskostnader och faktiska eller potentiella risker.

## 3 Fler GDPR tjänster

Våra tjänster kan anpassas för att passa er organisations behov. Notera att för många av lagkraven är aktiviteter för att nå efterlevnad till stor del beroende av registerförteckningen för effektivt och kvalitativt resultat.

För flera av de tjänster som vi erbjuder är GAP/mognads-analys en viktig utgångspunkt för att rikta insatser dit de bäst behövs och nå kvalitativt resultat på ett effektivt sätt.

### 3.1 Exempel på andra integritetstjänster som vi erbjuder

- Utvärdering av konsekvenserna på personuppgiftsbehandling utifrån Schrems II domslut
- Risk och konsekvensanalys (DPIA) på behandlingar, system eller andra objekt.
- Implementera eller förbättra personuppgifts-incidenthanteringen
- Implementera, utvärdera eller förbättra rättighetsprocesserna exempelvis registerutdrag, rätt att få sina uppgifter raderade eller rättade
- Granska eller ta fram stöddokumentation för dataskyddsarbetet, som riktlinjer och rutiner
- Stötta i att definiera ansvarsfördelning inom organisationen så att effektivt dataskyddsarbete uppnås, genomföra lämplig utbildning för organisationen
- Granska eller producera integritetsmeddelande som riktar sig till de registrerade.

- Öka kunskap och medvetenhet inom dataskyddsarbetet. Vilket kan innefatta allt från "vad betyder kraven i dataskyddsförordningen egentligen?", "vad i dataskyddsförordningen är mest viktigt för vår organisation?", "hur vet vi om vi möter lagkraven?", eller ge generell utbildning i hantering av personuppgiftsincidenthantering, begäran om registerutdrag eller andra rättigheter som registrerade har.
- Stötta i minimering av personuppgiftsbehandling eller att klargöra avsikten med behandling.
- Ta fram riktlinjer som möter kraven på inbyggt dataskydd och dataskydd som standard
- Utvärdering av, eller framtagning av personuppgiftsbiträdesavtal, granskning av biträdets dataskyddsarbete.
- Implementera plan och struktur för långsiktigt upprätthållande av dataskyddet.