TOPCERTIFIER
www.topcertifier.com

SERVICEMETOD GDPR

ALLMÄNT DATASKYDD FÖRORDNING

TOPCERTIFIER
www.topcertifier.com

INTRODUKTION TILL GDPR

GDPR-kraven gäller för varje medlemsstat i Europeiska Unionen, i syfte att skapa fler konsekvent skydd av konsumentdata och personuppgifter i alla EU-länder. Några av nyckeln integritets- och dataskyddskraven i GDPR inkluderar:

- Kräver samtycke från försökspersoner för databehandling
- Anonymisera insamlad data för att skydda integriteten
- Tillhandahålla meddelanden om dataintrång
- Säker hantering av överföring av data över gränserna
- Att kräva att vissa företag utser ett dataskyddsombud för att övervaka efterlevnaden av GDPR

GDPR kräver regulatoriska krav för alla företag som hanterar EU-medborgares data till bättre skydda behandlingen och överföringen av medborgarnas personuppgifter.

AVSPARK

Kickoffmöte är ett viktigt verktyg för att kommunicera och planera för genomförandet av projektet med minimalt hinder och för att slutföra projektet inom planerad tid och kostnad. Agenda för kick off mötet är:

- Projektplansdiskussion: Detta inkluderar diskussion om ansvar och ansvar för intressenter. milstolpar och leveranser i projektet
- Tjänsternas omfattning
- Lagliga och regulatoriska krav

SKAPANING AV KÄRNLAG

- Utnämning av dataskyddsombud (DPO)
- Utnämning av intern GDPR/GRC-kommitté (Governance Risk & Compliance) (*Om så krävs)

GDPR-Medvetenhetsutbildning

GDPR-medvetenhetsutbildning kommer att genomföras för de anställda i din organisation. Utbildningen session är att hjälpa anställda att få kunskap, förstå begreppen GDPR och anpassa sig processer och praxis för att uppnå och etablera, implementera, underhålla och ständigt förbättra en efterlevnadsbaserad systemarbetsmiljö. När staber har varit utbildade kan de tänka & agera och bidra till att nå målen.

TOPCERTIFIER
www.topcertifier.com

GDPR - FASVIS IMPLEMENTERING

FAS I - GAPANALYS

Under denna fas genomför vi en gapanalys för att kontrollera hur stor del av dina nuvarande metoder är i linje med kraven. Din nuvarande praxis verifieras mot nedanstående två referenskriterier,

- GDPR-krav
- Juridiska, regulatoriska och lagstadgade krav

Resultaten av denna analys presenteras i form av en Gap Analysis Report. Denna rapport fungerar som en lista över åtgärder för påminnelse om projektet

FAS II - BEDÖMNING AV INFORMATIONSFLÖDE

I denna fas hjälper vi till med identifiering av informationskällor och bearbetning infrastruktur som involverar personal, teknik och fysisk infrastruktur med avseende på GDPR

FAS III – KONSEKVENSBEDÖMNING FÖR DATASIKRITET (DPIA))

En Data Protection Impact Assessment (DPIA) är en process där potentiella integritetsproblem och risker identifieras och granskas ur alla intressenters perspektiv. Detta tillåter organisation att förutse, ta itu med de sannolika effekterna av nya initiativ genom specifika åtgärder för att minimera/minska riskerna. DPIA är utformade för att minimera risken för skada som kan orsakas av användning / missbruk av personlig information genom att adressera dataskydd & integritetsproblem vid design- och utvecklingsstadiet av ett projekt

Vi hjälper till att utveckla ett DPIA-förfarande och DPIA-register genom att samordna med funktionären huvudet så att det ska gynna organisationen genom att hantera risker, undvika skador på anseende, se till att rättsliga skyldigheter uppfylls och förbättra relationen med intressenter.

FAS IV - SÄKER ANALYS AV PERSONUPPGIFTER

Vi hjälper till att analysera vilka personuppgifter som överförs utanför ditt företag och när vi också hjälper till med att utforma nödvändiga säkerhetsåtgärder för att adekvat skydd personuppgifter och även de personuppgifter som överförs utanför företaget

FAS V – INSTÄLLNING AV PROCESS FÖR DATABROTTSHÄNDER

Vi hjälper till med att sätta upp processer för att identifiera och hantera personuppgiftsintrång. (T.ex. Data rutiner för överträdelsemeddelanden) och även hjälpa till med att utveckla rutiner för incidentrapportering till den berörda tillsynsmyndigheten

FAS VI - DOKUMENTATIONSSTÖD

Vi hjälper till med genomförandet av nödvändiga organisatoriska och tekniska åtgärder för att skyddapersonuppgifter om registrerade och även hjälpa till med att utforma relevant dokumentationmed styrpolicyer och rutiner som säkerställer att GDPR är väl inbäddad i organisationsprocesser

TOPCERTIFIER
www.topcertifier.com

DATASKYDDSMÅL INTERNREVISIONSUTBILDNING

GDPR Internal Auditor (IA) Utbildning kommer att ges till DPO. Denna utbildning kommer att utrusta sådana personal för att analysera behovet av IA, planera och schemalägga IA, förbereda revisionschecklistor och genomföra en IA och att dokumentera och rapportera sina observationer till högsta ledningen

GDPR INTERN REVISION

Våra experter kommer att övervaka genomförandet av internrevision av din DPO. Denna internrevision kommer identifiera fortfarande existerande luckor i systemet och visa beredskapsnivån för att möta efterlevnadsrevision. Denna revision ger organisationen en chans att identifiera och åtgärda alla icke-överensstämmelser innan du går vidare till efterlevnadsrevisionen. Högsta ledningen underrättas om internrevisionsresultat.

GDPR - ROTORSAKSANALYS (RCA) OCH KORRIGERANDE ÅTGÄRDER

Alla avvikelser som identifierats under internrevisionen, klient- eller tredjepartsrevisioner eller från Riskregister, DPIA-register, incidentloggar, databackuploggar, rapporter om dataintrång, Vulnerability Assessment & Penetration Test (VAPT), datalagringsloggar och andra källor måste listas. RCA utförs med tekniker som brainstorming och fiskbensmetoder. De optimala korrigerande och korrigerande åtgärderna genomförs och effektiviteten av sådana åtgärder dokumenteras och granskas via en GDPR Corrective Action Report (CAR)

Våra experter kommer att vara närvarande med ditt team för att guida genom processen.

TOPCERTIFIER
www.topcertifier.com

GRANSKNING AV GDPR-HANTERING MÖTE (MRM)

MRM är en möjlighet för alla intressenter att träffas med schemalagda intervaller för att granska, diskutera och planera åtgärder på agendapunkterna nedan,

- Det rapporterar DPIA
- Avvikelser på efterlevnadsaspekter
- Rapporter om aktiviteter efter leverans
- Handlingsplan för att lösa eventuella öppna objekt
- Möjligheter till förbättringar och förändringar som behövs i systemet

REVISION AV GDPR-ÖVERENSSTÄMMELSE

När beredskapsnivåerna har nått tillräckliga nivåer, processen för efterlevnadcertifieringen börjar. En utsedd revisor från certifieringsorganet (CB) verifierar beredskapenvia en extern revision. Detta innebär att revisorn granskar policyerna, processerna, SOP:s, kritiska operativa register, och IA- och MRM-poster. Eventuella större avvikelser från CB:s förväntningar kommer att meddelas vid denna tidpunkt för att ta med nödvändiga korrigeringar. Detta minskar chanserna för större avvikelser under certifieringsrevisionen. TOPCertifier kommer att ha kontakt med alla intressenter och övervaka ett smidigt genomförande av revisionen.

FORTSÄTTNING AV ÖVERENSSTÄMMELSE

TOPCertifier kommer att vara en del av din organisations efterlevnadsresa och hjälper dig regelbundet intervaller med nödvändiga utbildningar, systemstöd och puppningar, interna och externa revisioner och regelbunden förnyelse av din efterlevnadscertifiering.