TOPCERTIFIER
www.topcertifier.com

SERVICEMETHODOLOGIE GDPR

ALGEMENE GEGEVENSBESCHERMING VERORDENING

TOPCERTIFIER
www.topcertifier.com

INLEIDING TOTGDPR

GDPR eisen zijn van toepassing op elke lidstaat van de Europese Unie, met als doel er meer te creëren consistente bescherming van consumentengegevens en persoonsgegevens in alle EU-landen. Een deel van de sleutel privacy- en gegevensbeschermingsvereisten van de GDPR omvatten:

- Het vereisen van de toestemming van de betrokkenen voor gegevensverwerking
- Anonimiseer verzamelde gegevens om de privacy te beschermen
- Het verstrekken van meldingen over datalekken
- Veilig omgaan met de overdracht van gegevens over de grenzen heen
- Van bepaalde bedrijven eisen dat ze een functionaris voor gegevensbescherming aanstellen om toezicht te houden op de naleving van de GDPR naleving

GDPR stelt wettelijke vereisten vast voor alle bedrijven die gegevens van EU-burgers verwerken de verwerking en het verkeer van de persoonsgegevens van burgers beter te waarborgen.

AFTRAP

De kickoff meeting is een essentieel instrument om te communiceren en plannen te maken voor de uitvoering van het project met minimale belemmering en om het project binnen de geplande tijd en kosten te voltooien. Agenda voor de kick-off bijeenkomst is:

- Bespreking van het projectplan: Dit omvat discussie over aansprakelijkheid en verantwoordelijkheid van belanghebbenden. mijlpalen en resultaten in het project
- Omvang van de diensten
- Wettelijke en regelgevende vereisten

CREATIE VAN EEN KERNTEAM

- Benoeming van een functionaris voor gegevensbescherming (DPO)
- Benoeming van een interne AVG/GRC-commissie (Governance Risk & Compliance) (*indien nodig)

GDPR bewustzijnstraining

GDPR Er worden bewustwordingstrainingen gegeven aan de medewerkers van uw organisatie. De opleiding De sessie is bedoeld om werknemers te helpen kennis op te doen, de concepten van de GDPR, te begrijpen en op één lijn te brengen processen en praktijken met het oog op het bereiken en vaststellen, implementeren, onderhouden en het voortdurend verbeteren van een op compliance gebaseerde systeemwerkomgeving. Wanneer het personeel is geweestopgeleid kunnen zij denken & handelen en bijdragen aan het behalen van de doelstellingen.

TOPCERTIFIER
www.topcertifier.com

GDPR - FASEWIJZE IMPLEMENTATIE

FASE I - GAP-ANALYSE

Tijdens deze fase voeren we een gap-analyse uit om te controleren hoeveel van uw huidige praktijken zijn in lijn met de eisen. Uw huidige praktijken worden geverifieerd aan de hand van de onderstaande twee referentiecriteria,

- GDPR Vereisten
- Wettelijke, regelgevende en wettelijke vereisten

De resultaten van deze analyse worden gepresenteerd in de vorm van een Gap Analysis Report. Dit rapport fungeert als de lijst met actiepunten ter herinnering aan het project

FASE II - BEOORDELING VAN INFORMATIESTROOM

In deze fase helpen we bij het identificeren van informatiebronnen en de verwerking ervan infrastructuur waarbij personeel, technologie en fysieke infrastructuur betrokken zijn GDPR

FASE III - IMPACTBEOORDELING VAN GEGEVENSPRIVACY (DPIA)

Een Data Protection Impact Assessment (DPIA) is een proces waarbij mogelijke privacykwesties en risico's worden geïdentificeerd en onderzocht vanuit het perspectief van alle stakeholders. Hierdoor kan de organisatie om te anticiperen en de waarschijnlijke impact van nieuwe initiatieven aan te pakken door middel van specifieke maatregelen maatregelen om de risico's te minimaliseren/verminderen. DPIA zijn ontworpen om het risico op schade te minimaliseren kan worden veroorzaakt door het gebruik/misbruik van persoonlijke informatie door het aanpakken van gegevensbescherming en privacykwesties in de ontwerp- en ontwikkelingsfase van een project

Wij helpen bij het ontwikkelen van een DPIA-procedure en DPIA-register door afstemming met de functionele zodanig dat de organisatie hiervan profiteert door risico's te beheersen en schade te voorkomen reputatie, zorgt ervoor dat aan wettelijke verplichtingen wordt voldaan en verbetert de relatie met belanghebbenden.

FASE IV - ANALYSE VAN BEVEILIGDE PERSOONLIJKE GEGEVENSOVERDRACHT

Wij helpen bij het analyseren welke persoonlijke gegevens buiten uw bedrijf worden overgedragen terwijl we ook helpen bij het ontwerpen van noodzakelijke beveiligingsmaatregelen om adequaat te beschermen persoonsgegevens en ook de persoonsgegevens die buiten het bedrijf worden overgedragen

FASE V – PROCES OPZETTEN VOOR INCIDENTEN VAN GEGEVENSBREUK

Wij helpen bij het opzetten van de processen om inbreuken op persoonsgegevens te identificeren en af te handelen. (Bijv. gegevens procedures voor melding van inbreuken) en helpen ook bij het ontwikkelen van procedures voor het melden van incidenten mechanisme aan de betrokken toezichthoudende autoriteit

TOPCERTIFIER
www.topcertifier.com

FASE VI - DOCUMENTATIEONDERSTEUNING
Wij helpen bij de implementatie van noodzakelijke organisatorische en technische maatregelen om depersoonsgegevens van betrokkenen en helpen ook bij het ontwerpen van relevante documentatiemet controlebeleid en -procedures die ervoor zorgen dat de GDPR goed is ingebed in de organisatieprocessen

DATABESCHERMINGSOFFICIER INTERNE AUDIT-TRAINING

GDPR Er wordt een opleiding tot Interne Auditor (IA) aangeboden aan de DPO. Deze training zal dergelijke uitrusting uitrusten personeel om de behoefte aan IA te analyseren, IA te plannen en in te plannen, auditchecklists op te stellen en uit te voeren een IA en om hun observaties te documenteren en te rapporteren aan het topmanagement

GDPR INTERNE AUDIT

Onze experts houden toezicht op de uitvoering van de interne audit door uw DPO. Deze interne audit zal dat wel doen nog steeds bestaande hiaten in het systeem te identificeren en de mate van bereidheid aan te tonen om deze aan te pakken nalevingsaudit. Deze audit geeft de organisatie de kans om alle niet-conformiteit alvorens over te gaan tot de nalevingsaudit. Het topmanagement wordt op de hoogte gesteld van de bevindingen van interne audits.

GDPR - OORZAAKANALYSE (RCA) EN CORRIGERENDE ACTIES

Alle non-conformiteiten die zijn vastgesteld tijdens de interne audit, audits van klanten of derden, of van Risicoregister, DPIA-register, Incidentlogboeken, Databack-uplogboeken, Meldingsrapporten Datalekken, Vulnerability Assessment & Penetration Test (VAPT), gegevensretentielogboeken en andere bronnen vermeld moeten worden. RCA wordt uitgevoerd met behulp van technieken als Brainstorming en Fish-Bone-methoden. De optimale correctie en corrigerende acties worden geïmplementeerd en de effectiviteit daarvan acties worden gedocumenteerd en beoordeeld via een GDPR Corrective Action Report (CAR)

Onze experts zijn samen met uw team aanwezig om u door het proces te begeleiden.

TOPCERTIFIER
www.topcertifier.com

GDPR MANAGEMENTREVIEW VERGADERING (MRM)

Het MRM is een gelegenheid voor alle belanghebbenden om met geplande tussenpozen bijeen te komen om de zaken te beoordelen en te bespreken en acties plannen op de onderstaande agendapunten,

- DPIA-rapporten
- Afwijkingen op compliance-aspecten
- Activiteitenrapporten na de levering
- Actieplan om eventuele openstaande posten op te lossen
- Kansen voor verbetering en veranderingen die nodig zijn in het systeem

GDPR NALEVING-AUDIT

Wanneer de niveaus van paraatheid een adequaat niveau hebben bereikt, begint het proces voor compliance certificering begint. Een aangewezen auditor van de Certificatie-Instelling (CI) verifieert de paraatheid via een externe audit. Dit houdt in dat de auditor het beleid, de processen en de SOP's beoordeelt die cruciaal zijn operationele gegevens en IA- en MRM-gegevens. Eventuele grote afwijkingen van de verwachtingen van de CI zal op dit punt worden geïnformeerd over het doorvoeren van de nodige correcties. Hierdoor wordt de kans kleiner grote non-conformiteiten tijdens de certificeringsaudit. TOPCertifier zal met iedereen contact onderhouden belanghebbenden en ziet toe op een vlotte afronding van de audit.

VOORTZETTING VAN NALEVING

TOPCertifier zal deel uitmaken van het compliance-traject van uw organisatie en u regelmatig assisteren intervallen met noodzakelijke trainingen, systeemondersteuning en pupaties, interne en externe audits en regelmatige verlenging van uw Compliance-certificering.