CISO-a-a-S @ 12secure-u

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dat moment zijn sommige organisaties verplicht een functionaris voor de gegevensbescherming (FG) oftewel een Security Officer (CISO) aan te stellen.

De SO/FG/DPO is een onafhankelijk en deskundig persoon binnen de organisatie die toezicht houdt op de toepassing en naleving van de AVG met o.a. als taak informeren en adviseren over de omgang met persoonsgegevens. De functionaris mag een werknemer zijn of een extern ingehuurde kracht.

U en de klanten van uw organisatie beschikken over veel soorten gegevens. Deze gegevens dienen uiterst zorgvuldig te worden behandeld, het betreft veelal vertrouwelijke gegevens. Ongeautoriseerde toegang door derden en het verkeerd omgaan met de gegevens kan leiden tot problemen bij de klanten van uw organisatie en heeft daardoor direct invloed op de continuïteit van uw organisatie.

Redenen voor de klanten van …… om de beveiliging van de gegevens uiterst serieus te nemen. Het is voor de klanten van ……; op zoek naar een organisatie die hen kan ondersteunen met het opstellen van de documenten rondom informatiebeveiliging en het vervullen van de functie Security Officer as a Service as a Service o.a. in het kader van ISO 27001.

De opdracht luidt:

Eén (1) dag (of meer) per maand het vervullen van de functie Security Officer as a Service.

Als eerste zal een plan van aanpak c.q. werkplan worden opgesteld.

Doel van het plan van aanpak is om zowel voor 12secure-u als voor …… duidelijk te kunnen maken welke verwachtingen er zijn ten aanzien van de vervulling van de rol en welke stappen moeten worden gezet om te voldoen aan de AVG al dan niet binnen de ISO 27001.

Op basis van dat plan van aanpak zal voor één (1) dag per maand de functie van Security Officer as a Service as a Service worden vervuld. Gedurende het gehele traject zal maandelijks een schriftelijke terugkoppeling plaatsvinden met de opdrachtgever(s).

Ruwweg zal het plan van aanpak t.a.v. de ISO ingaan op de volgende stappen:

1. Vaststellen van het informatiebeveiligingsbeleid;
2. Inventarisatie van de scope en de processen;
3. Uitvoeren van de risicoanalyse per dienst/systeem;
4. Opstellen ontwerp van het beveiligingssysteem (ISMS);
5. Invoeren van de maatregelen;
6. Inrichten van de beveiligingsorganisatie;
7. Opstellen verklaring van toepasselijkheid;
8. Uitvoeren van audits om de stand van zaken in opzet, bestaan en werking vast te stellen;
9. Laten uitvoeren van de certificering;
10. Inventarisatie van de scope en de processen; Opstellen van procedures en maatregelen (op basis van ITIL);

Als rode draad bij stap 5, 6 en 7 gelden de hoofdnormen van NEN ISO 27002: 1. 2. 3. 4. 5. 6. 7. 8. 9.

1. Beveiligingsbeleid;
2. Organisatie van informatiebeveiliging;
3. Beheer van middelen voor de informatievoorziening;
4. Beveiligingseisen t.a.v. personeel;
5. Fysieke beveiliging en beveiliging van de omgeving;
6. Beheer van communicatie- en bedieningsprocessen;
7. Toegangsbeveiliging;
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen;
9. Beveiligingsincidenten;
10. Continuïteitsbeheer;
11. Naleving wet- en regelgeving.

Door te voldoen aan de ISO27001 voldoet u ook grotendeels aan de AVG v.w.b. beveiliging.

Personele inzet 12secure-u

Op basis van de vraagstelling laten wij de werkzaamheden uitvoeren door een bevoegd medewerker van 12secure-u. Door hun ervaringsgebied kan hij/zij u hierbij optimaal van dienst zijn.

Alle gegevens zullen door 12secure-u en de bij haar werkzame personen met de uiterste zorgvuldigheid en vertrouwelijkheid worden behandeld. De in deze offerte voorgestelde medewerkers zijn gescreend en zullen desgewenst aanvullend een geheimhoudingsverklaring ondertekenen.

Personele inzet overig Indien dit tijdens de uitvoering van de opdracht noodzakelijk blijkt, kunnen wij beschikken over gedetailleerde kennis op vrijwel alle ICT-aspecten. Er wordt alleen gebruik gemaakt van derde partijen na overleg met de opdrachtgever.

Wij schatten in dat het MT van …… ongeveer 1 uur per maand beschikbaar moeten zijn voor afstemming en inrichting. Verder dient u bij aanvang van het project een contactpersoon voor de Security Officer as a Service aan te stellen die beschikbaar zal zijn voor het afstemmen van de werkzaamheden.

Kosten

Voor onze werkzaamheden berekenen wij een honorarium dat is gebaseerd op het ervarings- en deskundigheidsniveau van de betrokken consultants. De initiële inzet is op basis van 8 uur per maand. Deze ondersteuning bieden wij graag aan voor een fixed-price tarief van € 1.200,- per dag exclusief BTW.

Indien tijdens de uitvoering blijkt dat de scope moet worden uitgebreid, kan dit eventueel leiden tot meerwerk. Dit zal altijd eerst met de opdrachtgever worden afgestemd.