Samenwerkingsovereenkomst CISO/DPO

1. CONTEXT

Vanuit de visie dat de regio ZWVL wil samenwerken om de dienstverlening naar de burger te verbeteren zet SHIFT in op het faciliteren van digitale transformatie bij alle betrokken besturen. Dit door in te zetten op verschillende pijlers.
Om naar 'the next level' te kunnen stappen met de organisatie en dus effectief te gaan transformeren moet op alle pijlers tegelijk ingezet worden en liefst op een gelijkwaardige manier.

De omschreven pijlers zijn:
1. De burger en dienstverlening
2. De medewerker en digitale maturiteit van de organisatie
3. De digitale dimensie zijnde IT en software
4. De digitale infrastructuur zijnde data en connectiviteit
5. Strategie

Wat doorheen al deze pijlers loopt en ook meer aandacht vraagt naarmate we op alle pijlers inzetten, is '**veiligheid**'. SHIFT bekijkt de mogelijkheid om profielen te delen die binnen verschillende lokale contexten met de specifieke software aan de slag gaan.

Er is nood aan een regionaal kader over hoe we omgaan met persoonsgegevens en andere data en hoe we dit technisch kunnen vertalen. Welke graad van beveiliging hebben we in onze regio voor ogen? Kunnen we streven naar een consensus? Hoe vertalen we dit 'minimum' in concrete acties?

Het delen van de veiligheidsstrategie kan winsten opleveren op lokaal niveau. Eens die oefening is gebeurd, de visie is uitgedacht, bestaat er een duidelijk kader. Aan de hand van dit kader kan een DPO of andere security medewerker lokale acties opzetten.

2. PARTNERS

Binnen SHIFT wordt gewerkt met een 'coalition of the willing'.

Voor deze samenwerkingsovereenkomst is er een samenwerking tussen:
- Gemeente Deerlijk,
- Stad Harelbeke
- Stad Kortrijk,
- Gemeente Kuurne,
- Gemeente Lendelede,
- Stad Menen,
- SHIFT die de regio ZWVL vertegenwoordigt.

Verder de deelnemende besturen genoemd

3. DIENSTEN

Volgende diensten worden aangeboden via deze overeenkomst:

- de rol van CISO (Chief Information Security Officer of Informatieveiligheidsconsulent)
- de rol van DPO (Data Protection Officer)

Binnen de beschikbare tijd worden deze beide rollen zo optimaal mogelijk opgenomen.

De CISO / DPO coördineert de Informatie Veiligheids Cel (IVC). Binnen de IVC wordt het informatieveiligheidsplan en de daarbij horende acties opgesteld

Zie Bijlage 1 voor een niet bindende en niet limitatieve oplijsting van de taken van de CISO en DPO.

4. RANDVOORWAARDEN

Om de rollen van CISO en DPO volwaardig te kunnen opnemen is het belangrijk dat volgende randvoorwaarden voldaan zijn binnen de deelnemende besturen:

- Er is een aanspreekpunt aangesteld via wie de communicatie verloopt en via wie de evaluatie van de samenwerking verloopt.
- De organisatie engageert zich om informatieveiligheid en GDPR formeel en actief op de agenda te zetten.
- Actieve ondersteuning door hogere management (mandaat).
- Partnership (ondersteunend), draagvlak en ruimte voor interne afstemming zijn aanwezig voor de praktische invulling & lokale vertaling.
- Toegang tot informatie en kennis die noodzakelijk zijn om de rol van CISO en DPO volwaardig te kunnen opnemen, is aanwezig en wordt gegarandeerd: bv. toegang tot info, tot diensten en afdelingen, gegevens en activiteiten.
- Onafhankelijk kunnen werken en adviseren.

Het huidig veiligheidsmaturiteitsniveau binnen de deelnemende besturen zal mee de snelheid bepalen waarmee acties kunnen gerealiseerd worden.

5. DE PRAKTISCHE ORGANISATIE

Binnen Stad Kortrijk zijn 2 CISO/DPO's actief die samen de deelnemende besturen bedienen.

Elk bestuur krijgt een dedicated CISO/DPO toegewezen die het eerste aanspreekpunt is voor het bestuur. De dedicated CISO/DPO is op regelmatige basis aanwezig in de deelnemende besturen. De exacte invulling wordt samen met elk deelnemend bestuur besproken.

De deelnemende besturen hebben opgegeven hoeveel dagdelen ze afnemen binnen deze samenwerkingsovereenkomst. Deze zijn:

- Gemeente Deerlijk 2 halve dagen per week
- Stad Harelbeke 3 halve dagen per week
- Gemeente Kuurne 2 halve dagen per week
- Gemeente Lendelede 1 halve dag per week
- Stad Menen 2 halve dagen per week

Opgeteld komt dit op 1 FTE.

6. AANSTURING

De hiërarchische aansturing verloopt vanuit Stad Kortrijk.

De inhoudelijke sturing wordt opgenomen binnen de verschillende besturen. De besturen bepalen mee de prioriteiten van de op te nemen taken binnen hun bestuur. Dit gebeurt binnen de schoot van de Informatie Veiligheids Cel (IVC).

Er wordt gestreefd om binnen de verschillende besturen dezelfde principes en prioriteiten te bepalen, dit met ruimte tot individualisering per bestuur.

7. NAGESTREEFDE RESULTATEN

De CISO / DPO coördineert de InformatieVeiligheidsCel (IVC). Binnen de IVC worden het informatieveiligheidsplan en de daarbij horende acties opgesteld.

Er wordt gewerkt volgens het "CyberFundamentals Framework"[1] (soms ook het CyFun Framework genoemd) dat via het CCB (Centre for Cybersecurity Belgium) ter beschikking gesteld en ondersteund wordt. Via dit framework wordt toegewerkt naar een NIS2 compliant organisatie.

Doelstellingen voor de deelnemende besturen:

- Informatieveiligheidsplan
  - is opgesteld
  - wordt op regelmatige basis geëvalueerd en bijgestuurd waar nodig
- GDPR-maatregelen worden opgenomen in het informatieveiligheidsplan. De acties binnen het plan zijn gedefinieerd (en gedragen binnen de IVC).
- De opvolging/coördinatie van de te ondernemen acties.
- De besturen zijn zoveel mogelijk GDPR-compliant.

Doelstellingen voor de besturen die deelnemen via SHIFT maar niet nominatief opgenomen zijn in de SWO:

- Kennisdeling opgedane kennis via kennisdelingsmomenten doorheen het jaar
- Opmaak van een principieel kader over de graad van beveiliging die we nastreven in de regio Zuid-West-Vlaanderen. Er wordt bewaakt dat dit kader praktisch genoeg is opgesteld zonder technologische keuzes voorop te stellen.

De vertaling van dit principieel kader in concrete mogelijke acties waarmee de interne CISO/DPO aan de slag kan o.a. door het aanreiken van sjablonen en handleidingen[2].
Belangrijk: Sommige te ondernemen acties kunnen budgettaire impact hebben voor de deelnemende besturen (bv. de investering in bijkomende hard- of software om de beveiliging te verhogen). De CISO/DPO geeft hierin advies. De finale beslissing rond de investering blijft bij het deelnemend bestuur.

[1] Zie: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework
[2] Paar mogelijke voorbeelden: back-up policy, DPIA sjabloon, hoe omgaan met USB sticks, …

8. HET KOSTENDELINGSMODEL

De dienstverlening naar de deelnemende besturen wordt opgenomen door 2 CISO / DPO op A-niveau die op de payroll staan van Kortrijk. Voor deze samenwerking werd een bijkomende (regionale) CISO /DPO aangeworven op de payroll van de stad Kortrijk.

Concreet gaat dit over

- Nick Vandommele 2 halve dagen per week
- Merel Steeland 8 halve dagen per week

Alle kosten (exclusief de effectieve aanwervingskost) die hierbij komen kijken, worden doorgerekend naar de deelnemende besturen.

De door te rekenen kosten zijn de volgende

- Bruto loonkost
- Gemaakte onkosten (o.a. verplaatsingkosten, ..)
- Hierbovenop wordt 5% gerekend voor de overhead die het aanwervende bestuur op zich neemt.

De deelnemende besturen kunnen ten allen tijde deze berekening opvragen en inkijken.

In het eerste kalenderjaar van de samenwerking neemt SHIFT 1/5 van de kost op binnen de SHIFT project kosten. Dit om de regionale doelstelling beschreven onder “nagestreefde resultaten ” te realiseren.

De verdeelsleutel bedraagt bijgevolg

	Jaar 1	Jaar 2 en volgende
Gemeente Deerlijk	16 %	20%
Stad Harelbeke	24%	30%
Gemeente Kuurne	16%	20%
Gemeende Lendelede	8%	10%
Stad Menen	16%	20%
SHIFT	20%	

Ter info: De gemiddelde kostprijs (incl 5% overhead, excl onkosten) van een halve dag wordt op 9/7/24 geraamd op 10.800 euro op jaarbasis.

De facturatie gebeurt per kwartaal.

Als er bijkomende besturen willen toetreden tot de samenwerking, wordt de verdeelsleutel herbekeken.

9. DE CLAUSULE INZAKE VERTROUWELIJKHEID EN AANSPRAKELIJKHEID[3]

Alle deelnemende besturen verbinden zich er uitdrukkelijk toe het vertrouwelijk karakter en de veiligheid van de persoonsgegevens die in het kader van de overeenkomst verwerkt worden, te waarborgen. Alle personeelsleden of aangestelden die toegang hebben tot de persoonsgegevens zullen het vertrouwelijk karakter en de veiligheid van deze persoonsgegevens respecteren. Alle deelnemende besturen zullen erop toezien dat personeelsleden of aangestelden enkel toegang verkrijgen tot persoonsgegevens nadat ze behoorlijk gebonden zijn door een wettelijke en contractuele vertrouwelijkheidsverplichting.

De rol van CISO/DPO zoals opgenomen door Stad Kortrijk voor de andere deelnemende besturen is een adviserende en beleidsondersteunende rol. Stad Kortrijk kan niet aansprakelijk gesteld worden voor de rechtstreekse of onrechtstreekse gevolgen van een cyberincident of het niet compliant zijn met de GDPR, tenzij voor bewezen schade die door een toerekenbare fout of nalatigheid van Stad Kortrijk zou zijn veroorzaakt.

10. DE AANVANG, DUUR EN BEËINDIGING VAN DE SAMENWERKING

De samenwerkingsovereenkomst gaat in vanaf 8/7/2024 en loopt tot 30/6/2027.

De samenwerkingsovereenkomst wordt daarna jaarlijks stilzwijgend verlengd.

De overeenkomst kan ontbonden worden waarbij rekening dient gehouden te worden met een realistisch uitdoofscenario van 6 maand.

De overeenkomst wordt jaarlijks geëvalueerd en bijgestuurd waar nodig. In voorkomend geval zal een addendum opgemaakt worden bij deze overeenkomst.

11. PROCES BIJ GESCHILLEN

Bij conflicten proberen de deelnemende besturen onderling te zoeken naar een minnelijke oplossing. Een vordering in rechte is pas mogelijk als er geen minnelijk akkoord kan worden bereikt.

Bij gebrek aan minnelijke regeling tussen de deelnemende besturen, zal elk geschil beslecht worden voor de bevoegde rechtbank van het bevoegde gerechtelijke arrondissement. Deze overeenkomst valt onder de toepassing van de Belgische wetgeving.

Indien een clausule uit deze overeenkomst ongeldig wordt bevonden, tast dit niet de geldigheid van de gehele overeenkomst aan. De deelnemende besturen zullen zich inspannen om een nieuwe, geldige clausule op te stellen die zo dicht mogelijk de ongeldige clausule benadert binnen de strekking van de overeenkomst.

[3] Deze clausules worden verder uitgewerkt in de Verwerkersovereenkomst die afgesloten wordt tussen de deelnemende besturen en de Stad Kortrijk.

Gedaan te Kortrijk op 8/7/2024 in 7 originele exemplaren waarvan elke partij erkent een exemplaar ontvangen te hebben.

Gelezen en goedgekeurd,

Voor Gemeente Deerlijk Jo Tijgat Voorzitter gemeenteraad Karel Bauters Algemeen Directeur	Stad Harelbeke Rita Beyaert Voorzitter gemeenteraad Hans Piepers Algemeen Directeur
Gemeente Kortrijk Helga Kints Voorzitter gemeenteraad Carlo Daelman Algemeen Directeur	Gemeente Kuurne Chris Delneste Voorzitter gemeenteraad Els Persyn Algemeen Directeur
Gemeente Lendelede Bruno Vanoverbeke Voorzitter gemeenteraad Christophe Vandecasteele Algemeen Directeur	Stad Menen Tom Vlaeminck Voorzitter gemeenteraad Eva Vandenheede Algemeen Directeur
SHIFT Sofie Hatse Projectleider	

BIJLAGE 1

Hieronder staat een niet limitatief overzicht van wat de taken van een DPO en CISO inhouden:

Wettelijke taken van de DPO[4]:

- Bestendige focus
    - Verzamelen informatie om verwerkingsactiviteiten te identificeren.
    - Analyseren en controleren van naleving van de verwerkingsactiviteiten.
    - Informatie en advies verstrekken, en aanbevelingen doen.
    - Adviseren over gegevensbeschermingseffectbeoordeling en toezien op uitvoering ervan.
    - Bijhouden register verwerkingsactiviteiten.
- Occasioneel
    - Samenwerken met en optreden als contactpunt voor de toezichthoudende autoriteit.
    - Contactpunt voor personen die hun rechten wensen uit te oefenen bij de verwerkingsverantwoordelijke.

Taken van de CISO[5]:

- Definieert informatiebeveiligingsbeleid en -strategie obv risico gebaseerde benadering, rekening houdend met continu veranderend dreigingsbeeld, trends en organisatiebehoeften.
- Richt informatiebeveiligingsorganisatie in, definieert daarvoor benodigde middelen en wijst ze toe.
- Initieert en coördineert implementatie van informatiebeveiliging voor de hele organisatie, houdt toezicht vanuit een tweedelijnsrol en rapporteert aan het management.
- Zorgt voor geschikt niveau van informatiebeveiliging en -gedrag in organisatie, obv behoeften en risicobereidheid van organisatie.

[4] https://www.gegevensbeschermingsautoriteit.be/professioneel/avg/functionaris-voor-gegevensbescherming/taken
[5] https://assets.vlaanderen.be/image/upload/v1678370531/flyer_-_de_rol_van_de_ciso_mcsufd.pdf