Gemeente Vlaardingen

Informatiebeveiliging en privacy binnen de 3d’s

J. Van der Vlies

Jeroen Van Der Vlies C|CISO CRISC CISA LPT CHFI

CISO at City Council Vlaardingen

Rotterdam Area, Netherlands | Information Technology and Services

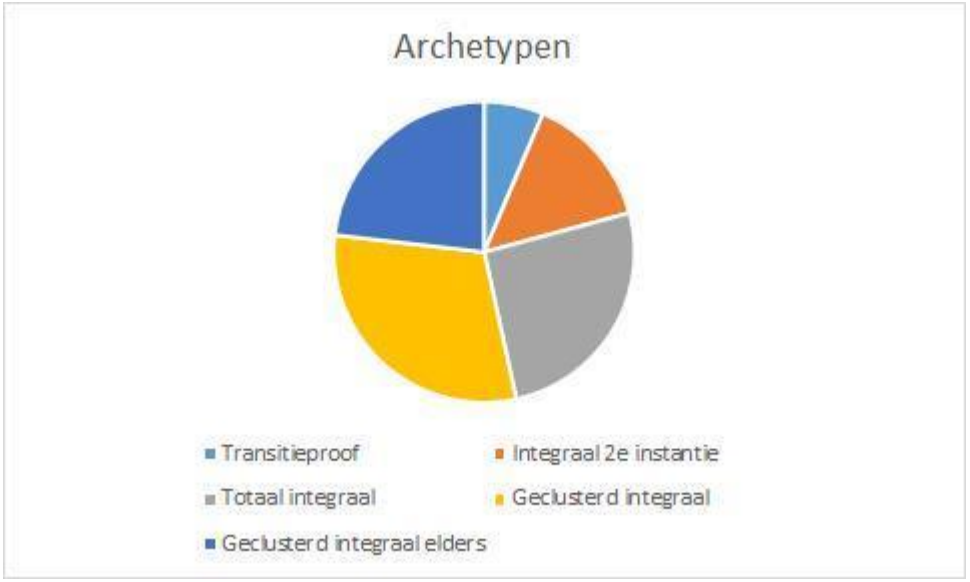
Current City Council Vlaardingen, Government

Gemeente Vlaardingen

About Me

3D's Ken je ze nog!

Gemeente Vlaardingen



- Wat voor soort archetype ben jij businesswise?
  - Zelf doen
  - Gedeeltelijk zelf
  - Regiegemeente

Welke Asset ?

Gemeente Vlaardingen

- Welke relatie is er met de BIG,SUWINET,BRP en natuurlijk de wet bescherming persoonsgegevens vanuit jou Business

Een aanpak

Gemeente Vlaardingen

- Checklist Aanrijking vanuit VNG t.b.v. stelsel
- Hoe en wat en welke rollen en verantwoordelijkheden operationalisatie 3D’s
- Self assessment
- Project Monitoring risico’s informatiebeveiliging en privacy!
- Third party Audit

Gemeente Vlaardingen

Aanrijking VNG VISD programma

- Privacy Scan VISD juni 2014 (als checklist)
- Doelstelling: Voldoet de informatieverwerking aan de wettelijke verplichting van de wet Bescherming Persoonsgegevens en gebruik BRP zoals opgenomen in het Privacy Beleid en Beveiligings beleid zoals contractueel en of beleidsmatig is afgesproken.

Gemeente Vlaardingen

Rollen en verantwoordelijkheden

RegieGemeente

- Zoveel mogelijk uitbesteden
  - Eigendom gegevens?
  - IT Governance:
    - sturing?
    - privacy?
    - security?
    - stabiliteit kosten?
    - beleids- en managementinformatie?
- Gemeente eindverantwoordelijk voor gegevens en informatievoorziening burgers
  - Gemeente als 'data hub'
    - Alle data in eigen databases?
    - Schaal en kosten?
    - Alle nodige competenties in eigen dienst?
    - Datawarehouse met externe koppelingen?

Partij	Taak
	zijnde casus regisseur en verantwoordelijke van het gezinsplan en in te zetten diensten en producten. zijnde uitvoerende voor de ondersteunende processen te weten financiële afhandeling tussen de zorg partijen en juridische toetsing plan/opstellen beschikking. Verzorgt eveneens de betaling met de ingekochte zorgbetaling Informatiebeheerder gebruikte informatiesystemen tav registratie en administratieve verwerking en contract hosting partij.
	Hosting partij van de informatiesystemen die gebruikt worden bij het ROGplus en indirect bij MINTERS.
Gemeente Vlaardingen	Beheerder en verantwoordelijk BRP(Gba) informatie richting ROGplus als zijnde informatiebeheerder en verantwoordelijk voor de verbinding richting Ormer IT en verantwoordelijk voor het sociale zaken systeem GWS4All.

Self Assesment conform VISD CHECKLIST

Gemeente Vlaardingen

- Governance
- 1.1 functionaris benoemd
- 1.2 taken geregeld
- 1.3 Juridisch gecheckt
- 1.4 Raad betrokken

Self Assesment conform VISD CHECKLIST

Gemeente Vlaardingen

- Beleid
- 2.1 Is er privacy beleid
- 2.2 wettelijke kaders
- 2.3 Contracten geregeld?

Self Assesment conform VISD CHECKLIST

Gemeente Vlaardingen

- Werkprocessen en triage
- 3.1 processen beschreven
- 3.2 Rollen en verantwoordelijkheden belegd
- 3.3 Doel en grondslag vastgelegd
- 3.4 bezwaar en beroepprocedure geregeld
- 3.5 Kan de burger zijn informatie raadplegen

Self Assesment conform VISD CHECKLIST

Gemeente Vlaardingen

- Opslag en beheer gegevens
- 4.1 Overzicht systemen
- 4.2 Informatie analyse gedaan
- 4.3 systeeminrichting op orde
- 4.4 bewaartermijnen geregeld

Self Assesment conform VISD CHECKLIST

Gemeente Vlaardingen

- Bewustwording en communicatie
- 5.1 Gedragscode
- 5.2 trainingen beschikbaar
- 5.3 Burger actief informeren

Project Monitoring

Gemeente Vlaardingen

- Uitgangspunt privacy by design en informatiebeveiliging en privacy richtlijnen

Daar de informatie alleen voor statische doeleinden zal worden gebruikt (Regie informatie) zal alle persoonlijke informatie en of informatie wat herleidbaar is tot een persoon worden geanonimiseerd. Na annonimisatie zijn de volgende uitgangspunten van toepassing.

1. Retentie en of archiefwet zijn van toepassing echter de informatie kan en mag als trend informatie worden gebruikt en behouden.
2. De informatie beschikbaar stellen binnen de gemeente voor de (beleids) ambtenaar.
3. Profiling is niet mogelijk zodat men voldoet aan de Wet Bescherming Persoonsgegevens
4. Risico t.a.v. datalekken gemitigeerd omdat persoonlijke informatie niet beschikbaar is
5. Opt in en of Opt out toestemming van de betrokkenen niet strikt noodzakelijk is

Verwerking gegevens

Gemeente Vlaardingen

De volgende uitgangspunten worden gehanteerd en zijn van toepassing.

1. Overdracht van informatie zal middels een beveiligde(geencrypte verbinding) omgeving plaatsvinden. Voorkeur op basis van een zogenaamde API middels Homomorphic encryptie middels autorisatie en voor gedefinieerde informatie. De voorkeur gaat uit dat informatie zoveel mogelijk bij de informatieleverancier als zijnde verwerker wordt geaggregeerd en geanonimiseerd. Audit log van het ophalen van de informatie is beschikbaar en herleidbaar naar functionaris en tijdstip.

2. Verantwoordelijk voor de overdracht betreft een ambtenaar in dienst van de hostende partij als zijnde functioneel verantwoordelijke voor de BI verwerking en omgeving.

3. Overgedragen informatie van de informatieleverancier die niet anoniem betreft zal niet langer dan gedurende 2 uur on geanonimiseerd beschikbaar zijn voor eventuele anonimisatie staging. Alle persoonlijke informatie is na 2 uur van overdracht vernietigd en geregistreerd dat vernietiging heeft plaatsgevonden door de betrokken functionaris. De betrokkene functionaris zal de informatie niet inzien maar alleen verwerken middels een automatisch script waarin vernietiging is geborgd.

4. Ongestructureerde informatie vanuit dossiers mag niet worden opgeslagen binnen de BI omgeving dit mede omdat het risico bestaat dat deze informatie niet kan worden geanonimiseerd en geen doelbinding betreft.

5. Persoonlijke informatie zoals bsn, namen, huis nummer en straat zal niet worden opgeslagen binnen de BI omgeving en of databases. (Deze informatie mag voor de verwerking c.q. aggregatie worden gebruikt echter zal per verwerking worden vernietigd middels een beschreven procedure en mogen alleen door ambtenaren worden verwerkt die functioneel verantwoordelijk zijn voor de BI omgeving. Zie ook 3)

6. Indien bepaalde analyse leidt tot een minimale eenheid en indirect herleidbaar is tot een persoon en of gezin situatie te weten <10 zal k anonymity en of Differential (bewuste ruis) in de presentatie worden toegepast door dit alleen op hoofd niveau te tonen (bijvoorbeeld stad).

7. Alle informatie binnen de BI omgeving zal zijn geanonimiseerd op database c.q. veld niveau. Alle BI data mag zonder toestemming van de afnemer (datacontroller) niet verlaten.

8. De security van de systemen voldoen aan de strategische en tactische beveiligingsplan van de gemeente (BIG)

9. Informatie en of data blijven binnen de EU.

Er zal jaarlijks een Privacy Impact Assessment plaatsvinden op de BI omgeving zodat alle punten blijven gewaarborgd.

Denk aan

- gegevensknooppunt
- Corv
- CISO versus DPO

Kan handig zijn

Third Party Pre-Audit

- Onafhankelijk
- Meer zekerheid
- Verbeteren

Gemeente Vlaardingen

KEEP CALM AND GOOD LUCK