LEGENDA

- **AVG**: Algemene Verordening Gegevensbescherming, wettelijk kader.
- **BIO** : Baseline Informatiebeveiliging Overheid, opvolging BIG, verplicht beveiligingskader voor overheidsorganisaties.
- **BIV**: Beschikbaarheid, Vertrouwelijkheid en Integriteit ; de drie pijlers waarop organisatie, processen, informatiemiddelen en data beschermd dient te worden
- **CERT**: Computer Emergency Response Team, in het geval van de gemeente is dat de **IBD** en/of **NCSC**. Bij (grote) cyberincidenten moet dit gemeld worden en volgt ondersteuning bij onderzoek en oplossing.
- **CIO**: Chief Information Officer, strategisch verantwoordelijke functie voor de informatievoorziening binnen een organisatie.
- **CISO**: Chief Information Security Officer, strategisch/tactische functie binnen het taakveld informatiebeveiliging, verplichte functie vanuit de overheid.
- **Cryptshare**; de huidige oplossing voor veilig mailen, aanvullend op e-mail om van en naar de organisatie op veilige wijze vertrouwelijke informatie, waaronder gevoelige persoonsgegevens, te communiceren.
- **DPIA:** Data Protection Impact Assessment, wettelijke methodiek t.a.v. risicobepaling en beheersing van verwerking van persoonsgegevens en het bepalen van noodzakelijke en wenselijke maatregelen.
- **FG**: Functionaris Gegevensbescherming, wettelijke verplicht toezichthouder op het privacy taakveld binnen de organisatie, strategisch niveau.
- **FTE**: fulltime-equivalent, afkorting om aan te geven hoeveel functie eenheden nodig zijn of beschikbaar zijn. 1 FTE komt overeen met een functie voor 36 uur p.w.
- **IBD:** Informatiebeveiligingsdienst. De IBD ondersteunt gemeenten op het gebied van informatieveiligheid en privacy, dit is een onderdeel vanuit de VNG.
- **IB & P**: Informatiebeveiliging en Privacy.
- **ISMS**: Information Security Management System, als ondersteunende oplossing voor de managementsystematiek, dan wel het geheel van beleid, organisatorische, procesmantige en technische maatregelen om te komen tot continue verbetering en het aantoonbaar “in control” zijn op de informatieveiligheid.
- **ISO**: Information Security Officer, tactisch/operationele functie binnen het taakveld informatiebeveiliging.
- **ITIL**: Information Technology Infrastructure Libracy, de facto de standard in service support en delivery procesvoering van organisaties; referentiekader voor inrichting van beheer- en support processen in de volledige lifecycle van informatiesystemen, ook tussen klant en leverancier.
- **NCSC**: Nationaal Cyber Security Centrum.
- **NPCF** : Norea Privacy Control Framework; toetsingskader voor privacy vanuit Norea, beroepsorganisatie van auditors.
- **PDCA**: plan - do – check – act, beheerste en gecontroleerde cyclus om te komen tot het proces van continue verbetering.
- **PIMS**: Privacy Management System, zie ISMS maar dan op Privacy. De management systematiek als oplossing wordt veelal gedeeld opgezet tussen informatieveiligheid en privacy.
- **SOC/SIEM**: Security Operations Center, de organisatorisch en procesmatige invulling van het onderzoeken, beoordelen, classificeren en opvolgen van beveiligingsmeldingen en incidenten. Het Security Incident en Event Management (SIEM) is de technische oplossing om melden en events centraal te registreren en correleren zodat het SOC hierop kan acteren.
- **TISO**: Technical Information Security Officer - technisch, operationele security functie binnen ICT gericht op informatiebeveiliging.

- **TBV**: Taken, Bevoegdheden en Verantwoordelijkheden, essentieel binnen de governancestructuur om te komen tot beheersing en instandhouding (van informatieveiligheid en privacy).
- **VOG**: Verklaring Omtrent Gedrag, wettelijk beschikbaar middel om op bepaalde functie aspecten betrouwbaarheid/integriteit te toetsen.