**ONS**
**Shared service centrum**
**Afdeling ICT**

Postbus 10007
8000 GA Zwolle

Luttenbergstraat 2

# Strategisch beleid

# Informatieveiligheid & Privacy

Versie: 1.0
12 februari 2018

# 1. Informatieveiligheid is randvoorwaardelijk voor realisatie van ONSe ambities en doelen

ONS geeft middels dit beleid op strategisch niveau een duidelijke richting aan informatieveiligheid en privacy. Dit beleid is kaderstellend en beschrijft ook de wijze waarop de verantwoordelijkheden zijn belegd.

### De informatiesamenleving en ontwikkelingen

We leven in een informatiesamenleving. We zijn en worden in steeds grotere mate afhankelijk van betrouwbare informatiesystemen en data. Die afhankelijkheid wordt veroorzaakt door diverse ontwikkelingen die kansen bieden om de bedrijfsvoering en dienstverlening effectiever en efficiënter in te richten, en te innoveren waardoor voldaan kan worden aan de (veranderende) behoeften en wensen om ONS heen, bij ONSe partners, ONSe klanten en ONS zelf.

De ontwikkelingen en uitdagingen waar ONS voor staat zijn (niet-limitatief):

- 24/7 samenleving waarin steeds digitale dienstverlening plaatsvindt en waarbij Het Nieuwe Werken steeds meer gewoon wordt;
- Er worden hogere eisen aan service gesteld, vergelijkbaar met aanbieders als Coolblue, wat effect heeft op de beschikbaarheid van netwerken en applicaties;
- Technologie, als bijvoorbeeld big-data, maken het mogelijk om op basis van beschikbare gegevens hoogwaardige informatie te genereren door gegevens in samenhang te laten zien. Hiermee kunnen betere voorspellingen worden gedaan en beleidseffecten worden gemeten en fraude worden opgespoord;
- Het flexibel en modulair inrichten van processen en systemen is een randvoorwaarde om ontwikkelingen te kunnen managen die een zware wissel trekken op de organisaties. Denk hierbij aan nieuwe wet- en regelgeving in combinatie met de overdracht van uitvoeringstaken van het Rijk aan gemeenten;
- Toenemende aandacht voor privacy;
- Ervoor zorgen dat informatiebeveiliging aantoonbaar op orde is;
- Binnen de overheid vindt steeds meer (keten)samenwerking en schaalvergroting plaats, waardoor gegevens op grotere schaal worden verwerkt en gedeeld;
- Verhoging van kwaliteit, continuïteit en meer efficiency dienen bereikt te worden.

Naast de beschreven ontwikkelingen, zijn ook andere belangrijke ontwikkelingen te benoemen als robotisering, blockchain, internet-of-things (waarbij alles aan internet wordt gekoppeld) en de Digitale Agenda 2020 (VNG-realisatie). Zonder deze ontwikkelingen uitgebreid toe te lichten, zijn ook dit ontwikkelingen die zich in razendtempo ontwikkelen en die in de nabije toekomst een effect hebben op de bedrijfsvoering en dienstverlening.

Zoals eerder beschreven, bieden al deze ontwikkelingen ONS kansen voor het bereiken van haar doelstellingen op een effectievere en efficiëntere wijze. Deze kansen brengen echter ook risico's met zich mee die gemanaged moeten worden. Het maakt de organisatie, en de producten en diensten die zij levert, namelijk kwetsbaarder.

## Informatieveiligheid[1] als randvoorwaarde voor een professionele organisatie

Het Nationaal Cyber Security Centrum (NCSC) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) constateren dat overheden steeds vaker het doelwit worden (en gaan worden) van cyberaanvallen. Overheden hebben zogenaamde 'kroonjuwelen' (te beschermen belangen) die bewaakt moeten worden. Denk hierbij aan bevolkingsdata, privacygevoelige informatie, (bovenregionale) beleidsstukken, bedrijfseconomische ontwikkelingen, aanbestedingsinformatie, vertrouwelijke bedrijfsgegevens, ICT-beveiliging, medewerkers/kennis en dergelijke.
Digitale spionage, verstoring van de ICT, datalekken en diefstal van informatie nemen toe. Daarom is het belangrijk om informatieveiligheid en privacy te integreren binnen de (bedrijfsvoerings)processen van ONS, zodat ONS en haar partners weerbaar zijn tegen deze dreigingen. Hierdoor worden de belangen adequaat bewaakt van de provincie Overijssel, de gemeenten Zwolle en Kampen en ONS. Informatieveiligheid is daarmee randvoorwaardelijk voor het zijn van een professionele organisatie, en het kunnen leveren van hoogwaardige producten en diensten aan ONSe klanten en partners.

## Doel informatieveiligheid

Met informatieveiligheid wordt gestreefd naar het voorkomen van schade door verstoring, uitval of misbruik van informatiesystemen en, indien er toch schade is ontstaan, het herstellen hiervan.

Informatieveiligheid waarborgt de betrouwbaarheid van de informatie(systemen). Betrouwbaarheid betekent dat informatie beschikbaar en integer (juist, actueel, tijdig) moet zijn, en dat de vertrouwelijkheid van deze informatie moet zijn geregeld waar dat noodzakelijk is. Dit heeft als doel dat de continuïteit van de bedrijfsvoering en dienstverlening wordt gewaarborgd. Hierbij dienen persoonsgegevens zorgvuldig, veilig, proportioneel en vertrouwelijk te worden verzameld, bewaard, beheerd en gebruikt, zodat de persoonlijke levenssfeer van inwoners wordt gerespecteerd. Inwoners moeten daarop kunnen vertrouwen; privacy is immers een grondrecht.

Kortom, informatieveiligheid waarborgt dat ONS haar missie, visie en doelen kan realiseren. In het programma- en jaarplan Informatieveiligheid en Privacy 2018-2020 van ONS is beschreven op welke wijze informatieveiligheid en privacy hierin van toegevoegde waarde zijn.
Om de ONS-doelen te realiseren moeten kansen en ontwikkelingen benut worden, en dienen risico's gemanaged te worden.

## Risicomanagement

100% informatieveiligheid bestaat niet, want dat maakt de organisatie gesloten; het voldoende weerbaar zijn houdt de organisatie open en verbonden met de (veranderenden) behoeften en wensen van klanten en partners. Het maakt de organisatie flexibel. Risico's moeten voldoende beheerst worden, wat betekent dat een risico-gestuurde aanpak essentieel is. Dit proces is beschreven in ons Inofrmation Security Management System (ISMS) dat gebaseerd is op de plan-do-check-act-cyclus. Ondanks dat 100% informatieveiligheid niet bestaat, bestaat 100% inzet wel. Door risico's inzichtelijk te hebben, kunnen afgewogen besluiten worden genomen om uitvoering te geven aan de missie, visie en doelen van ONSe organisatie en die van ONse partners en klanten.

[1] Met informatieveiligheid wordt ook privacy bedoeld in voorliggend document

# 2. Strategisch Beleid Informatieveiligheid & Privacy

Het MT van ONS heeft het ‘Strategisch Beleid Informatieveiligheid & Privacy’ vastgesteld.

### Artikel 1. Definities

1. **Informatieveiligheid**: is gericht op het waarborgen van de betrouwbaarheid van de informatie(voorziening). Dit betekent dat informatie beschikbaar, tijdig, juist en actueel is, en dat informatie niet beschikbaar is voor onbevoegden.
2. **(Informationele) privacy**: gaat om de informatie die geclassificeerd wordt als persoonsgegeven. Privacy is afhankelijk van adequate informatieveiligheid. Om de privacy te waarborgen geldt de verplichting om adequate passende technische en organisatorische maatregelen te treffen. Hier gaat het om de effectiviteit van informatieveiligheid. Is de Informatieveiligheid niet op orde, dan kan de privacy niet gewaarborgd worden.
3. **Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)**: dit is het leidende basisnormenkader voor ONS ten aanzien van informatieveiligheid.
4. **Algemene Verordening Gegevensbescherming (AVG)**: dit is een privacywet die geldt binnen de hele Europese Unie (EU). Hiermee is de bescherming van persoonsgegevens binnen de hele EU op dezelfde manier geregeld. Vanaf 25 mei 2018 verdwijnt de Wet bescherming persoonsgegevens (Wbp) en is de AVG van toepassing.

### Artikel 2. Doel

Het waarborgen van een betrouwbare informatievoorziening en daarmee de kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen (informatieveiligheid). Hierbij wordt zorgvuldig, veilig, proportioneel en vertrouwelijk omgegaan met alle (persoons)gegevens die de persoonlijke levenssfeer raken. Mensen mogen erop vertrouwen dat hun privacy is geborgd en hun persoonlijke levenssfeer wordt gerespecteerd.

### Artikel 3. Beleidsregels

1. Informatieveiligheid en informationele privacy[2] dienen bij te dragen aan het realiseren van de organisatiedoelstellingen, rekeninghoudend met geldende wet- en regelgeving.
2. De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)[3] en de Algemene Verordening Gegevensbescherming (AVG) zijn leidend ten aanzien van respectievelijk informatieveiligheid en privacy.
3. De BIG en de AVG zijn tevens leidend en bepalend voor de leveranciers met wie ONS samenwerkt.
4. Het inrichten van de informatievoorziening volgens dit beleid in opzet, bestaan en werking, geeft afdoende garantie dat informatie betrouwbaar en correct wordt behandeld.
5. Het beveiligingsniveau is in lagen uitbreidbaar.
   Dit betekent dat het basis beveiligingsniveau uitgaat van de BIG en de AVG. Daar waar nodig of vereist kunnen extra maatregelen getroffen worden boven op het basisniveau. Een uitgevoerde baseline informatiebeveiligingstoetst of een privacy impact assessment kunnen hiertoe aanleiding geven.
6. Een baseline informatiebeveiligingstoetst en een privacy impact assessment worden uitgevoerd bij de invoering van nieuwe systemen, projecten of processen.

---

[2] in het vervolg aangehaald als privacy
[3] Vanaf 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO)

7. Voor het verwerken van persoonsgegevens dient altijd een doel en grondslag te zijn, waarbij adequate passende beveiligingsmaatregelen worden getroffen en de beginselen uit de AVG worden gewaarborgd. Bij de implementatie van beveiligingsmaatregelen uit de BIG geldt het pas-toe-of-leg-uit principe, waarbij rekening wordt gehouden met drie afwegingselementen: de stand der techniek, kosten van de tenuitvoerlegging en risico's.
8. Het primaire uitgangspunt is risicomanagement. De klassieke aanpak waarbij inperking van de mogelijkheden de boventoon voert, maakt plaats voor veilig en verantwoord faciliteren.
9. Informatieveiligheid en privacy vereisen een integrale aanpak.
   De principes 'Security and privacy by design and default' staan daarom centraal.
   Dit betekent dat maximale privacy en informatieveiligheid wordt betracht en dat dit tevens wordt meegenomen bij de ontwikkeling en inrichting van informatiesystemen, processen en diensten.
10. Verantwoord en bewust gedrag van medewerkers is essentieel. Structureel en planmatig wordt gewerkt aan het bewustzijn.
11. Het systeem van zelfregulering staat centraal, waarbij jaarlijks opzet, bestaan en werking van de beleidsregels wordt geëvalueerd. Op basis hiervan wordt een verbeterplan opgesteld en wordt via de p&c-cyclus horizontaal verantwoording aflegd door ONS aan haar partners. Er wordt gewerkt conform de plan-do-check-act verbetercyclus.
12. Ten behoeve van implementatie en uitwerking van voorliggend stratetgisch beleid, wordt een doorvertaling gemaakt van dit beleid in een concernarchitectuur voor informatieveiligheid en privacy. Deze wordt waar nodig vertaald in vakspecifieke procedures. Dit geschiedt in ieder geval voor het waarborgen van de kwaliteit en beveiliging van de DigiD-aansluitingen.
13. Vakspecifiek(e) procedures, werkinstructies en dergelijke ten aanzien van informatieveiligheid en privacy worden op het laagst mogelijke niveau vastgesteld door de verantwoordelijke. Indien het alleen betrekking heeft op één team, dan kan de teammanager dit op het laagste niveau vaststellen. Naar mate dit meer team- en/of afdelingsverstijgend is, wordt trapsgewijs opgeschaald naar een hoger gremium. Beleid wordt vastgesteld door het MT van ONS.
14. ONS gaat op een veilige manier om met persoonsgegevens en respecteert de privacy van betrokkenen. ONS houdt zich hierbij aan de volgende beginselen:
    *a)* *Rechtmatigheid, behoorlijkheid, transparantie*
    Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
    *b)* *Grondslag en doelbinding*
    ONS zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt.
    Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.
    *c)* *Dataminimalisatie*
    ONS verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. ONS streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
    *d)* *Bewaartermijn*
    Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

e) *Integriteit en vertrouwelijkheid*
ONS gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Persoonsgegevens worden alleen verwerkt voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt ONS voor passende beveiliging van persoonsgegevens.

f) *Delen met derden*
In het geval van samenwerking met externe partijen (zoals leveranciers), waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt ONS afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. ONS houdt toezicht op naleving van deze afspraken.

g) *Subsidiariteit*
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

h) *Proportionaliteit*
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

i) *Rechten van betrokkenen*
ONS respecteert de rechten van de betrokkene die betrokkene toekomt vanuit de AVG, zoals het recht van: inzage, dataportabiliteit, rectificatie, beperking van de gegevensverwerking, wissing van persoonsgegevens, intrekken van de toestemming en bezwaar.

## Artikel 4. Verantwoordelijkheden

1. De algemeen directeur van ONS is integraal eindverantwoordelijk voor de informatieveiligheid en privacy van ONS; en het lijnmanagement is verantwoordelijk voor risicomanagement, implementatie en naleving van het beleid.
2. De Chief Information Security Officer (CISO) voor informatieveiligheid en de Functionaris Gegevensbescherming (FG) voor privacy ondersteunen vanuit een onafhankelijke positie bij het bewaken en verhogen van het niveau van informatieveiligheid en privacy. Zij adviseren (on)gevraagd, stellen beleid op en coördineren de implementatie, ondersteunen bij het uitvoeren van risicoanalyses, verzorgen integrale statusrapportages, monitoren naleving, doen voorstellen tot implementatie c.q. verbeteringen. Zij zorgen ervoor dat de verantwoordelijken hun verantwoordelijkheid kunnen nemen. Hiervoor hebben zij een rechtstreekse rapportagelijn naar de desbetreffende verantwoordelijken.