centrum informatiebeveiliging en privacybescherming

Testen met persoonsgegevens

5 juni 2020 [Versie 2.0]

Titel	Testen met persoonsgegevens
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Status	Actualisering van gelijknamige CIP-publicatie uit 2013/2014 Versie 2.0 Becommentarieerde praktijk (zie: https://cip-overheid.nl/totstandkoming/)
Auteurs:	Fokke Dijkstra (gemeente Hellendoorn); Eddy van de Werken (Centric); Jan-Pieter Wind (gemeente De Wolden en gemeente Hoogeveen)
Reviewers:	Leden van de CIP-Domeingroep
Bijdrage(n) van	Ruud de Bruijn (CIP), Elleke Oosterwijk (CIP)
Datum	5 juni 2020
Bestandsnaam	Testen met persoonsgegevens 2.0 DEF.docx

Considerans

CIP-producten steunen op kennis van mensen uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op https://www.cip-overheid.nl/contact/

Inhoud

1 Inleiding en leeswijzer

Doel

Het doel van deze notitie is richtlijnen te geven over het gebruik van persoonsgegevens bij het testen van software, binnen of buiten de productieomgeving. De inhoud is in lijn met de AVG, de algemeen gangbare baselines, normenkaders en 'best practices' zoals de ISO-normen, de Code voor Informatiebeveiliging en de BIR-TNK, voor zover van toepassing. De nadruk ligt vooral op het geven van praktische aanwijzingen en opletpunten, die in een betrekkelijk kort bestek een verantwoord overzicht en advies geven over deze problematiek. Gedetailleerde juridische uitwerking c.q. verantwoording laten wij graag aan anderen.

Herkomst en status

Dit stuk is een bewerking/actualisering van een eerdere notitie van het CIP, oorspronkelijk gedateerd 3 juni 2013, en voor het laatst bijgewerkt op 4 april 2014. Bewerking en actualisering zijn noodzakelijk om twee redenen:

- Juridisch: de Wet bescherming persoonsgegevens (Wbp) is vervangen door de AVG;
- Technisch: tal van technische ontwikkelingen rechtvaardigen aanpassing van de richtlijnen.

Verantwoording

In deze notitie worden op inhoud richtlijnen gegeven. Deze richtlijnen zijn op basis van expertise, maar ook door discussie tot stand gekomen[1]. Een essentieel verschil ten opzichte van de eerste notitie betreft de richtlijn dat het testen met 'echte' persoonsgegevens niet is toegestaan, tenzij. De wetgever laat principieel geen ruimte voor het testen van systemen of software waarbij gebruik gemaakt wordt van persoonsgegevens, binnen noch buiten een productieomgeving. -Uit AVG artikel 32 kun je *afleiden* dat er een kleine opening is voor situaties waarin aantoonbaar geen alternatieven beschikbaar zijn om de correcte werking of de inbraakgevoeligheid van een systeem te kunnen testen en het ongetest in gebruik nemen ervan tot risico's zou kunnen leiden voor de bescherming van de privacy. Dit is, in het kort, de juridische context.

Ook de technische omgeving is veranderd. Er zijn mogelijkheden gekomen om te testen met 'vervangende persoonsgegevens'. Speciaal voor het testen zijn sets van persoonsgegevens beschikbaar, die niet zijn gekoppeld aan 'natuurlijk personen'.

Tot slot: vertrouw in de besluitvorming over wel of niet testen met persoonsgegevens nooit uitsluitend op deze notitie. Lees of laat je adviseren over de wettelijke bepalingen. Vooral AVG artikel 6.4 is hierbij belangrijk - maar dit artikel kan alleen ten volle worden begrepen in de context van de gehele wettekst.

[1] Dit is waarschijnlijk de eerste CIP-publicatie op initiatief en met inbreng van leden van de CIP-community die geheel conform de Corona-richtlijnen van het RIVM tot stand is gekomen.

2 Reikwijdte en definities

2.1 Definitie van Testen

Het testen van een (geautomatiseerd) systeem kan worden omschreven als een verzameling van activiteiten die worden uitgevoerd om een af meer kenmerken van een systeem te toetsen volgens een gespecificeerde procedure op werking en kwaliteit, conform de gestelde eisen (ISO/IEC,1991). Kenmerken waarop een systeem kan worden getest zijn: effectiviteit, betrouwbaarheid, gebruikersvriendelijkheid, flexibiliteit, onderhoudbaarheid, beheerbaarheid, beveiliging/privacy en efficiency.

Daarnaast kan er in verschillende (ontwikkel)fases verschillend worden getest. Als voorbeelden: met een regressietest wordt gecontroleerd of niet aangepaste onderdelen van een applicatie nog steeds juist werken, bij een acceptatietest gaat het erom of de uiteindelijke gebruiker, dus degene die verantwoordelijke is voor de werkprocessen, op basis van de werkelijke resultaten het verantwoord acht om het systeem in gebruik te nemen. Bij een loadtest gaat het erom te kijken of het systeem een piekbelasting aankan.

2.2 Juridische aspecten (AVG)

De artikelen in de AVG die betrekking kunnen hebben op dit onderwerp zijn:

Artikel	Omschrijving	Toelichting
4.2	Verwerking persoonsgegevens	Bevat een beschrijving van bewerkingen van persoonsgegevens
6	Rechtmatigheid van de verwerking en verenigbaar belang	Wanneer zou een verwerking 'voor een ander doel' rechtmatig kunnen zijn?
15	Recht op inzage voor de burger	Inzage in de verwerkingsdoeleinden van zijn/haar persoonsgegevens
25.1	Gegevensbescherming als uitganspunt	Het treffen van passende organisatorische en technische maatregelen bij ontwerp en standaardinstellingen
32	Beveiliging	Een verwerking wordt beveiligd door passende technische en organisatorische maatregelen
39	Taken van de FG	Adviseren over en toezicht houden op de verwerking van persoonsgegevens binnen een organisatie

Korte toelichting per artikel

In AVG artikel 4.2 staat een uitgebreide lijst van verwerkingen van persoonsgegevens, al dan niet geautomatiseerd. 'Testen' als verwerking staat daar niet bij. Het woord 'testen' in deze zin komt trouwens precies één keer voor in de Nederlandse versie van de AVG, in art 32.

Artikel 6.1 geeft aan wanneer een verwerking van persoonsgegevens rechtmatig is, zoals onder andere wanneer de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting of voor de vervulling van een taak van algemeen belang. Pas op met de interpretatie van 'algemeen belang': het kan alleen wanneer *een wettelijke grondslag* bestaat voor de uitvoering van de taak in het kader waarvan de gegevens worden verwerkt.

In alle gevallen is een verwerking van persoonsgegevens alleen toegestaan voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. Testen is dat maar zelden.

Artikel 6.4 geeft aan dat een verwerking voor andere dan de oorspronkelijke doelen ook rechtmatig kan zijn wanneer er sprake is van *verenigbaar gebruik*. Gecombineerd met artikel 32 (zie verderop) is dit de enige basis waarmee het testen met persoonsgegevens - onder voorwaarden - gerechtvaardigd zou kunnen zijn. Over toestemming van de betrokkene komen we nog te spreken.

In artikel 15 staat dat de burger recht heeft op inzage in de verwerking van zijn/haar persoons-gegevens. Als de kans bestaat dat met deze gegevens wordt getest, dan is dat een verwerking waarvan de burger op de hoogte moet kunnen zijn. Opname in het verwerkingsregister is geboden en mogelijk is ook een vermelding in de (publieke) privacyverklaring nodig of nuttig. Wanneer de gegevens daadwerkelijk voor testen zijn gebruikt dan moet dat ook worden vermeld bij een inzageverzoek.

Artikel 25.1 gaat over 'privacy by design' en 'privacy by default'. In het ontwerpproces moet (gelet op techniek en kosten) maximaal worden ingezet op realisatie van de uitgangspunten die gelden voor privacy en moeten alle standaardinstellingen eveneens maximale privacy bewerkstelligen.

Dat de verwerking van persoonsgegevens beveiligd moet gebeuren, wordt nog eens benadrukt in artikel 32. Als instrumenten worden in lid 1.a. genoemd: pseudonimisering en versleuteling van persoonsgegevens. Maar ook, in lid 1.d, dat de beveiligingsmaatregelen op gezette tijden getest moeten worden op doeltreffendheid.

Tot slot de Functionaris Gegevensbescherming, die als onafhankelijk functionaris een wettelijke basis heeft om toezicht te houden op de juiste verwerking van persoonsgegevens. Zijn taken staan in artikel 39. In dit artikel staat dat hij kan beoordelen of een verwerking in overeenstemming is met de privacywetgeving, gelet op risico, aard, omvang en context van de verwerking. Dit betekent dat, wanneer wordt overwogen om de escape bij art. 6.4. toe te passen, het verstandig is de FG hierbij te betrekken.

2.3 Reguliere en bijzondere persoonsgegevens

Het maakt uit of het testen plaatsvindt met 'gewone' persoonsgegevens, zoals naam adres en woonplaats, of met gevoelige (zoals BSN) of bijzondere persoonsgegevens. Immers, als hoofdlijn geldt dat de beveiligingsmaatregelen toenemen wanneer de gevoeligheid van gegevens toeneemt. Maar dat betekent niet dat je met 'gewone' persoonsgegevens wellicht wel zou kunnen testen als

dat goed beveiligd gebeurt. Het mag niet, en de reden daarvoor is eenvoudig: de persoonsgegevens zijn niet verzameld voor het doel om ermee te testen, hiervoor geldt geen onderscheid tussen reguliere of bijzondere persoonsgegevens. De AP is daar duidelijk over. Doelbinding zoals verwoord in AVG artikel 5 lid 1b is dus leidend.

Ook als betrokkene toestemming geeft moet je oppassen. De grondslag 'toestemming' is juridisch gezien zwak. Toestemming is alleen een geldige grondslag als betrokken ook werkelijk vrij en voldoende geïnformeerd is om 'ja of nee' te zeggen[2]. Toestemming is bovendien praktisch lastig: iedere betrokkene moet vooraf op de hoogte zijn en de toestemming kan te allen tijde weer worden ingetrokken.

2.4 Systemen in productie en testomgeving

In principe is er geen verschil, juridisch gezien, tussen testen van software in een testomgeving of een productieomgeving. De persoonsgegevens zijn niet voor testdoeleinden afgestaan en verwerkt, dus mogen ze hiervoor niet worden gebruikt, in welke omgeving dan ook. Als er toch een uitzondering moet zijn, zoals aangegeven in paragraaf 5, dan moet je er alles aan doen om risico's zo klein mogelijk te houden. Wanneer bijvoorbeeld testen worden uitgevoerd door personen die regulier toch al toegang hebben tot de betreffende gevoelige productiegegevens, dan kun je beargumenteren dat er geen grotere risico's zijn dan gebruikelijk.

2.5 Pseudonimiseren en anonimiseren

Twee manieren om persoonsgegevens versleuteld te bewaren zijn pseudonimiseren en anonimiseren. Beide kunnen veilig zijn, maar er is een wezenlijk verschil tussen de twee.

Bij pseudonimiseren worden persoonsgegevens versleuteld, waardoor niet meer is te zien om welke 'natuurlijke' persoon het gaat. De 'sleutel' die hiervoor wordt gebruikt wordt op een andere plaats bewaard en is alleen toegankelijk voor geautoriseerde personen. Hierdoor ontstaat een extra beveiligingslaag. Met behulp van die sleutel kunnen de gegevens indien nodig weer terug worden gehaald.

Bij geanonimiseerde gegevens zijn de persoonsgegevens eveneens versleuteld, maar kunnen niet meer terug worden gehaald. De sleutel is vernietigd, er bestaat geen 'schaduwbestand' meer. Anonimisering is dus onomkeerbaar en om deze reden vallen geanonimiseerde gegevens niet langer onder de AVG: het zijn geen tot natuurlijke personen herleidbare gegevens meer.

Het is overigens niet altijd absoluut het een of het andere. Er zijn gradaties mogelijk. Een set persoonsgegevens kan, als dat veilig is en een belangrijke praktische reden heeft, deels worden gepseudonimiseerd en deels worden geanonimiseerd.

[2] In een onderzoek van de AP naar het verzamelen van persoonsgegevens door de gemeenten Nijmegen en Zaandam binnen het sociaal domein komt de conclusie naar voren dat 'toestemming' als grondslag vrijwel nooit kan worden gehanteerd, vanwege *de afhankelijkheidsrelatie* tussen betrokkene en de gemeente. Merk op dat dit een situatie is waar veel overheidsorganisaties rekening mee moeten houden.

3 De hoofdregel

De wetgever laat, behoudens na vooraf gegeven toestemming van de betrokkenen, geen ruimte voor het testen van systemen met 'echte' persoonsgegevens[3], waarbij het onderscheid 'binnen of buiten de productieomgeving' er niet toe doet. En er hoeft mogelijk ook niet met 'echte' persoonsgegevens te worden getest, want er zijn alternatieven.

Voor het testen van interne en externe ketens is bij CIP een KetenTestDorp (KTD) ontwikkeld. De KetenTestDorp-data is een set van gefingeerde data[4].

Er bestaan ook sets van persoonsgegevens die niet zijn gekoppeld aan 'natuurlijk personen'. Deze zijn te vinden de proefomgeving BV.BSN van de Rijksdienst voor Identiteitsgegevens[5] en bij het commerciële Testdorp.nl[6].

Er zijn tal van leveranciers die tools leveren om persoonsgegevens van natuurlijk personen eenmalig te pseudonimiseren of te anonimiseren, specifiek om er veilig mee te kunnen testen. Overigens is anonimisering tot op heden niet altijd een oplossing gebleken die betrouwbaar testen mogelijk maakt tegen redelijke inspanning/kosten.

Rechtmatigheid bij verenigbaar gebruik (artikel 6.4) zet de deur voor testen met persoonsgegevens (met een 'laag' privacyrisico) op een kier: wanneer de betrouwbaarheid van een verwerking c.q. de verwerkende systemen op geen andere manier te testen is dan met persoonsgegevens, dan vormt dat mogelijk een risico voor het voldoen aan een wettelijke verplichting of de vervulling van een taak van algemeen belang, en daarmee ook een mogelijk risico voor de betrokkenen. De verwerkingsverantwoordelijke moet dan wel stevig rekening houden met een aantal in het artikel genoemde factoren en omstandigheden en zich daar altijd over kunnen verantwoorden.

Wanneer vorenstaande voorzieningen geen soelaas bieden, bijvoorbeeld bij een acceptatietest binnen een complexe productieomgeving, dan kun je onder strikte voorwaarden en om redenen van kosten of technische (on)mogelijkheden een gemotiveerd beroep doen op artikel 6.4.

In paragraaf 5 gaan we in op de zorgvuldige stappen die dan moeten worden gezet.

[3] Ook wel: "life data" genoemd.
[4] https://cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/ketenproducten/#Testdorp
[5] https://www.rvig.nl/bsn/proefomgeving-bv-bsn
[6] https://www.testdorp.nl/p/index.html ; dit is een commercieel aanbod, niet te verwarren met het vrijelijk te gebruiken KetenTestDorp van het CIP.

4 Hoe te testen

4.1 Testen met specifieke data sets

Het is mogelijk om te testen met een specifieke dataset bestaande uit een aantal fictieve natuurlijke personen met een geaccepteerd BSN, zoals in de eerder genoemde proefomgeving bij de Rijksdienst voor de Identiteitsgegevens. Het KTD van CIP is gevuld met gefingeerde data waarbij iedere organisatie in de ketentest eigen specifieke gegevens kan toevoegen. In de praktijk zal het hierbij gaan om niet te gecompliceerde testen, zoals een regressietest.

4.2 Testen met specifieke tool

Omdat het onder de werking van de AVG verboden is om te testen met persoonsgegevens van natuurlijk personen, zijn softwareleveranciers op zoek gegaan naar tools die testen toch mogelijk maken. Soms worden tools, die wereldwijd beschikbaar zijn, aangepast aan de Europese of Nederlandse situatie (in overeenstemming gebracht met de AVG), soms worden specifieke tools ontwikkeld. De tool wordt dan gebruikt om persoonsgegevens te pseudonimiseren of, wanneer de omstandigheden dat toelaten, te anonimiseren. Hier gaat het dus om een totaalbestand persoonsgegevens dat in de volle omvang wordt versleuteld. Hiermee kan bijvoorbeeld de piekbelasting worden getest.

4.3 Testen in een netwerkomgeving

Moet een systeem worden getest dat zelfstanding draait, zonder koppelingen naar andere systemen of netwerken, dan zal het testen met een specifieke set data of een tool zoals hiervoor beschreven prima mogelijk zijn. Maar is een systeem gekoppeld met allerlei andere systemen, dan is er sprake van een ketentest. Vaak is testen dan een veel complexere opgave, en is het onduidelijk of onzeker of betrouwbaar kan worden getest met een specifieke set of een tool. Dit zijn de situaties die kunnen leiden tot een beroep op de uitzonderingsgronden.

4.4 Software voorbereiden op testen

Bij de selectie van nieuw te gebruiken/aan te schaffen software kan overwogen worden om als criterium toe te voegen: "de werking van de software kan getest worden zonder gebruik te maken van echte persoonsgegevens". Hiermee vraagt de opdrachtgever nadrukkelijk om een 'testmodus by design'.

5 De uitzondering

'Nood breekt wet' is in deze notitie de onderliggende gedachte bij een uitzonderingsituatie (verenigbaar gebruik) waarin er moet worden getest met 'echte' persoonsgegevens. Het is, zoals al gezegd, een afweging van risico's: het risico van ongetest in productie gaan, tegenover het risico op inbreuk op de privacy van betrokkenen met de kans op nadelige gevolgen. Het eerste risico is alleen af te dekken door zonder uitzondering feilloos te programmeren en te installeren. De praktijk wijst uit dat dit niet mogelijk is. Het tweede risico (nadelige gevolgen) is goed te beheersen door het treffen van bijkomende beschermende maatregelen.

5.1 Afweging

De afweging hierbij kan worden gemaakt vanuit twee invalshoeken:

- Technisch: het is onomstotelijk gebleken dat het testen met een set gefingeerde persoonsgegevens of met behulp van een versleutelingstool onvoldoende garandeert dat het systeem of de aanpassing ervan werkt. Dit is bijvoorbeeld denkbaar in een omgeving waarin meerdere gekoppelde systemen betrokken zijn en een van deze systemen geen gefingeerde of versleutelde gegevens accepteert. Vaak zal het hierbij gaan om een (keten)acceptatietest.
- Financieel: de kosten van het testen met behulp van versleutelde of fictieve persoonsgegevens kost zoveel extra, dat het inzetten van deze maatregelen daarom niet verantwoord wordt geacht. Een bedrag of percentage van een bedrag is lastig te geven. Richtlijn zou kunnen zijn dat de testkosten door de inzet van dergelijke technieken twee keer zo hoog worden als het testen met een set 'echte' persoonsgegevens.

5.2 Voorwaarden

Als, gelet op vorenstaande, de conclusie van de zorgvuldige afweging is dat betrouwbaar testen alleen mogelijk is met 'echte' persoonsgegevens, dan gelden ten minste de volgende voorwaarden:

- Een risicoanalyse (wat zijn de risico's van het gebruik van 'echte' persoonsgegevens), zie hierna onder Risicoanalyse;
- Degene die beslissingsbevoegd is in een organisatie maakt een goed onderbouwd, op basis van zwaarwegende belangen opgesteld advies, met bijbehorend voorstel.

In dit concept advies/voorstel staat verder;

- Wanneer wordt getest (tijdstippen en duur);
- Wat wordt getest (op welke onderdelen);
- Waar wordt getest (is de locatie en het evt. transport veilig);
- Met welke persoonsgegevens wordt getest (niet meer dan noodzakelijk);
- Wie test (uiteraard zo beperkt mogelijk);
- Hoe alles wordt gelogd (toezicht en verantwoording);
- Welke (extra) securitymaatregelen zijn genomen om de privacy van betrokkenen te garanderen (anonimiseren/pseudonimiseren);
- Wat er gebeurt na het testen met de resultaten, de persoonsgegevens en het testrapport (verspreiding, opslag, bewaartermijnen, vernietiging).

De Functionaris Gegevensbescherming (zie AVG art. 37, 38, 39) heeft het toezicht hierop en kan er desgewenst over een adviseren. Daarna valt een definitief schriftelijk besluit door de beslissingsbevoegde. Dit besluit en bijbehorende argumentatie, testplan, werkwijze en evaluatie (zijn er dingen fout gegaan?) worden gearchiveerd.

5.3 Risicoanalyse

Als onderdeel in de afweging om te komen tot een testsituatie met 'echte' persoonsgegevens, wordt het maken van een risicoanalyse aangegeven. Die analyse is essentieel omdat de afgelopen jaren in de praktijk is gebleken dat het testen met echte gegevens onvermoede en ernstige gevolgen voor de privacy kan hebben. Dat geldt met name voor applicaties die in netwerken hangen of anderszins verbonden zijn met andere systemen. Zo kregen burgers vanuit een testsituatie opeens brieven met naheffingen of rekeningen toegestuurd omdat de printstraat en postverwerking niet afgekoppeld waren, of werden onbedoeld alarmeringsmailtjes aan medewerkers verzonden. Dat kan een flinke schadepost tot gevolg hebben, zowel financieel als qua imago van de organisatie.

Hoewel een DPIA is bedoeld om periodiek privacygevoelige processen te screenen, of om te toetsen of een nieuwe verwerking van persoonsgegevens op een veilige manier plaatsvindt, kan een DPIA ook als een onderlegger worden gebruikt voor het goed inschatten van de risico's bij testen en het expliciet maken van de gevolgen van deze risico's.

6 Overige aspecten

6.1 Verwerkersovereenkomst

Wanneer sprake is van een externe verwerking van persoonsgegevens, onder verantwoordelijkheid van de organisatie die zorg draagt voor een goede verwerking van de persoonsgegevens, dan is het zaak om verantwoordelijkheden en afspraken betreffende het testen, conform de hoofdlijn geschetst in deze notitie, vast te leggen in de verwerkersovereenkomst (art. 28 lid 3 AVG). Spreek ook helder af hoe na de testperiode met (de vernietiging van) gebruikte persoonsgegevens wordt omgegaan.

6.2 Register van Verwerkingen

In het Register van verwerkingen (art. 30 AVG) staan alle processen in een organisatie waarbij persoonsgegevens worden verwerkt. Indien getest moet worden met 'echte' persoonsgegevens, dan is er sprake van een verwerking die ook moet worden opgenomen in dit Register.

6.3 Rol FG en CISO

De rol van de FG is om toezicht te houden op alle verwerkingen in een organisatie waarbij persoonsgegevens zijn betrokken. De FG werkt daarbij samen met de Autoriteit Persoonsgegevens (AP). Dus houdt de FG ook toezicht op hoe wordt getest met persoonsgegevens. Desgewenst geeft de FG een advies.

De CISO, mocht een organisatie die hebben, adviseert over, houdt toezicht op en rapporteert over informatieveiligheid. Daarbij hanteert hij diverse kwaliteitsnormen, baselines informatieveiligheid (bijvoorbeeld de BIO) en eventuele zelfevaluaties (denk aan ENSIA of CIP-PriSA[7]). Zijn rol kan vooral bij dit onderwerp het technisch adviseren over het testen met persoonsgegevens zijn.

6.4 Rechten van betrokkene

In artikel 15 van de AVG is geregeld dat een betrokkene, dus een klant of burger waarvoor de betreffende organisatie persoonsgegevens verwerkt, bij die organisatie inzage kan vragen in zijn persoonsgegevens. Ook het eventueel testen met gebruik van deze gegevens valt hieronder. Dus is het zaak, zoals al eerder aangegeven, een dergelijke verwerking goed te beargumenteren en goed te documenteren[8].

[7] Zie resp. https://www.ensia.nl/ en https://cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/privacy-bescherming/#self-assessment-tool-privacy-volwassenheid-prisa-.

[8] De AVG stelt specifieke eisen aan begrijpelijkheid en toegankelijkheid van de informatie voor en communicatie met betrokkene; simpelweg een logboek overhandigen (bij wijze van spreken) volstaat dus niet, je moet helder en overtuigend kunnen uitleggen waarom er met zijn gegevens is getest.

Bijlage: Gebruikte afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIR-TNK	Baseline Informatiebeveiliging Rijksdienst; TNK = Tactisch Normenkader
BSN	Burgerservicenummer
CISO	Chief Information Security Officer
DPIA	Data Protection Impact Assessment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris (voor de) Gegevensbescherming
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
KTD	KetenTestDorp
CIP-PriSa	Privacy Selfassessment van CIP