Tactisch Beleid testdata

« DEFINITIEF »

Gemeente Alphen aan den Rijn

Derogee, Maurice & Marloes Versloot

Versiebeheer

Versie 0.91	Initiële document
Versie 1.0	Definitieve versie.

Afkortingen

AVG	Algemene Verordening Gegevensbescherming
CISO	Chief Information Security Officer
IB&P	Informatiebeveiliging & privacy

Definities

Anonimiseren / geanonimiseerde data	Het verwijderen van alle (combinaties van) attributen uit de gegevensset die het mogelijk maken om de gegevens te herleiden tot een individu. Herleidbaarheid moet blijvend onmogelijk gemaakt zijn.
Betrokkene	Degene wiens persoonsgegevens worden verwerkt.
Fictieve data	Geheel van gefabriceerde gegevens die geen oorsprong hebben in productiedata.
Persoonsgegeven(s)	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de Betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
Pseudonimiseren (gepseudonimiseerde data)	Het verwerken van persoonsgegevens op zodanige wijze dat deze niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om eerdergenoemde koppeling te voorkomen.
(Verwerkings)verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen
Verwerking / verwerken van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

Inhoud

1. Introductie

Inleiding

De gemeente Alphen aan den Rijn en Kaag en Braassem hechten waarde aan zorgvuldige omgang met persoonsgegevens. Dat betekent dat persoonsgegevens niet zonder meer verwerkt worden voor testdoeleinden. Wat er wel en niet geoorloofd is onder bepaalde omstandigheden en welke waarborgen er met de keuze voor een bepaald type testdata gepaard dienen te gaan, wordt beschreven in dit beleid.

Dit beleid bestaat uit een beleidsregel c.q. uitgangpunt. Dit uitgangspunt is niet in alle gevallen houdbaar. Daarom wordt voorzien in een drietal uitzonderingen op dit uitgangspunt. Naar mate de testactiviteit meer de eigenschappen krijgt van een verwerking van persoonsgegevens, worden de eisen die aan deze activiteit gesteld worden, geleidelijk strenger. Dit is om voldoende waarborgen ten aanzien van gegevensbescherming te bieden.

Achtergrond

Persoonsgegevens mogen slechts in overeenstemming met de Algemene Verordening Gegevensbescherming (hierna: AVG) worden verwerkt. De AVG stelt onder meer het principe van **doelbinding** centraal: persoonsgegevens mogen in principe alleen worden verwerkt voor het doel waarvoor ze zijn verzameld. Dit doel moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.

Wil men deze persoonsgegevens ook verwerken voor andere doeleinden? Dan is een van de voorwaarden dat het aanvankelijke verzameldoel en het nieuwe verwerkingsdoel **niet onverenigbaar** zijn.

Uitgangspunt ‘Beleid testdata’

Het uitgangspunt van dit beleid is dat er **niet getest wordt met persoonsgegevens**. Dit uitgangspunt is niet in alle gevallen houdbaar. In specifieke gevallen zijn uitzonderingen mogelijk. Bijvoorbeeld wanneer een (welbepaald, uitdrukkelijk omschreven en gerechtvaardigd) verwerkingsdoel, dat verenigbaar is met het verzameldoel, niet bereikt kan worden zónder verdere verwerking van de persoonsgegevens.

De voorwaarden die aan deze uitzonderingen zijn verbonden, worden in dit beleid voorgeschreven. Hierbij is het regel: **hoe groter de relatie van de gebruikte data met de productiedata is, hoe zwaarder de randvoorwaarden zijn** (zie figuur 1). De hoeveelheid tijd die je kwijt bent aan het voldoen aan die voorwaarden, neemt ook exponentieel toe. Het loont dus om zoveel mogelijk met niet-persoonsgegevens te testen.

***Figuur 1**: schematische weergave van de verhouding tussen voorgeschreven voorzorgsmaatregelen en de mate waarin de onderhavige data de eigenschappen van persoonsgegevens hebben.*

Indien een uitzonderingssituatie zich voordoet, dient aan de genoemde voorwaarden te worden voldaan **voordat** de benodigde persoonsgegevens worden verwerkt.

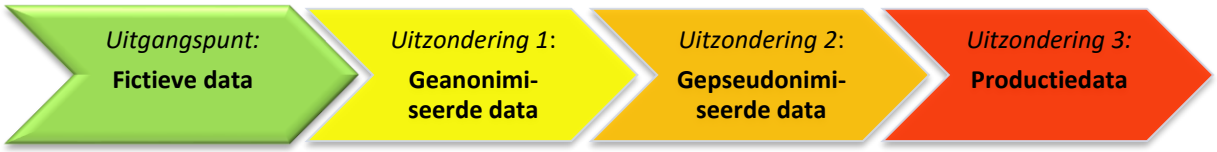
Omdat de gemeente moet kunnen aantonen dat zij in overeenstemming met de AVG handelt, dienen overwegingen, maatregelen, keuzes en toestemmingen te zijn vastgelegd en op ieder moment kunnen worden overlegd.

2. Beleid Testdata

Samenvatting

Het beleid omtrent testdata van de gemeente luidt als volgt: **Er wordt niet getest met persoonsgegevens, slechts met fictieve data**. Op dit uitgangpunt zijn – onder omstandigheden – **uitzonderingen** mogelijk. Of er sprake is van een uitzonderingssituatie en welke deze is, dient systematisch (trapsgewijs) te worden getoetst. Met andere woorden: pas wanneer is vastgesteld dat de test niet met fictieve data kan worden uitgevoerd, kijkt men naar uitzondering 1, is dit eveneens onmogelijk? Dan pas naar uitzondering 2. Wederom onmogelijk? Dan pas naar uitzondering 3.

1. *Uitgangspunt:* Testen gebeurt met fictieve data
2. *Uitzondering 1:* Testen gebeurt met anonieme data
3. *Uitzondering 2:* Testen gebeurt met pseudonieme data
4. *Uitzondering 3:* Testen gebeurt met productiedata



Uitgangspunt

Dat er niet getest wordt met persoonsgegevens, betekent in beginsel dat testen alleen worden uitgevoerd met **fictieve data**[1], tenzij het doel van de test dit onmogelijk maakt.

Uitzondering 1

In die gevallen wordt onderzocht of de test kan worden uitgevoerd met **geanonimiseerde data**[2]. Indien dit mogelijk is, wordt de test in beginsel uitgevoerd met een anonieme dataset die reeds voorhanden is. Is er geen geanonimiseerde dataset beschikbaar waarmee de test kan worden uitgevoerd, dan dient er een geanonimiseerde dataset te worden gegenereerd. Om een geanonimiseerde dataset te genereren, moeten persoonsgegevens worden verwerkt. Aan het genereren van een geanonimiseerde dataset zijn in dit beleid voorgeschreven eisen verbonden.

Uitzondering 2

Indien het testen met geanonimiseerde data niet mogelijk is, wordt onderzocht of er getest kan worden met **gepseudonimiseerde data**[3]. Gepseudonimiseerde persoonsgegevens zijn nog steeds persoonsgegevens. Een test met gepseudonimiseerde persoonsgegevens wordt dus altijd voorafgegaan door een opdracht van de verwerkingsverantwoordelijke. Het genereren van en testen met een gepseudonimiseerde dataset is aan in dit beleid voorgeschreven eisen verbonden.

[1] Ook wel synthetische data genoemd: een dataset die geheel is gefabriceerd en geen relatie heeft met productiedata.
[2] Geanonimiseerde datasets vinden hun oorsprong in productiedata. Alle gegevens die een record herleidbaar maken tot een individu zijn echter gemaskeerd, gehasht, overschreven met fictieve data of verwijderd zodat van herleidbaarheid niet langer sprake is. Dit proces moet onomkeerbaar zijn. Indien anonimiseren juist wordt toegepast, is niet langer sprake van 'persoonsgegevens'.
[3] Pseudonimiseren is het vervangen van direct identificerende persoonsgegevens met een pseudoniem, bijvoorbeeld een versleuteld gegeven op basis van een bepaald algoritme. Het algoritme zorgt steeds voor het berekenen van hetzelfde versleutelde gegeven, waardoor het koppelen van het gegeven uit meerdere bronnen mogelijk is. Een belangrijke factor is dus dat de bewerking omkeerbaar is.

Uitzondering 3

Indien het onmogelijk is om de test uit te voeren met een synthetische, geanonimiseerde of gepseudonimiseerde gegevensset, kan worden onderzocht of de test uitgevoerd kan worden met onbewerkte productiedata. Ook dit scenario wordt altijd voorafgegaan door een opdracht van de verwerkingsverantwoordelijke. Aan het testen met **productiedata** worden door dit beleid de strengste eisen gesteld.

Onmogelijkheid

Met 'onmogelijkheid' wordt in dit beleid bedoeld: **het testdoeleinde kan niet bereikt worden met het desbetreffende type testdata**. De onmogelijkheid om met een bepaald type gegevensset te testen, wordt altijd zorgvuldig onderbouwd.

Procedure

Verwerking van persoonsgegevens

Wanneer getest wordt met een **fictieve** of een **reeds geanonimiseerde gegevensset**, is geen sprake van het verwerken van persoonsgegevens. Dergelijke testen kunnen vrijelijk worden uitgevoerd.

In overige gevallen is **wel sprake** van testen met persoonsgegevens of het voor testdoeleinden verwerken van persoonsgegevens. Het betreft de volgende gevallen:

1. het **genereren** van geanonimiseerde datasets uit productiedata (althans: persoonsgegevens);
2. het **genereren** van gepseudonimiseerde datasets uit productiedata (althans: persoonsgegevens);
3. het **testen** met **gepseudonimiseerde** datasets;
4. het **testen** met **productiedata** (althans: persoonsgegevens).

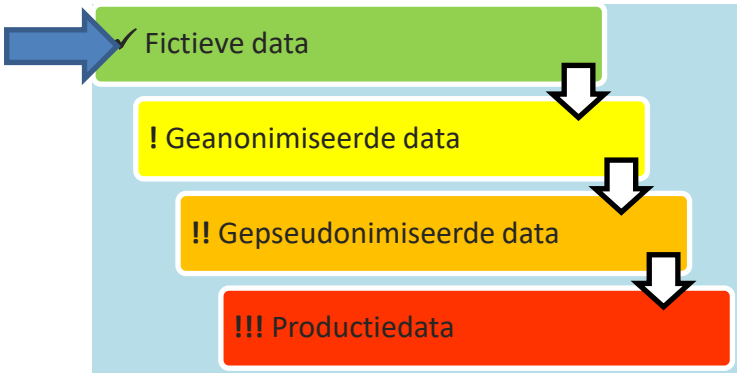
In deze gevallen dient te worden voldaan aan de voorwaarden die in dit beleid gesteld worden aan het gebruik van het gewenste type testdata.

In de gevallen 2, 3 en 4, moeten overwegingen worden gedocumenteerd (in het daartoe bestemde formulier) en ter advisering worden voorgelegd aan de Privacy Officer en CISO. In die gevallen zullen de Privacy Officer en CISO beide vanuit hun eigen discipline een advies geven over de voorgenomen (test)activiteit.

Risicoacceptatie

In principe wordt het advies van de Privacy Officer en CISO opgevolgd. Is degene onder wiens verantwoordelijkheid de testactiviteit wordt uitgevoerd, echter niet bereid het advies op te volgen, dan wordt het risico dat daarmee gelopen wordt volledig in kaart gebracht en expliciet geaccepteerd door degene onder wiens verantwoordelijkheid de testactiviteit wordt uitgevoerd.

Uitgangpunt: Fictieve data



- Testen en analyses worden zoveel mogelijk met **fictieve data** uitgevoerd.

- *Definitie*: ***Fictieve data is gegenereerde data en heeft geen relatie met productiedata. Fictieve data bevat geen persoonsgegevens. Het toegestane gebruik ervan wordt dan ook niet beperkt door de AVG.***

Privacyvoorwaarden

- De fictieve data moet – voor zover dat redelijkerwijs controleerbaar is – **zo min mogelijk relatie** hebben met daadwerkelijke persoonsgegevens.

> *Bijvoorbeeld*:
> postcode *1111 AA* lijkt fictief maar is een bestaande postcode, gebruik van dergelijke gegevens moet – zo veel als redelijkerwijs mogelijk is – voorkomen worden. Toelichting: Een fictief persoon op geldige postcode en huisnummer kan ook weer ongewenste gevolgen hebben voor de werkelijke persoon op dit adres. Redelijkerwijs is de regel.

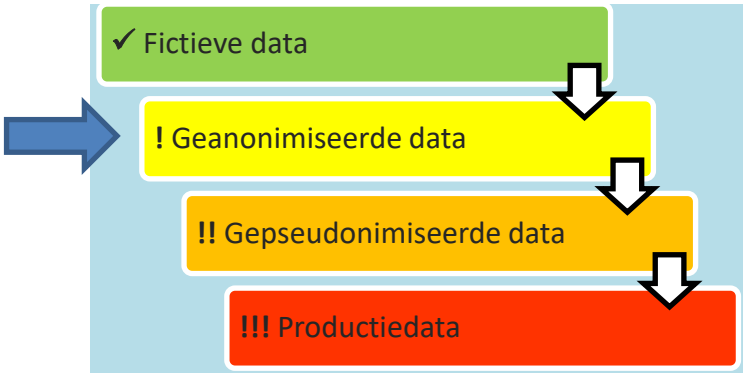
Informatiebeveiligingsvoorwaarden

Ten aanzien van de classificatie van data als basis voor het stellen van eisen aan de beveiliging, gelden de volgende niveaus van vertrouwelijkheid als uitgangspunt.

- **Openbaar (0):**
  Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.
- **Bedrijfsvertrouwelijk (1)**
  Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.
- **Vertrouwelijk (2)**
  Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.
- **Geheim (3)**
  Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen.

De beveiligingseisen voor fictieve data zijn gebaseerd op **niveau 1 Bedrijfsvertrouwelijk**.
De personen belast met de tests hebben toegang door middel van rechtengroepen en gedefinieerde rollen binnen de applicatie zelf. Er zijn maatregelen genomen die **voorkomen** dat de fictieve data – om welke reden dan ook– op een **productieomgeving** geplaatst wordt.

Uitzondering 1: Geanonimiseerde data



- Indien het gebruik van fictieve data **niet mogelijk** is (omdat het doel van de test niet bereikt kan worden met gebruikmaking van fictieve data), wordt de test in beginsel met **geanonimiseerde data** uitgevoerd.

- *Definitie*:
    - ***Anonimiseren** is het bewerken van de gegevensset, op een zodanige wijze dat de records (registraties) in de gegevensset niet langer zijn te herleiden tot een natuurlijke persoon (bijv. door het wissen of overschrijven van de identificerende velden zoals naam, geboortedatum, adres en BSN). **Deze bewerking moet onomkeerbaar zijn.***

    - ***Geanonimiseerde** (of anonieme) **gegevenssets**, zijn gegevenssets die op zodanige wijze zijn bewerkt dat deze niet langer te herleiden zijn tot natuurlijke personen.*

Scenario A: Geschikte anonieme dataset reeds voorhanden

Een op juiste wijze geanonimiseerde dataset bevat geen persoonsgegevens. De gegevensset valt daarmee ook niet meer onder het bereik van de AVG. Een reeds beschikbare anonieme gegevensset mag daarom vrijelijk gebruikt worden voor testdoeleinden. Slechts de voorwaarden gesteld aan het gebruik van fictieve data zijn van toepassing.

Scenario B: Geschikte anonieme dataset niet voorhanden

Wanneer er geen geschikte anonieme dataset voorhanden is – en testen met anonieme data mogelijk is – kan het zijn dat er een dataset geanonimiseerd dient te worden. Hieraan zijn de volgende voorwaarden verbonden:

Privacyvoorwaarden

- Keuze om de activiteit met geanonimiseerde data uit te voeren moet worden **onderbouwd**.
- Het algoritme waarmee geanonimiseerd wordt, zorgt ervoor dat relaties/patronen die in productiedata aanwezig zijn, **onherleidbaar** worden.
    - Bij het op juiste wijze toepassen van anonimiseren, wordt rekening gehouden met:
        - **Singling out**: het o.b.v. gegevens kunnen onderscheiden van een persoon van andere personen.

- **Linkability**: het leggen van relaties tussen records met persoonsgegevens in dezelfde dan wel verschillende databases.
- **Inference**: het deduceren met een grote mate van zekerheid van de waarde van een attribuut op basis van een de waarde van de andere attributen.

- De methode waarop de dataset wordt geanonimiseerd, dient goed **gedocumenteerd** te worden.

Informatiebeveiligingsvoorwaarden

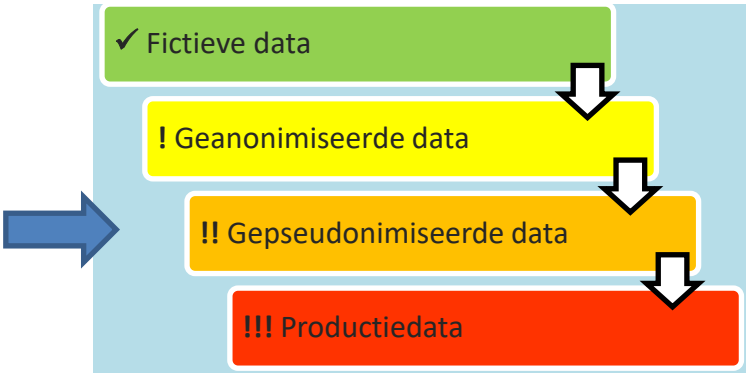
- Anonimiseren vindt plaats ***vanuit* de productieomgeving naar test, of vanuit de testomgeving zelf** (althans, zo dicht mogelijk bij de bron van de productiedata);
- Direct na anonimiseren worden – indien van toepassing – connectie gegevens waarmee toegang tot de productieomgeving alsnog kan worden opgezet aantoonbaar **vernietigd**;
- Anonimiseren vindt plaats met een **erkend veilige** (sterke) sleutel. Periodiek wordt de sterkte van de sleutel geëvalueerd en bijgewerkt op basis van de stand van de techniek. Bij vernietiging moet er een *beginning-to-end-trace* van de sleutel in kaart gebracht worden, en aangetoond worden dat alle mogelijke kopieën vernietigd zijn;
- **Basis beveiligingsvereisten** voor de inrichting niet-productieomgeving zijn van toepassing.

Ten aanzien van de classificatie van data als basis voor het stellen van eisen aan de beveiliging, gelden de volgende niveaus van vertrouwelijkheid als uitgangspunt.

- **Openbaar (0):**
  Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.
- **Bedrijfsvertrouwelijk (1)**
  Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.
- **Vertrouwelijk (2)**
  Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.
- **Geheim (3)**
  Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen.

De beveiligingseisen voor fictieve data zijn gebaseerd op **niveau 1 Bedrijfsvertrouwelijk**. Voorwaarde hierbij is dat de testomgeving pas beschikbaar mag worden gesteld door de functioneel applicatiebeheerder **nadat** de data geanonimiseerd is.

Uitzondering 2: Gepseudonimiseerde data



- Indien het gebruik van **fictieve** en **geanonimiseerde data onmogelijk is**, dan is het onder voorwaarden toegestaan de activiteit uit te voeren met gepseudonimiseerde data.

- *Definitie*: ***Pseudonimiseren is het vervangen van direct identificerende persoonsgegevens met een pseudoniem, bijvoorbeeld een versleuteld gegeven op basis van een bepaald algoritme. Het algoritme zorgt steeds voor het berekenen van hetzelfde versleuteld gegeven, waardoor het koppelen van het gegeven uit meerdere bronnen mogelijk is. Een belangrijke factor is dus dat de bewerking omkeerbaar is.***

Algemene voorwaarden

- Er wordt een **formulier** (zie bijlage 1) ingevuld en ter advisering voorgelegd aan de Privacy Officer en CISO. Hiermee kan (ten minste ten dele) de uitvoering van onderstaande eisen worden aangetoond.
- De test vindt niet plaats zonder **voorafgaand advies** ingewonnen te hebben van een Privacy Officer en CISO.

Privacyvoorwaarden

- Een **bewaartermijn** wordt bepaald voor de gepseudonimiseerde dataset;
- Slechts een **minimaal benodigde hoeveelheid aan data** (hoeveelheid records en benodigde attributen) wordt gepseudonimiseerd en gebruikt;
- **Alleen de benodigde set** aan data wordt uit de productiedata gehaald;
- De methode van pseudonimiseren dient **gedocumenteerd** te zijn;
- Besluiten en (ontwerp)keuzes worden **vastgelegd;**
- Keuze om de activiteit met gepseudonimiseerde data uit te voeren moet worden **onderbouwd**. Deze onderbouwing:
  - maakt duidelijk wat het **doel** van de test is;
  - maakt duidelijk waarom testen met fictieve of anonieme data **onmogelijk** is;
  - wordt **per testtype** (bijv. acceptatie-, performance- etc.) gegeven;
  - maakt duidelijk welke persoonsgegevens noodzakelijk zijn voor de test en waarom dat het geval is.

Informatiebeveiligingsvoorwaarden

- Pseudonimiseren vindt plaats ***in* de productieomgeving** (althans: zo dicht mogelijk bij de bron productiedata);
- Sleutel(s) van het algoritme voor pseudonimiseren zijn **fysiek gescheiden** van de data;
- Sleutel(s) word(en) opgeslagen in een **hoog beveiligde container**:
  - De sleutel wordt opgeslagen op een van encryptie voorziene USB-stick;
  - Deze wordt opgeslagen in een kluis;
  - De sleutel wordt beheerd door de CISO.
- Pseudonimiseren vindt plaats met een **erkend veilige** (sterke) sleutel. Periodiek wordt de sterkte van de sleutel geëvalueerd en bijgewerkt op basis van de stand van de techniek;
- De gepseudonimiseerde dataset mag **beperkt bewaard** worden. Wanneer duidelijk is dat de pseudonimiteit van de dataset niet langer gegarandeerd kan worden (bijvoorbeeld omdat het algoritme gebroken is), moet de dataset worden **vernietigd**;
- Toegang tot, en het gebruik van de sleutels wordt **gelogd**. De logging wordt regelmatig gecontroleerd om ongeautoriseerde toegang vast te stellen;
- De omgeving waarin de activiteit plaatsvindt voldoet aan de **beveiligingseisen** zoals bij de (beoogde) productieomgeving;
- Data in de betreffende testomgeving wordt na uitvoering van de test **geschoond**.

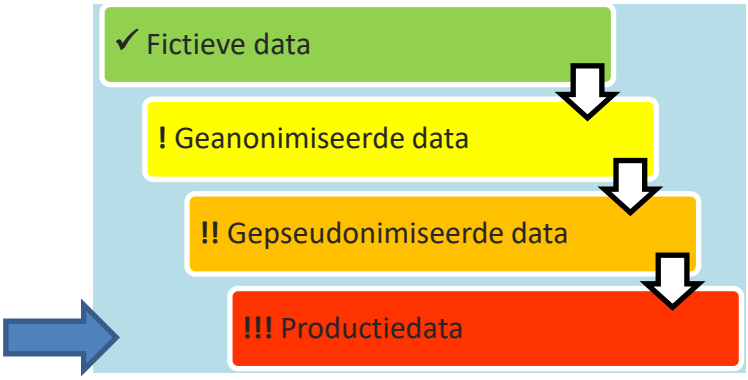
Ten aanzien van de classificatie van data als basis voor het stellen van eisen aan de beveiliging, gelden de volgende niveaus van vertrouwelijkheid als uitgangspunt.

- **Openbaar (0):**
  Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.
- **Bedrijfsvertrouwelijk (1)**
  Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.
- **Vertrouwelijk (2)**
  Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.
- **Geheim (3)**
  Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen.

Gepseudonimiseerde data volgt het classificatie niveau van de productieomgeving. In basis wordt uitgegaan van **niveau 2 Vertrouwelijk.** De functioneel beheerder stelt de testset pas beschikbaar aan de testgroep nadat pseudonimisering gecontroleerd heeft plaatsgevonden. Hierbij geldt het 4-ogen-principe. De applicatiebeheerder laat de gegevens ter bevestiging controleren door een *key user*. Omdat de gegevens door testers zelf niet herleidbaar zijn tot de werkelijke personen, gelden de basis beveiligingseisen voor logische toegang (rechtengroepen; applicatierechten). Sleuteltoegang wordt in bijzondere gevallen verleend na toestemming en onder controle van de CISO. Na gebruik van de sleutel wordt de dataset gecontroleerd volgens het principe van eerste oplevering (alsof het een

geheel nieuwe set betreft). Deze handelingen worden geregistreerd, en kunnen worden gebruikt in audits.

Uitzondering 3: Productiedata



- Indien de activiteit met fictieve, geanonimiseerde of gepseudonimiseerde data niet mogelijk is, kan onder **uitzonderlijke voorwaarden** toestemming worden verleend om de activiteit met productiedata uit te voeren;

Algemene voorwaarden

- Er wordt een **formulier** (zie bijlage 1) ingevuld en ter advisering voorgelegd aan de Privacy Officer en CISO. Hiermee kan (ten minste ten dele) de uitvoering van onderstaande eisen worden aangetoond.
- De test vindt niet plaats zonder **voorafgaand advies** ingewonnen te hebben van een Privacy Officer en CISO.
- De test vindt niet plaats zonder dat de **verantwoordelijke teamleider** het met de test gemoeide risico heeft geaccepteerd.

Privacyvoorwaarden

- Keuze om de testactiviteit met productiedata uit te voeren moet worden **onderbouwd**, deze onderbouwing:
  - maakt duidelijk wat het **doel** van de test is;
  - maakt duidelijk waarom testen met fictieve, anonieme of pseudonieme data **onmogelijk** is;
  - wordt **per testtype** (bijv. acceptatie-, performance- etc.) gegeven;
  - maakt duidelijk welke persoonsgegevens noodzakelijk zijn voor de test en waarom dat het geval is.
- **De minimaal benodigde hoeveelheid** aan data (hoeveelheid records en benodigde attributen) wordt gebruikt bij de activiteit;
- **Alleen de benodigde set** aan data wordt uit de productiedata gehaald;
- Besluiten, (ontwerp)keuzes en relevante procedurele stappen worden **vastgelegd**;

Informatiebeveiligingsvoorwaarden

- De testactiviteit met de productiedata vindt plaats in een omgeving die in een **sandbox** draait;
- De omgeving waarin de activiteit plaatsvindt, voldoet aan de **beveiligingseisen** zoals bij de (beoogde) **productieomgeving**;
- Data in de betreffende niet-productieomgeving wordt direct na uitvoering van de activiteit **geschoond**. Op basis van een *begin-to-end trace* wordt de scope van de opschoning in overleg met de CISO vastgesteld, het aftekenen voor opschoning van de gebruikte omgeving(en) wordt geregistreerd in TopDesk;
- Alle medewerkers die toegang tot de data moeten hebben dienen hiervoor **expliciete toestemming** te hebben van de (proces)**verantwoordelijke teamleider** met betrekking tot het informatiesysteem. Deze geeft akkoord op de lijst met medewerkers die toegang hebben.

Ten aanzien van de classificatie van data als basis voor het stellen van eisen aan de beveiliging, gelden de volgende niveaus van vertrouwelijkheid als uitgangspunt.

- **Openbaar (0):**
  Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.
- **Bedrijfsvertrouwelijk (1)**
  Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.
- **Vertrouwelijk (2)**
  Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.
- **Geheim (3)**
  Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen.

Voor testen op basis van een kopieslag van een (beperkte) set productiegegevens, geldt hetzelfde beveiligingsniveau als bij de productieapplicatie. **Dit niveau kan dus variëren tussen niveau 2 Vertrouwelijk en niveau 3 Geheim.** Toegang tot deze testomgeving volgt eenzelfde autorisatiematrix, waarbij elke handeling binnen de applicatie gelogd dient te worden (audit trail). De data in de databaseomgeving dient indien mogelijk versleuteld te zijn, en mag op geen enkele wijze worden uitgewisseld met derden. Indien een leverancier ten behoeve van het opsporen van fouten in de applicatie een kopie van de testdatabase wenst te ontvangen, dan geldt hier; omgang gelijk aan productie. Versleutelde uitwisseling met een veilig medium; verwerkersovereenkomst; afspraken omtrent de vernietiging van de kopie bij leverancier.

Over het algemeen genomen is er sprake van ketensystemen. De in dit document opgenomen aanwijzingen en voorwaarden gelden niet enkel voor de te testen applicatie, maar ook voor alle aan deze omgeving gekoppelde systemen. Het koppelen van een testomgeving aan een productiesysteem in een keten is uitgesloten.

Indien de bronapplicatie gegevens verwerkt en uitwisselt met ketenpartners (Digikoppeling; e-mailsystemen; zaaksystemen; etc.), dan moet een testketen zijn ingericht zoveel als **redelijkerwijs** mogelijk is. Er moet worden voorkomen dat door middel van tests op productie kopieën kunnen resulteren in acties op de werkelijke persoon.

Indien data uit de testomgeving met productiekopie door welke handeling dan ook in handen komt van een niet tot deze data bevoegde persoon, dan is er sprake van een datalek. In dat geval dient de reguliere datalek-procedure gevolgd te worden.

Formulier | Verwerken van persoonsgegevens voor testdoeleinden v1.0

Kenmerk testaanvraag:			
Naam:		**Telefoon:**	
E-mail:		**Datum:**	

Dit formulier kan elektronisch worden aangeboden via TopDesk.

NB.: Dit formulier wordt eenmaal geregistreerd voor gelijksoortige handelingen binnen hetzelfde systeem. Enkel bij wijzigingen word deze opnieuw ingediend. Een eventueel via partner ontvangen Riskletter kan dit formulier vervangen. De gevraagde kopieslag samen met de Riskletter is dan voldoende.

1. **Omschrijf de beoogde test**

Klik hier als u tekst wilt invoeren.

2. **Noem het beoogde testtype (FAT, SIT, GAT, PAT, KIT etc.[4])**

Klik hier als u tekst wilt invoeren.

3. **Omschrijf het belang en het doel van de beoogde test**

Klik hier als u tekst wilt invoeren.

4. **Selecteer met welke type testdata de test uitgevoerd dient te worden**

- ☐ Fictieve data of een reeds geanonimiseerde dataset (invullen van dit formulier niet vereist)
- ☐ Een geanonimiseerde dataset, die nog gegenereerd moet worden
- ☐ Een gepseudonimiseerde dataset
- ☐ Productiedata

5. **Kan de test worden uitgevoerd met een fictieve dataset?**

- ↘ **Ja:** test moet uitgevoerd worden met fictieve data.
- ↘ **Nee:** voorzie je antwoord van een toelichting. Ga verder met vraag 6.

Klik hier als u tekst wilt invoeren.

6. **Kan de test worden uitgevoerd met een geanonimiseerde dataset?**

Deze vraag hoef je alleen te beantwoorden indien je de vorige vraag (vraag 5) met NEE hebt beantwoord.

- ↘ **Ja:** test moet worden uitgevoerd met geanonimiseerde data. Ga verder met vraag 7.
- ↘ **Nee:** voorzie uw antwoord van een toelichting. Ga verder met vraag 8.

Klik hier als u tekst wilt invoeren.

7. **Kan de test worden uitgevoerd met een reeds beschikbare geanonimiseerde dataset?**

Deze vraag hoeft u alleen te beantwoorden indien je de vorige vraag (vraag 6) met JA hebt beantwoord.

- ↘ **Ja:** test moet uitgevoerd worden met een bestaande geanonimiseerde dataset.
- ↘ **Nee:** geanonimiseerde dataset dient gegenereerd te worden. Ga verder met vraag 10.

Klik hier als u tekst wilt invoeren.

8. **Kan de test worden uitgevoerd met een gepseudonimiseerde dataset?**

Deze vraag hoef je alleen te beantwoorden indien je de vorige vraag (vraag 6) met NEE hebt beantwoord.

[4] Functionele acceptatietest, Systeemintegratietest, Gebruikersacceptatietest, Productie-acceptatietest, Ketenintegratietest etc.)

- ↘ **Ja:** test moet uitgevoerd worden met gepseudonimiseerde data. Ga verder met vraag 10.
- ↘ **Nee:** voorzie uw antwoord van een toelichting. Ga verder met vraag 9.

Klik hier als u tekst wilt invoeren.

9. **Moet de test per se uitgevoerd worden met productiedata?**

Deze vraag hoef je alleen te beantwoorden indien je de vorige vraag (vraag 8) met NEE hebt beantwoord.

- ↘ **Ja:** Voorzie uw antwoord van een toelichting. Ga verder met vraag 10.
- ↘ **Nee:** heroverweeg de benodigde type testdata.

Klik hier als u tekst wilt invoeren.

10. **Noem alle categorieën van persoonsgegevens en het aantal betrokkenen (**personen**) in de gekozen dataset**

Klik hier als u tekst wilt invoeren.

11. **Omschrijf het verzameldoel zo specifiek en expliciet mogelijk**

Klik hier als u tekst wilt invoeren.

12. **Beargumenteer waarom het doel waarvoor de persoonsgegevens zijn verzameld en het testdoel verenigbaar zijn.**

Betrek in je antwoord de volgende onderdelen:

- het **verband** tussen de doeleinden;
- het kader waarin de persoonsgegevens zijn **verzameld** (met name verhouding betrokkene – verwerkingsverantwoordelijke);
- de **aard** van de persoonsgegevens;
- de mogelijke **gevolgen** voor de betrokkene;
- bestaan van passende **waarborgen**.

Klik hier als u tekst wilt invoeren.

13. **Beschrijf hoe aan de toepasselijke privacy- & informatiebeveiligingseisen is voldaan**

Zie hiervoor het beleid 'Testdata'.

Klik hier als u tekst wilt invoeren.

Indien er getest wordt met productiedata dient de verantwoordelijke teamleider akkoord te geven.

Handtekening ter goedkeuring
Verantwoordelijke teamleider

Naam:
Klik hier als u tekst wilt invoeren.