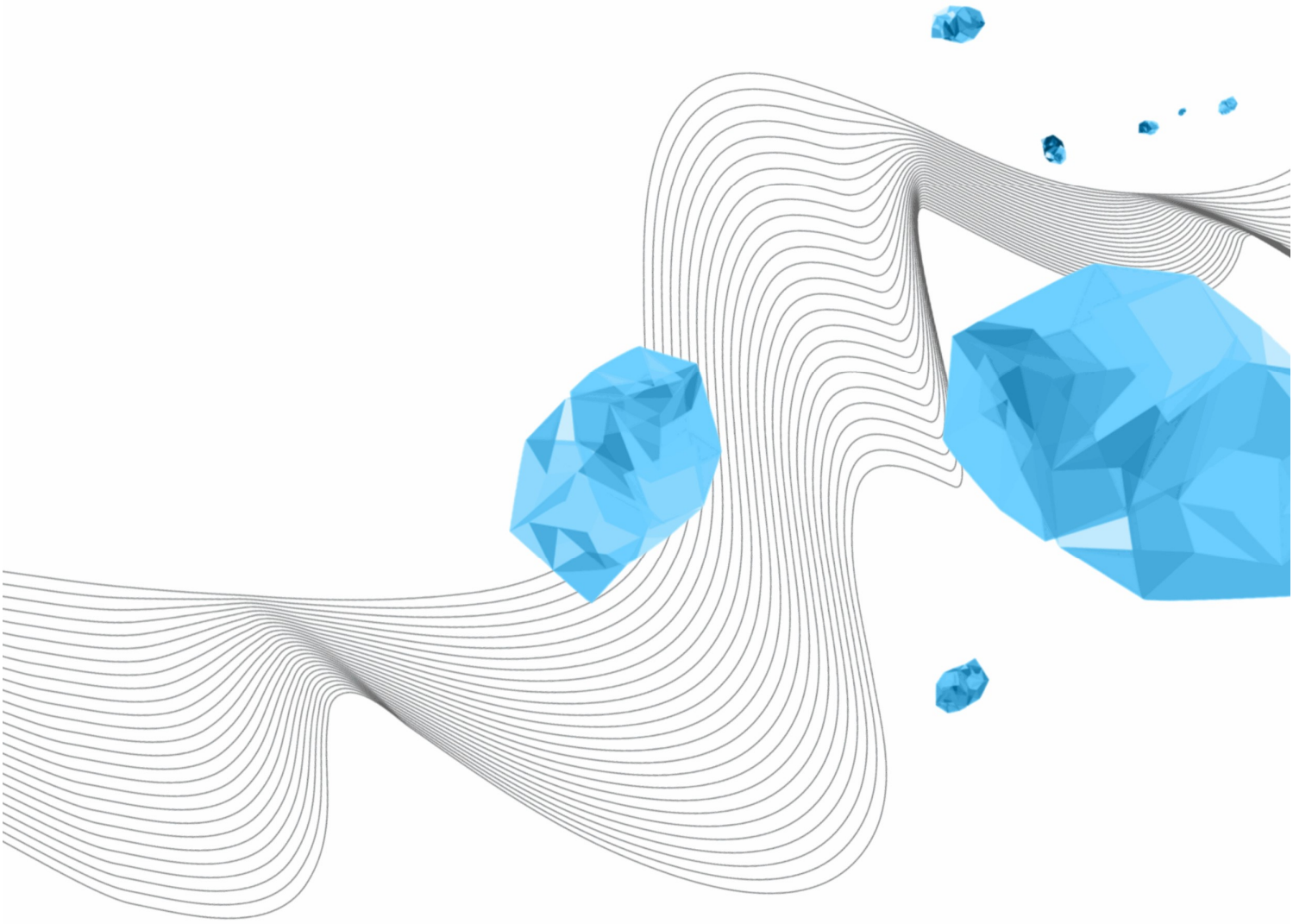
RICHTLIJN: TESTEN MET PERSOONSGEGEVENS ONDER DE AVG

Floris Aanstoot

3.0

19-12-2023



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Richtlijn: testen met persoonsgegevens onder de AVG

VERSIE (STATUS)
3.0

DATUM
19-12-2023

AUTEUR(S)
Floris Aanstoot

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
0.1	10-07-2018	Floris Aanstoot	Initiële versie
0.2	12-07-2018	Floris Aanstoot	Interne review verwerkt. Uitvoering uitgewerkt, voorbeelden persoonsgegevens toegevoegd.
0.3	20-07-2018	Floris Aanstoot, Erik van den Bosch	Reviewcommentaar verwerkt: Marc Berenschot, Rianne te Brake, Joyce Pasman en Erik van den Bosch. Herschreven van advies naar richtlijn.
0.4	12-09-2018	Floris Aanstoot	Richtlijn afgerond
0.5	21-09-2018	Floris Aanstoot, Erik van den Bosch	Reviewcommentaar Erik van den Bosch verwerkt.
0.6	08-10-2018	Floris Aanstoot	Reviewcommentaar en akkoord van de leden van het I-Beraad verwerkt.
1.0	08-11-2018	Floris Aanstoot	Akkoord van de leden van het Centraal Directeuren Overleg (CDO) verwerkt.
1.1	04-02-2020	Meike Davids	Advies van advocaat Mirjam Elferink verwerkt in richtlijn
1.2	17-02-2020	Meike Davids	Reviewcommentaar Henk Swaters verwerkt; procedure toegevoegd
2.1	08-06-2022	Floris Aanstoot, Meike van de Ven	N.a.v. gezamenlijk overleg de richtlijn geüpdatet
2.2	29-08-2023	Floris Aanstoot, Annika van der Putten	Aanpassing hoofdstuk 2 nav arrest okt 2022
3.0	19-12-2023	Annika van der Putten	Reviewcommentaar René van Arnhem verwerkt

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
0.2	12-07-2018	Floris Aanstoot	Erik van den Bosch, Henk Swaters, Joyce Pasman, Arno Holterman, Marc Berenschot, Rianne te Brake en Daisy Oolbekkink
0.3	20-07-2018	Floris Aanstoot, Erik van den Bosch	Erik van den Bosch
0.4	19-09-2018	Floris Aanstoot	Erik van den Bosch
0.5	21-09-2018	Floris Aanstoot, Erik van den Bosch	Jan Evers, Erik van den Bosch, leden van het I-Beraad.

0.6	08-10-2018	Floris Aanstoot	Jan Evers, Erik van den Bosch, leden van het I-Beraad.
1.0	08-11-2018	Floris Aanstoot	Publiek beschikbaar gesteld op de cyber safety website
2.1	10-06-2022	Floris Aanstoot, Meike van de Ven	Bijgewerkt op de cyber safety website
3.0	19-12-2023	Floris Aanstoot, Annika van der Putten	Bijgewerkt op de cyber safety website

INHOUDSOPGAVE

1 INLEIDING

1.1 Aanleiding

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat er sinds die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

De Universiteit Twente (UT) gebruikt persoonsgegevens[1] bij het testen van haar informatiesystemen. De uitleg van de AVG als het gaat over testgegevens is niet eenduidig en aan vele interpretaties onderhevig. Om hierin een lijn te trekken is een analyse uitgevoerd die heeft geleid tot een richtlijn voor de omgang met testgegevens binnen de UT. Dit document beschrijft die richtlijn.

1.2 Scope

Deze richtlijn beperkt zich tot de instellingssystemen van de UT. Deze systemen kennen een hoge mate van integratie, waardoor er ook samenhang bestaat tussen de gegevensverzamelingen van deze systemen. Deze richtlijn is dan ook opgesteld met deze samenhang in het achterhoofd: hoe kunnen we zo goed mogelijk tot een integrale oplossing komen als het gaat om testdata.

Deze richtlijn, of delen daaruit, is waarschijnlijk ook goed toepasbaar voor niet-instellingssystemen, maar deze systemen zijn geen onderdeel geweest van de analyse.

1.3 Doel van het document

Deze richtlijn beschrijft hoe de UT omgaat met persoonsgegevens bij het testen van haar instellingssystemen.

[1] Zie https://www.utwente.nl/nl/cyber-safety/privacy/avg/ voor meer informatie over de AVG en https://www.utwente.nl/nl/cyber-safety/privacy/avg/avg-terminologie/ voor begrippen uit de AVG.

2 UITGANGSPUNTEN TESTEN MET PERSOONSGEGEVENS

Testen met persoonsgegevens wordt aangemerkt als een verwerking van persoonsgegevens. Een verwerking van persoonsgegevens moet aan de vereisten van de AVG voldoen. Zo moet er een gerechtvaardigd doel zijn voor de verwerking en een rechtsgrondslag en dient te worden voldaan aan de beginselen uit de AVG (waaronder verplichting tot dataminimalisatie en het waarborgen van integriteit en vertrouwelijkheid). Ook dient deze verwerking geregistreerd te worden in het Verwerkingsregister.

In de AVG is bovendien vastgelegd dat persoonsgegevens in beginsel niet verder mogen worden verwerkt ("verdere verwerking") op een - met de oorspronkelijk vastgestelde doeleinden waarvoor de persoonsgegevens verkregen zijn - onverenigbare wijze. Bij het testen met persoonsgegevens is dit relevant. De persoonsgegevens zijn immers in eerste instantie voor een bepaald doel verzameld/verwerkt en kunnen met het testen van persoonsgegevens voor een ander doel worden verwerkt. De vraag is of dit doel (het testen van het systeem) onverenigbaar is met het oorspronkelijke doel. Wanneer dit niet het geval is, moet er nog aan de overige voorwaarden uit de AVG worden voldaan, maar is een aparte grondslag niet vereist.

De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.[2] De AP heeft in het verleden aangegeven dat ze het niet aanraden om te testen met persoonsgegevens. Dit omdat testen een complex proces is, waarvoor zorgvuldigheid en meerdere gescheiden omgevingen nodig zijn. Het testen met persoonsgegevens brengt namelijk risico's met zich mee.

Het Europees Hof [3]behandelt verzoeken van nationale rechtbanken om een prejudiciële beslissing, bepaalde nietigverklaringen en beroepszaken. In oktober 2022 hebben zij uitspraak gedaan inzake een zaak die deels betrekking heeft gehad op het testen van persoonsgegevens. [4] In deze uitspraak hebben zij aangegeven dat wanneer het testen verenigbaar is met het doeleinde waarvoor de persoonsgegevens zijn verzameld, dat het testen dan niet in strijd is met de AVG. Het testen met persoonsgegevens is verenigbaar met het doel als bijvoorbeeld het doel van het testen het verbeteren is dan een dienst waar de persoonsgegevens primair ook voor zijn verzameld.

Aangezien met testgegevens soms onzorgvuldiger wordt omgegaan dan met productiegegevens ligt het risico op een datalek op de loer. Daarom zal ook altijd moeten worden afgewogen of er niet een minder zwaar alternatief is om te testen met persoonsgegevens, bijvoorbeeld testen met fictieve gegevens.

In bijlage 2 bij dit document is een stappenplan opgenomen dat dient te worden doorlopen voordat wordt gewerkt in een testomgeving. De verdere onderbouwing van de verschillende stappen volgt in hoofdstuk 4 van deze richtlijn.

[2] Taken en bevoegdheden van de AP | Autoriteit Persoonsgegevens
[3] CURIA - Algemene presentatie - Hof van Justitie van de Europese Unie (europa.eu)
[4] EUR-Lex - 62021CJ0077 - EN - EUR-Lex (europa.eu)

3 DE IDEALE SITUATIE

…. En waarom deze niet volledig haalbaar is op de UT ….

In een ideale situatie zou de UT geen persoonsgegevens gebruiken bij het testen van haar instellingssystemen. Er zijn enkele maatregelen die toegepast kunnen worden om die ideale situatie te bereiken. Deze maatregelen komen erop neer dat er gegevens gebruikt worden die niet te herleiden zijn naar natuurlijke levende personen.

- Testen met geanonimiseerde gegevens
    - Om een testset te creëren wordt een kopie gemaakt van de gegevens uit de productie omgeving. De persoonsgegevens in deze testset worden d.m.v. speciale software geanonimiseerd.
- Testen met fictieve gegevens
    - De volledige testset wordt ontworpen, er wordt geen gebruik gemaakt van een kopie van de gegevens uit de productie omgeving.

De houders van instellingssystemen hebben een impactanalyse uitgevoerd voor beide maatregelen. Uit deze impactanalyse is gebleken dat het niet voor alle instellingsystemen haalbaar is om volledig zonder persoonsgegevens te testen. Redenen hiervoor zijn:

- In enkele instellingssystemen is het technisch niet mogelijk om alle persoonsgegevens te anonimiseren aangezien sommige persoonsgegevens deel uitmaken van de technische sleutel in de database
- Instellingssystemen werken samen in ketens en dit voegt complexiteit toe door het aantal relaties dat tussen gegevens ontstaat. Voor elke te anonimiseren gegevensverzameling moet worden beoordeeld welke gegevens geanonimiseerd moeten worden, omdat vermeden moet worden dat resulterende niet-geanonimiseerde gegevens kunnen worden gecombineerd tot een identificeerbaar persoon (denk bv. aan een geboortedatum en een postcode). Omdat de combinatie van geanonimiseerde gegevens tot een herleidbaar persoon ook kan ontstaan in de keten, is dit een heel complexe actie.
- In instellingssystemen wordt gebruik gemaakt van gestructureerde informatie (bv. tabellen in een database) en ongestructureerde informatie (bv. e-mail, documenten, log files etc.). Artikelen over anonimisering en ook de software voor anonimisering richten zich voornamelijk op gestructureerde informatie. Over het anonimiseren van ongestructureerde informatie zijn weinig artikelen geschreven, ook lijken er geen kant en klare oplossingen op de markt beschikbaar.
- De UT beschikt niet over de benodigde test expertise om een testset met alleen maar fictieve gegevens te creëren.
- De UT heeft niet voldoende kennis van de productiedata om een representatieve testset met fictieve gegevens te creëren.

Bovenstaande punten zorgen ervoor dat niet gegarandeerd kan worden dat in een keten geen persoonsgegevens voorkomen.

4 RICHTLIJN

Uit de AVG volgt onder andere dat er niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk. Dat betekent in de praktijk dat moet worden bekeken hoe het doel op een zo privacy vriendelijk mogelijke manier kan worden bereikt. Wanneer blijkt dat minder inbreuk makende alternatieven niet mogelijk zijn, dient dat te worden uitgelegd. Daarom is het uitgangspunt van deze richtlijn: per instellingssysteem in principe geen, en anders zo weinig mogelijk persoonsgegevens gebruiken bij het testen.

De houder van een instellingssysteem is verantwoordelijk voor het voldoen aan de AVG, dus ook voor het voldoen aan de AVG als het gaat om het testen met persoonsgegevens. Een randvoorwaarde hierbij is dat ketentesten mogelijk moeten blijven. Ketentesten garanderen namelijk de juiste werking van de keten van informatiesystemen die de primaire processen van de UT ondersteunen en die in voorkomende gevallen ook geëist wordt door de accountant; die werking kan niet worden gegarandeerd of aangetoond zonder ketentesten.

Uit intern onderzoek is gebleken dat het niet mogelijk is om een set maatregelen te definiëren die universeel op alle instellingssystemen van de UT toegepast kunnen worden. Daarom bevat deze richtlijn twee sets met maatregelen voor het testen met persoonsgegevens.

- De eerste set bevat maatregelen die voor elk instellingssysteem toegepast moeten worden.
- De tweede set bevat maatregelen die stuk voor stuk voor elk instellingssysteem, in samenwerking met LISA, op impact geanalyseerd moeten worden.

Voor de tweede set maatregelen wordt het principe ‘pas toe of leg uit’ gehanteerd. De houder moet onderzoeken op welke wijze elke maatregel toegepast kan worden. Indien het niet mogelijk is om een maatregel toe te passen moet de houder uitleggen waarom de maatregel niet toegepast kan worden. Als laatste stap moeten de genomen maatregelen door de houder getoetst worden aan de privacy basisprincipes (zoals beschreven in hoofdstuk 4.5).

4.1 Gehanteerde uitgangspunten bij deze richtlijn

- Zelfs door het toepassen van alle voorgestelde maatregelen worden mogelijk persoonsgegevens gebruikt. Door zoveel mogelijk maatregelen toe te passen en vervolgens de genomen maatregelen te toetsen aan de privacy basisprincipes is de UT van mening dat zij zorgvuldig omgaat met de privacy van betrokkenen (er ontstaan geen extra risico's voor de persoonlijke levenssfeer van de betrokkenen).
- De UT ziet een acceptatieomgeving als onderdeel van een productieomgeving. De acceptatieomgeving dient ter verificatie van wijzingen die op de productieomgeving doorgevoerd moeten worden. De UT is daarom van mening dat op een acceptatieomgeving gebruik gemaakt mag worden van persoonsgegevens.
- Het analyseren van productieverstoringen wordt door de UT niet gezien als het testen van een informatiesysteem. Fictieve of geanonimiseerde data kan in veel gevallen niet gebruikt worden voor de analyse van productieverstoringen. Deze richtlijn is daarom niet van toepassing op het analyseren van productieverstoringen.
    a. Als maatregel kan voor het analyseren van productieverstoringen gebruik gemaakt worden van een kopie van de productieomgeving die alleen tijdens de analyse van de productieverstoring beschikbaar gesteld wordt (bv. door gebruik te maken van virtualisatie technieken).
- Het valideren van datasets (bv. aanlevering van een salaris testbestand aan ADP en het controleren van managementrapportages) wordt door de UT niet gezien als het testen van een informatiesysteem. Deze richtlijn is daarom niet van toepassing op het valideren van datasets.
- De UT maakt onderscheid tussen informatiesystemen die in ketens samenwerken en standalone informatiesystemen (bv. het Stage Volg Systeem van Technische Geneeskunde). Voor standalone systemen is het eenvoudiger om geen persoonsgegevens te gebruiken bij het testen. De reden hiervoor is dat er bij bv. het anonimiseren van persoonsgegevens uit de productieomgeving geen rekening gehouden hoeft te worden met afhankelijkheden met andere informatiesystemen.
- De voorgestelde maatregelen hebben tot doel transparant te zijn over de wijze waarop de UT omgaat met persoonsgegevens tijdens testen en om het risico voor de persoonlijke levenssfeer van de betrokkenen te verkleinen (Risico = Kans * Impact).
- Niet voor elk instellingssysteem hoeft een ontwikkel-, test-, acceptatie- en een productieomgeving (OTAP) ingericht te zijn.

4.2 Verplichte maatregelen

De onderstaande maatregelen moeten door de houders van instellingssystemen voor elk instellingssysteem toegepast worden.

A. Voorafgaand aan het uitvoeren van een test moet er een goed doordacht en gedocumenteerd testplan opgesteld worden.
    a. Doel van deze maatregel is het verkleinen van de kans op datalekken door testfouten door vooraf goed over het testen en de testgevallen na te denken.
    b. Bij het ontwerpen van testgevallen moet er reeds nagedacht worden over de risico's die het uitvoeren van een specifiek testgeval met zich meebrengt (privacy by design). Dit kan bijvoorbeeld betekenen dat door een applicatie verzonden e-mails afgevangen worden zodat deze niet naar de eindgebruiker verstuurd worden, of dat bepaalde attributen verwijderd of gewijzigd worden.
    c. Wanneer wordt getest met persoonsgegevens, dienen betrokkenen hiervan voorafgaand aan de test op de hoogte te worden gesteld, bijvoorbeeld door middel van een privacy statement[5]. Ook dient dit te worden opgenomen in het verwerkingsregister. Hiervoor kan contact worden opgenomen met de functionaris gegevensbescherming of met een Privacy Contact persoon van de desbetreffende dienst/faculteit[6].

B. Acceptatieomgevingen worden opgenomen in het verwerkingsregister en betrokkenen worden over de verwerking geïnformeerd in het privacy statement. Hiervoor kan contact worden opgenomen met de functionaris gegevensbescherming.
    a. Doel van deze maatregel is transparantie naar betrokkenen zodat zij op de hoogte zijn van het gebruik van persoonsgegevens in acceptatieomgevingen.
    b. Op de UT privacy website kun je vinden welke informatie dient te worden opgenomen in het privacy statement. Voor het verwerkingsregister kan contact worden opgenomen met de functionaris gegevensbescherming.

[5] Algemene Verordening Gegevensbescherming (AVG) | AVG terminologie | Cyber Safety (utwente.nl)
[6] Contact | Cyber Safety (utwente.nl)

4.3 Maatregelen die zoveel mogelijk toegepast moeten worden

Voor de maatregelen in dit hoofdstuk wordt het principe ‘pas toe of leg uit’ gehanteerd.

C. Geen persoonsgegevens uit productie in ontwikkel- en testomgeving
    a. Doel van deze maatregel is het verkleinen van de kans en impact dat een datalek op één van deze omgevingen optreedt door geen gebruik te maken van persoonsgegevens.
    b. Indien er voor een instellingsysteem een ontwikkel- en/of testomgeving beschikbaar is worden in deze omgevingen geen persoonsgegevens gebruikt. Dit kan bereikt worden door gebruik te maken van fictieve of geanonimiseerde gegevens.

Indien maatregel C niet toepasbaar is op een ontwikkel- en/of testomgeving moeten de overige maatregelen in dit hoofdstuk voor de ontwikkel- en/of testomgeving onderzocht worden.

D. Ontwikkel- en/of testomgeving alleen beschikbaar stellen ten tijde van een test (‘on-demand’)
    a. Doel van deze maatregel is het verkleinen van de kans dat een datalek op de ontwikkel- en/of testomgeving optreedt door deze omgeving alleen beschikbaar te stellen tijdens de periode dat er testen uitgevoerd worden.
    b. Door gebruik te maken van virtualisatie technieken is het mogelijk om alleen gedurende de testperiode een kopie van de productieomgeving beschikbaar te stellen als ontwikkel- en/of testomgeving.

E. Op de ontwikkel- en/of testomgeving testen met een subset van de persoonsgegevens van de productieomgeving
    a. Doel van deze maatregel is het verkleinen van de impact als een datalek op de ontwikkel- en/of testomgeving optreedt door op deze omgeving met een subset van de persoonsgegevens van de productieomgeving te werken. In het geval van een datalek zijn er daardoor minder betrokkenen waarvan de persoonsgegevens gelekt worden.
    b. Bij het gebruik van een subset in een keten van informatiesystemen moet er wel rekening mee gehouden worden dat in de gehele keten dezelfde subset gebruikt wordt. Het uitvoeren van ketentesten is namelijk een randvoorwaarde voor de UT.

F. Autorisaties op de ontwikkel-, test- en acceptatieomgeving beperken
    a. Doel van deze maatregel is het verkleinen van de kans dat een datalek op een omgeving optreedt door het aantal mensen die toegang hebben tot de omgeving te beperken tot diegene die de testen uitvoeren.
    b. Het is in veel gevallen niet noodzakelijk dat bv. ontwikkelaars toegang hebben tot een acceptatieomgeving.

4.4 Optionele maatregelen die onderzocht kunnen worden

G. Niet testen door de UT (kan niet toegepast worden bij maatwerk software)
    a. Doel van deze maatregel is het verkleinen van de kans en impact dat een datalek optreedt door geen ontwikkel-, test- en acceptatieomgeving met persoonsgegevens beschikbaar te stellen.
    b. Het doel van testen is het vooraf kunnen maken van een risico inschatting, testen is daardoor een maatregel in het kader van risicomanagement. Als testen niet meer door de UT uitgevoerd worden moet er gezocht worden naar andere risico maatregelen. Hierbij kan gedacht worden aan contractuele afspraken met leveranciers. Voor sommige informatiesystemen zijn met leveranciers reeds dergelijke afspraken gemaakt. Voorbeelden van afspraken zijn bv. het laten testen door de leverancier en de leverancier beschikbaar laten zijn om eventuele verstoringen bij upgrades op te lossen.
        i. Pure Portal[7]: De leverancier host de Pure Portal en zorgt ervoor dat deze getest wordt op een testomgeving van de leverancier. De UT heeft geen test- of acceptatieomgeving. De leverancier installeert de upgrades op de productieomgeving en is beschikbaar voor het herstellen van fouten die optreden bij upgrades op de productieomgeving.
        ii. Microsoft Exchange (e-mail): met de leverancier is een contract afgesloten waarin afgesproken is dat de leverancier upgrades test op een eigen testomgeving en dat de leverancier beschikbaar is voor het herstellen van fouten die optreden bij upgrades op de productieomgeving.

[7] University of Twente Research Information (utwente.nl)

4.5 Toetsing van de genomen maatregelen aan de privacy basisprincipes

Voor elk instellingssysteem moeten de houders, nadat de genomen maatregelen bepaald zijn, een toets uitvoeren van de privacy basisprincipes[8]. Doel van deze toetsing is aantonen dat de houders met de gekozen maatregelen in de geest van de AVG handelen en zorgvuldig omgaan met de privacy van betrokkenen.

- Rechtmatigheid, behoorlijkheid en transparantie
  - *De persoon van wie de gegevens verwerkt worden, moet hierover worden geïnformeerd. Ook dient de persoon te worden geïnformeerd over zijn/haar rechten.*
- Doelbinding
  - *De persoonsgegevens worden alleen voor specifieke en gerechtvaardigde doeleinden verwerkt. Verwerking van persoonsgegevens mag alleen plaatsvinden ten aanzien van deze doeleinden of voor doelen die daarmee verenigbaar zijn.*
- Dataminimalisatie
  - *Alleen voor het beoogde doel noodzakelijke persoonsgegevens mogen verwerkt worden.*
- Juistheid
  - *De persoonsgegevens moeten correct zijn en blijven.*
- Opslagbeperking
  - *De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor het beoogde doel.*
- Integriteit en vertrouwelijkheid
  - *De persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden en tegen verlies of vernietiging.*
- Verantwoordingsplicht
  - *De Verwerkingsverantwoordelijke moet kunnen aantonen aan de regels te voldoen.*

4.6 Vastlegging van gemaakte keuzes

Om ervoor te zorgen elke houder voor elk instellingssysteem kan aantonen dat er aandacht aan de privacy van betrokkenen wordt besteed, leggen de houders voor elke niet-productieomgeving van elk instellingssysteem de gemaakte keuzes vast in het verwerkingsregister:

- Welke maatregelen uit deze richtlijn zijn toegepast en op welke wijze;
- Welke maatregelen uit deze richtlijn niet toegepast zijn, inclusief onderbouwing;
- Indien persoonsgegevens worden verwerkt, dan dient ook te worden uitgelegd op welke wijze bovengenoemde privacy basisprincipes worden nageleefd.

4.7 Uitvoering van deze richtlijn

Omdat per houder per instellingssysteem een impactanalyse uitgevoerd moet worden, en de houders waarschijnlijk zelf niet alle kennis en kunde in huis hebben om zelfstandig deze impactanalyse uit te voeren, kan via het afdelingshoofd van LISA-PD een impactanalyse workshop aangevraagd worden.

[8] Vrij vertaald naar: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf (AVG). Hoofdstuk 2, Artikel 5 'Beginselen inzake verwerking van persoonsgegevens'

Tijdens een impactanalyse workshop worden de maatregelen, die beschreven zijn in hoofdstukken ‘4.2 Verplichte maatregelen’, ‘4.3 Maatregelen die zoveel mogelijk toegepast moeten worden’ en ‘4.4 Optionele maatregelen die onderzocht kunnen worden’, stuk voor stuk door alle belanghebbenden op impact geanalyseerd. De uitkomsten van de impactanalyse worden tijdens deze workshop vastgelegd in de betreffende beschrijving van de gegevensverwerking.

Onderstaande opsomming is een voorstel voor de belanghebbenden die bij een impactanalyse workshop betrokken moeten worden

- Systeemeigenaar of gedelegeerd systeemeigenaar
- Functioneel beheerder
- Privacy Contact Persoon
- Applicatiebeheerder
- Technisch beheerder
- Contactpersoon c.q. projectleider van LISA-PD

Na afloop van de impactanalyse workshop is de houder verantwoordelijk voor het (laten) uitvoeren van de maatregelen die afgesproken zijn, waarbij het noodzakelijk kan zijn deze op te nemen als project in het UT IT-Projectenportfolio.

5 BIJLAGE 1: PROCEDURE TESTEN MET PERSOONSGEGEVENS

5.1 Stap 1: testplan opstellen

Doel

Het doel van het opstellen van een testplan is:

1. Het gebruik van persoonsgegevens in testomgevingen zoveel mogelijk beperken;
2. verkleinen van de kans op datalekken door testfouten;
3. vooraf goed nadenken over het testen en de testgevallen indien persoonsgegevens zijn betrokken.

Wie

De houder van het betreffende systeem is verantwoordelijk voor het opstellen van het testplan.

Wat

Voorafgaand aan het uitvoeren van een test moet er een goed doordacht en gedocumenteerd testplan opgesteld worden. Onderdeel van het testplan is een impactanalyse waarbij wordt gekeken of het mogelijk is om zonder persoonsgegevens te testen.

Impactanalyse

Bij de impactanalyse wordt onderzocht of het mogelijk is om te testen met:

- geanonimiseerde gegevens: om een testset te creëren wordt een kopie gemaakt van de gegevens uit de productie omgeving. De persoonsgegevens in deze testset worden d.m.v. speciale software geanonimiseerd; of
- fictieve gegevens: volledige testset wordt ontworpen, er wordt geen gebruik gemaakt van een kopie van de gegevens uit de productie omgeving.

Van belang is dat goed wordt vastgelegd waarom de maatregelen eventueel niet mogelijk zouden zijn.

Testen zonder persoonsgegevens

Wanneer blijkt dat testen zonder persoonsgegevens mogelijk is, dan wordt daarmee doorgegaan.

Testen met persoonsgegevens

Blijkt het niet mogelijk om zonder persoonsgegevens te testen, dan moet er bij het ontwerpen van testgevallen reeds nagedacht worden over de risico's die het uitvoeren van een specifiek testgeval met zich meebrengt (privacy by design). Dit kan bijvoorbeeld betekenen dat door een applicatie verzonden e-mails afgevangen worden zodat deze niet naar de eindgebruiker verstuurd worden, of dat bepaalde attributen verwijderd of gewijzigd worden.

Ook moet in het testplan worden besproken welke van de volgende maatregelen worden getroffen. Hierbij geldt het principe 'pas toe of leg uit':

A. Ontwikkel- en/of testomgeving alleen beschikbaar stellen ten tijde van een test ('on-demand')

a. Doel van deze maatregel is het verkleinen van de kans dat een datalek op de ontwikkel- en/of testomgeving optreedt door deze omgeving alleen beschikbaar te stellen tijdens de periode dat er testen uitgevoerd worden.

b. Door gebruik te maken van virtualisatie technieken is het mogelijk om alleen gedurende de testperiode een kopie van de productieomgeving beschikbaar te stellen als ontwikkel- en/of testomgeving.

B. Op de ontwikkel- en/of testomgeving testen met een subset van de persoonsgegevens van de productieomgeving

a. Doel van deze maatregel is het verkleinen van de impact als een datalek op de ontwikkel- en/of testomgeving optreedt door op deze omgeving met een subset van de persoonsgegevens van de productieomgeving te werken. In het geval van een datalek zijn er daardoor minder betrokkenen waarvan de persoonsgegevens gelekt worden.

b. Bij het gebruik van een subset in een keten van informatiesystemen moet er wel rekening mee gehouden worden dat in de gehele keten dezelfde subset gebruikt wordt. Het uitvoeren van ketentesten is namelijk een randvoorwaarde voor de UT.

C. Autorisaties op de ontwikkel-, test- en acceptatieomgeving beperken

a. Doel van deze maatregel is het verkleinen van de kans dat een datalek op een omgeving optreedt door het aantal mensen die toegang hebben tot de omgeving te beperken tot diegene die de testen uitvoeren.

b. Het is in veel gevallen niet noodzakelijk dat bv. ontwikkelaars toegang hebben tot een acceptatieomgeving.

Wanneer met persoonsgegevens wordt getest, volgt stap 2.

5.2 Stap 2: verwerking laten opnemen in het verwerkingsregister en privacy statement opstellen/aanpassen

Doel

Het doel van het opstellen dan wel aanpassen van een privacy statement is transparantie naar betrokkenen zodat zij op de hoogte zijn van het gebruik van persoonsgegevens in acceptatieomgevingen. Daarnaast moeten verwerkingen van persoonsgegevens worden opgenomen in het verwerkingsregister. Hiervoor kan contact worden opgenomen met de functionaris gegevensbescherming.

Wie

De houder van het betreffende systeem is verantwoordelijk voor het opstellen /wijzigen van het privacy statement en de registratie in het verwerkingsregister. Bij de functionaris gegevensbescherming of de privacy contact persoon van de desbetreffende dienst of faculteit kan een template privacy statement worden opgevraagd, evenals een document voor het verwerkingsregister.

De houder kan de privacy contact persoon van zijn/haar dienst/afdeling vragen hierbij te helpen.

Wat

Acceptatieomgevingen worden opgenomen in het verwerkingsregister. Ook dienen betrokkenen te worden geïnformeerd over de verwerking van hun persoonsgegevens in een privacy statement. Bij de functionaris gegevensbescherming kan een template privacy statement worden opgevraagd, evenals een document voor het verwerkingsregister.