Gezamenlijke elektronische Voorzieningen SUWI

Keten Dossier Afspraken & Procedures SUWI versie 14.1

Gebaseerd op de GeVS Keten SLA versie 14.0

Inhoud

1. Inleiding

1.1 Achtergrond en doel van het GeVS Keten DAP

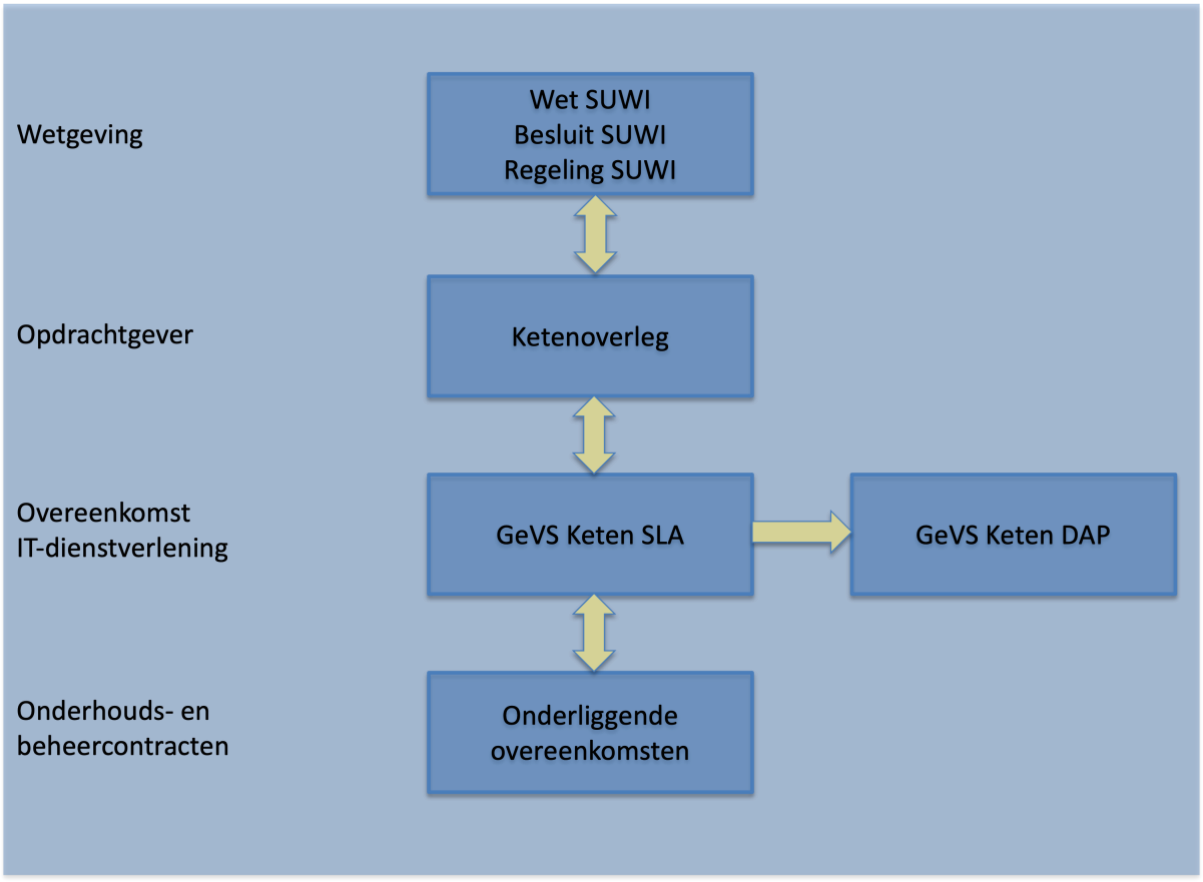
Het Gezamenlijke elektronische Voorzieningen Suwi Keten Dossier Afspraken en Procedures (verder genoemd Keten DAP) is een nadere uitwerking van de GeVS Keten SLA (verder te noemen Keten SLA) en bevat nadere afspraken en procedures met betrekking tot de ICT-beheerprocessen die van toepassing zijn op de dienstverlening door de (keten) partijen. Mochten de Keten SLA en het Keten DAP elkaar tegenspreken is de Keten SLA altijd leidend.

De partijen op wie de Keten SLA van toepassing is, zijn ook de partijen voor deze Keten DAP. Bij elke nieuwe versie van de Keten SLA wordt altijd een nieuwe versie van de Keten DAP gemaakt met daarin eventuele noodzakelijke aanpassingen. Deze twee documenten worden tezamen goedgekeurd door de Domeingroep ICT Beheer.

De Domeingroep ICT Beheer is beheerder van deze Keten DAP en borgt dat dit document in lijn blijft met de vigerende versie van de Keten SLA.

1.2 Positie van de GeVS Keten DAP

In onderstaande figuur is de positie van het Keten DAP t.o.v. andere afspraken weergegeven.



Afbeelding 1: Voor de keten geldende regels en afspraken.

1.3 Leeswijzer

In de volgende hoofdstukken wordt per onderwerp weergegeven welke afspraken en procedures de partijen zijn overeengekomen. De hieraan gerelateerde prestatienormen zijn vastgelegd in de Keten SLA.

1.4 Vastelling, publicatie, evaluatie, duur en wijziging van de Keten DAP

De Keten DAP wordt vastgesteld door de Domeingroep ICT Beheer (DIB). Als er een nieuwe versie van de Keten SLA vastgesteld wordt, zal er ook altijd een nieuwe versie van de Keten DAP met hetzelfde versie nummer gepubliceerd worden. De Keten DAP geldt vanaf het moment van publicatie blijft geldig tot vervanging door een nieuwe Keten DAP. De Keten DAP wordt minimaal één keer per jaar geëvalueerd door de DIB.

De Keten DAP wordt na vaststelling gepubliceerd op www.bkwi.nl.

2. Dienstenniveau beheer

2.1. Openstellingstijden voor de productieomgeving en ondersteuning

- Uitzonderingen en aanvullingen op de openstellingstijden, voor zover vooraf bekend, worden gepubliceerd op bkwi.nl. De uitzonderingen en aanvullingen worden voorafgaande aan de publicatie te goedkeuring voorgelegd aan de Domeingroep ICT Beheer.

2.2 Onderhoudstijden van de productieomgeving

- Gepland onderhoud, uitgevoerd door (één van) de partijen, aan (een onderdeel van) de diensten, vindt uitsluitend plaats buiten de beschreven openstellingstijden.
- In de keten SLA zijn partij specifieke onderhoudsmomenten vastgelegd.
- Onderhoud moet vooraf worden gemeld aan de Suwidesk. De Suwidesk informeert de betrokken (keten)partijen.
- Partijen die genoodzaakt zijn om werkzaamheden tijdens de openstellingstijden uit te voeren, dienen in de aanvraag goed te onderbouwen waarom het niet mogelijk is dit onderhoud buiten de openstellingstijden uit te voeren.
- BKWI draagt zorg dat het verzoek van de ketenpartij bij het DIB-lid van die partij wordt neergelegd.
- De vertegenwoordiger in de DIB van de partij die werkzaamheden tijdens de openstellingstijden wil uitvoeren, draagt er zorg voor dat dit verzoek wordt voorgelegd aan de DIB-leden.
- Verzoeken tot onderhoud binnen de beschreven openstellingstijden worden vervolgens door de partijen in de DIB behandeld.

2.3 Extra openstellingstijden van de productieomgeving

- Wanneer een partij extra openstelling van de Suwinet-Services wenst, stuurt deze per e-mail een aanvraag naar de Suwidesk.
  Dit verzoek moet minimaal de volgende elementen bevatten:
  - de partij die de aanvraag doet;
  - de contactpersoon/contactpersonen van de aanvragende partij (zowel voor de aanvraag als gedurende de extra openstelling);
  - de gewenste functionaliteit(en);
  - de reden waarom de extra openstelling is gewenst;
  - de datum waarop extra openstelling wordt gewenst, inclusief tijd (van .. tot ..).
- Een aanvraag voor extra openstellingstijd moet tenminste twee weken voorafgaand aan de datum waarop de extra openstelling gewenst is bij het BKWI binnen zijn. De aanvraag voor extra openstelling kan maximaal 6 weken van tevoren worden ingediend bij de Suwidesk.
- Het BKWI registreert de aanvraag als service request onder een uniek referentienummer. De Suwidesk stuurt de aanvraag onder vermelding van het registratienummer binnen één werkdag na ontvangst door naar de contactpersonen van de betreffende partijen waarvan extra beschikbaarheid gewenst wordt.
- De partijen die de aanvraag hebben ontvangen, beoordelen het verzoek en geven aan of het mogelijk is op de aangegeven datum aan het verzoek te voldoen.

- Als aan het extra openstellen kosten zijn verbonden, dan is het uitgangspunt dat de kosten worden gedragen door de partij die de openstelling verleent. Bij uitzonderingen vindt er overleg plaats tussen de partijen.
- De partijen sturen het resultaat van de beoordeling uiterlijk binnen vijf werkdagen na ontvangst van de aanvraag aan de Suwidesk. De Suwidesk verzamelt de verschillende beoordelingen en stuurt dit totaalbeeld binnen 1 werkdag naar de aanvrager.
- Voor extra ondersteuning tijdens extra openstellingtijd kunnen partijen kosten in rekening brengen bij de aanvrager. Tenzij anders afgesproken verleent BKWI tijdens extra openstellingtijden geen ondersteuning.

2.4 Gebruik Ketenbrede Test Omgeving

- Er is een Ketenintegratie Test omgeving (KIT) inclusief testdata voor Suwinet beschikbaar voor de partijen.
- De KIT is gekoppeld aan testsytemen van ketenpartijen, waar mogelijk/gewenst biedt BKWI standaard teststubs aan om testomgevingen van ketenpartijen te simuleren.
- De KIT staat standaard gereserveerd voor BKWI om producten te kunnen testen.
- Als een partij (een wijziging) wil testen dan reserveert hij/zij dit twee weken van tevoren bij het BKWI. Het BKWI zorgt ervoor dat de testomgeving beschikbaar is en naar gewenst naar een bronsysteem of teststub wijst.
- Bij gebruik van de testomgeving terwijl de testomgeving door een andere partij is gereserveerd zijn er geen garanties voor een juiste werking.
- Gebruik testomgeving zonder reservering is toegestaan als dit de test van de partij die gereserveerd heeft, niet in de weg kan zitten.
- BKWI registreert de reserveringen in de Suwinet agenda.

3. Servicedesk

- Partijen zijn niet verplicht om een servicedesk in te richten, wel moet elke partij zorgen voor een enkelvoudig communicatiekanaal (single point of contact) met de Suwidesk van BKWI.
- Deelnemende partijen zijn zelf verantwoordelijk voor gebruikersbeheer en de eerstelijnsondersteuning van de eigen gebruikers en zelf bepalen zij op welke wijze zij deze eerstelijnsondersteuning invullen.
- Communicatie over incidenten of onderbrekingen in de dienstverlening verlopen in beginsel via de Suwidesk.
- Partijen informeren bij een incident eerst de eigen eerstelijnsondersteuning,
- De verschillende servicedesken (of degene die die rol heeft gekregen bij een ketenpartij) zijn aanmelder van incidenten en tevens oplosgroep voor ketenbrede incidenten.
- De Suwidesk vervult de rol van centrale regievoerder op het keten brede incidentbeheer en informeert de partijen over de status en voortgang van openstaande incidenten.
- De Suwidesk communiceert met de servicedesk van ketenpartijen of de door de ketenpartij aangedragen single point of contact.
- Iedere partij informeert zelf haar eigen gebruikers over de status en voortgang van incidenten en van tijdelijke onderbrekingen van de dienstverlening.

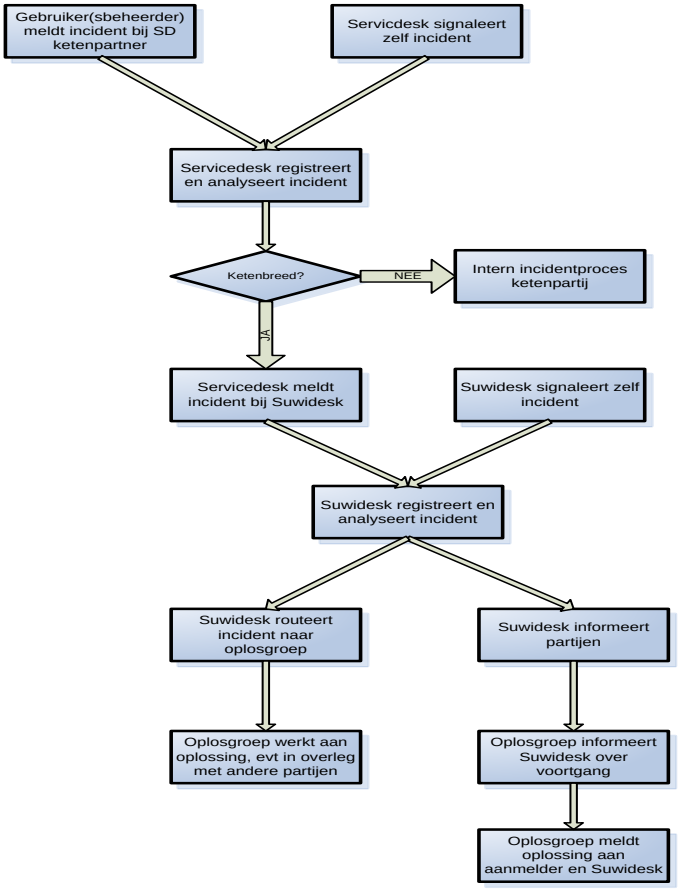
- In beperkte mate verleent de Suwidesk tweedelijns en derdelijns ondersteuning aan de partijen, zoals benoemd en afgesproken in de Keten SLA.

4. Configuratiebeheer

- De Suwidesk houdt binnen het incidentregistratietool voor ketenbrede incidenten een overzicht bij van ketencomponenten waar incidenten aan gekoppeld kunnen worden.
- Iedere partij heeft een eigen CMDB waarin partij specifieke componenten zijn opgenomen. Deze moeten actueel en volledig zijn. De status van een component moet bewaakt kunnen worden.
- De inhoud van de CMDB van de ketenpartijen wordt actueel gehouden, en minimaal jaarlijks gecontroleerd.

5. Configuratiebeheer

- Het doel van de afspraken met betrekking tot het proces incidentbeheer is dat na het optreden van een incident zo snel mogelijk een herstelde dienstverlening volgens de afspraken in de Keten SLA wordt gerealiseerd.



Afbeelding 2: Procedure schema incidentbeheer

5.1 Incident aanmelden en registreren

- Gebruikers van de Suwinet-Services melden de geconstateerde incidenten en service requests in eerste instantie binnen de eigen organisatie.
- Verstoringen binnen het eigen beheerdomein, zonder ketenimpact, zijn de verantwoordelijkheid van de eigen partij en vallen buiten de scope van het Ketenbreed Incidentbeheer.
- Een ketenbreed incident is een verstoring waarvoor geldt dat;
    - de oorzaak in het beheerdomein ligt van één van de SUWI-partijen en
    - één of meer partijen - anders dan de veroorzakende partij – gevolgen ondervindt van deze verstoring.
- Iedere partij meldt actief incidenten met ketenimpact aan de Suwidesk, inclusief eigen referentienummer.
- Bij incidenten waarbij de oorzaak van het incident ligt bij de ketenpartij zelf wordt tevens een inschatting gegeven van de te verwachten oplostermijn.
- De Suwidesk prioriteert een incident conform de afspraken uit de Keten SLA, registreert het incident en geeft het referentienummer van de Suwidesk aan de 'aanmeldende' servicedesk.
- Incidenten krijgen bij registratie een prioriteit met daaraan gekoppeld een indicatieve oplostijd (zie tabel incidentbeheer /prioriteiten in de Keten SLA). Vaak zal dat het geval zijn bij incidenten over de kwaliteit van gegevens, omdat oplossing van deze incidenten vaak een langere doorlooptijd kennen.

5.2 Incident routeren en oplossen

- De Suwidesk informeert de partijen via mail over storingen met behulp van verzendlijsten, die naast servicedesken ook beheerders en andere belanghebbenden kan bevatten.
- De Suwidesk routeert ketenbrede incidenten binnen de vastgestelde reactietijd (zie Keten SLA) naar een oplosgroep. Hierbij wordt het referentienummer (van de Suwidesk) van het incident vermeld.
- Indien nodig wordt een ketenbreed incident door een partij gerouteerd naar een leverancier van een ketenpartij. De Servicedesk van de ketenpartij blijft echter altijd verantwoordelijk voor de monitoring van de voortgang en de communicatie naar de indiener en/of Suwidesk. De Suwidesk verspreidt deze informatie vervolgens via de geëigende route aan afnemers.
- Terugkoppeling van de voortgang aan de Suwidesk vindt altijd plaats onder vermelding van Suwidesk incidentnummer. Ook wordt - voor zover bekend - altijd de oorzaak van het incident teruggekoppeld.
- De oplosgroep zal de Suwidesk tijdig op de hoogte brengen van een dreigende overschrijding van de oplostijden. Aanmelder en oplossende partij overleggen of de overschrijding wordt geaccepteerd of dat de escalatieprocedure wordt gestart.
- De oplosgroep draagt zorg voor terugkoppeling van de voortgang aan de Suwidesk onder vermelding van het Suwidesk incidentnummer
- Bij incidenten met classificatie 1 en 2 heeft de Suwidesk het recht om de toegang tot de vrijgegeven testomgeving in te trekken en deze zelf te gaan gebruiken voor de afhandelingen van één of meerdere incidenten.

- Als onduidelijk is bij welke partij de oorzaak van de storing ligt of de afgesproken oplostijd van een incident dreigt te worden overschreden, neemt BKWI de regie op het incident. De regie ligt dan bij de voorzitter van het KIPO of plaatsvervanger. De voorzitter van het KIPO stelt dan een kleine oplosgroep samen die gezamenlijk het incident onderzoeken en /of acties uitzetten.

5.3 Incidentprocedure privacy- en beveiligingsincidenten

Het ketenbrede incidentbeheer kent specifieke incidenten van het type privacy- en beveiligingsincident. Dit onderdeel is een richtlijn over wanneer het kenmerk 'privacy- en beveiligingsincident' van toepassing is op een incident en hoe de ernst van een privacy- en beveiligingsincident wordt bepaald.

Definitie gebruikte termen

Privacy:	de mate waarin persoonsgegevens zijn beschermd tegen het in handen vallen van onbevoegden.
Beveiliging:	omvat de volgende deelgebieden:
Beschikbaarheid:	de mate waarin een faciliteit beschikbaar is op momenten dat dit voor een ketenproces is gewenst en/of is afgesproken
Integriteit:	de mate waarin de werking van processen en de gegevens zonder fouten zijn
Vertrouwelijkheid:	de mate waarin processen en gegevens slechts beschikbaar zijn voor diegenen die daar recht op hebben, ook wel exclusiviteit genoemd.

5.4 Onderscheid tussen de P&B-aspecten bij de behandeling van incidenten

De afhandeling van incidenten en calamiteiten die uitsluitend betrekking hebben op het aspect **Beschikbaarheid**, wordt verzorgd door de standaard incidentafhandelingsprocedure aanvullende eisen worden er niet gesteld.

Voorbeelden van ***vertrouwelijkheid*-incidenten**:
Personen of applicaties kunnen/konden[1] toegang krijgen tot beschermde faciliteiten en/of gegevens[2] zonder dat zij daar recht op hadden, bijvoorbeeld:

1. Aan een persoon of applicatie is een autorisatie gegeven zonder dat hiervoor toestemming is verleend door een bevoegd persoon.
2. Een onbewaakte computer die niet is vergrendeld.
3. De toegangsmiddelen[3] (bijvoorbeeld username/password) worden (al dan niet opzettelijk) gebruikt door een andere geautoriseerde[4].
4. Autorisatiemechanismen worden omzeild, bijvoorbeeld:
    a. door het niet of onvoldoende functioneren van beveiligingsmechanismen;
    b. doordat de werkende beveiligingsmechanismen onvoldoende bescherming bieden;

1 Hiervan is dus ook sprake wanneer van de ongeautoriseerde toegang geen gebruik is gemaakt.

2 Het betreft hier zowel gegevens die beschermd zijn door een applicatie als gegevens op een beveiligde informatiedrager.

3 Verkregen al dan niet met de medewerking van een andere geautoriseerde

4 Dit geldt ook wanneer de overtreder dezelfde autorisatie bezit.

c. vanwege een succesvolle aanval door een hacker.

Voorbeelden van ***privacy*-incidenten**:
Persoonsgegevens zijn of waren[5] beschikbaar voor personen voor wie deze niet zijn bedoeld, bijvoorbeeld vanwege:

1. het verwerken van persoonsgegevens zonder doelbinding.
2. de zichtbaarheid voor onbevoegden van persoonsgegevens op een beeldscherm of document op een onvoldoende bewaakte[6] werkplek.
3. het opbergen van documenten of onbeschermde gegevensdragers met persoonsgegevens in een onvoldoend bewaakte of afgesloten kast of lade.
4. het opslaan van elektronische persoonsgegevens op een onvoldoend beschermd of bewaakt medium.
5. het afdrukken van persoonsgegevens op een onvoldoend bewaakte printer of kopieerapparaat.
6. het transport van documenten of onbeschermde gegevensdragers met persoonsgegevens op een onvoldoend beschermde wijze.

Verantwoordelijkheid voor beoordeling en afhandeling
Bij het beoordelen en het proces van afhandelen van beveiligingsincidenten hebben de security- en privacyfunctionarissen van de betrokken organisaties een prominente rol. En zijn verantwoordelijk voor de coördinatie en afhandeling van incidenten.

5.5 Beoordeling Ernst incidenten

De ernst van het aspect beveiliging en privacy wordt beoordeeld op basis van de onderstaande tabel.

Ernst	Omschrijving per aspect
Licht	De schending blijft binnen de hieronder omschreven criteria: *Een schending van de privacy en/of de exclusiviteit was/is beperkt van omvang en kon/kan worden gecorrigeerd zonder dat de privacy van de betreffende personen hiervan schade ondervinden of hebben ondervonden[7].* Een dergelijk incident heeft, vergeleken met niet-P&B incidenten, een afwijkende afhandeling nodig, gericht op het: * zo nodig opheffen van oorzaak van de gebeurtenis; * zo nodig herstellen van de schade; * starten van een wijziging ter voorkoming van een herhaling van de gebeurtenis De laatste actie mag pas worden overgeslagen als het risico[8] van een herhaling gering is en de kosten en inspanning daarmee onevenredig hoog zijn.
Hoog	De schending blijft binnen de omschreven criteria:

5 Hiervan is sprake, wanneer van deze beschikbaarheid geen gebruik is gemaakt.

6 De eisen aan de kwaliteit van de afsluiting, bescherming of bewaking hangt af van de gevoeligheid van de informatie; deze eisen moeten zijn vermeld in een ter plaatse geldend en bekendgemaakt document, bijvoorbeeld over documentclassificatie.

7 Als een persoon wiens privacy het betreft een klacht heeft ingediend die verband houdt met dit incident, dan is de ernst "Hoog".

8 Risico is het product van de kans dat het incident zich herhaalt en de schade die daarvan het gevolg kan zijn.

	Een schending van de privacy en/of de exclusiviteit was/is van aanzienlijke omvang en kon/kan niet worden gecorrigeerd zonder dat de privacy van de betreffende personen hiervan schade ondervinden of hebben ondervonden of hiervoor een reëel risico lopen of liepen[9]*.* Een dergelijk incident heeft, vergeleken met niet-P&B incidenten, een afwijkende afhandeling nodig, gericht op het zo spoedig mogelijk: * opheffen van de oorzaak van de gebeurtenis; * zonodig informeren van de betrokkenen; * herstellen van de schade; * starten van een wijziging ter voorkoming van een herhaling van de gebeurtenis
Zeer Hoog =Calamiteit	De schending voldoet aan de volgende criteria: Een schending van de privacy en/of beveiliging was/is van omvang zodanig dat deze de bedrijfsvoering van één of meerdere SUWI-partijen raakt, het ministerie raakt, of een publieke zaak wordt. Een dergelijk incident escaleert naar de verantwoordelijke vertegenwoordiger(s) van betrokken partijen. Als is aangetoond dat de schadelijke werking van een P&B-calamiteit kan worden opgeheven door het uitschakelen van (een deel) van Suwinet, dan zal de Security Officer van het BKWI, in overleg met de betrokken Security Officers van de ketenpartijen en mogelijk met technisch deskundigen, hiertoe opdracht geven aan de Suwidesk.

5.6 Datalekken

De meldplicht datalekken geldt al sinds 2016. Onder de Europese privacywet die sinds 25 mei 2018 geldt, de Algemene verordening gegevensbescherming (AVG), blijft de meldplicht datalekken bestaan. De Autoriteit Persoonsgegevens kan hoge boetes opleggen als organisaties zich niet houden aan de AVG, waaronder het niet (tijdig) melden van datalekken.

De meldplicht en boetedreiging dwingt organisaties om naar de AP en naar de getroffen personen transparant te zijn over datalekken en om datalekken zo snel mogelijk te dichten.

Een datalek gaat altijd over persoonsgegevens en niet over (gevoelige) bedrijfsinformatie. Bij een datalek is sprake van een ‘inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking’. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van persoonsgegevens, maar ook vernietiging daarvan en andere vormen van onrechtmatige verwerking.

Ook een vermoeden van datalek dient gemeld te worden aan de Autoriteit Persoonsgegevens. Als het vermoeden vals alarm blijkt te zijn kan de melding weer ingetrokken worden.

Procesgang

9 Als een persoon wiens privacy het betreft een klacht heeft ingediend die verband houdt met dit incident, dan is de ernst minimaal “Hoog”.

Als er een (vermoeden van een) datalek is, wordt dit als een prio 1 incident gemeld bij de Suwidesk. Bij een vermoeden van datalek wordt het partij eigen proces gevolgd en daarnaast de Suwidesk geïnformeerd. Dit dient zowel schriftelijk (per mail aan Suwidesk@bkwi.nl) en daarnaast ook verplicht telefonisch gemeld te worden. Dit in verband met de 72 uur termijn die staat voor de melding aan de Autoriteit Persoonsgegevens.
Bij de melding aan de Suwidesk wordt in elk geval het volgende aangegeven:

- of er mogelijk sprake is van een datalek
- zo ja, of het een meldenswaardig datalek is
- Van hoeveel personen is de data gelekt?
- Welke persoonsgegevens zijn gelekt?
- Wat is de oorzaak van het lek?
- Is het lek onder controle?
- Welke maatregelen zijn er (al) getroffen?

Verder volgt dit datalek het proces van incidentbeheer prio 1 met als enige verschil de mogelijke melding bij de Autoriteit Persoonsgegevens. Elke partij heeft zijn eigen verantwoordelijkheid bij het melden van een datalek bij de Autoriteit Persoonsgegevens. Als bij BKWI een datalek geconstateerd wordt door BKWI vindt deze melding plaats via UWV.

6. Probleembeheer

- Het doel van probleembeheer is het vinden van oplossingen voor veelvoorkomende incidenten, waarmee uiteindelijk incidenten voorkomen (kunnen)worden.
- Er is sprake van een probleem wanneer (en/of):
  - sprake is van herhaling van een incident;
  - het incident niet nog een keer op mag treden;
  - de service levels onder druk komen te staan;
  - analyse van de infrastructuur de kans van incidenten aantoont.

Probleem registreren

- Elke ketenpartij registreert problemen die zij zelf constateren (als van toepassing inclusief referentienummers van de bijbehorende incidenten) en meldt deze centraal aan de Suwidesk. De coördinator Suwidesk analyseert en beslist of het een probleem betreft. De coördinator Suwidesk registreert het probleem en meldt dit terug aan de meldende partij inclusief het Suwidesk referentienummer. De coördinator Suwidesk beslist of de overige ketenpartners ingelicht dienen te worden. Het KIPO wordt altijd ingelicht. Terugkoppeling moet binnen één werkdag geschieden.
- Als het geen ketenprobleem is, maar een probleem bij/met slechts één van de ketenpartners, dan zal de coördinator Suwidesk in contact treden met de probleem-coördinator van de meldende partij om gezamenlijk het probleem af te handelen.

Oplostermijnen problemen

- Het KIPO wordt bij problemen met hoge prioriteit bij elkaar geroepen.
  Het KIPO beoordeelt het probleem en koppelt een oplostermijn aan het probleem. Oplostermijnen voor problemen kunnen in tegenstelling tot incidenten niet vooraf gedefinieerd worden, maar is afhankelijk van het onderzoek, gekozen oplossing en hierbij horende doorlooptijd.

- Partijen streven ernaar om binnen twee weken het onderzoek naar de oorzaak af te ronden. Bij de conclusies van het onderzoek moet ook een oplossing voorstel en termijn genoemd worden.

7. Wijzigings en releasebeheer

Het doel van wijzigings- en releasebeheer is het gestructureerd en gecontroleerd doorvoeren van ketenbrede wijzigingen en releases, waarmee de risico's op verstoringen geminimaliseerd zijn. De afspraken over wijzigingsbeheer zijn beschreven in het document "Uitvoeringsafspraken Ketenbrede wijzigingen en releases" en wordt gepubliceerd op www.bkwi.nl .

Het document "Uitvoeringsafspraken Ketenbrede wijzigingen en releases" is in beheer bij het Keten CAB. Aanpassingen in het document worden voorgelegd aan de Domeingroep ICT Beheer ter vaststelling.

De jaarlijkse releasekalender wordt door het Keten CAB vastgesteld en gepubliceerd op www.bkwi.nl.

8. Continuïteit en uitwijk

- Voor de centrale omgeving werkt BKWI met een dubbel uitgevoerde omgeving die beide actief zijn (de omgeving draait volledig op twee fysiek gescheiden datacenters en zal bij uitval van één omgeving gewoon blijven werken). Dit houdt in dat er voor de centrale omgeving geen uitwijk voorziening meer nodig is omdat de beschikbaarheid met deze inrichting al gegarandeerd is.
- Ketenpartijen dragen zelf zorg voor de inrichting van het continuïteitsbeheer /uitwijk en zijn vrij hier zelf invulling aan te geven, als zij maar kunnen garanderen binnen een acceptabele termijn de dienstverlening kunnen herstellen. De acceptabele termijn is ter beslissing van het MT van de verschillende organisaties.

9. Autoriseren gebruikersbeheerder Suwinet-Inkijk

Aan wie worden beheerrechten toegekend

- Niemand kan autorisatie(s) voor zichzelf aanvragen; altijd vraagt een binnen de organisatie gemandateerde medewerker de benodigde autorisaties aan.
- Elke aangesloten partij autoriseert zelf haar personeel en stelt hiervoor gebruikersbeheerders aan.
- Op verzoek van een gemandateerde medewerker kent BKWI aan betreffende gebruikersbeheerders de rechten toe, die passen bij deze partij. Hiertoe geeft

betreffende partij voor zowel een nieuwe situatie[10] als bij wijziging van bestaande situatie formeel aan BKWI door wie zij het gebruikersbeheer wil laten uitvoeren. Dit formeel doorgeven bestaat uit een door directeur of gemeentesecretaris ondertekende brief, waarin de partij verzoekt beheerrechten toe te kennen aan met naam, functie en contactgegevens vermelde personen.

Welke rechten worden toegekend

- De rechten die worden toegekend zijn: het kunnen toekennen van die toegangsrechten, welke voor betreffende partij zijn vastgesteld.

Het delegeren van beheerrechten

- Wanneer een partij taken binnen de eigen organisatie uitbesteedt, dan kan de gebruikersbeheerder doorgeven welke persoon/personen vanuit welk organisatieonderdeel beheerrechten toegekend mogen krijgen en welke toegangsrechten deze beheerder mag toekennen.
- Wanneer een partij taken uitbesteedt aan een andere organisatie, dan moet betreffende partij dit formeel aanvragen bij het BKWI. De opdracht moet dus komen van de aangesloten organisatie.
- Dit formeel doorgeven bestaat uit een door directeur of gemeentesecretaris ondertekende brief, waarin de partij verzoekt de in de brief genoemde beheerrechten toe te kennen aan de met naam, functie en contactgegevens vermelde gebruikersbeheerder(s) van deze andere organisatie.

Welke gegevens moeten worden doorgegeven

1. naam van de organisatie en/of organisatieonderdeel
2. naam, functie en contactgegevens van de aanvrager
3. naam, functie en contactgegevens van de te autoriseren beheerder
4. toe te kennen beheerrechten; de toe te kennen autorisatierollen volgen uit het aansluitproces.

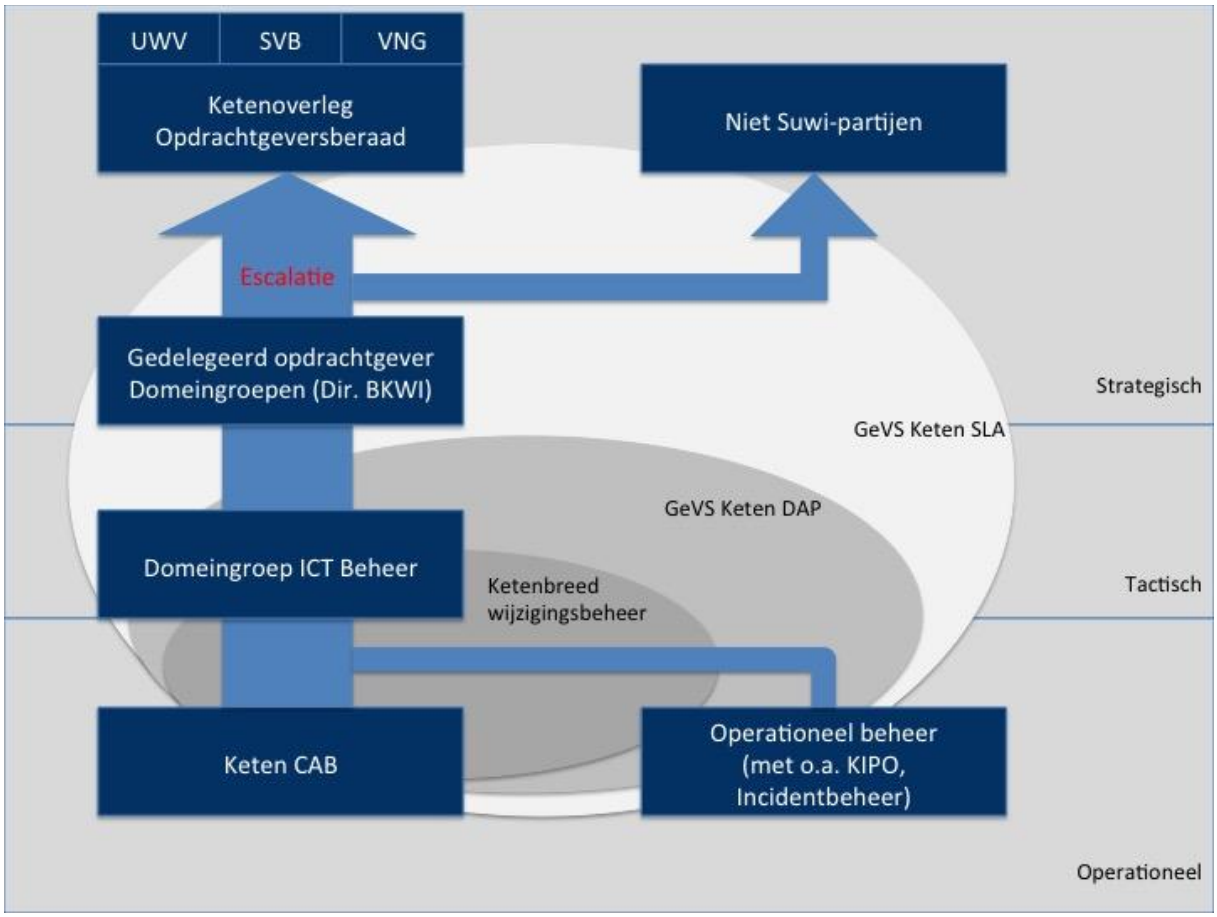
10. Configuratiebeheer

Escalaties kunnen om verscheidene redenen worden uitgevoerd, hierbij moet gedacht worden aan overschrijding van de oplostermijn van incidenten, wijzigingen die niet tijdig worden doorgevoerd, maar ook het niet nakomen van ketenbrede afspraken zoals gemaakt in de verschillende domeingroepen.

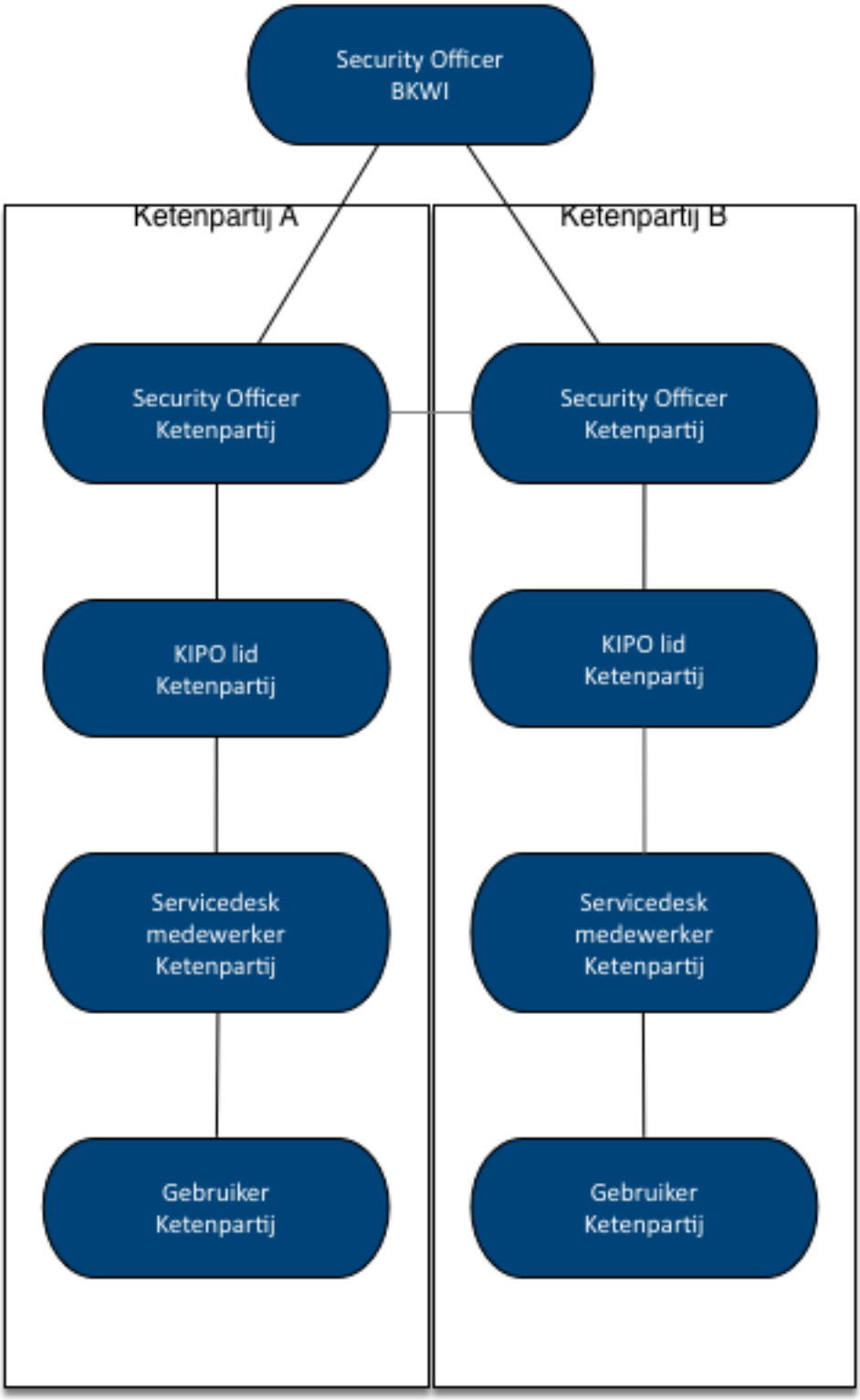
- Doel van de escalatieprocedure is het forceren van een doorbraak bij ongewenste situaties
- Als de oplostijd conform Keten SLA wordt overschreden, vindt escalatie volgens onderstaand schema plaats. Binnen een partij worden verticaal geëscaleerd. Tussen organisaties ALTIJD horizontaal. Escalaties verlopen altijd via de voorzitter van de domeingroep voor zover het onderwerp past binnen deze domeingroep.
- Escalaties worden opgelost door de gedelegeerd opdrachtgever van de Domeingroepen (lees; directeur BKWI). Hierbij enkel in de rol als onafhankelijk gedelegeerd opdrachtgever en dus niet als directeur BKWI (Afbeelding 3).

10 Vanuit het aansluitproces voor nieuwe partijen wordt vastgesteld welke persoon/personen het centrale gebruikersbeheer uitvoeren.

- In geval van (vermoeden van) een beveiligingsincident, vindt altijd escalatie plaats, volgens onderstaand schema (Afbeelding 4).



Afbeelding 3 Escalatieschema geschillen



Afbeelding 4: Escalatieladder bij beveiligings of privacy incidenten.

11. Aanvraagprocedures

Niet alle afnemers maken gebruik van alle beschikbare Suwinet producten. Voor alle producten die binnen het SUWI-domein beschikbaar zijn gelden specifieke aanvraagprocedures.

Bijlage 1 – Verklarende woordenlijst

Beschikbaarheid	De mate waarin een informatiesysteem gebruiksgereed is op het moment dat de organisatie het nodig heeft. % beschikbaarheid = werkelijke beschikbare tijd / overeengekomen tijd x 100%.
Beveiligings-incident	Een beveiligingsincident is een gebeurtenis die ervoor heeft gezorgd, of ervoor had kunnen zorgen, dat bedrijfsmiddelen zijn beschadigd of verloren zijn geraakt. Een handeling die in strijd is met de beveiligingsprocedures van het bedrijf, is ook een beveiligingsincident.
CMK	Centraal Meldpunt Ketenwijzigingen. Het CMK registreert, publiceert, coördineert en routeert ketenwijzigingen en releases.
Centrale omgeving	De centrale omgeving van Suwinet bevat het Suwikoppelpunt, servers, routers, reverse proxy's en bijbehorende verbindingen ten behoeve van Suwinet-Inkijk, Suwinet-Mail en Suwinet-Meldingen.
Domeingroep ICT Beheer (DIB)	Een overleg dat wordt gevormd door de Service Level Managers van de betrokken partijen en wordt voorgezeten door het BKWI. Het overleg behandelt de inrichting en kwalitatieve groei van ketenbreed ICT Beheer.
Incident	Verstoring in de afgesproken dienstverlening of een vraag over de dienstverlening.
Incidentbeheer	Het registreren, prioriteren en (doen) verhelpen van gebeurtenissen die een onderbreking of vermindering van de kwaliteit van de dienstverlening veroorzaken.
Ketenbreed incident	Een ketenbreed incident is een verstoring waarvoor geldt dat (a) de oorzaak ligt in het beheerdomein van de Suwi-partijen, en (b) één of meer Suwi-partijen - naast de veroorzakende partij – ondervindt gevolgen van deze verstoring.
Ketencomponent	Kleinste gedefinieerde onderdeel van de Suwinet infrastructuur, vastgelegd in de CMDB van het CMK.
Keten Incidenten & Problemen Overleg (KIPO)	Keten Incidenten en Problemen Overleg, overleg waarin de incidentmanagers van de ketenpartijen ketenbrede incidenten en problemen bespreken en waar incidenten worden gepromoveerd tot problemen en worden toegewezen aan een oplosgroep.
Keten DAP	Keten Dossier Afspraken en Procedures Suwinet, het document waarin de afspraken van de Keten SLA nader zijn uitgewerkt.
Ketenbrede wijziging	Een ketenbrede wijziging is een wijziging in een ketencomponent waarvoor geldt dat (a) het initiatief ligt bij één van de Suwi-partijen, en (b) één of meer Suwi-partijen - naast de veroorzakende partij - ondervindt gevolgen van deze wijziging. Er wordt onderscheid gemaakt tussen voorgenomen veranderingen, ketenwijzigingen en ketencomponentwijzigingen.

Onderhoud	Het uitvoeren van preventieve of proactieve werkzaamheden aan Configuratie Items die van invloed zijn op de beschikbaarheid van de diensten.
Openstellingstijden	Afgesproken tijdstippen waarbinnen de diensten beschikbaar zijn.
Oplosgroep	Organisatie(onderdeel), verantwoordelijk voor het oplossen van een incident. Dit kan een Suwi-partij zijn, maar ook een leverancier van een Suwi-partij.
Oplostijd	De maximale tijd die is afgesproken voor het oplossen van een incident, op basis van de prioriteit van het incident.
Overzichtspagina	Een pagina waarmee gegevens, afkomstig van (soms meerdere) bronnen, op één pagina worden verzameld en getoond.
Prioriteit	Code waaraan een oplostijd is gekoppeld, afhankelijk van de urgentie en impact van een incident, probleem of wijziging.
Probleem	Onbekende onderliggende oorzaak van een of meerdere incidenten.
Probleembeheer	Het registreren, prioriteren en structureel (doen) verhelpen van gebeurtenissen die het functioneren van de IT-infrastructuur aantasten.
Reactietijd	De tijd die een opdrachtnemer heeft om statusmeldingen aan de opdrachtgever terug te melden.
Release	Een cluster van wijzigingen in één of meer ketencomponenten dat gelijktijdig wordt geïmplementeerd.
Responsetijd	De responsetijd van een applicatie of systeem geeft de tijd weer tussen het opvragen en de beschikbaarstelling van de applicatie of het systeem.
SLA	Service Level Agreement, het document waarin het afgesproken kwaliteitsniveau van de dienstverlening beschreven staat.
SNO	Service Niveau Overeenkomst; een overeenkomst waarin afspraken tussen partijen zijn vastgelegd omtrent bedrijfsprocessen, informatiestromen en gegevensuitwisseling.
Stelselontwerp	De beschrijving van de technische voorzieningen, de functionaliteiten en de specificaties die worden toegepast bij de inrichting en de werking van Suwinet. Zie voor de wettelijke omschrijving artikel 66 van de Wet structuur uitvoeringsorganisatie werk en inkomen.
Suwidesk	De tweedelijns helpdesk van BKWI-Exploitatie, waar ketenbrede incidenten, problemen en wijzigingen behandeld worden en waar de centrale technische voorzieningen van Suwinet beheerd worden.
Suwinet	Set van afspraken, regelgeving, overlegorganen en het fysieke netwerk dat de netwerken van Suwi-partijen koppelt, om zo een gestroomlijnde gegevensuitwisseling mogelijk te maken. Zie voor de wettelijke omschrijving van Suwinet artikel 1, onder p. jo. Artikel 62, tweede lid, van de Wet structuur uitvoeringsorganisatie werk en inkomen.
Suwinet-Inkijk	Het geheel van systemen dat medewerkers van Suwi-partijen online inzicht verschaft in relevante, door Suwi-partijen geregistreerde gegevens van hun cliënten.
Suwinet-Inlezen	Het geheel van systemen waarmee inlezende applicaties via XML-berichten gegevens kunnen ophalen met als doel deze in de eigen applicatie(s) op te nemen.
Suwinet-Mail	Dienst met als doel dat ‘secure mail’ tussen partijen kan worden

	verzonden.
Suwinet-Meldingen	Gestandaardiseerde elektronische gegevensoverdracht tussen Suwi-partijen voor bijvoorbeeld een vooraankondiging WW of reïntegratieadvies. Ook wel elektronische ketenberichten genoemd.
SUWI-organisaties	De organisaties die deel uitmaken van de keten van werk en inkomen: UWV, GSD, Inlichtingenbureau, BKWI, SVB en de Nederlandse Arbeidsinspectie Ook wel ketenpartners genoemd.
SUWI-partijen	De Suwi-organisaties die partij zijn in de Service Level Agreement.
Underpinning contracts	Overeenkomsten op het gebied van onderhoud en beheer, waarin afspraken zijn vastgelegd die deze SLA ondersteunen.
Wet Suwi	Wet structuur uitvoeringsorganisatie werk en inkomen. Via deze wet is de samenwerking tussen de partijen op het gebied van 'Werk en Inkomen' en de elektronische gegevensuitwisseling geregeld.
Wijzigingsbeheer	Het gecontroleerd doorvoeren van noodzakelijke wijzigingen en het voorkomen van verstoringen als gevolg van die wijzigingen.