**PROTOCOL DATALEKKEN**

**Procesgang rondom (mogelijke) datalekken bij Stichting Landschapsbeheer Zeeland.**

# Inhoudsopgave



# Bijlagen:

Bijlage 1 Formulier voor melding datalek
Bijlage 2 "De meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels" van de AP
Bijlage 3 lijst met verantwoordelijke medewerkers per 1 juli 2017 (alleen intern)

# Documentstatus:

Status definitief
Datum 15 juni 2017
Auteur: Ewoud Voogd

# 1. Doel

Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. Sindsdien geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.
De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt.

Deze procedure beschrijft hoe te handelen binnen Stichting Landschapsbeheer Zeeland, indien er sprake is van een datalek of wanneer een datalek vermoed wordt. De meldplicht is eveneens van toepassing op Stichting Landschapsbeheer Zeeland als het datalek bij een derde is ontstaan, indien deze derde in opdracht van SLZ persoonsgegevens bewerkt.
Deze procedure is mede gebaseerd op de beleidsregels van de AP inzake de meldplicht datalekken in de Wet bescherming persoonsgegevens.

Per gemeld datalek behoudt het MT van Stichting Landschapsbeheer Zeeland de vrijheid te beoordelen of de procedure gevolgd kan worden, danwel afwijking van deze procedure gerechtvaardigd is.

Het doel van deze procedure is vast te leggen, welke stappen genomen moeten worden door Stichting Landschapsbeheer Zeeland bij het vermoeden van of kennis nemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek.

Het volgende resultaat wordt hiermee nagestreefd:
- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van Stichting Landschapsbeheer Zeeland, het individu dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk) datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde (mogelijk) datalek.

In de procedurebeschrijving zijn de te doorlopen stappen verwoord.

# 2. Definities

***AP***
Autoriteit Persoonsgegevens, de nieuwe naam van het College Bescherming Persoonsgegevens (CBP) m.i.v. 1-1-2016.

***Bestand***
Elk gestructureerd geheel van persoonsgegevens (op papier als digitaal, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze), dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen (artikel 1c, Wbp).

***Betrokkene***
Degene op wie een persoonsgegeven betrekking heeft (artikel 1f, Wbp).

***Beveiligingslek***
Een inbreuk op de beveiliging (zoals bedoeld in artikel 34a, lid 1, Wbp) waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een datalek.

***Bewerker***
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1e, Wbp)

***Datalek***
Een inbreuk op de beveiliging (zoals bedoeld in artikel 34a, lid 1, Wbp) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 13, Wbp) bescherming moesten bieden.

***Derden***
De bij het incident betrokken externe partij, anders dan betrokkene. Bv. een bewerker van persoonsgegevens t.b.v. Stichting Landschapsbeheer Zeeland.

***Genodigden***
Interne betrokkenen die uitgenodigd zijn bij de bespreking(en) van het incident bij het MT van Stichting Landschapsbeheer Zeeland.

***Incident***
Een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een incident, niet ieder incident is een datalek.

***Persoonsgegeven***
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon Wbp (artikel 1a, Wbp).

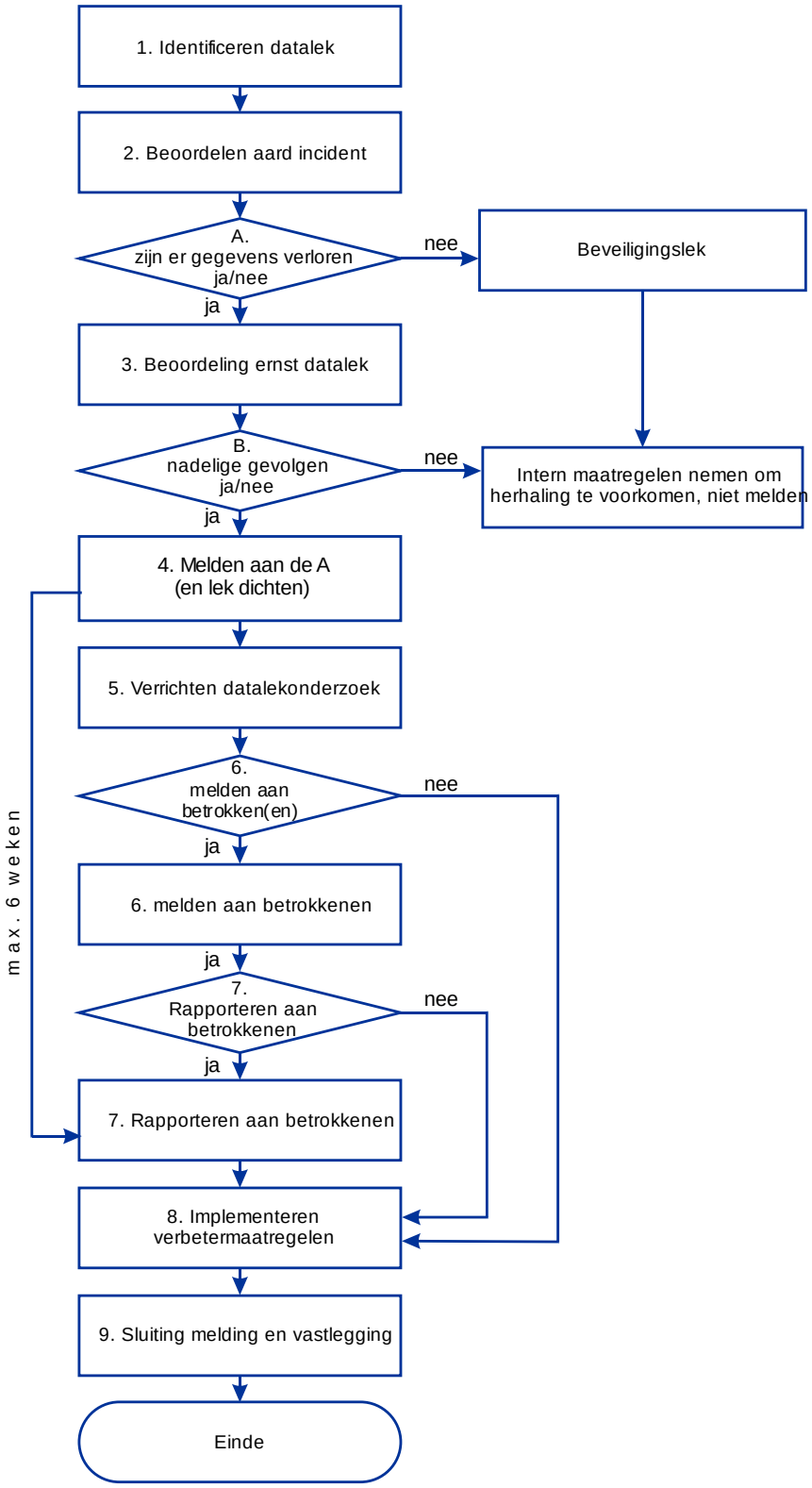
***Wbp***
Wet bescherming persoonsgegevens.

***Verantwoordelijke***
De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1d, Wbp).

***Verwerking van persoonsgegevens***
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1b, Wbp).

# 3. Toepassingsgebied
Deze procedure wordt gehanteerd bij het melden en afhandelen van (mogelijke) datalekken bij Stichting Landschapsbeheer Zeeland, dan wel van (mogelijke) datalekken die buiten Stichting Landschapsbeheer Zeeland hebben plaatsgevonden, doch waarvoor Stichting Landschapsbeheer Zeeland als verantwoordelijke wel de eindverantwoordelijkheid draagt (bv. bij een Bewerker).

# 4. Werkwijze
Ten behoeve van het totaal overzicht is een processchema opgesteld. Vervolgens wordt specifieke informatie per processtap over de te verrichten activiteiten en bijbehorende verantwoordelijkheden en bevoegdheden uitgewerkt.




Stappenplan datalekken

### 4.1. Identificeren van een datalek
De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij een medewerker automatisering en de directe leidinggevende. Deze melden het incident per omgaande aan het MT.

De procedure Meldplicht Datalekken wordt dan gestart.

### 4.2. Beoordeling aard incident; datalek ja/nee
Een medewerker automatisering bespreekt met de medewerker die een (mogelijk) datalek heeft geconstateerd welk soort gegevens eventueel zijn kwijtgeraakt of op een andere manier in het bezit van personen of organisaties zijn gekomen voor wie de bedoelde gegevens niet bestemd waren. Aan de hand van dit gesprek wordt bepaald of het een datalek betreft of niet. In geval van twijfel wordt het voorval met een MT-lid besproken. Als het betreffende bestand persoonsgegevens bevat is het een datalek.

### 4.3. Beoordeling ernst datalek: nadelige gevolgen ja/nee
(Een lid van) het MT beoordeelt samen met een medewerker nautomatisering of het betreffende bestand gegevens bevat welke een persoon of organisatie kunnen schaden. Het maakt hierbij niet uit of de personen bij Stichting Landschapsbeheer Zeeland werkzaam zijn of niet.
Tevens kan in dit overleg worden beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen. Tevens kan worden beoordeeld of het datalek meldingsplichtig is voor de politie in geval van vermoeden van een strafbaar feit.
De beoordeling of er sprake is van een incident, dat gemeld moet worden aan de AP kan tot stand komen met behulp van de schema's te vinden in de Beleidsregels "Meldplicht datalekken in de Wet bescherming persoonsgegevens" van de AP (zie Bijlage 2).

Bij de beoordeling spelen o.a. een rol:
- is er sprake van verlies van persoonsgegevens; dit houdt in dat Stichting Landschapsbeheer Zeeland deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
- is er sprake van onrechtmatige verwerking van persoonsgegevens; hieronder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging;
- kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid;
- zijn er persoonsgegevens van gevoelige aard gelekt;
    - bijzondere persoonsgegevens conform artikel 16 Wbp;
    - gegevens over de financiële of economische situatie van de betrokkene;
    - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
    - gebruikersnamen, wachtwoorden en andere inloggegevens;

        - gegevens die kunnen worden gebruikt voor (identiteits) fraude;
    - leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen; betrek hierbij factoren als
        - de omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen;
        - de impact van verlies of onrechtmatige verwerking;
- Een medewerker automatisering draagt, in samenspraak met een MT-lid, zo spoedig mogelijk zorg voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier t.b.v. melding datalek'.
- In geval geoordeeld wordt, dat sprake is van een (mogelijk) datalek, wordt tevens het communicatietraject richting betrokkene(n) en indien van toepassing de bewerker besproken;
- In geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Melding aan de AP is dan niet aan de orde. Wel kan in het overleg besloten worden, dat het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen.

### 4.4. Melden aan de Autoriteit Persoonsgegevens

- Een door het MT aangewezen persoon, meestal een medewerker automatisering, verzorgt de tijdige (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. Dit met inachtneming van richtlijnen van de AP terzake. De aangewezen persoon fungeert als contactpersoon inzake de communicatie naar de AP. Dit geldt ook ingeval nog niet duidelijk is dat het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken.
- Een MT-lid is regievoerder over de interne afhandeling van het (mogelijke) datalek in al zijn facetten, over de externe afhandeling, waaronder het AP, betrokkenen en bewerker.
- Het MT draagt ervoor zorg dat de bij het incident betrokken medewerkers worden geïnformeerd. Het MT zorgt ervoor dat de betrokken medewerkers bij het incident, het mogelijke datalek, zo snel mogelijk een eigen verslag opstellen over de toedracht van het incident. In ernstige gevallen wordt de schriftelijke informatie aan het bestuur van Stichting Landschapsbeheer Zeeland verstrekt.
- De AP zal na het melden van een datalek een ontvangstbevestiging sturen. Alleen indien de melding daartoe aanleiding geeft zal de AP contact opnemen.
- Bij een datalek als gevolg van een (niet-ethische) hack (art. 138ab van het Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico’s van misbruik voor de betrokkene(n) zijn. Bij een hack ligt naast melding bij de AP, ook aangifte bij de politie in de rede in verband met de opsporing van de daders. Aangifte loopt via een eventueel beschikbare contactfunctionaris richting politie.

## 4.5. Verrichten datalek onderzoek

- Een MT-lid of een door het MT aangewezen persoon stelt in overleg met een medewerker automatisering, eventueel in overleg met de externe netwerkbeheerder, binnen de gestelde termijn een (systematisch) (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek.
- Een MT-lid of de door het MT aangewezen persoon onderzoekt samen met de medewerker automatisering verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen (het vermijdbaarheidsaspect).
- De bevoegdheden van het MT-lid of de door het MT aangewezen persoon zijn:
  - de mogelijkheid met iedereen te spreken;
  - alle relevante documenten in te zien;
  - toegang te hebben tot alle plaatsen. Dit alles in het kader van wat het MT nodig acht ten behoeve van een zorgvuldige analyse;
  - in relatie tot de externe bewerker gelden de afspraken zoals vastgelegd in de bewerkersovereenkomst
- Het MT-lid of de door het MT aangewezen persoon heeft binnen 4 weken na de melding bij de AP het onderzoek afgerond.
- Het MT-lid of de door het MT aangewezen persoon kan besluiten om externe deskundigen te betrekken bij het onderzoek.
- Het MT-lid of de door het MT aangewezen persoon analyseert alle gegevens conform Bijlage 2 Beleidsregels ”Meldplicht datalekken in de Wet bescherming persoonsgegevens” van de AP.
- Het MT-lid of de door het MT aangewezen persoon legt het conceptrapport ter correctie op feitelijke onjuistheden voor aan de interne en externe geïnterviewden.
- Het MT stelt vervolgens het rapport vast.

## 4.6. Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

- Indien een datalek is gemeld aan de AP dient tevens vast gesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat.
- Dit ter beoordeling van en advisering door de Datalekken Commissie. De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van de schema’s te vinden in de beleidsregels ”Meldplicht datalekken in de Wet bescherming persoonsgegevens” van de AP (zie Bijlage 2).
  Bij de beoordeling speelt onder meer een rol:
  - Indien Stichting Landschapsbeheer Zeeland passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven (artikel 34a, lid 6, Wbp). Bij twijfel hierover dient het datalek gemeld te worden aan de betrokkene(n).
  - Het datalek moet aan de betrokkene(n) worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, lid 2, Wbp).
    Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet bijvoorbeeld gedacht worden aan onrechtmatige

publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen. - De melding aan de betrokkene(n) mag achterwege blijven, als daarvoor zwaarwegende redenen aanwezig zijn (artikel 43 Wbp). Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op de belangen die worden genoemd in dit artikel. Op grond van artikel 43, onder e, Wbp mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.

### 4.7. Rapporteren aan de betrokkene(n)

- Een MT-lid of een door het MT aangewezen persoon stelt een kennisgeving aan betrokkene(n) op.
- Het MT bepaalt wat aan de betrokkene(n) wordt gemeld.
- De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van Stichting Landschapsbeheer Zeeland informatiepunt waar de betrokkene(n) meer informatie over de inbreuk kan krijgen, en de maatregelen die Stichting Landschapsbeheer Zeeland de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.
- De betrokkene(n) worden individueel geïnformeerd.
- Indien het datalek gemeld moet worden aan de betrokkene(n) dan mag Stichting Landschapsbeheer Zeeland na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat Stichting Landschapsbeheer Zeeland de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Wel dient hierbij rekening gehouden te worden dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder Stichting Landschapsbeheer Zeeland de betrokkene(n) daarover informeert, hoe eerder deze in actie kan komen.
- In de melding aan de AP is al aangegeven of Stichting Landschapsbeheer Zeeland het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer Stichting Landschapsbeheer Zeeland dat gaat doen. De termijn die Stichting Landschapsbeheer Zeeland in de melding aan het AP aangeeft, moet Stichting Landschapsbeheer Zeeland ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat Stichting Landschapsbeheer Zeeland dit aan de AP weten door middel van een aanpassing van de melding.

### 4.8. Implementeren verbetermaatregelen

- Het MT-lid in wiens domein de verbetermaatregelen liggen is verantwoordelijk dat de vastgestelde verbetermaatregelen worden geïmplementeerd, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering, en rapporteert over de voortgang aan het MT van Stichting Landschapsbeheer Zeeland.
- Indien bij een bewerker verbetermaatregelen nodig zijn, is de manager die opdrachtgever is van deze bewerker daartoe verantwoordelijk.

- Het aangewezen MT-lid bewaakt de voortgang, onder eindverantwoordelijkheid van het gehele MT van Stichting Landschapsbeheer Zeeland.

### 4.9. Sluiten melding en vastlegging

- De directeur informeert het bestuur van Stichting Landschapsbeheer Zeeland op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.
- Het datalek dossier wordt door het MT gearchiveerd voor de duur van minimaal 1 jaar. Er kunnen redenen zijn om gedurende langere tijd te archiveren, de richtlijn zoals beschreven in Bijlage 2 "Meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels" zal worden gehanteerd.

**Bronnen**

Wet bescherming persoonsgegevens
Meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels.

Deze Procedure Meldplicht Datalekken is vastgesteld in de vergadering van het MT van Stichting Landschapsbeheer Zeeland d.d. 04-07-2017

Handtekening .....