

Gemeente Brunssum

**PROCEDURE MELDPLICHT DATALEKKEN**

Procesgang rondom (mogelijke) datalekken in gemeente Brunssum

Versie 1.0

23 maart 2017

### Documentbeheer

Versie	Datum	Actie	Auteur	Revisie
v.0.1	08-11-2016	Opstellen procedure meldplicht datalekken	Ton Rittimon	
v.0.2	18-12-2016	Opmerkingen / aanpassingen uitgevoerd	Jos Boeren	
v.0.3	05-01-2017	Spelling- en grammaticacon- trole uitgevoerd. Layout aan- gepast.	Ton Rittimon	
v.0.4	10-01-2017	Opmerkingen van Wim Reumkens, Johan Demartean en Willem Spelthan verwerkt in samenwerking met Jos Boe- ren.	Ton Rittimon	
v.0.5	31-01-2017	Opmerkingen van Willem Spelthan verwerkt. Meldings- formulier toegevoegd aan de procedure.	Ton Rittimon	
v.1.0	23-3-2017	Finaliseren van de rapportage	Ton Rittimon	

### Geaccordeerd door

Versie	Datum	Naam	Paraaf

## Samenvatting

Vanaf 1 januari 2016 is met de Meldplicht Datalekken een wijziging in de Wet bescherming persoonsgegevens (Wbp) van kracht en kan de Autoriteit Persoonsgegevens (AP) substantiële boetes (tot 820.000 per incident) opleggen indien een datalek niet of niet tijdig is aangemeld. Om aan de Wbp te voldoen op het gebied van datalekken heeft de gemeente Brunssum maatregelen getroffen, zoals beschreven in dit document.

Een datalek is een beveiligingsincident waarbij het gaat om persoonsgegevens van gevoelige aard, of er is om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens. Afhankelijk van de aard en omvang dient het datalek gemeld te worden bij de Autoriteit persoonsgegevens en betrokkenen. Afwegingen die hierbij gemaakt moeten worden zijn:

- Is er een beveiligingslek, zo ja
- Heeft het beveiligingslek geleid tot een beveiligingsincident?
- Zijn er bij het beveiligingsincident persoonsgegevens verloren gegaan of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten? Zo ja dan datalek.
- Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van verwerkte persoonsgegevens? Zo ja dan melden aan Autoriteit Persoonsgegevens.
- Waren niet alle gelekke gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Zo ja melden aan betrokkene.

Binnen de gemeente Brunssum is deze procedure opgesteld om adequaat te kunnen handelen in geval van een mogelijk datalek. Een korte samenvatting van de meldingsprocedure binnen de gemeente Brunssum is als volgt:

Alle beveiligingsincidenten en datalekken worden door de Informatiebeveiliging functionaris (IBF) vastgelegd in TOPDESK. Van beveiligingsincidenten categorie 2 of hoger en datalekken die worden gemeld bij de Autoriteit persoonsgegevens, zal door de IBF respectievelijk de functionaris Gegevensbescherming (FG) binnen 6 weken na ontdekking een rapportage worden opgesteld met onder andere lessons learned.

## Inhoudsopgave

1. Inleiding .....	4
1.1 Randvoorwaarden.....	4
1.2 Definities: .....	4
2 Wat is een datalek?.....	5
3. Procedure datalek incident Brunssum .....	8
3.1. Doelstelling .....	9
3.2 Wat te doen bij een datalek? .....	9
3.2.1 Medewerker.....	9
3.2.2 Afdelingshoofd.....	10
3.2.3 Informatiebeveiliging functionaris (IBF) .....	10
3.2.4 Functionaris Gegevensbescherming (FG).....	10
3.2.5 Directie .....	10
3.3 Flowchart Meldplicht datalekken IBF en FG.....	10
4. Organisatie bij datalek.....	11
4.1. Het Incident Response Team (IRT) .....	11
4.2. Het Privacy Response Team (PRT) .....	11
4.3 Taken en verantwoordelijkheden .....	12
5. Rapportage en evaluatie .....	12
Bijlage 1: Toelichting flowchart IBF .....	13
Bijlage 2: Toelichting flowchart FG .....	16
Bijlage 3: beveiliging categorieën.....	21

## **1. Inleiding**

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet bescherming persoonsgegevens (verder te noemen Wbp). Hierin staat dat de organisaties die persoonsgegevens verwerken, deze gegevens moet beveiligen tegen verlies en tegen onrechtmatige verwerking (artikel 13 Wbp). Vanaf 1 januari 2016 is met de Meldplicht Datalekken een wijziging in de Wbp van kracht en kan de Autoriteit Persoonsgegevens (verder te noemen AP) substantiële boetes opleggen indien een datalek niet of niet tijdig is gemeld aan de AP als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, eerste lid, Wbp). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp).

Om aan de Wbp te voldoen op het gebied van datalekken heeft de gemeente Brunssum maatregelen getroffen, zoals beschreven in onderhavig document.

### **1.1 Randvoorwaarden**

Onderhavig document is in eerste instantie gericht op de verplichtingen voortvloeiende uit de Meldplicht datalekken. Omdat datalekken onlosmakelijk verbonden zijn met beveiligingsincidenten wordt in onderhavig document, waar mogelijk, aansluiting gezocht bij algemene beveiligingsbeleid van de gemeente Brunssum (Verseon kenmerk 660439, augustus 2016). Daarnaast heeft de AP-beleidsregels “De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)” (Verseon kenmerk 660380, december 2015) opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de AP en eventueel aan de betrokkene.

### **1.2 Definities:**

**Persoonsgegevens;** Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

**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.

**Bestand:** Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

**Verantwoordelijke:** De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt.

**Bewerker:** Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

**Betrokkene:** Degene op wie een persoonsgegeven betrekking heeft.

**Derde:** Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te bewerken.

**Ontvanger:** Degene aan wie de persoonsgegevens wordt verstrekt.

## **2 Wat is een datalek?**

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan.

Voorbeelden van beveiligingsincidenten zijn:

- Het kwijtraken van een USB-stick;
- He diefstal van een laptop;
- Een inbraak door een hacker;
- Een malware besmetting;
- Een calamiteit zoals brand in het datacentrum.
- Persoonsgegevens bij oud papier gezet;
- Per ongeluk gepubliceerde persoonsgegevens ;
- Persoonsgegevens verstuurd via e-mail aan verkeerd geadresseerde.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitgesloten kan worden en leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft door de FG dan geen melding te worden gedaan aan de AP en/of betrokkene.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp. Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens

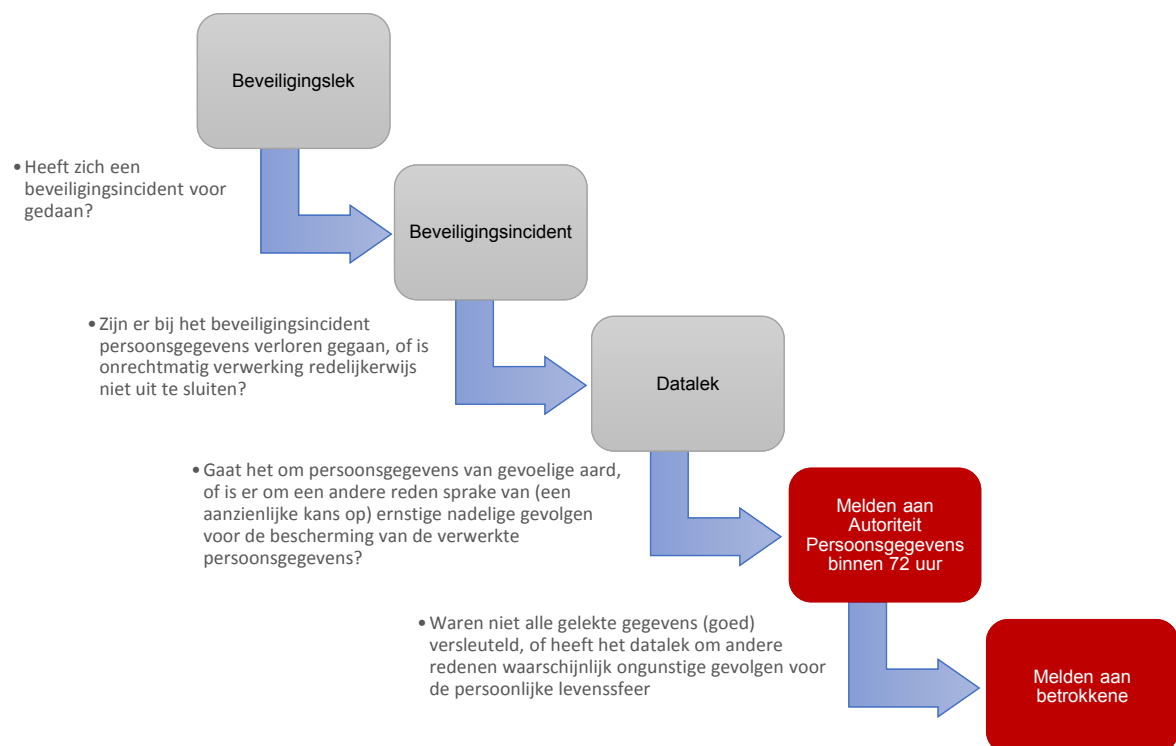
toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservice Nummer (BSN).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat u een datalek moet melden waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

In bepaalde gevallen moet de gemeente Brunssum ook de betrokkenen informeren over het datalek. Dat zijn de personen, zoals werknemers en burgers, van wie persoonsgegevens worden verwerkt. Ook hierbij hangt het van de ernst van het datalek af of dit wel of niet moet gebeuren. De betrokkenen worden alleen geïnformeerd als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.

De melding aan de betrokkenen mag eventueel achterwege worden gelaten als passende technische beschermingsmaatregelen zijn getroffen, waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden (bijvoorbeeld door versleuteling). Communicatie naar betrokkenen dient zorgvuldig uitgevoerd te worden.



**Figuur 1: Afweging meldingsprocedure.**

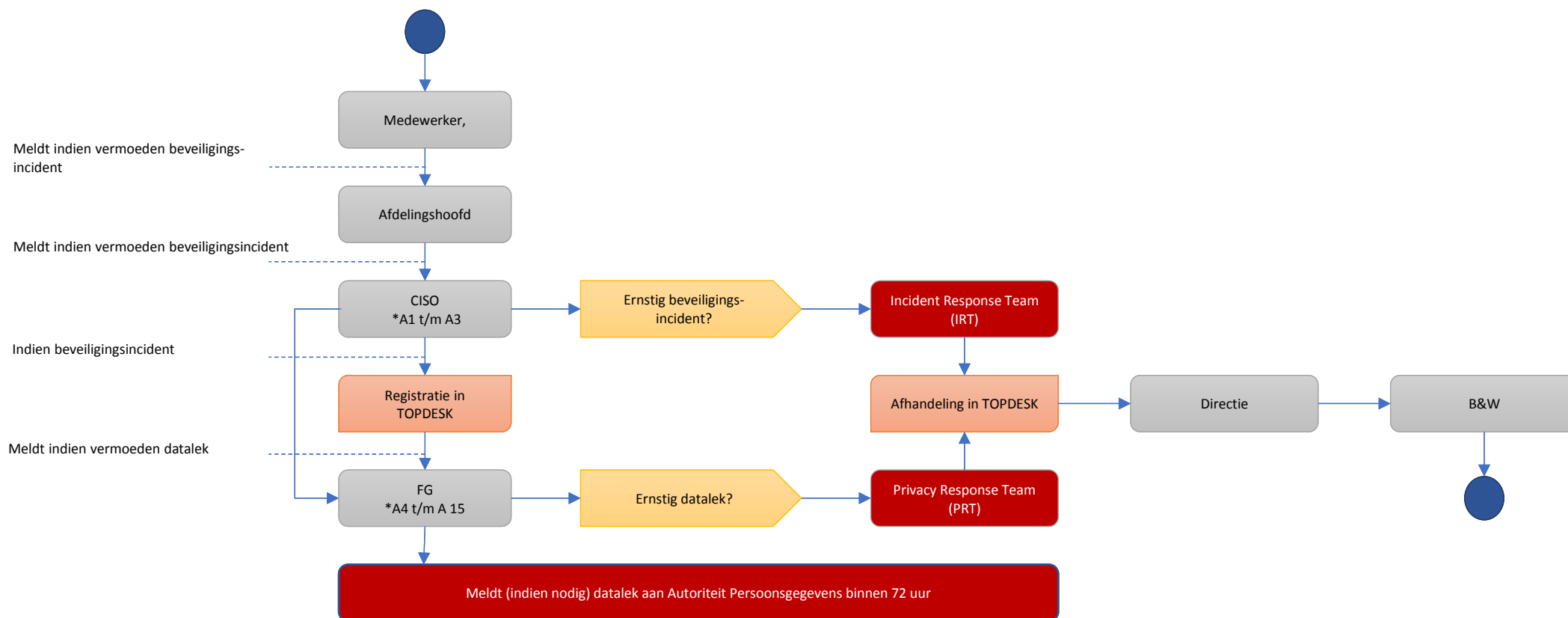
Voorbeelden van datalekken welke gemeld moeten worden bij de AP zijn:

- Binnen de gemeente wordt gesignaleerd dat door een haperende beveiliging (technische storing) medische gegevens zijn ingezien door onbevoegden;

- Een journalistiek programma confronteert de gemeente met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen, bankgegevens en wachtwoorden) van werknemers op de server van de gemeente door onbevoegden zijn ingezien;
- Een medewerker verliest een laptop met onversleutelde, financiële klantgegevens;
- Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens.
- Een medewerker van de gemeente heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens kon komen.
- Een envelop met bijzondere persoonsgegevens (godsdienst en levensovertuiging, ras, gezondheid, seksuele geaardheid, lidmaatschap vakvereniging) van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstreekte ze aan andere personen.
- De gemeente biedt de gebruikers de mogelijkheid om details van hun gemeenteaccount te zien. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd.
- Een medewerker verstuurt een e-mail met bijlage (niet geëncrypt) met gevoelige informatie over probleemgezinnen naar een verkeerde groep (personen).



### 3. Procedure datalek incident Brunssum



- Bijlage 1

Afbeelding 2. Flowchart rol bij een datalek melding binnen de gemeente Brunssum

### 3.1. Doelstelling

De doelstelling is om in het geval van een geconstateerd datalek van persoonsgegevens, tijdig (binnen 72 uur) en zo volledig mogelijk de vereiste informatie aan de AP aanleveren om boetes of andere materiële en immateriële schade zoveel mogelijk te voorkomen.

### 3.2 Wat te doen bij een datalek?

#### 3.2.1 Medewerker

Indien een medewerker een beveiligingsincident en/of datalek constateert of het vermoeden heeft dat er sprake is van een beveiligingsincident en/of datalek, neemt hij/zij direct, uiterlijk binnen 4 uur telefonisch contact op met zijn/haar direct leidinggevende. Het afdelingshoofd bepaalt of het incident gemeld moet worden bij de IBF. Indien het afdelingshoofd niet bereikbaar is, meldt de medewerker het incident telefonisch rechtstreeks bij de IBF. Indien de IBF niet bereikbaar is, zal de betreffende medewerker telefonisch contact opnemen met de FG.

De medewerker dient daarbij, zoveel mogelijk de onderstaande gegevens te overleggen:

- Samenvatting van het beveiligingsincident;
- De aard van het beveiligingsincident; Lezen(vertrouwelijkheid), kopiëren, veranderen (integriteit), verwijderen of vernietigen (beschikbaarheid), diefstal, nog niet bekend.
- De data en/of tijdvakken van het beveiligingsincident; Het (vooralsnog bekende en/of redelijkerwijs te verwachten) negatieve gevolg van het beveiligingsincident;
- Zijn er al maatregelen getroffen om het beveiligingsincident te stoppen en/of de negatieve gevolgen te beperken.

De (vermoedelijke) hoeveelheid personen van wie persoonsgegevens betrokken zijn bij het beveiligingsincident (min –max en omschrijving van de groep mensen);

- De aard van de persoonsgegevens die betrokken zijn bij het beveiligingsincident;
  - Naam-, adres- en woonplaatsgegevens
  - Telefoonnummers
  - E-mailadressen of andere adressen voor elektronische communicatie
  - Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)
  - Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
  - Burgerservicenummer (BSN) of sofinummer
  - Paspoortkopieën of kopieën van andere legitimatiebewijzen
  - Geslacht, geboortedatum en/of leeftijd
  - Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
  - Overige gegevens, namelijk (vul aan)
- De (vermeende) oorzaak van het beveiligingsincident;
- Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?
  - Stigmatisering of uitsluiting
  - Schade aan de gezondheid
  - Blootstelling aan (identiteits)fraude
  - Blootstelling aan spam of phishing
  - Anders, namelijk (vul aan)

### 3.2.2 Afdelingshoofd

Het afdelingshoofd beoordeelt direct de melding. Indien de afdelingshoofd constateert of het vermoeden heeft dat er sprake is van een beveiligingsincident en/of datalek, neemt de leidingafdelingshoofd direct contact op met de IBF. Indien de IBF niet bereikbaar is, meldt het afdelingshoofd het incident rechtstreeks bij de FG.

### 3.2.3 Informatiebeveiliging functionaris (IBF)

- De IBF meldt het beveiligingsincident in het registratiesysteem TOPDESK;
- De IBF bepaalt de ernst van de melding en beslist of het een beveiligingsincident en/of datalek is en of er verdere actie nodig is;
- Indien beveiligingsincident categorie 2 of hoger (zie bijlage 2) richt de IBF een Incident Response Team (IRT) in om ervoor te zorgen dat de schade beperkt blijft;
- De IBF licht, bij het inrichten van een IRT, direct de directie in;
- Indien het naast een beveiligingsincident tevens een datalek is, neemt de IBF direct contact op met de FG.

In de flowchart zijn de taken van de IBF verder uitgewerkt (bijlage 1)

### 3.2.4 Functionaris Gegevensbescherming (FG)

- De IBF overlegt met de FG of het beveiligingsincident tevens een datalek is;
- Indien beveiligingscategorie 2 of hoger (zie bijlage 2) en het datalek betreft persoonsgegevens richt de FG een Privacy Response Team (PRT) in om ervoor te zorgen dat de AP tijdig (doch uiterlijk binnen 72 uur) worden geïnformeerd;
- De FG licht, bij het inrichten van een PRT, direct de directie in;
- Afhankelijk van aard en omvang datalek worden naast de AP, de betrokkenen geïnformeerd;
- Indien het qua tijd niet mogelijk is om eerst overleg te hebben met PRT doet de FG zelfstandig een melding aan de AP.

In de flowchart zijn de taken van de FG verder uitgewerkt (bijlage 2)

### 3.2.5 Directie

- Indien er een incident is vastgesteld van beveiligingscategorie 2 of hoger en er wordt een IRT en/of PRT geformeerd, dan wordt de directie per direct geïnformeerd door de IBF en/of FG;
- De directie informeert de betrokken B&W over het datalek.

## 3.3 Flowchart Meldplicht datalekken IBF en FG

Op grond van artikel 34a Wbp dient een datalek, dat voldoet aan bepaalde specificaties, gemeld te worden aan AP en/of betrokkenen. Onderhavige flowchart en activiteitenlijst zullen te allen tijde door de IBF en FG als leidraad voor de melding van een datalek gehanteerd worden.

De onderhavige flowchart bestaat uit een aantal opeenvolgende vragen die beantwoord moet worden voordat een datalek melding aan de Autoriteit Persoonsgegevens kan worden gedaan. In de flowchart staan verwijzingen naar de activiteitenlijst in bijlage 1,2 en de beleidsregels van de AP<sup>1</sup>. In de activiteitenlijst is weergegeven welke acties uitgevoerd moeten worden en wie voor de uitvoering verant-

---

<sup>1</sup> De meldplicht datalekken in de Wbp: beleidsregels voor toepassing van art. 34a Wbp" Autoriteit persoonsgegevens, 8 december 2015

woordelijk is. De beleidsregels voor toepassing van artikel 34a Wbp worden gebruikt ter verduidelijking van de vragen in de flowchart.

De IBF en de FG dienen kennis te nemen van de crisisplannen en procedures omtrent crisiscommunicatie. (Vooraf) overleg bij de PR/Communicatieafdeling is hiervoor noodzakelijk, met name wanneer naar betrokkenen moet worden gecommuniceerd.

De toelichting en flowchart worden weergegeven in bijlage 1 en 2.

## **4. Organisatie bij datalek**

Bij een beveiligingsincident en/of datalek zijn, indien noodzakelijk, twee teams betrokken:

- Het Incident Response Team;
- Het Privacy Response Team.

### **4.1. Het Incident Response Team (IRT)**

Het IRT richt zich op (beveiligings)incidenten en handelt zoals beschreven in de (beveiligings) incidenten procedure. De IRT heeft als doelstelling de schade te beperken bij een beveiligingsincident. Bij een (mogelijk) datalek streeft het IRT ernaar de schade te beperken door het beveiligingsincident binnen de daarvoor gestelde tijdslijnen op te lossen en een (mogelijk) datalek te melden bij de FG.

De IBF is de spil in het IRT en vervult een coördinerende en controlerende rol bij een melding. Het IRT bestaat daarom uit enkele vaste leden en, afhankelijk van het type datalek, uit wisselende leden.

#### Vaste leden:

- De IBF (coördinatie);
- Medewerkers van de afdeling Informatiemanagement belast met applicatiebeheer, coördinatoren Informatiemanagement, Hoofd Informatiemanagement. Medewerkers van Parkstad-IT

#### Wisselende leden:

- Medewerkers van getroffen afdeling of proceseigenaar;
- De FG;
- Communicatie/persvoorlichter (interne en externe communicatie);
- Adviseur Facilitaire Zaken (indien sprake van inbreuk fysieke beveiliging);
- Leidinggevend (proceseigenaar, indien meerdere processen, hoger leidinggevende);

### **4.2. Het Privacy Response Team (PRT)**

Het PRT dient ingelicht te worden bij een mogelijk privacy incident. Het PRT richt zich op een goede afhandeling van meldingen aan de AP en betrokkenen in geval van een datalek en/of andere crisissituatie binnen de gemeente Brunssum op het gebied van privacy. Daarnaast draagt het PRT ook zorg voor het na-traject van een datalek in de herstelfase. Herstel na een datalek is gericht op:

- Lessons learned;
- Het leveren van nazorg aan betrokkenen door hen ondersteuning te bieden bij het beperken van eventuele schadelijke gevolgen;
- Het opkomen voor het organisatiebelang. Dit betreft het afleggen van verantwoording en, indien van toepassing, het afhandelen van schadeclaims en boetes.

De FG is de spil in het PRT en vervult een coördinerende en controlerende rol bij een melding. Het PRT bestaat daarom uit enkele vaste leden en, afhankelijk van het type datalek, uit wisselende leden.

#### Vaste leden:

- De FG (coördinatie);
- De IBF (ondersteuning);
- De proceseigenaar en/of melder; - de juridische afdeling.

#### Wisselende leden:

- Hoofd Informatiemanagement, Coördinatoren Informatiemanagement, Applicatiebeheerders Informatiemanagement, Medewerkers Parkstad-IT
- De communicatieadviseur (interne en externe communicatie);
- Adviseur Facilitaire Zaken (indien sprake van inbreuk fysieke beveiliging);
- Leidinggevend(en) proceseigenaar, indien meerdere processen, hoger leidinggevend(e);
- Medewerkers afdeling Financiën en Controlling inzake risicomanagement

### **4.3 Taken en verantwoordelijkheden**

Binnen de gemeente kunnen beveiliging, privacy en melding datalekken niet los van elkaar gezien worden. In onderstaand schema worden daarom naast de taken en verantwoordelijkheden vanuit de meldplicht datalekken tevens specifiek beveiligingsincidenten weergegeven.

Proces	Directie	IBF	FG	Afdelingshoofd	Communicatieadviseur
Beveiligingsincident	V	P	C	C	I
Datalek incident	V	C	P	C	C

Tabel 1. Taken en verantwoordelijkheden

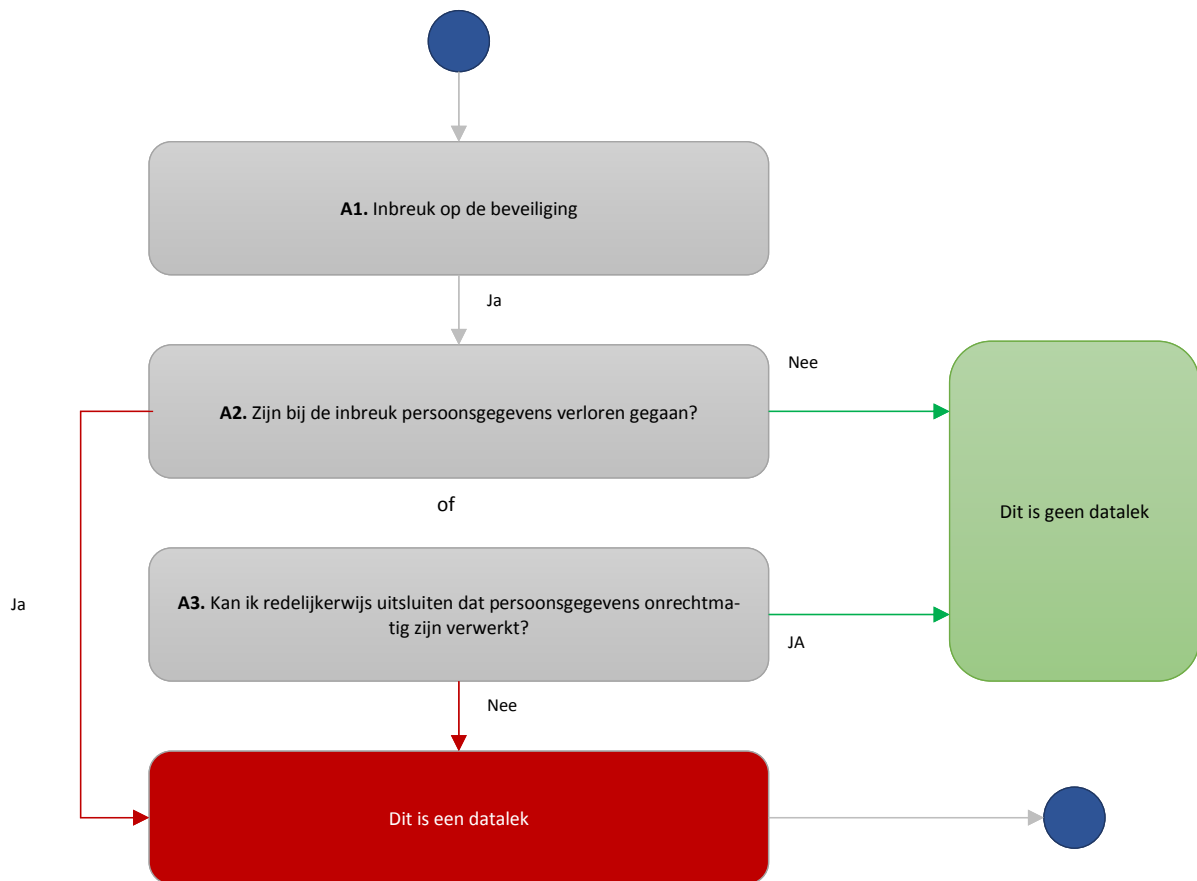
- V: Eindverantwoordelijk  
P: Proces verantwoordelijk  
C: Consulterend  
I: Geïnformeerd

## **5. Rapportage en evaluatie**

Alle beveiligingsincidenten en datalekken worden door de IBF vastgelegd in TOPDESK. Van beveiligingsincidenten categorie 2 of hoger en datalekken die worden gemeld bij de Autoriteit persoonsgegevens, zal door de IBF respectievelijk de FG binnen 6 weken na ontdekking een rapportage te worden opgesteld waarin minimaal moet worden meegenomen:

- Aard en omvang incident;
- Getroffen maatregelen om incident te verhelpen;
- Evaluatie IRT en/of PRT
- Lessons learned;
- Genomen procedurele, organisatorische of technische maatregelen om herhaling te voorkomen.

## Bijlage 1: Toelichting flowchart IBF



Afbeelding 3. Flowchart IBF m.b.t. datalek

### Activiteit 1 – Inbreuk beveiliging

Act. 1	Toelichting	Uitvoerend
	<p>Er heeft een inbreuk op de beveiliging plaatsgevonden.</p> <p><u>IBF</u></p> <ul style="list-style-type: none"> <li>beoordeelt de melding;</li> <li>heeft vastgesteld dat er sprake is van een beveiligingsincident aan de hand van de beveiligingsincident categorie 0-4;</li> <li>verzamelt informatie;</li> <li>treft maatregelen om het beveiligingsincident te stoppen om schade te beperken;</li> <li>stelt gegevens veilig;</li> <li>registreert de melding in het registratiesysteem TOPDESK;</li> <li>start een IRT op indien de beveiligingscategorie 2 of hoger en stuurt het IRT aan;</li> <li>escaleert het incident, indien beveiligingscategorie 2 of hoger naar de directie.</li> </ul>	IBF
	Verwijzing in het document “De meldplicht datalekken in Wbp:	§3.1

	beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	
--	---	--

#### Activiteit 2 – Controle op bezit van verloren persoonsgegevens

Act. 2	Toelichting	Uitvoerend
	<p>Er dient gecontroleerd te worden of de gegevens, en in het bijzonder persoonsgegevens, nog in het bezit zijn van de gemeente en/of derden, vernietigd zijn of op enige andere wijze verloren zijn gegaan. Ook wordt gecontroleerd of de gegevens zijn aangetast, of dat er sprake is van onbevoegde kennisneming of verstrekking.</p> <p><u>IBF:</u></p> <ul style="list-style-type: none"> <li>▪ vergaart nadere informatie met betrekking tot de blootgestelde gegevens;</li> <li>▪ controleert of mogelijke persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking;</li> <li>▪ delegeert taken om informatie te vergaren;</li> <li>▪ consulteert medewerkers om informatie te vergaren;</li> <li>▪ bepaalt aan de hand van vergaarde informatie of er sprake is van een verlies of vernietiging van persoonsgegevens;</li> <li>▪ stelt de FG direct op de hoogte van een mogelijke datalek en voorziet de FG van gedetailleerde informatie.</li> </ul> <p><u>IRT:</u></p> <ul style="list-style-type: none"> <li>▪ neemt maatregelen om de impact van het incident te beperken aan de hand van procedures (incident management procedure);</li> <li>▪ stelt overlegstructuur en taakverdeling vast.</li> </ul>	<p>IBF</p> <p>IRT</p>
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§3.2

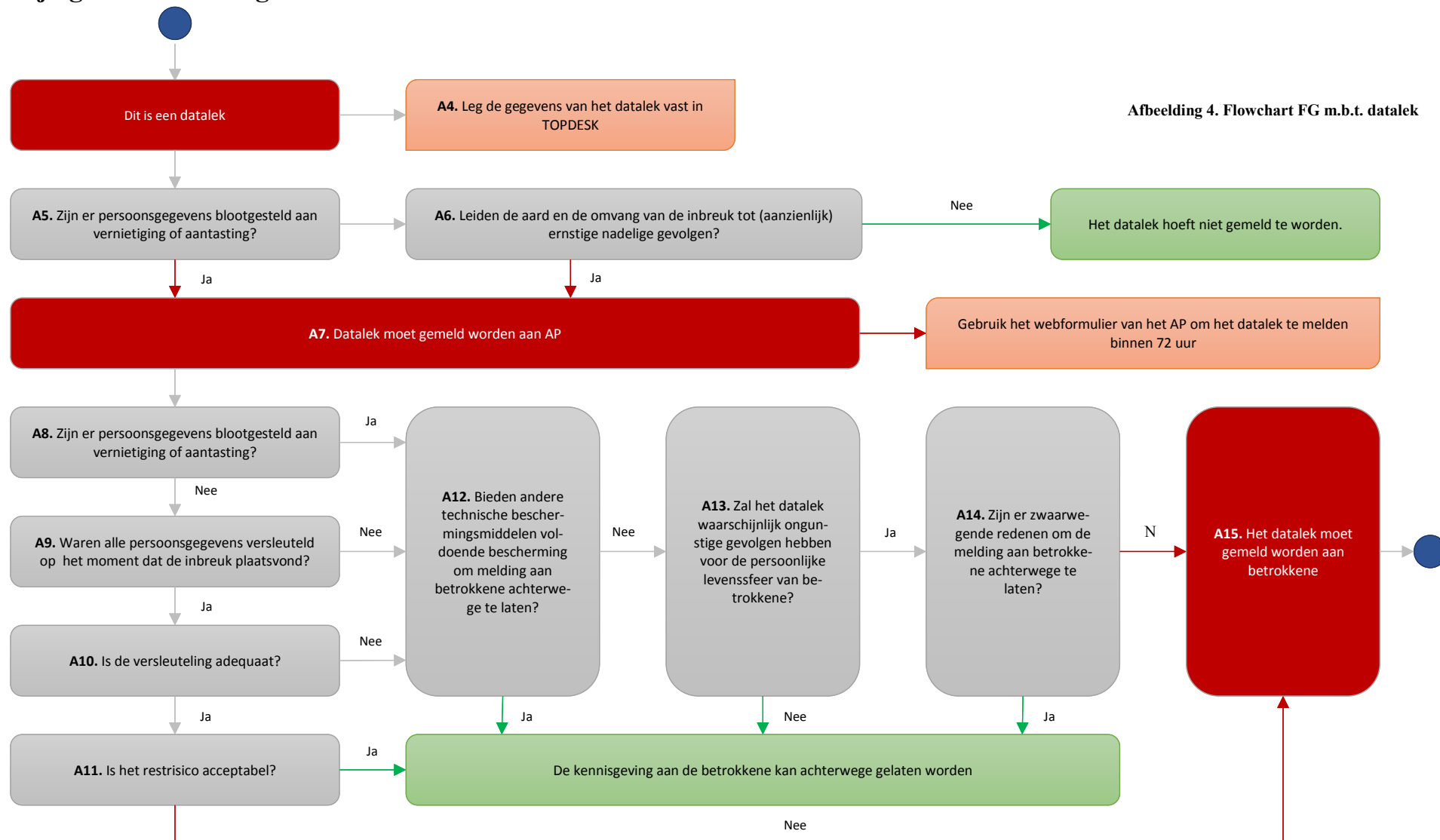
#### Activiteit 3 – Beoordeling onrechtmatige verwerking persoonsgegevens

Act. 3	Toelichting	Uitvoerend
	<p>Er dient beoordeeld te worden of redelijkerwijs uitgesloten kan worden dat persoonsgegevens onrechtmatig zijn verwerkt.</p> <p><u>IBF:</u></p> <ul style="list-style-type: none"> <li>▪ vergaart nadere informatie met betrekking tot de blootgestelde gegevens;</li> <li>▪ controleert of mogelijke persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking;</li> <li>▪ delegeert taken om informatie te vergaren;</li> <li>▪ consulteert medewerkers om informatie te vergaren;</li> <li>▪ bepaalt aan de hand van vergaarde informatie of er sprake is</li> </ul>	<p>IBF</p>

	<p>van een verlies of vernietiging van persoonsgegevens;</p> <ul style="list-style-type: none"> <li>▪ stelt de FG direct op de hoogte van een mogelijke datalek en voorziet de FG van gedetailleerde informatie.</li> </ul> <p><u>IRT:</u></p> <ul style="list-style-type: none"> <li>▪ neemt maatregelen om de impact van het incident te beperken aan de hand van procedures (incident management procedure);</li> <li>▪ stelt overlegstructuur en taakverdeling vast.</li> </ul>	IRT
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015 en Art 6-24 Wbp (Voorwaarden voor de rechtmatigheid van verwerking van persoonsgegevens)	§3.3



## Bijlage 2: Toelichting flowchart FG



#### Activiteit 4 – Registratie van gegevens datalek

A4	Toelichting	Uitvoerend
	<p>Per datalek, dat onder de meldplicht valt, worden feiten en gegevens in een overzicht opgenomen.</p> <p>FG legt per datalek in TOPDESK vast (<i>gebruik hiervoor bijlage 4. Meldingsformulier Datalek</i>):</p> <ul style="list-style-type: none"> <li>▪ Aard van de melding;</li> <li>▪ Wettelijk kader van de melding;</li> <li>▪ Gegevens datalek: <ul style="list-style-type: none"> <li>○ Samenvatting incident;</li> <li>○ Aantal betrokkene;</li> <li>○ Aard betrokkene;</li> <li>○ Datum/tijdstip incident;</li> <li>○ Aard van het incident;</li> <li>○ Welke persoonsgegevens;</li> <li>○ Gevolgen persoonlijke levenssfeer</li> </ul> </li> <li>▪ Vervolgactie(s);</li> <li>▪ Inlichten betrokkenen (indien noodzakelijk);</li> <li>▪ Technische beschermingsmaatregelen (o.a. encryptie);</li> <li>▪ Internationale aspecten.</li> </ul>	FG

#### Activiteit 5 – Vaststellen of persoonsgegevens van gevoelige aard zijn gelekt

A5	Toelichting	Uitvoerend
	<p>Indien er sprake is van een datalek, moet gecontroleerd worden of persoonsgegevens van gevoelige aard zijn gelekt.</p> <p><u>FG:</u></p> <ul style="list-style-type: none"> <li>▪ beoordeelt de aard van de gelekte persoonsgegevens;</li> <li>▪ consulteert medewerkers om informatie te vergaren;</li> <li>▪ bepaalt of het datalek aan de AP moet worden gemeld.</li> </ul>	FG
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§4.2.1

#### Activiteit 6 – Beoordeling aard en omvang inbreuk

A6	Toelichting	Uitvoerend
	<p>De aard en de omvang van de inbreuk zijn van invloed op de kans op nadelige gevolgen.</p> <p><u>FG</u></p> <ul style="list-style-type: none"> <li>▪ beoordeelt de aard van de inbreuk;</li> <li>▪ beoordeelt de omvang van de inbreuk;</li> </ul>	FG

	<ul style="list-style-type: none"> <li>▪ consulteert medewerkers om informatie te vergaren;</li> <li>▪ rapporteert / escaleert aan/naar MT-team</li> <li>▪ bepaalt of het datalek aan de AP moet worden gemeld.</li> <li>▪ overlegt met en koppelt terug aan de communicatieadviseur;</li> <li>▪</li> </ul>	
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§4.2.2

#### Activiteit 7 – Melding datalek bij AP

A7	Toelichting	Uitvoerend
	<u>FG:</u> <ul style="list-style-type: none"> <li>▪ Start een PRT op (indien aard en omvang aanzienlijk, beveiligingscategorie 2 of hoger) en stuurt aan;</li> <li>▪ Overlegt en koppelt terug aan de communicatieadviseur;</li> <li>▪ verzamelt informatie met betrekking tot de aan de AP verstrekken informatie;</li> <li>▪ bewaakt meldingstermijn en meldt het datalek <b><u>uiterlijk 72 uur</u></b> na ontdekking van het datalek aan AP;</li> <li>▪ doet binnen 72 uur in ieder geval een voormelding als nog niet alle gegevens bekend zijn;</li> <li>▪ gebruikt het webformulier van AP om het datalek te melden;</li> <li>▪ doet een kopie van de melding ter registratie en archivering, aan de TOPDESK toekomen.</li> </ul>	FG

#### Activiteit 8 – Vaststellen of dat persoonsgegevens zijn vernietigd of zijn aangetast.

A8	Toelichting	Uitvoerend
	<u>IBF:</u> <ul style="list-style-type: none"> <li>▪ stelt vast of er persoonsgegevens zijn vernietigd of verloren gegaan;</li> <li>▪ stelt vast of er persoonsgegevens zijn aangetast;</li> <li>▪ consulteert medewerkers om technische informatie te vergaren indien nodig;</li> <li>▪ overlegt met FG.</li> </ul>	IBF
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.2.1

#### Activiteit 9 – Vaststellen van versleuteling van persoonsgegevens.

A9	Toelichting	Uitvoerend
	<u>IBF:</u> <ul style="list-style-type: none"> <li>▪ stelt vast of de gelekte persoonsgegevens op het moment van de inbreuk versleuteld waren;</li> </ul>	IBF

	<ul style="list-style-type: none"> <li>delegeert taken om informatie te vergaren;</li> <li>overlegt met FG.</li> </ul>	
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.2.2

Activiteit 10 – Vaststellen dat versleuteling persoonsgegevens voldoende adequaat is.

A10	Toelichting	Uitvoerend
	<u>IBF:</u> <ul style="list-style-type: none"> <li>stelt vast of de versleuteling voldoende bescherming biedt;</li> <li>delegeert taken om informatie te vergaren;</li> <li>overlegt met FG.</li> </ul>	FG
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.2.3

Activiteit 11 – Accepteren restrisico omtrent versleuteling van persoonsgegevens

A11	Toelichting	Uitvoerend
	<u>FG:</u> <ul style="list-style-type: none"> <li><u>stelt vast of het restrisico acceptabel is.</u></li> </ul>	FG
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.2.4

Activiteit 12 – Vaststellen of andere technische beschermingsmiddelen voldoende bescherming bieden om melding aan de betrokkene achterwege te laten.

A12	Toelichting	Uitvoerend
	<u>IBF:</u> <ul style="list-style-type: none"> <li>stelt vast of andere technische beschermingsmiddelen voldoende bescherming bieden om melding aan de betrokkene achterwege te laten en consulteert FG;</li> <li>consulteert medewerkers om informatie in te winnen om technische beschermingsmiddelen indien nodig.</li> </ul>	IBF
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.3

Activiteit 13 – Vaststellen van ongunstige gevolgen voor de betrokkene.

A13	Toelichting	Uitvoerend
	<u>FG:</u> <ul style="list-style-type: none"> <li>stelt vast of het datalek waarschijnlijk ongunstige gevolgen zal</li> </ul>	

	hebben voor de persoonlijke levenssfeer van de betrokkene; <ul style="list-style-type: none"> <li>▪ consulteert medewerkers om informatie in te winnen.</li> </ul>	
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.4

Activiteit 14 – Vaststellen of melding aan de betrokkene(n) achterwege kan worden gelaten.

A14	Toelichting	Uitvoerend
	FG: <ul style="list-style-type: none"> <li>▪ stelt vast of er zwaarwegende redenen zijn om de melding aan de betrokkene(n) achterwege te laten;</li> <li>▪ consulteert medewerkers om informatie in te winnen.</li> </ul>	
	Verwijzing in het document “De meldplicht datalekken in Wbp: beleidsregels voor toepassing van art 34a Wbp”, AP, 8 december 2015	§7.5

Activiteit 15 – Melden datalek aan betrokkene (n).

A15	Toelichting	Uitvoerend
	FG: <ul style="list-style-type: none"> <li>▪ overlegt met de communicatieadviseur (afhankelijk van de grootte en de verwachte impact van het datalek).</li> </ul>	FG
	Communicatieadviseur: <ul style="list-style-type: none"> <li>▪ informeert de betrokkene(n)</li> </ul>	Communicatie-adviseur

### Bijlage 3: beveiliging categorieën

De beveiliging categorieën dient nog nader uitgewerkt te worden in zowel incident management procedure en/of dataclassificatie beleid. Voor als nog wordt de impact op het/de bedrijfsproces /betrokkene beoordeeld op basis van de volgende schalen:

	Persoonsgegevens	Wettelijke en reglementaire verplichtingen	Financieel verlies	Beleid en werking van de gemeentelijke overheid
<b>Categorie 0: Verwaarloosbare schade</b>	Geen ongemak	Geen verplichtingen	Geen verlies	Geen invloed
<b>Categorie 1: Enige schade</b>	Ongemak voor een persoon, maar er wordt geen inbreuk gemaakt op een wet of op regelgeving.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schade- vergoeding/boete van minder dan € 5.000.-	Resulteert direct of indirect in verliezen van minder dan € 10.000.-	Draagt bij aan het niet efficiënt opereren van een deel van de organisatie.
<b>Categorie 2: Serieuze schade</b>	Een inbreuk op wet- of regelgeving, resulterend in licht ongemak voor een persoon of groep personen.	Civiele procedure of strafrechtelijke vervolging in een schadevergoeding/ boete tussen € 5.000.- en € 10.000.-	Resulteert direct of indirect in verliezen tussen € 10.000.- en € 100.000.-	Benadeelt het goed besturen en/of functioneren van een deel van de organisatie.
<b>Categorie 3: Zeer grote schade</b>	Een inbreuk op wet- of regelgeving resulteren in aanzienlijk ongemak voor een persoon of groep personen.	Civiele procedure of strafrechtelijke vervolging. Resultierend in een schadevergoeding/ boete	Resulteert direct of indirect in verliezen boven € 100.000.-	Benadeelt het goed besturen en/of functioneren van de gehele organisatie.

## Bijlage 4. Meldingsformulier Datalek

Dit formulier wordt gebruikt indien persoonsgegevens betrokken zijn bij een beveiligingsincident. Het formulier wordt gebruikt voor de eerste melding (constatering) en vervolgens voor het bewaken van de voortgang/afhandeling van het incident in Topdesk.

Het formulier bestaat uit 2 gedeelten:

1. Het eerste gedeelte wordt ingevuld door melder of afdelingshoofd
2. De rest van het formulier wordt ingevuld door de FG

Dit formulier wordt in Topdesk opgeslagen als bijlage door FG.

---

### 1. Algemene informatie en contactpersoon. In te vullen door melder-afdelingshoofd.

---

#### Over welke organisatie of welk bedrijf gaat het?

Gemeente Brunssum  
Lindeplein 1  
6444 AT Brunssum

Registratienummer bij de Kamer van Koophandel : 14129999

#### In welke sector is de organisatie of het bedrijf actief?

Openbaar bestuur - Gemeente

#### Wie meldt het incident /datalek?

Naam

Functie

E-mailadres

Telefoonnummer

Omschrijving van het incident

---

## 2. In te vullen door functionaris Gegevensbescherming (FG)


---

**Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding? (invullen door FG)**

Geeft datalek aanleiding tot melding bij AP:

Categorie melding ☐ 0 ☐ 1 ☐ 2 ☐ 3

Toelichting:



**Contactpersoon:**

Naam

Functie

E-mailadres

Telefoonnummer

**Gegevens over het datalek**


Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest





Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?

Naam van de organisatie waaraan de verwerking is uitbesteed

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Is bekend wanneer de inbreuk was?

- ☐ Ja  
☐ Nee

Is de exacte datum bekend wanneer de inbreuk was?

- ☐ Ja  
☐ Nee

Startdatum van de periode waarbinnen de inbreuk was

Einddatum van de periode waarbinnen de inbreuk was

Wanneer werd de inbreuk ontdekt?

### **Wat is de aard van de inbreuk?**

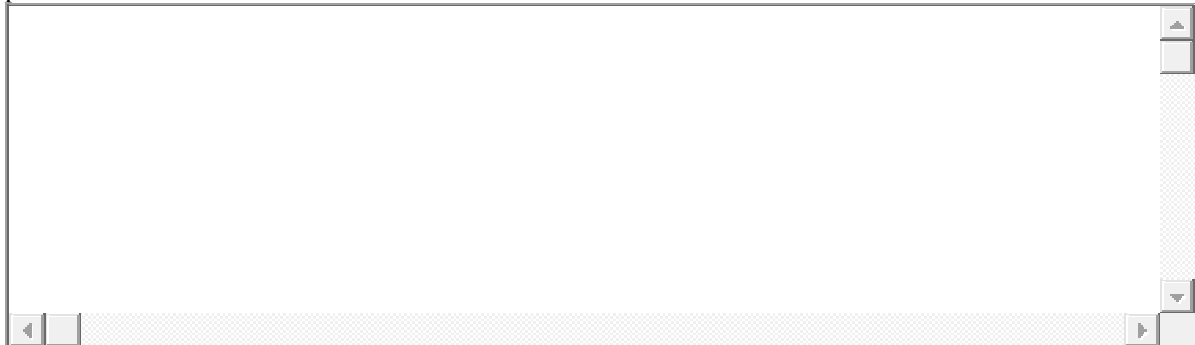
Selecteer één of meerdere opties:

- ☐ Lezen (vertrouwelijkheid)  
☐ Kopiëren  
☐ Veranderen (integriteit)  
☐ Verwijderen of vernietigen (beschikbaarheid)  
☐ Diefstal  
☐ Nog niet bekend




### Vervolgacties naar aanleiding van het datalek

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?



### Melding aan Betrokkene(n)

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?

Kies er een 

Indien **nee** ga dan naar “Waarom ziet u af van het melden van het datalek aan de betrokkenen?”

Wanneer heeft u het datalek gemeld aan de betrokkenen?

Wanneer gaat u het datalek melden aan de betrokkenen?

Wat is de inhoud van de melding aan de betrokkenen?



Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?



**Waarom ziet u af van het melden van het datalek aan de betrokkenen?**


Kies er een 

Toelichting:



**Technische beschermingsmaatregelen**

Waren de persoonsgegevens op het moment van het ontdekken van het datalek versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?

Kies er een 

Toelichting:




Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?



### Internationale aspecten

Heeft de inbreuk betrekking op personen in andere EU-landen?

Kies er een 

Ja, namelijk:



☐ Heeft uw organisatie of bedrijf, het datalek gemeld bij toezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?

Toezichthouder(s) van andere landen waar het datalek is gemeld

