Procesbeschrijving

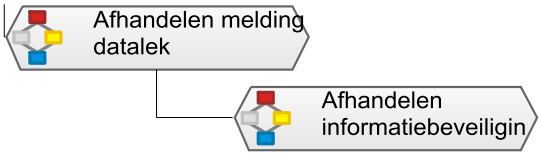
Afhandelen melding datalek

Droog, W.M. (Wieteke)

Type	Ingecheckt
Incheckdatum	03/27/18 14:58:52
Versie	2.0
Status	Gepubliceerd
Gebruiker	Lith, R. (Roy)
Creatiedatum	2-5-2018 15:10:16
Afgedrukt door	Droog, W.M. (Wieteke)

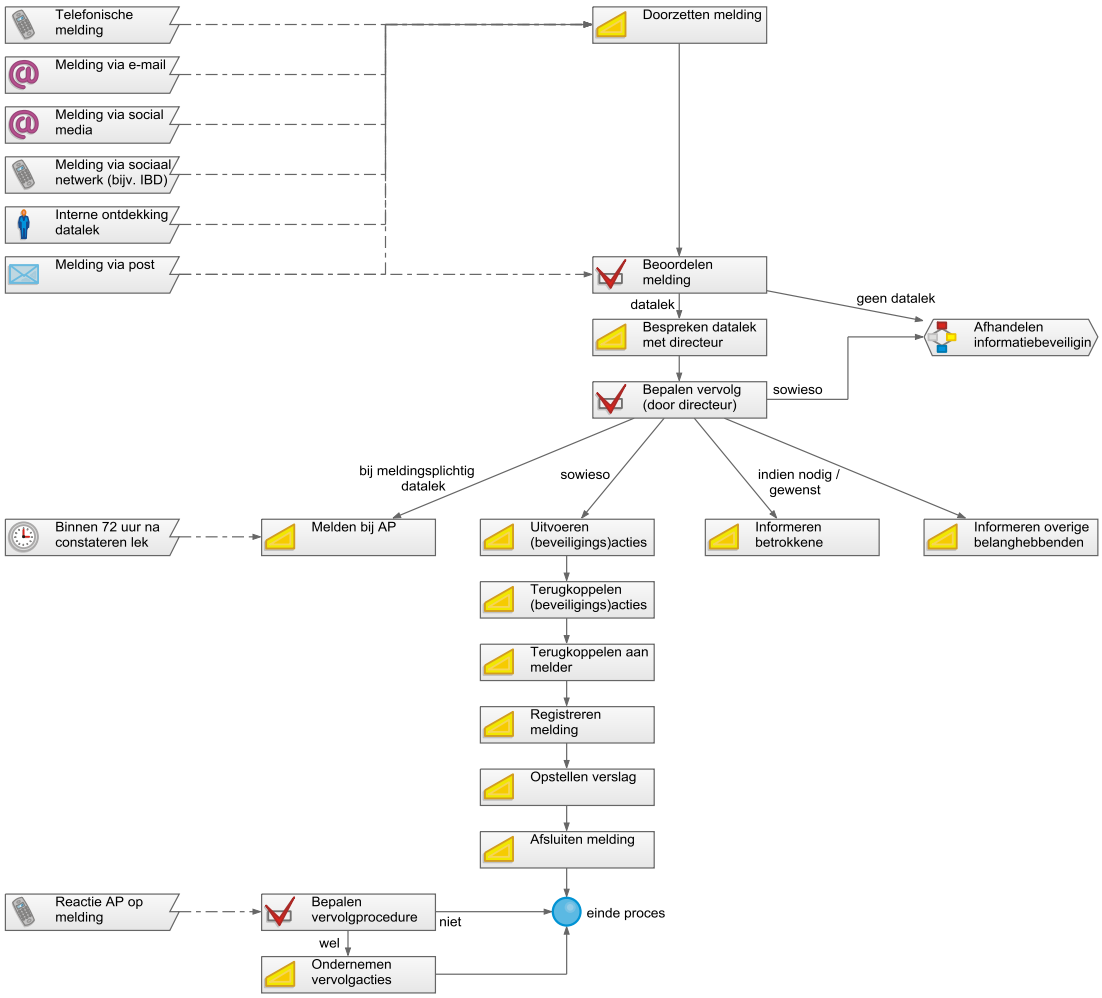
Inhoudsopgave

1 Processtructuur



2 Processchema's

2.1 Afhandelen melding datalek



2.1.1 Beschrijving

Proceseigenaar
Domeindirecteur Bedrijfsvoering en Diensten

Doel
Beoordelen of er een datalek is geweest en indien nodig het treffen van beveiligingsmaatregelen en zonodig melding doen bij de Autoriteit Persoonsgegevens (AP) / kennisgeving doen aan betrokkene(n).

Globale omschrijving
Zowel intern als extern kan er melding gedaan worden van (mogelijke) datalekken. Medewerkers die een mogelijk datalek ontdekken dienen dit te melden bij het Meldpunt datalekken en/of de medewerker Informatiebeveiliging.

Een lek is een datalek wanneer er persoonsgegevens zijn gestolen, zoekgeraakt, verloren of zichtbaar zijn voor daartoe onbevoegde personen.

Voorbeelden van datalekken:
- een e-mail met een bestand aan persoonsgegevens welke is verzonden naar een verkeerde adres
- een verloren tablet die niet beveiligd (vergrendeld) is. Mogelijk is er dan gevoelige informatie blootgesteld aan anderen dan de eigenaar van de tablet, waar mogelijk misbruik van kan worden gemaakt.
- cyberaanvallen / een gehackte applicatie; van buitenaf is er ingebroken in een applicatie en zijn er gegevens gestolen
- onbedoeld (vertrouwelijke) persoonsgegevens van klanten openstellen aan onbevoegden o.a. op het internet of lokale netwerk (meerdere schijven) etc.
- een verloren of zoekgeraakte USB-stick met persoonsgegevens die in verkeerde handen kan vallen

NB. Deze procesbeschrijving geldt voor een datalek waar het college/burgemeester van Purmerend voor verantwoordelijk is. Indien de raad (van Purmerend of Beemster) of bestuursorganen van Beemster verantwoordelijk zijn, dan wordt het vervolg bepaald door de medewerkers van het Meldpunt datalekken i.p.v. de directeur(en). E.e.a. zal dan in overleg met de Griffie gebeuren. De resterende activiteiten zijn dan wel hetzelfde.

Prestatie-indicatoren
- Indien meldingsplichtig dient het datalek binnen 72 uur na ontdekking gemeld te worden bij de Autoriteit Persoonsgegevens;
- Treffen van (beveiligings)maatregelen (mogelijk ook opgelegd door de Autoriteit Persoonsgegevens) om het datalek te dichten;
- Bijhouden van de gemelde datalekken (bij de gemeente Purmerend); in dit overzicht staat om wat voor een soort datalek het gaat, wie het gemeld heeft, welke (beveiligings)maatregelen er (door wie) genomen moeten worden en hoe de melding is afgerond.

2.1.2 Activiteiten, Triggers en Subprocessen

Telefoon	**Telefonische melding**
Beschrijving	Een melding van een (mogelijk) datalek die via de telefoon binnenkomt.

E-mail	**Melding via e-mail**
Beschrijving	Een melding van een (mogelijk) datalek die via e-mail binnenkomt.
Triggerinhoud	Melding datalek

E-mail	Melding via social media
Beschrijving	Een melding van een (mogelijk) datalek die via social media (Facebook of Twitter) binnenkomt.
Triggerinhoud	Melding datalek

Telefoon	Melding via sociaal netwerk (bijv. IBD)
Beschrijving	Een melding van een (mogelijk) datalek dat binnenkomt via een (sociaal) netwerk, zoals het IBD of via connecties bij een ander collegiaal netwerk.

Mens	Interne ontdekking datalek
Beschrijving	Een medewerker van de gemeente Purmerend ontdekt een (mogelijk) datalek.

Post	Melding via post
Beschrijving	Een melding van een (mogelijk) datalek die via de post binnenkomt.
Triggerinhoud	Poststuk met melding datalek

Basis	Doorzetten melding
Uitvoerende	Medewerker gemeente Purmerend
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Neem contact op met een medewerker van het Meldpunt datalekken. Dit kan zowel door te bellen, mailen of langs te gaan. Noteer in ieder geval de contactgegevens, zodat er naderhand contact opgenomen kan worden met de melder. Indien je gebeld wordt en er spoed bij is, kan er ook direct doorverbonden worden met een medewerker van het Meldpunt datalekken. Indien je gaat mailen, dan kan je de e-mail versturen naar: datalek@purmerend.nl. NB. In de meeste gevallen zal het Meldpunt zelf benaderd worden.

Controle	Beoordelen melding
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Neem de melding door en ga na wat er aan de hand is en of er inderdaad sprake is van een datalek (en/of een informatiebeveiligingsincident). Neem indien nodig contact op met de melder voor meer informatie. • ALS er sprake is van een datalek, ga DAN over tot het bespreken van het datalek met de (betreffende) Domeindirecteur; • ALS er geen sprake is van een datalek, maar wel van een informatiebeveiligingsincident, ga DAN over tot de activiteiten welke zijn benoemd in het subproces Afhandelen informatiebeveiligingsincident; • ALS er geen sprake is van een datalek (of een informatiebeveiligingsincident), koppel dit DAN terug aan de melder. Beëindig hiermee het proces.
Data	
Optioneel	Scan van poststuk met melding datalek (document, Bestand, intern)
	Doorgezette melding datalek (document, e-mail, intern)
	Melding datalek (document, Bestand, in)

Linkmodel	Afhandelen informatiebeveiligingsincident

Basis	Bespreken datalek met directeur
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Bespreek het datalek met de betreffende Domeindirecteur en geef aan wat de impact is, wat de risico's zijn etc. en adviseer wat er zou moeten gebeuren. Stuur daarnaast ter bevestiging ook een e-mail met alle informatie. NB. Indien de betreffende Domeindirecteur niet direct beschikbaar is, neem dan contact op met een directeur die wel beschikbaar is; dit kan een andere Domeindirecteur zijn, maar ook de Algemeen Directeur, bijvoorbeeld.
Data	
Optioneel	Scan van poststuk met melding datalek (document, Bestand, intern)
	Doorgezette melding datalek (document, e-mail, intern)
	Melding datalek (document, Bestand, in)
Betrokkenen	
Geraadpleegd en geïnformeerd	Domeindirecteur

Controle	Bepalen vervolg (door directeur)
Uitvoerende	Domeindirecteur
Verantwoordelijke	Domeindirecteur
Beschrijving	Laat sowieso overgaan tot het uitvoeren van (beveiligings)acties, maar bepaal daarnaast welke vervolgacties er genomen moeten worden. • ALS er sprake is van een meldingsplichtig datalek, ga DAN over tot het melden bij de Autoriteit Persoonsgegevens (AP); • ALS het nodig of gewenst wordt geacht, ga DAN over tot het informeren van de betrokkene en eventueel overige belanghebbenden.
Betrokkenen	
Geraadpleegd en geïnformeerd	Overige directieleden

Tijd	Binnen 72 uur na constateren lek
Beschrijving	Binnen 72 uur nadat het datalek is geconstateerd.

Basis	Melden bij AP
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Meld het datalek volgens de procedure (webformulier) bij de Autoriteit Persoonsgegevens (AP). Laat dit document registreren via DIV. NB. de meeste datalekken zijn meldingsplichtig.
Data	
Gecreëerd	Webformulier datalek site AP (document, Bestand, uit)

Basis	Informeren betrokkene
Uitvoerende	Medewerker Domein
Verantwoordelijke	Domeindirecteur
Beschrijving	Stel de betrokkene op de hoogte. Doe dit door de kennisgeving 'Informeren betrokkene' op te stellen en te versturen. NB. Laat deze brief registreren bij DIV.
Data	
Gecreëerd	Brief Informeren betrokkene (document, papier, uit)

Basis	Informeren overige belanghebbenden
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Informeer de overige belanghebbenden die op de hoogte moeten zijn van het datalek. Per geval kan dit verschillend zijn en dit wordt vooraf met de Domeindirecteur besproken. Te denken valt aan: • betreffende Wethouder • medewerkers van team Communicatie (Woordvoerder of Adviseur) • Concerncontroller • betreffende (beleids)medewerkers en proceseigenaren (Teammanagers) etc. NB. Informeer in ieder geval ook de Domeindirecteur Bedrijfsvoering en Diensten.
Betrokkenen	
Geraadpleegd	Domeindirecteur Bedrijfsvoering en Diensten
Geïnformeerd	Medewerker Communicatie
Geïnformeerd	Wethouder
Geïnformeerd	Concerncontroller
Geïnformeerd	Medewerker domein / Medewerker ICT
Geïnformeerd	Teammanager Domein

Basis	Uitvoeren (beveiligings)acties
Uitvoerende	Medewerker domein / Medewerker ICT
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Voer alleen of met hulp van team ICT (Functioneel Beheer / Systeembeheer) de benodigde beveiligingsmaatregelen uit.

Basis	Terugkoppelen (beveiligings)acties
Uitvoerende	Medewerker Domein
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Koppel de uitgevoerde beveiligingsmaatregelen terug aan het Meldpunt datalekken en andere belanghebbenden (met name de Domeindirecteur).
Betrokkenen	
Geïnformeerd	Medewerker Meldpunt datalekken
Geïnformeerd	Domeindirecteur

Basis	Terugkoppelen aan melder
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Koppel terug aan de melder wat de status is van het datalek. Intern kan dit op vele manieren (bellen, mailen, langsgaan). Indien dit een externe betreft, stel dan de kennisgeving 'Informeren (externe) melder' op en verstuur deze. Hierin wordt bevestigd dat het datalek onderzocht is, zo nodig gemeld is bij de Autoriteit Persoonsgegevens (AP) en of er beveiligingsmaatregelen worden genomen. Laat deze brief registreren bij DIV. NB. Tijdens de afwikkeling van het datalek wordt er natuurlijk ook onderling afgestemd met de belanghebbenden (waaronder de Domeindirecteur).
Data	
Gecreëerd	Brief informeren externe melder (document, papier, uit)

Basis	Registreren melding
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Maak een registratie in het meldingenoverzicht datalekken.
Data	
Gecreëerd	Overzicht datalekken (document, Bestand, intern)

Basis	Opstellen verslag
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Maak het verslag aan m.b.t. de afwikkeling van het datalek en stuur deze naar alle betrokken medewerkers. NB. Tijdens de afhandeling van het datalek zal het voorkomen dat er meerdere malen verslag wordt gedaan over de status aan de betrokkenen.
Data	
Gecreëerd	Verslag datalek (document, Bestand, intern)

Basis	Afsluiten melding
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Voeg de laatste informatie toe aan de registratie in het meldingenoverzicht en sluit de melding af.
Data	
Aangepast	Overzicht datalekken (document, Bestand, intern)

Telefoon	Reactie AP op melding
Beschrijving	De Autoriteit Persoonsgegevens (AP) reageert n.a.v. de melding, waar alsnog mogelijke vervolgacties uit voortkomen.
Triggerinhoud	Reactie AP

Controle	Bepalen vervolgprocedure
Uitvoerende	Medewerker Meldpunt datalekken
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Bepaal of er nadere actie nodig is. • ALS er nadere actie nodig is, geef dit DAN aan bij het betreffende domein en/of team ICT; • ALS er geen nadere actie nodig is, beëindig DAN het proces.

Basis	Ondernemen vervolgacties
Uitvoerende	Medewerker domein / Medewerker ICT
Verantwoordelijke	Domeindirecteur Bedrijfsvoering en Diensten
Beschrijving	Onderneem de vervolgacties die volgens de Autoriteit Persoonsgegevens nog uitgevoerd moeten worden. Dit zal worden doorgegeven vanuit het Meldpunt datalekken. NB. Wat er precies moet gebeuren en door wie, wordt verder niet uitgewerkt, aangezien het van alles kan zijn.