Protocol Respons Datalekken

5.1.2.e

DATUM	13 oktober 2021
AUTEUR	[redacted] 5.1.2.e
CLASSIFICATIE	Bedrijfsvertrouwelijk
VERSIE	3.5 Definitief

Inhoud

Versie	Datum	Auteur(s)	Status	Opmerking
1.0	6 juli 2016	[redacted] 5.1.2.e	Definitief	Gezamenlijk met GGD
2.1	10 augustus 2017	[redacted] 5.1.2.e	Concept	Nieuwe opzet VRGZ
3.0	7 november 2017	[redacted] 5.1.2.e	Definitief	Weer in lijn met GGD
3.1	28 februari 2018	[redacted] 5.1.2.e	Definitief	Contactpersonen toegevoegd
3.2	17 april 2019	[redacted] 5.1.2.e	Definitief	Contactpersonen gewijzigd
3.3	21 januari 2020	[redacted] 5.1.2.e	Definitief	Contactpersonen gewijzigd
3.4	26 juli 2021	[redacted] 5.1.2.e	Definitief	Contactpersonen gewijzigd
3.5	13 oktober 2021	[redacted] 5.1.2.e	Definitief	Herziening

Introductie

Vanaf 1 januari 2016 bestaat een wettelijke plicht om datalekken te melden. De Algemene Verordening Gegevensbescherming (AVG) bevat een aanscherping op de verplichting om datalekken te melden. Er worden aanvullende eisen gesteld aan organisaties die persoonsgegevens beheren en/of verwerken. Als VRGZ moeten we sinds 25 mei 2018 voldoen aan de eisen van de AVG.
In onze informatiemaatschappij is steeds meer aandacht voor de wijze waarop (digitale) informatie wordt gebruikt en bewaard. Persoonsgegevens hebben daarbij speciale aandacht. Hoewel de Meldplicht Datalekken zich vooral richt op het afhandelen van incidenten met persoonsgegevens, is het nodig dat een organisatie preventief de juiste beveiligingsmaatregelen neemt om datalekken te voorkomen. En omdat dit een verantwoordelijkheid betreft van iedereen binnen de organisatie, is bewustwording hiervan en passend gedrag van bestuur, management en medewerkers essentieel.
Een organisatie die data laat lekken of persoonsgegevens niet volgens de regels van de wet verwerkt, loopt kans op een flinke boete. Ook het niet-melden van een datalek kan strafbaar zijn.

Datalek

Bij een datalek gaat het om toegang tot persoonsgegevens of vernietiging, wijziging of vrijkomen van gegevens zonder dat dat de bedoeling is van de betreffende organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

In artikel 4 onder 12 AVG is een datalek gedefinieerd als een inbreuk in verband met persoonsgegevens. Dit betekent "een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens"

Voorbeelden datalekken

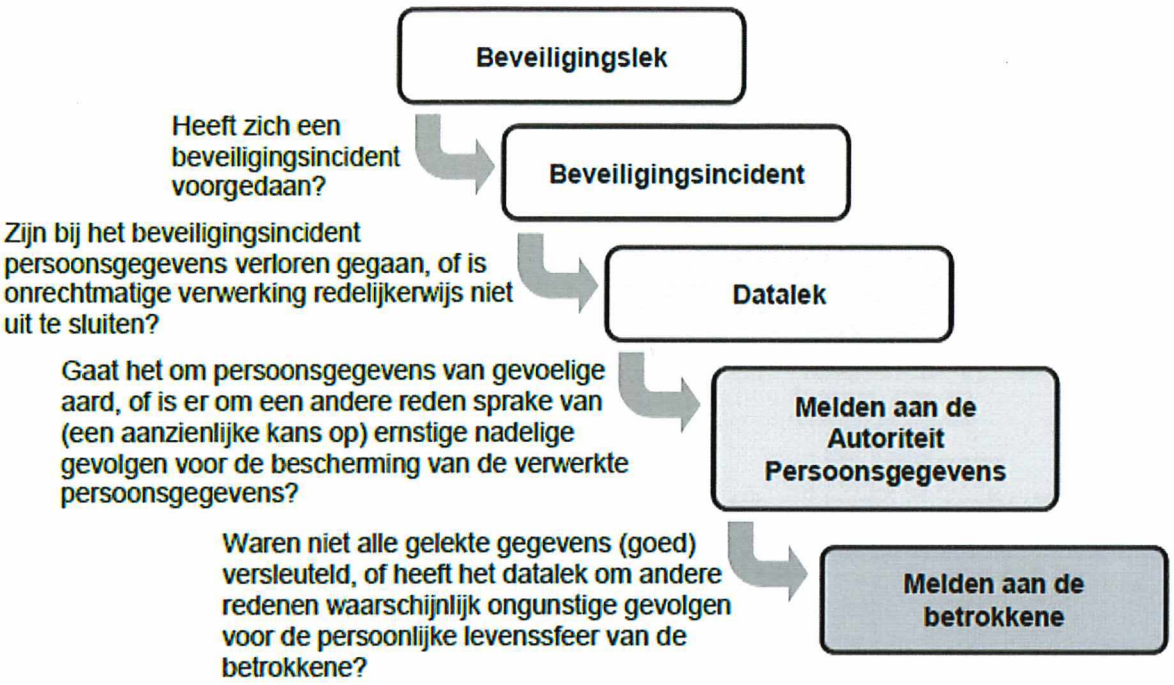
Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een naar de verkeerde ontvanger gestuurde mail waarin persoonsgegevens staan.

Bron: Autoriteit Persoonsgegevens

Een datalek is zonder boete al een ingrijpend voorval. Is het bijvoorbeeld veilig en verantwoord om tijdens een datalek door te gaan met de dagelijkse bedrijfsvoering? Welke maatregelen zijn nodig om de bedreiging te elimineren? Dit protocol biedt ondersteuning bij het voorbereiden op - en het bestrijden van - een datalek en helpt voorkomen dat een datalek ook nog eens leidt tot een boete vanwege procedurele fouten.

Afwegingskader: datalek of niet?

Niet ieder beveiligingsincident is een datalek. En niet ieder datalek hoeft gemeld te worden aan de Autoriteit Persoonsgegevens (AP) en de betrokkene. De AP heeft hiervoor een beslisboom opgesteld die we binnen VRGZ hanteren:



Anticiperen op een datalek

Anticiperen heeft als primair doel het voorkomen van een datalek. Om een datalek te kunnen voorkomen is het van belang de essentiële factoren die een rol spelen bij een datalek in beeld te hebben. Deze factoren en voorbeelden van de bijbehorende preventieve en reducerende maatregelen zijn:

Onbewust menselijk handelen Per abuis emailadressen in "aan" in plaats van in "bcc", afdrukken of documenten rond laten slingeren Bewustwording door voorlichting en instructie	Bewust menselijk handelen Hacken, phishing Firewalls, virusscanners en spamfilters
Ondoelmatig ingerichte systeemprocessen Toegang tot meer gegevens dan nodig voor de taak Periodiek toetsen op doelmatigheid en waar nodig aanpassen. Werken met autorisatieprofielen	Ontoereikende beveiliging van systemen Wachtwoorden op een Post-it of standaard toegangscodes als [redacted]5.1.2.h Systeembeveiliging voldoende complex en gedragsregels

Door de essentiële factoren te beschrijven en maatregelen te implementeren wordt de kans op een datalek aanzienlijk verkleind.
Als zich desondanks een datalek voordoet, dan ontbreekt de tijd en de rust om ad-hoc te bedenken wat er moet gebeuren en wie dat gaat doen. Het secundaire doel van de voorbereiding op een datalek is om het 'WAT' - de acties die dan moeten uitgevoerd – en 'HOE' - de inachtneming van de juiste procedures en termijnen- scherp te hebben, en om te bepalen 'WIE' hierin welke rol heeft. Dit secundaire doel is het onderwerp van voorliggende procedure.

Fasen van een datalek

Om een beeld te krijgen van wat er allemaal moet gebeuren bij een datalek is het goed om te kijken hoe een datalek zich ontwikkelt. Een datalek heeft een begin en een eind en doorloopt een aantal 'standaard' fases, waardoor gesproken kan worden van een levenscyclus van een datalek. Schematisch ziet dat er als volgt uit.

Stappenplan bij een datalek

Bij elke stap uit de hiervoor beschreven cyclus moeten er verschillende acties ondernomen worden en zijn er diverse actoren verantwoordelijk voor die acties. In het schema hieronder wordt dit in detail uitgewerkt.

We onderkennen hierbij de volgende actoren:

Melder Dit is degene die het potentiële datalek ontdekt. Dit kunnen alle interne VRGZ medewerkers zijn, maar ook externe organisaties of burgers.

Servicedesk De eerstelijns ICT helpdesk

FG Functionaris Gegevensbescherming; houdt toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

Responsteam Het responsteam voert de coördinatie bij het oplossen van het datalek. In het responsteam zitten:

- De FG (coördinator)
- De informatiemanager
- De servicemanager ICT (= tevens coördinator uitvoering in het calamiteitenteam)
- Een communicatieadviseur
- Een jurist
- Een leidinggevende van het team waar het datalek zich heeft voorgedaan

Directeur De directeur van VRGZ. Deze neemt alle benodigde besluiten op advies van het responsteam

Calamiteitenteam Het calamiteitenteam neemt de uitvoerende maatregelen om het datalek te dichten en neemt preventieve maatregelen om datalekken in de toekomst te voorkomen. In het calamiteitenteam zitten:

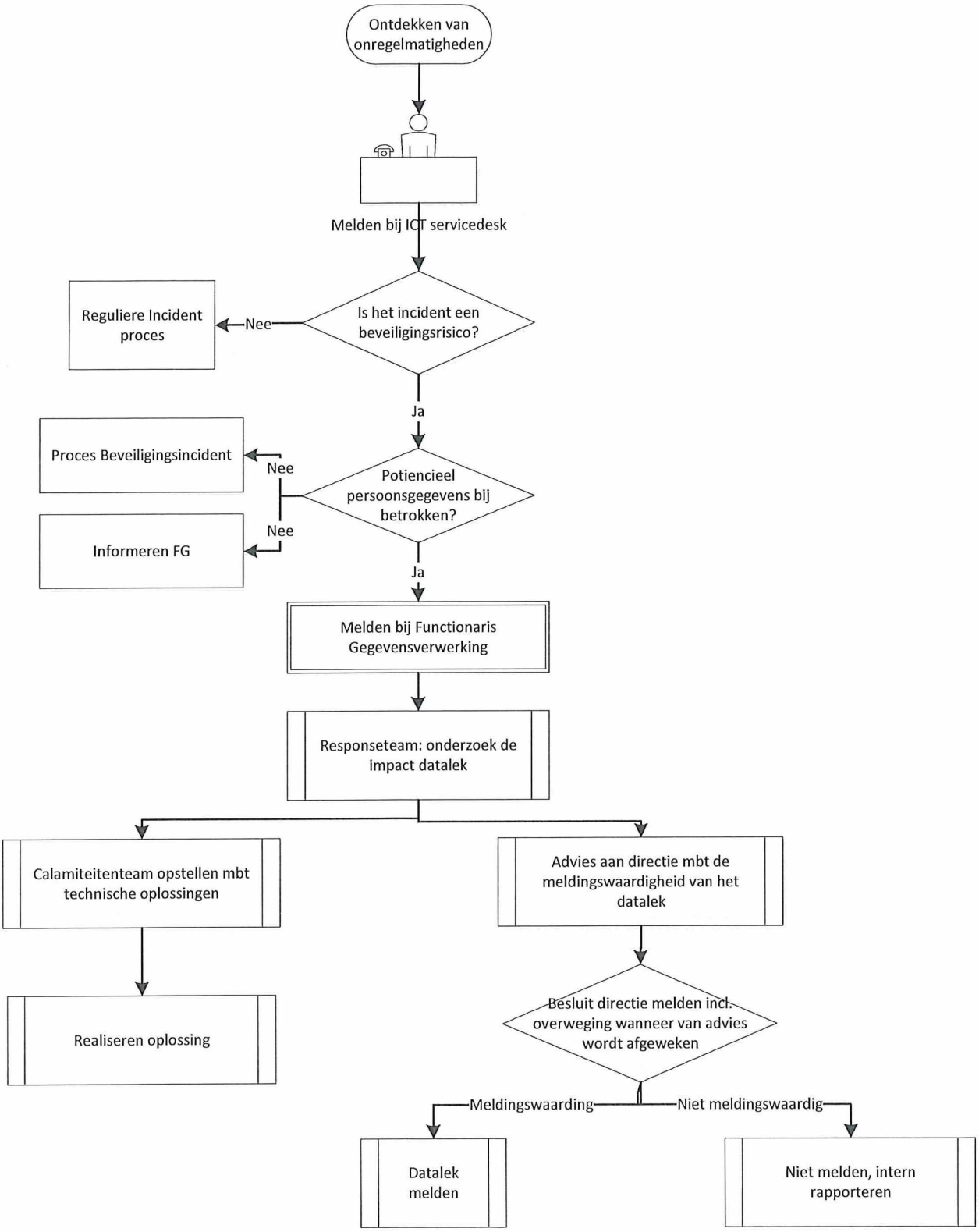
- De servicemanager ICT (coördinator)
- Een servicedeskmedewerker
- De applicatiebeheerder van de afdeling waar het datalek zich voordoet
- Optioneel: betrokken leveranciers en externe deskundigen

Wat?	Wie?	Hoe?	Tijdspad
1. Ontdekken	Melder Servicedesk	1. De melder ontdekt onregelmatigheden en meldt deze bij het 'Meldpunt Informatiebeveiliging' dat wordt beheerd door de servicedesk 2. De servicedesk registreert de melding en geeft terugkoppeling aan de melder 3. De servicedesk informeert de FG	Afhandeling binnen 2 uur na de melding
2. Onderzoek impact	Servicedesk & melder Servicedesk Servicedesk FG	1. De servicedesk verzamelt gegevens over het incident bij de melder en via het systeem 2. De servicedesk beoordeelt of het een beveiligingsincident en / of een potentieel datalek is 3. De servicedesk draagt het verzamelde dossier over aan de FG 4. De FG voert een impactanalyse uit (hoe ernstig, wat is het aantal getroffenen, aan wie is de data blootgesteld, hoe lang bestaat het lek?)	Afhandeling binnen 24 uur na de melding
3. Opschalen	FG	1. De FG brengt de directeur van VRGZ op de hoogte van het potentiële datalek 2. De FG roept het responsteam datalekken bijeen 3. Het responsteam doet een nadere analyse en formuleert een advies voor de directeur over wel/niet melden van het datalek bij de AP en het wel/niet stoppen van bedrijfsprocessen 4. De FG adviseert de directeur over het wel/niet melden van het datalek en het wel/niet stoppen van bedrijfsprocessen 5. De directeur neemt een besluit over wel/niet melden en wel/niet stoppen van bedrijfsprocessen. Dit besluit en eventuele afwijking van het advies wordt schriftelijk vastgelegd	Afhandeling binnen 40 uur na de melding
4. Melden	FG	1. De FG meldt het datalek bij de AP conform de geldende procedure	Afhandeling binnen 48 uur[1] na de melding
5. Bestrijden	Responsteam Calamiteitenteam	1. Het responsteam roept het calamiteitenteam bijeen, deelt het dossier en coördineert de door het calamiteitenteam te ondernemen maatregelen 2. Het calamiteitenteam neemt maatregelen om het datalek te dichten en schakelt zo nodig externe expertise in. Het calamiteitenteam zorgt voor regelmatige terugkoppeling aan het responsteam	Afhandeling binnen 96 uur na de melding

[1] De wettelijke termijn is 72 uur.

6. Communiceren	FG FG Communicatie-adviseur en betrokken afdeling FG Communicatie-adviseur	1. De FG communiceert over de getroffen maatregelen met de AP 2. De FG houdt de directeur op de hoogte over de getroffen maatregelen 3. De communicatieadviseur zorgt voor het informeren van externe betrokkenen 4. De FG communiceert over de getroffen maatregelen met de melder 5. De communicatieadviseur informeert de organisatie over het datalek	Afhandeling binnen 96 uur na de melding
7. Rapporteren	Responsteam	1. Het responsteam vult het dossier aan met de getroffen maatregelen, gemaakte afspraken en met wie waarover gecommuniceerd is. In geval van cybercrime doen ze aangifte bij de politie	Afhandeling binnen 100 uur na de melding
8. Preventieve maatregelen	Calamiteitenteam Communicatie-adviseur	1. Het calamiteitenteam neemt preventieve maatregelen om een nieuw datalek te voorkomen en legt deze maatregelen vast 2. De communicatieadviseur informeert zo nodig de organisatie over nieuw ingevoerde maatregelen ter preventie van datalekken	Afhandeling binnen 148 uur na de melding
9. Dagelijkse routine	Responsteam FG FG	1. Het responsteam ontbindt het calamiteitenteam 2. De FG ontbindt het responsteam 3. De FG verzorgt een eindrapportage aan de directeur	Afhandeling binnen 150 uur na de melding

Stroomschema Ontdekking onregelmatigheden voor de Servicedesk / functioneel beheer



Checklist response team datalekken

Checklist Responsteam Datalekken

☐ Leg een logboek aan

ontdekking op		om	
ontdekt door			
symptomen			

inschatting impact	aard informatie	getroffenen	blootgesteld aan	classificatie

noodmaatregelen			
getroffen door			
op		om	

☐ responsteam ingeschakeld op ____ om ____

leden	rol

☐ zorg voor een veilige werkomgeving en verzamel bewijs (screenshots, foto's, logboeken), leg dit vast

☐ voorkom verder verlies van data, haal geïnfecteerde/gehackte servers en systemen offline, leg deze akties vast

☐ meld het datalek bij CBP via het formulier op www.cbpweb.nl en leg dit vast

☐ verzamel zoveel mogelijk informatie bij de personen die bij de ontdekking betrokkenen waren en leg deze vast

☐ bestrijd het datalek, leg de handelingen vast

☐ schakel bij kwaadwillendheid de politie/cybercrimespecialisten in, leg dit vast

☐ communiceer over het datalek met CBP en met (potentieel) getroffenen over de mogelijke gevolgen, leg dit vast

☐ doe in geval van cybercrime aangifte bij de politie en leg dit vast

☐ rapporteer alle handelingen aan het toepasselijke bestuurlijke niveau, leg dit vast

☐ voer preventieve maatregelen door om herhaling te voorkomen, leg dit vast

☐ terug naar dagelijkse routine, afschalen responsteam

responsteam ontbonden op ____ om ____

FAQ

https://autoriteitpersoonsgegevens.nl/nl

Woordenlijst / definities

Zie begrippenlijst datalekken.

Contactpersonen

Functie	Naam5.1.2.e	Mobiel5.1.2.e	Mailadres5.1.2.e
Functionaris Gegevensbescherming	[redacted]	[redacted]	[redacted]
Servicemanager ICT	[redacted]	[redacted]	[redacted]
Informatiemanager VRGZ	[redacted]	[redacted]	[redacted]
CISO VRGZ	[redacted]	[redacted]	[redacted]
Informatiemanager GGD	[redacted]	[redacted]	[redacted]
CISO GGD	[redacted]	[redacted]	[redacted]