Protocol melding en afhandeling beveiligings- of datalek Welzijnswerk Midden-Drenthe

Protocol

Melding en afhandeling beveiligings- of datalek

1. Inleiding

De achtergrond van deze procedure is de Meldplicht datalekken. Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens ('Wbp') aangevuld met artikel 34a Wbp.[1] Sindsdien geldt een meldplicht voor datalekken. Ook in de komende Algemene Verordening Gegevensbescherming ('AVG') is een dergelijke meldplicht voor datalekken opgenomen. Deze meldplicht houdt in dat organisaties een datalek onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP) (en in bepaalde gevallen ook aan de betrokkenen).

Dit document beschrijft de procedure die gehanteerd wordt bij (het vermoeden van) een beveiligings- of datalek binnen Welzijnswerk Midden-Drenthe, dan wel bij (het vermoeden van) een beveiligings- of datalek dat buiten Welzijnswerk Midden-Drenthe heeft plaatsgevonden maar waarvoor Welzijnswerk Midden-Drenthe toch de verantwoordelijkheid draagt (bij een 'verwerker'). Deze procedure is mede gebaseerd op de 'Beleidsregels voor de toepassing van artikel 34a van de Wbp' ('Beleidsregels') van de AP.[2]

Beveiligings- of datalekken zijn incidenten rondom verwerkingen van persoonsgegevens met een potentieel grote impact. Als Welzijnswerk als gevolg van een datalek een grote groep betrokkenen moet informeren kan dit grote kosten met zich meebrengen, naast een mogelijke boete van de toezichthouder. Het snel en adequaat onderzoeken, beperken van de gevolgen, het melden en afhandelen van een datalek zijn dan ook van groot belang.

Met het volgen van deze procedure wordt het volgende resultaat nagestreefd:

- voorspelbaar zijn voor alle belanghebbenden;
- waarborgen van de belangen van Welzijnswerk Midden-Drenthe en de betrokkenen;
- op zorgvuldige en systematische wijze analyseren van een (mogelijk) beveiligings- of datalek;
- bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen ervan.

Leeswijzer en onderhoud

De activiteiten in het protocol, bijbehorende verantwoordelijkheden en bevoegdheden worden in de volgende paragrafen stapsgewijs uitgewerkt.

Deze procedure wordt na het eerste gebruiksjaar en vervolgens 3-jaarlijks geëvalueerd door de directeur en/of medewerker p&o en opnieuw vastgesteld door de directie van Welzijnswerk Midden-Drenthe.
De medewerker p&o krijgt de opdracht toe te zien op de werking van de procedure en hierover in zijn kwartaalrapportage aan de directie verslag te doen.

2. Definities[3]

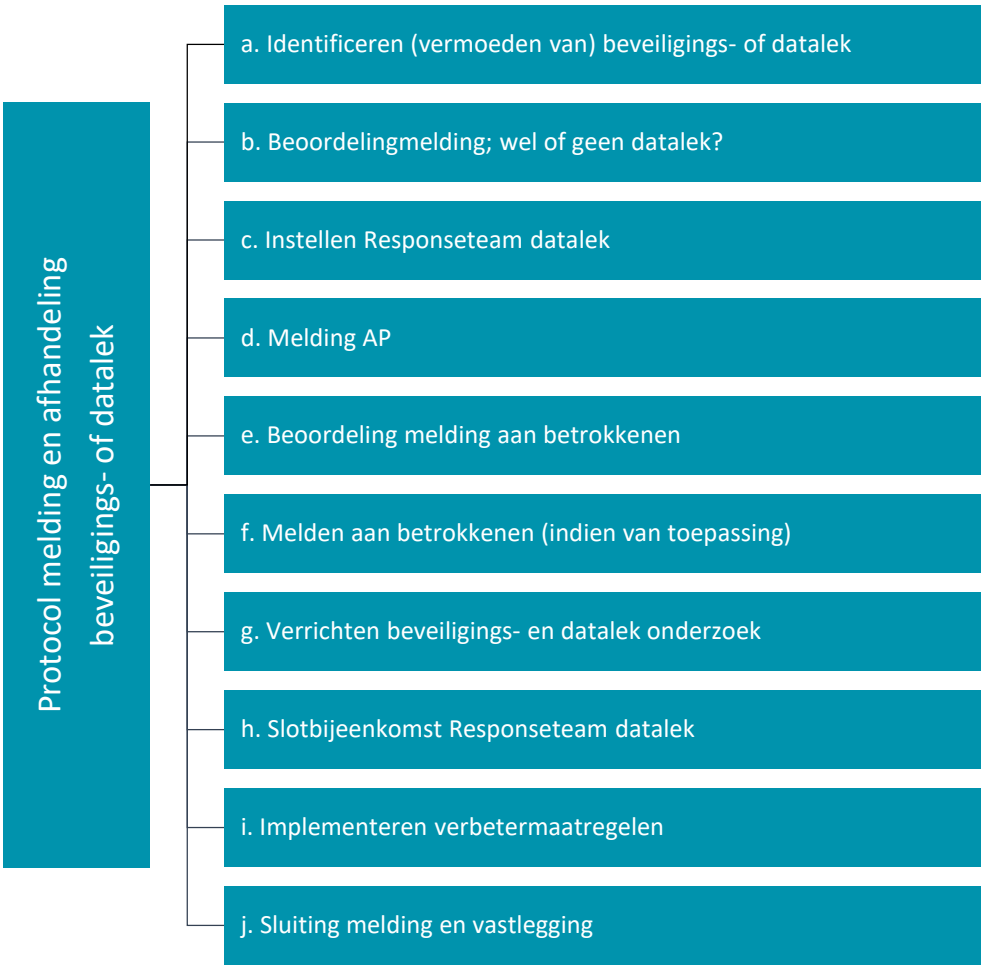
- **Betrokkene**: degene op wie een persoonsgegeven betrekking heeft.
- **Datalek**: een inbreuk op de beveiliging waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen bescherming hadden moeten bieden.
- **Eigenaar**: persoon die namens Welzijnswerk Midden-Drenthe de gedelegeerde verantwoordelijkheid heeft voor een informatiemiddel & -verwerkingen.
- **Beveiligingslek**: een mogelijk beveiligingslek, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens mogelijk zijn blootgesteld aan verlies

[1] Vanaf mei 2018 is de Algemene Verordening Gegevensbescherming van toepassing. Ook onder deze wetgeving is het melden van datalekken verplicht.
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf
[3] Voor zover dezelfde begrippen gelden als in het privacyreglement persoonsgegevens personeel wordt dezelfde definitie gehanteerd.

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 beveiligingslek, niet ieder beveiligingslek is een datalek.

- **Persoonsgegevens**: alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.
- **Response team datalekken**: een door directeur tijdelijk ingesteld team, die zorgdraagt voor een onderzoek en over de uitkomsten rapporteert aan de directie.
- **Verwerker**: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- **Verwerking van persoonsgegevens**: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens zoals bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
- **(Verwerkings-)verantwoordelijke**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In dit geval Welzijnswerk Midden-Drenthe .
- **Wet**: Wet bescherming persoonsgegevens (“Wbp”) en Algemene Verordening Gegevensbescherming (“AVG”).

3. Protocol



a. Identificeren van een beveiligings- of datalek

De melding van (een vermoeden) van een beveiligings- of datalek kan te allen tijde door iedereen worden gedaan, door personeelsleden van Welzijnswerk , maar ook door externen binnen en buiten Welzijnswerk Midden-Drenthe .[4] Eenieder die een (mogelijk) beveiligings- of datalek constateert, meldt dit incident per omgaande bij de [directeur en medewerker p&o) via datalek@welzijnswerkmd.nl.

Het doen van de melding is vormvrij, om de drempel laag te houden. Melder hoeft enkel een zo uitgebreid mogelijke beschrijving van het beveiligings- of datalek te geven. Melder kan eventueel documenten toevoegen ter onderbouwing van de melding. De melder kan urgentie meegeven aan de melding: response binnen een werkdag of een week. Dit leidt tot snellere start van de behandeling en bewaking van de voortgang.

Nadat de melding is gedaan ontvangen de (directeur en medewerker p&O) hiervan bericht en nemen zij de melding in behandeling. De (directeur en/of medewerker p&o) zorgen voor permanente bereikbaarheid middels e-mail.

De (directeur en/of medewerker p&o) begint met het aanleggen van een logboek, waarin alle relevante gebeurtenissen, beslissingen en tijdstippen worden vastgelegd. Indien relevant wordt ook informatie

[4] Ook een verwerker kan een (vermoeden van) een beveiligings- of datalek constateren en melden aan diens opdrachtgever binnen Welzijnswerk Midden-Drenthe .

veiliggesteld voor een eventuele juridisch vervolg van het incident.

b. Beoordeling melding; wel of geen datalek?

De [directeur of medewerker p&o] neemt op verzoek of eigen initiatief contact op met de melder (mits de melding niet anoniem is gedaan). De directeur of medewerker p&o zorgen zo spoedig mogelijk voor volledige en juiste informatie, zoals opgenomen in het meldingsformulier van AP[5] en zorgen voor een eerste analyse om te bekijken of er sprake is van een beveiligings- of datalek.

De beoordeling of er sprake is van een beveiligings- of datalek, en of er gemeld moet worden aan AP, komt tot stand met behulp van de (beslisbomen uit) Beleidsregels. Bij de beoordeling spelen o.a. een rol:

- is er enkel sprake van een dreiging van verlies (dus een beveiligingslek)?
- is er sprake van verlies van persoonsgegevens;
- is er sprake van onrechtmatige verwerking van persoonsgegevens;
- 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;
- leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen.

In geval dat het beveiligingslek niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Melding bij AP is dan niet aan de orde, maar de melding wordt dan wel geregistreerd door de [FG] en gerapporteerd aan de directie.

Blijkt uit de eerste analyse dat er sprake is van een (mogelijk) datalek, dan voert de medewerker p&o de volgende acties uit:

- hij informeert telefonisch de directie en bevestigd dit daarna per e-mail;
- hij roept het [RESPONSETEAM DATALEK] bijeen bij de eerste gelegenheid (indien nodig en mogelijk onmiddellijk anders naar het gezamenlijk oordeel van de directeur en medewerker p&o.

c. Instellen Responseteam datalek

Het team bestaat uit [directeur] (voorzitter), de leidinggevende onder wiens verantwoordelijkheid het (mogelijke) datalek heeft plaatsgevonden, de medewerker p&o, de betrokken [FUNCTIONEEL BEHEERDER] en eventueel een [TECHNISCH BEHEERDER]. Zo nodig kan advies worden gevraagd aan de externe jurist en de communicatie medewerker.
De directeur organiseert het [RESPONSETEAM], zorgt voor een agenda, de wijze van overleggen & communiceren, aanleg van een logboek met overwegingen en besluiten en verslaglegging.

Het [RESPONSETEAM] draagt zorgt voor (en legt vast):

- beoordeling van de melding;
- uitvoering noodzakelijke acties met betrekking tot het datalek (bijvoorbeeld datalek onmiddellijk dichten, sporen verzamelen, toegang tot informatie beperken en eventueel hulp inroepen voor nader onderzoek);
- of en wat gemeld gaat worden bij AP;
- wijze van afhandeling intern, inclusief communicatie naar de melder, betreffende afdeling-(en) en manager(s);
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden;
- het al dan niet doen van aangifte en vaststellen of er sprake is van strafrechtelijke verwijtbaarheid;
- besluiten over in-en externe communicatie: op welk moment, door welke actiehouder en welke boodschap;
- op welke wijze er intern wordt gerapporteerd;
- of eventuele schade is gedekt door de verzekeringspolis.

[5] https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

d. Melding AP
De directeur verzorgt, indien er sprake is van een datalek dat gemeld moet worden bij AP, tijdig (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) de elektronische melding bij AP[6]
De directeur of medewerker p&o registreert de ontvangstbevestiging van AP en slaat het meldingsformulier op. De directeur en medewerker p&o fungeren als contactpersoon inzake de communicatie met AP.

e. Beoordeling melding aan betrokkenen
Indien een datalek is gemeld aan AP dient tevens vastgesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat (betrokkenen) met behulp van de schema's uit de Beleidsregels.

f. Melden aan betrokkenen (indien van toepassing)
In opdracht van de directie stelt de medewerker p&o in samenspraak met de communicatie medewerker en een eventuele externe jurist een kennisgeving aan betrokkenen op.

De melding bevat in ieder geval de aard van de inbreuk, contactgegevens Welzijnswerk Midden-Drenthe , het informatiepunt waar de betrokkenen meer informatie over de inbreuk kan krijgen en de maatregelen die [Welzijnswerk Midden-Drenthe] de betrokkenen aanbeveelt om te nemen teneinde de negatieve gevolgen van de inbreuk te beperken.
Het is hierbij ook van belang om over verdere communicatie richting betrokkenen na te denken, bijvoorbeeld het openen van een responsekanaal, een FAQ-pagina op de website, een bijeenkomst en dergelijke.

g. Verrichten datalek onderzoek
De directie en/of medewerker p&o stelt een onderzoek in naar de feitelijke toedracht van het datalek. Met (naar haar mening) relevante leden van het [RESPONSETEAM] onderzoekt zij of en zo ja hoe dergelijke datalekken in de toekomst voorkomen kunnen worden.

De bevoegdheden van het [RESPONSETEAM] zijn:

- vrijheid om met alle partijen betrokken bij het datalek en de melding te spreken;
- alle relevant geachte documenten & data inzien en bewaren;
- toegang tot alle plaatsen die het team nodig acht ten behoeve van een zorgvuldige analyse;
- actie naar verwerkers conform afspraken in de toepasselijke verwerkersovereenkomst;
- het recht en de middelen om externe deskundigen in te zetten in het onderzoek.

Datalekken zijn soms eenvoudig te analyseren, vaak echter gaat het spoor schuil achter techniek en is externe expertise vereist. We streven ernaar hiervoor a priori afspraken te maken met een forensische onderzoekspartij. Hetzelfde geldt voor crisiscommunicatie. Competente ondersteuning kennen en weten hoe deze op het juiste moment kan worden ingeschakeld is belangrijk.

h. Slotbijeenkomst responseteam datalek
Zo snel als mogelijk presenteert de directeur en/of medewerker p&o de bevindingen & aanbevelingen aan de directie/bestuur, die daarop besluit:

- welke verbetermaatregelen getroffen moeten worden;
- of en hoe over het rapport en de aanbevelingen gecommuniceerd wordt.

i. Implementeren verbetermaatregelen
De eigenaar van het betrokken informatiemiddel of -verwerking is ook verantwoordelijk voor de implementatie van de vanuit het beveiligings- of datalek vastgestelde verbetermaatregelen. Hij ziet toe op de communicatie

[6] https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

rondom de verbetermaatregelen en dat de genomen maatregelen worden geëvalueerd op effectiviteit. Hij rapporteert over de voortgang van deze stappen aan de directeur/ het bestuur.

j. Sluiting melding en vastlegging

De directie en/of medewerker p&o informeert het [RESPONSETEAM], indien noodzakelijk het bestuur en de direct bij het incident betrokken personen op het moment dat het datalek definitief afgehandeld is en de melding gesloten is.

Het datalek wordt opgenomen in de registratie bij or. Ieder kwartaal doet de medewerker p&o verslag aan de directie over de behandelde meldingen van beveiligingslekken en datalekken in de reguliere rapportage.