PROCEDURE DATALEKKEN

Stichting “Woningstichting Van Alckmaer voor Wonen”

VERSIE April 2018

Vastgesteld op : 17 mei 2018

Directeur bestuurder

1. Inleiding

Dit document geeft een beschrijving van verschillende rollen en fases die binnen Van Alckmaer belangrijk zijn bij de afhandeling van beveiligingsincidenten en datalekken. Het proces gaat uit van drie rollen en zes fases. Een belangrijk uitgangspunt is dat het proces ertoe moet leiden dat alle relevante feiten goed worden vastgelegd gedurende de afwikkeling van een beveiligingsincident/mogelijk datalek. Het vastleggen van deze feiten gebeurd in het register datalekken..

Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan, waarbij persoonsgegevens onrechtmatig verwerkt zijn of wanneer het niet uitgesloten kan worden dat één van deze mogelijkheden plaats heeft gevonden. Wanneer Van Alckmaer tot de conclusie komt dat het om een datalek gaat, moet worden bepaald of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens. Afhankelijk daarvan wordt het datalek gemeld aan de Autoriteit Persoonsgegevens (hierna: AP) of niet.

2. Doelstelling

Een eenduidige afhandeling van beveiligingsincidenten.

3. Beoogd resultaat

A. Beveiligingsincidenten worden afgehandeld volgens de beschreven procedure.
B. Alle beveiligingsincidenten worden geregistreerd in het register datalekken.
C. Datalekken worden binnen 72 uur gemeld aan de AP.

4. Meldplicht datalekken: rolverdeling (drie rollen)

Om de juiste informatie tijdig op de juiste plek te krijgen voor de afhandeling van een beveiligingsincident onderscheidt Van Alckmaer 3 rollen:

Ontdekker
Degene die het beveiligingsincident en mogelijk datalek op het spoor komt, vaak ook degene die (in eerste instantie) over de meeste informatie beschikt.

Melder
Degene die belast is met het vergaren van de relevante informatie om op basis daarvan een melding te kunnen doen aan de AP en eventueel aan getroffen klanten. In de meeste gevallen is dit de afdeling Bedrijfsvoering.

Technicus
Degene die, indien het datalek een technische oorzaak heeft (wat vaak het geval zal zijn), maatregelen kan nemen zodat het lek ‘gedicht’ wordt. In de regel is dit de systeembeheerder.

4.1 Verantwoordelijkheden

De hierboven beschreven rollen hebben ieder hun eigen verantwoordelijkheden. Hierna worden deze kort omschreven.

Ontdekker
De ontdekker is degene die een beveiligingsincident/mogelijk datalek signaleert en daarover rapporteert bij de melder binnen Van Alckmaer. Naast de ontdekker binnen Van Alckmaer kan er ook sprake zijn van een situatie waarbij de ontdekker een persoon is buiten Van Alckmaer zoals bijvoorbeeld een leverancier. Om dit risico af te kunnen dekken zijn strikte bepalingen omtrent datalekken en de afhandeling ervan opgenomen in de verwerkersovereenkomst.

Melder
De melder is de spin in het web van de (formele) afhandeling van het beveiligingsincident en bij Van Alckmaer is dit belegd bij de afdeling Bedrijfsvoering. De afdeling Bedrijfsvoering verzamelt alle benodigde informatie. Aan de hand de verzamelde informatie bepaalt de afdeling Bedrijfsvoering of gemeld moet worden aan de AP of niet. En zo ja, of eveneens aan de betrokkenen gemeld moet worden dat zijn of haar persoonsgegevens zijn gelekt. De melder is ook degene die deze melding bij de AP daadwerkelijk doet en zorgt voor archivering van de melding. De afdeling Bedrijfsvoering informeert de directeur-bestuurder over het beveiligingsincident.

Technicus
De technicus is degene die de melder kan helpen met:
- De beantwoording van de vraag welke typen persoonsgegevens gelekt zijn.
- De beantwoording van de vraag wanneer het datalek heeft plaatsgevonden (incl. inzage in of analyse van logfiles).
- De beantwoording van de vraag of de data beveiligd is door bijvoorbeeld versleuteling of anderszins onbegrijpelijk is gemaakt voor derden en op welke wijze dit is gerealiseerd.
- Het repareren van het datalek.
- Voor overige technische vragen.

De melder moet aan de hand van de informatie die hij of zij van de ontdekker ontvangt, snel kunnen vaststellen welke technicus betrokken moet worden bij de afhandeling van het datalek. Van Alckmaer heeft hiertoe een overzicht opgesteld met alle aanwezige systemen en het daarbij behorende (technische) aanspreekpunt.

Bovengenoemde rollen sluiten elkaar niet uit: de ontdekker, maar vooral de technicus en melder kunnen, zeker in een kleine organisatie als Van Alckmaer, één en dezelfde persoon zijn.

5. Procedure meldplicht datalekken: zes fases

In de afhandeling van een beveiligingsincident en mogelijk datalek kunnen zes fases worden onderscheiden. Deze fases zijn niet per se strikt van elkaar gescheiden en de volgorde staat – uitzonderingen daargelaten - evenmin vast. De fases zijn:

1. Ontdekken;
2. Inventariseren;
3. Kwalificeren;
4. Repareren;
5. Melden;
6. Archiveren.

6.1 Ontdekken
De ontdekker komt een beveiligingsincident en daarmee een mogelijk datalek op het spoor. De ontdekker verzamelt relevante feiten voor de melder.
Het is wenselijk dat, voor zover mogelijk, de hierna genoemde informatie door de ontdekker wordt verstrekt aan de melder. Dit kan worden aangevuld door de technicus en de melder zelf. Het gaat om de volgende informatie:
- De samenvatting van het incident.
- Het aantal betrokkenen en van wie zijn de persoonsgegevens gelekt.
- Een omschrijving van de groep betrokkenen (klanten, medewerkers, etc.).
- Welke persoonsgegevens gelekt zijn (NAW-gegevens, IBAN, bijzondere of gevoelige gegevens, etc.).
- Of de eigen organisatie als verwerkingsverantwoordelijke of verwerker aan te merken is.
- Wanneer het datalek is ontstaan.
- Wat de oorzaak is van het datalek.
- Welke technische en/of organisatorische maatregelen er getroffen zijn om het datalek te dichten, en/of in de toekomst te kunnen voorkomen.

6.2 Inventariseren
Naast de gegevens die de melder ontvangt van ontdekker, zal het in sommige gevallen nodig zijn om aanvullende informatie omtrent het datalek te verzamelen. Deze informatie is nodig om af te wegen of er wel of geen verplichting is tot het melden van het datalek bij de AP en eventueel bij de betrokkenen. Het grootste gedeelte van de nog ontbrekende informatie zal van technische aard zijn. De melder zal bij de technicus te rade moeten gaan voor deze informatie.

Wanneer contact gelegd wordt met de technicus, zal deze direct de opdracht moeten krijgen om het beveiligingsincident/mogelijk datalek te (laten) repareren. De technicus zal de melder op de hoogte moeten houden van de ontwikkelingen hieromtrent. De melder registreert in het Register Datalekken het beveiligingsincident.

6.3 Kwalificeren
Wanneer de feiten zijn verzameld, kan de melder bepalen of het beveiligingsincident een datalek is en of het gemeld moet worden aan de AP en eventueel aan de betrokkenen. Dit gebeurt aan de hand van het beslissingsschema datalekken (zie bijlage 1). De uitkomst van deze kwalificatie moet eveneens in het Register Datalekken worden opgenomen.

6.4 Repareren
Onafhankelijk van de uitkomst van punt 6.3 zullen er maatregelen getroffen moeten worden om het beveiligingsincident/mogelijk datalek te dichten en ook eventueel te voorkomen in de toekomst. Dit gebeurt door de technicus. De technicus houdt de melder op de hoogte van de voortgang. Daarnaast wordt er waar nodig ook gewerkt aan structurele maatregelen zodat een dergelijk beveiligingsincident/mogelijk datalek onder gelijkblijvende omstandigheden zich in de toekomst niet nogmaals voordoet.

6.5 Melden
Indien het datalek onder de meldplicht valt, zal het moeten worden gemeld. De meldplicht is tweeledig: naast dat gemeld moet worden aan de AP, moet onder voorwaarden ook aan de betrokkenen gemeld worden. De melder heeft reeds onder stap 3 bepaald of en aan wie gemeld moet worden. De melder is ook degene die belast is met het daadwerkelijk doen van de melding. Het afschrift van de gedane melding, het meldingsnummer en de ontvangstbevestiging worden in het Register Datalekken ondergebracht.

6.6 Archiveren
Wanneer de zaak is afgerond, worden alle documenten gearchiveerd. De meeste informatie is reeds in het Register Datalekken ondergebracht.

<u>Register Datalekken</u>
Alle informatie over een beveiligingsincident en/of mogelijk datalek, wordt op een centrale plek verzameld en vastgelegd in het Register Datalekken. Deze vastlegging dient twee doelen:

a. De melder houdt overzicht over de lopende zaken. Er zijn nogal wat variabelen bij de afhandeling van een datalek. Zeker wanneer er mee dan één datalek tegelijk is, is het van belang om overzicht te kunnen houden.
b. Incidenten die onder het begrip datalek vallen, dienen te worden gedocumenteerd. De AP mag de documentatie van datalekken opvragen om naleving van de privacyverordening te controleren.