



Privacybeleid

Om te voldoen aan de eisen die aan ons gesteld worden vanuit de Algemene Verordening Gegevensbescherming is er voor Ala Care een privacyverklaring opgesteld. Voor het gebruik van bijvoorbeeld fotomateriaal is altijd toestemming nodig van de cliënt, deze toestemming wordt vastgelegd in de cliëntdossiers. De grondslagen voor het houden van persoonsgegevens staan hieronder:

Grondslag	Praktische invulling
Wet op de loonbelasting (artikel 28, lid 1 sub f)	- Kopie volledig ID bij indiensttreding opnemen in dossier medewerker - Er hoeft niet een nieuw bewijs te worden aangeleverd wanneer het gebruikte identificatiebewijs is verlopen
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (artikel 6)	- Bij intake documentnummer overnemen van identiteitsbewijs of paspoort gedocumenteerd (dus geen kopie!)

Procedure meldplicht datalekken

Met ingang van 1 januari 2016 geldt volgens de Wet bescherming persoonsgegevens (Wbp) de meldplicht voor datalekken. Per 25 mei 2018 is deze verplichting via de Algemene verordening Gegevensbescherming onderdeel van Nederlandse wet- en regelgeving.

Volgens deze meldplicht moeten organisaties die persoonsgegevens verwerken, datalekken melden aan Autoriteit Persoonsgegevens (AP) (en in bepaalde gevallen ook aan de betrokkenen) als het leidt tot (of een aanzienlijke kans dat dit leidt tot) ernstige nadelige gevolgen in relatie tot de integriteit / bescherming van persoonsgegevens.

Een datalek treedt op wanneer er persoonsgegevens inzichtelijk worden voor ongeautoriseerde personen, of wanneer persoonsgegevens onbeschikbaar worden (dus, als een computer crasht met daarop persoonsgegevens en je hebt geen backup).

Definitie 'Persoonsgegevens'

'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) (art.4, sub 1, AVG). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens.

Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, evt. in combinatie met het adres en de geboortedatum.

Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.

Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijk personen redelijkerwijs wordt uitgesloten'.

Ala Care heeft de plicht om iedere melding van een datalek te onderzoeken op ernst en impact. Als na onderzoek blijkt dat er sprake is van een datalek dat gemeld moet worden aan de AP, dan **dient deze melding binnen 72 uur plaats te vinden.**

Te denken valt aan:

- een kwijtgeraakte USB-stick
- een gestolen laptop
- een inbraak door een hacker
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden
- zichtbaar zijn voor alle andere geadresseerden
- een malware-besmetting
- een calamiteit zoals een brand in een datacentrum
- gecrashte computer met persoonsgegevens en je hebt geen backup

Definitie 'Betrokkenen'

'Is/zijn degene(n) van wie persoonsgegevens zijn gelekt'.

Een datalek moet naast aan de AP ook aan de betrokkene(n) worden gemeld als het datalek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkenen. (Achterliggende gedachte hierbij is dat betrokkenen in een zo vroeg mogelijk stadium in staat gesteld worden maatregelen te nemen teneinde de impact van het datalek op hun persoonlijke levenssfeer te beperken).

Doel procedure meldplicht datalekken

Het voldoen aan wetgeving door het op een juiste manier omgaan met persoonsgegevens en het verplicht melden van datalekken aan de AP.

Afspraken met een Verwerker:

- Ala Care heeft vastgelegd wie de specifieke verwerkers zijn van persoonsgegevens;
- Ala Care zorgt ervoor dat de verwerkers maatregelen treffen die nodig zijn, zodat we daarmee aan de meldplicht voor datalekken voldoen;
- Ala Care maakt afspraken met de verwerker over de volgende zaken en legt deze vast in contracten (of in een addendum);
- De verwerker is verplicht Ala Care te informeren over alle relevante incidenten;
- Ala Care hoort per incident alle relevante informatie te ontvangen van de verwerker;
- Hoe informeert de verwerker Ala Care over de incidenten?
- Wanneer precies behoort de verwerker Ala Care te informeren over de incidenten?
- De verwerker is verplicht om Ala Care onmiddellijk op de hoogte te houden van eventuele nieuwe ontwikkelingen rond het incident en van de maatregelen die de verwerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen. De

verwerker moet kunnen aantonen/vaststellen dat Ala Care daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt

Intern melden van een datalek

Zodra binnen of door Ala Care een datalek wordt geconstateerd, wordt deze onmiddellijk gemeld aan een de directie. (Indien melding wordt gedaan over poststukken/brieven die op straat gevonden worden, zal al het mogelijke worden gedaan om de post z.s.m. naar kantoor te krijgen). I.v.m. het beheren en monitoren van de melding, wordt alle informatie (t.a.v. de melding t/m de afhandeling) gelijktijdig toegedaan aan de Functionaris Gegevensbescherming.

Verwerking gegevens datalek

De gegevens m.b.t het datalek worden verzameld en geregistreerd en dienen als input voor verbeteracties en worden gecommuniceerd aan betrokkenen (in-/extern).

Extern melden van een datalek aan de Autoriteit Persoonsgegevens (AP) Nagegaan wordt welke specifieke datalekken moeten worden gemeld. Om vast te stellen of een specifiek datalek moeten worden gemeld aan de AP, worden de guidelines gevolgd

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf. Er is een voorbeeldlijst van datalekken die al dan niet gemeld moeten worden: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2020_voorbeeldlijst_wel_niet_melden_datalek_def.pdf Het datalek moet worden gemeld aan de AP via een speciaal meldingsformulier van de AP.

<https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0>

Het datalek moet onmiddellijk gemeld worden aan de AP. **(Uiterlijk op de tweede werkdag na de ontdekking van het incident moet de melding worden gedaan,** tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht valt. Evt. kan de melding naderhand nog worden aangevuld of ingetrokken. In de melding aan de AP moet aangeven worden of het datalek al aan de betrokkenen is gemeld en, zo niet, wanneer dat wordt gedaan. De termijn die we in de melding aan de AP aangeven, moeten we nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan moeten we dit aan de AP laten weten d.m.v. een aanpassing van de melding.

In de kennisgeving aan de betrokkene moet het volgende worden vermeld:

- de aard van de inbreuk
- de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen
- de maatregelen die we de betrokkene aanbevelen om te nemen, om de negatieve gevolgen van de inbreuk te beperken

Ala Care houdt een overzicht bij van alle datalekken die onder de meldplicht vallen. Per datalek staan in het overzicht in ieder geval de feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen.

Communicatie binnen Ala Care

Het geconstateerde datalek en benodigde acties worden binnen Ala Care gecommuniceerd met de betrokkenen.