PROCEDURE MELDPLICHT DATALEKKEN

Er is sprake van een Datalek indien persoonsgegevens als gevolg van een beveiligingsincident in handen vallen van onbevoegde derden. Het kan bijvoorbeeld gaan om een zoekgeraakte USB-stick, de diefstal van een laptop, een email die is verstuurd aan verkeerde (of ten onrechte zichtbare!) emailadressen of de inbraak door een hacker.

Gegevens Functionaris Gegevensbescherming

Naam : Bas Knoop
Telefoonnummer : 06-28722700

Inhoudsopgave

1. Inleiding

1.1. Dit document beschrijft de handelingen te verrichten door Alfa & Zorg BV bij een Datalek.

1.2. Een Datalek is gedefinieerd in de Algemene Verordening Gegevensverwerking ('AVG') als 'een inbreuk in verband met persoonsgegevens', hetgeen inhoudt dat er sprake is van 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.

1.3. Een Datalek dient zonder vertraging, binnen 72 uur nadat een mogelijk Datalek is vastgesteld, gemeld te worden aan de Autoriteit Persoonsgegevens ('AP'), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.

1.4. Deze meldplicht is eveneens van toepassing op Alfa & Zorg BV als het Datalek bij een derde is ontstaan, bijvoorbeeld een verwerker van persoonsgegevens van Alfa & Zorg BV('Verwerker').

1.5. Indien Alfa & Zorg BV zelf geen verwerkingsverantwoordelijke is, dan dient de melding zo snel mogelijk, binnen 24 uur nadat een mogelijk Datalek is vastgesteld, door de Functionaris Gegevensbescherming ('FG') of een (andere) medewerker aan de verantwoordelijke gemeld te worden. In dat geval is deze procedure niet verder van toepassing en draagt de FG of (andere) medewerker er voor zorg dat de verantwoordelijke kan voldoen aan haar verplichtingen uit hoofde van de AVG.

2. Interne melding van een datalek

2.1. De medewerker die een (mogelijk) Datalek constateert, meldt dit incident per omgaande bij de directie van Alfa & Zorg BV en aan de FG van Alfa & Zorg BV.

2.2. Een medewerker van Alfa & Zorg BV of een Verwerker is te allen tijde bevoegd zelfstandig een melding te doen aan de FG.

2.3. De FG ziet er op toe dat vervolgens deze Procedure Meldplicht Datalekken wordt doorlopen.

3. Wanneer moet een Datalek worden gemeld aan de AP?

3.1. Niet alle Datalekken hoeven aan de AP te worden gemeld; alleen Datalekken waarvan het waarschijnlijk is dat dit Datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Alfa & Zorg BV zal aan de hand van de AVG (artikel 33) en de door de AP beschikbaar gestelde beleidsregels vaststellen of sprake is van een Datalek dat gemeld moet worden.

3.2. Bij de beoordeling van de vraag of het Datalek gemeld moet worden speelt (i) de aard van de persoonsgegevens een rol (bijzondere persoonsgegevens, gegevens over de financiële situatie van betrokkene, gebruikersnamen en wachtwoorden, gegevens die kunnen worden gebruikt voor identiteitsfraude, etc) of (ii) andere factoren, zoals de hoeveelheid gelekte persoonsgegevens of het aantal betrokkenen van wie gegevens zijn gelekt.

3.3. Indien het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een Datalek maar van een beveiligingslek. In dat geval is melding aan de AP niet nodig.

4. Inventarisatie (mogelijk) Datalek?

4.1. Alfa & Zorg BV draagt zo spoedig mogelijk zorg voor het inventariseren en verzamelen van de informatie die benodigd is voor het (eventueel) melden van een Datalek aan de AP. Daarbij dient het formulier van de AP voor het melden van Datalekken als uitgangspunt dienen. Het formulier is te vinden op het volgende adres: https://Datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

4.2. Op basis van de verkregen informatie en bij het vermoeden van een Datalek wordt in overleg tussen de FG en de eventuele overige verantwoordelijke en/of betrokken personen in de organisatie van Alfa & Zorg BV of de betreffende Verwerker, beoordeeld of daadwerkelijk sprake is van een Datalek.

4.3. In het in het voorgaande lid bedoelde overleg wordt beoordeeld of er direct maatregelen dienen te worden genomen om verdere schade zoveel mogelijk te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen. Indien nodig kan advies gevraagd worden aan de (externe) juridisch adviseur.

5. Melden aan de Autoriteit Persoonsgegevens (AP)

5.1. De FG verzorgt de tijdige melding bij de AP volgens het hierboven onder 4.1 genoemde meldingsformulier van de AP. De melding dient onverwijld, zonder onnodige vertraging en niet later dan 72 uur na de ontdekking van het Datalek te geschieden. De Directie van Alfa & Zorg BV wordt tevens op de hoogte gesteld van de melding.

5.2. De FG fungeert als contactpersoon inzake de communicatie met de AP. Afhankelijk van de aard van het Datalek of indien blijkt dat het incident geen Datalek is kan de melding aan de AP worden aangevuld of ingetrokken.

5.3. De FG draagt er zorg voor dat de bij het incident betrokken medewerkers worden geïnformeerd en vraagt de bij het incident betrokken medewerkers om zo snel mogelijk een verslag op te stellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan de directie en de FG verstrekt behoeve van het Datalekkendossier van Alfa & Zorg BV.

5.4. Na ontvangst van de melding aan de AP zal de AP daarvan een ontvangstbevestiging sturen. De AP neemt alleen contact op indien de AP daartoe aanleiding ziet.

6. Is sprake van een (niet-ethische) hack?

6.1. Bij een Datalek als gevolg van een (niet-ethische) hack (artikel 138ab Wetboek van Strafrecht), is het van belang om vast te stellen wat de aard van de gelekte persoonsgegevens is en wat de risico's van misbruik voor de betrokkene(n) zijn. Bij een hack kan het naast het doen van de melding bij de AP ook zinvol zijn om aangifte te doen bij de politie. De FG zal daarvoor na overleg met de directie van Alfa & Zorg BV zorgdragen.

7. Dient het Datalek te worden gemeld aan betrokkene(n)?

7.1. Indien een Datalek is gemeld aan de AP dient te worden vastgesteld of het Datalek ook moeten worden gemeld aan degenen om wiens persoonsgegevens het gaat. De directie zal dat in overleg met de FG vaststellen.

7.2. De FG zal aan de hand van de AVG (artikel 34) en de door de AP beschikbaar gestelde beleidsregels vaststellen of betrokkenen dienen te worden geïnformeerd.

7.3. Melding aan betrokkenen vindt in ieder geval plaats als het Datalek *mogelijk* een groot risico voor de rechten en vrijheden van betrokkenen kan inhouden.

8. Handelwijze melding aan betrokkene(n)

8.1. In opdracht van de directie van Alfa & Zorg BV stelt de FG in samenspraak met de eventuele overige verantwoordelijke en/of betrokken personen in de organisatie een kennisgeving aan betrokkene(n) op. De FG bepaalt wat aan de betrokkene(n) wordt gemeld.

8.2. De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van Alfa & Zorg BV en een contactpersoon of informatiepunt waar de betrokkene(n) meer informatie over de inbreuk kan (kunnen) krijgen, de waarschijnlijke gevolgen van het Datalek en de maatregelen die Alfa & Zorg BV de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.

8.3. Het Datalek moet onverwijld gemeld worden aan de betrokkene(n). Daarbij dient rekening te worden gehouden met het (eventuele) feit dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het Datalek.

8.4. In de melding aan de AP is aangegeven of het Datalek aan betrokkene(n) wordt gemeld. Indien de aan de AP aangegeven termijn waarbinnen die melding aan de betrokkene(n) zou worden gedaan niet wordt gehaald dan dient de FG dit aan de AP door te geven door middel van een aanpassing van de eerdere melding.

9. Onderzoek naar het Datalek en vaststellen verbetermaatregelen

9.1. De FG stelt zo spoedig mogelijk na de vaststelling van het (mogelijke) Datalek een (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) Datalek en betrekt daarbij de vraag of en hoe dergelijke Datalekken in de toekomst kunnen worden voorkomen.

9.2. In overleg met de directie van Alfa & Zorg BV mag de FG daartoe met medewerkers van Alfa & Zorg BV en/of overige relevante personen (zoals eventueel medewerkers van de Verwerker(s) van Alfa & Zorg BV) spreken, alle relevante documenten inzien en toegang hebben tot alle plaatsen, voor zover noodzakelijk voor een zorgvuldig onderzoek;

9.3. De FG kan de directie van Alfa & Zorg BV voorstellen om waar nodig externe partijen te betrekken indien dat voor een deugdelijk onderzoek noodzakelijk is.

9.4. De FG rapporteert de conclusies van het hiervoor bedoelde onderzoek zo spoedig mogelijk aan de directie van Alfa & Zorg BV.

9.5. In overleg waarbij in ieder geval de directie van Alfa & Zorg BV en de FG aanwezig zijn zullen de uitkomsten van het hiervoor genoemde onderzoek worden besproken en

afspraken worden gemaakt over verbetermaatregelen om herhaling van het incident dat heeft geleid tot het Datalek zoveel mogelijk te voorkomen.

9.6. De directie van Alfa & Zorg BV besluit welke verbetermaatregelen worden geïmplementeerd en ziet toe op de implementatie daarvan. De maatregelen worden in de organisatie van Alfa & Zorg BV (en waar nodig extern, zoals aan een Verwerker) gecommuniceerd.

10. Vastleggen van Datalekken

Het Datalek-dossier wordt digitaal bij de FG en het secretariaat van de directie van Alfa & Zorg BV bewaard voor de duur van minimaal 1 jaar na afronding van het dossier. Er kan een langere termijn van minimaal 3 jaar van toepassing zijn zoals bedoeld in de beleidsregels 'Meldplicht Datalekken in de Wet bescherming persoonsgegevens' van de AP, pagina 46. De FG draagt zorg voor een overzicht van alle Datalekken die zich hebben geopenbaard. Eventuele nieuwe beleidsregels van de AP op basis van de AVG kunnen tot een aanpassing van de bewaartermijn leiden.

Aldus op 8 mei 2018 vastgesteld door de directie van Alfa & Zorg BV