PROTOCOL MELDPLICHT DATALEKKEN

Overwegingen:

1. SMT Zorg B.V hecht belang aan een goede beveiliging van haar (elektronische) systemenwaarin persoonsgegevens zijn opgeslagen en worden verwerkt
2. Het valt desalniettemin nooit volledig te voorkomen dat er een datalek zal plaatsvinden
3. SMT Zorg B.V.is op grond van de Algemene verordening gegevensbescherming (AVG)verplicht om (ernstige) datalekken te melden aan de Autoriteit Persoonsgegevens en aan de betrokkenen
4. SMT Zorg B.V. wenst aan haar wettelijke verplichtingen te voldoen
5. SMT Zorg B.V. heeft daarom een beleid geformuleerd om zo adequaat mogelijk te handelenindien er onverhoopt toch een datalek plaatsvindt

1 - Definitie datalek

Er is sprake van een datalek als er een inbreuk op de beveiliging plaatsvindt die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of de ongeoorloofde verstrekking vanof ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

2 - Interne verantwoordelijke melding datalekken

2. SMT Zorg B.V. heeft een interne verantwoordelijke voor de verwerking van datalekkenaangesteld die verantwoordelijk is voor de melding van een datalek.
3. Deze verantwoordelijke is de afdeling Administratie, met als 1e aanspreekpunt: Jos Harders, telefoonnummer: 053 888 2 666 e-mailadres: j.harders@smtzorg.nl hierna te noemen: '**interne verantwoordelijke**'.
4. 2e aanspreekpunt: Heleen Yangin, 06 44 89 7332 secretariaat@smtzorg.nl

3 - Interne melding bij ontdekking van een datalek

1. Degene die een datalek bij SMT Zorg B.V. ontdekt, meldt dit per omgaande aan de interneverantwoordelijke.
2. Indien mogelijk, zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelektegegevens meteen op afstand worden gewist of ontoegankelijk gemaakt.

4 - Onderzoek door de interne verantwoordelijke

De interne verantwoordelijke onderzoekt onder meer:

1. Of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden
2. Wie of welke afdelingen binnen de organisatie betrokken zijn bij het datalek
3. Of er een verwerker betrokken is bij het incident

5 - Bestrijding datalek

De interne verantwoordelijke stopt het datalek indien dat nog kan en neemt voorts de noodzakelijkemaatregelen om het datalek zo goed mogelijk te bestrijden.

- Vaststelling van de gevolgen van een datalek

De interne verantwoordelijke onderzoekt de mogelijke gevolgen van het datalek aan de hand van deaard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen van de betrokkenen kan zijn.

6 - Medewerking verstrekking gegevens omtrent het datalek

De ontdekker/melder van het datalek biedt alle medewerking aan de interne verantwoordelijk doorzo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:

- Wat is er gebeurd? (omschrijving van het incident)
- Ging het per ongeluk of is het veroorzaakt door kwade opzet (denk aan gehackte gegevens)?
- Wanneer is het gebeurd? (datum en tijdstip)
- Wanneer is het ontdekt?
- Wat voor gegevens(registers) zijn gelekt?
- Zijn de gegevens versleuteld, en zo ja hoe?
- Konden de gegevens op afstand worden gewist of ontoegankelijk gemaakt, en zo ja, is datgebeurd?
- Wat zijn de mogelijke gevolgen voor de betrokkenen?
- Welke groep(en) personen is/zijn hierdoor getroffen? (bijvoorbeeld: leerlingen, patiënten,premium leden)
- Hoeveel personen zijn hierdoor (bij benadering) getroffen?
- Zijn er ook gegevens van personen in andere EU-landen getroffen door het datalek?
- Konden er al technische en/of organisatorische maatregelen worden getroffen naaraanleiding van het incident?

7 - Beschikbaarheid personeel na ontdekking datalek

De verantwoordelijke van de afdeling vanuit waar het datalek heeft plaatsgevonden als ook de ontdekker van het datalek en iedereen die vanuit hun functie of kennis in staat is om organisatorische en/of technische maatregelen te treffen om de gevolgen van het datalek te beperken, houden zich de 1e 24 uur na ontdekking van het datalek beschikbaar voor overleg met deinterne verantwoordelijke c.q. eventueel door hem aangewezen experts en voor het zo nodig uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

8 - Beslissing melding datalekken

1. De interne verantwoordelijke beslist zo spoedig mogelijk doch in elk geval binnen 60 uur na ontdekking van het datalek - al dan niet in overleg met de verantwoordelijke van de afdeling vanuitwaar het datalek is ontdekt en/of door hem aangewezen experts - of het datalek dient te worden gemeld aan de Autoriteit Persoonsgegevens en/of de

betrokkenen.

2. Een datalek wordt in principe altijd gemeld aan de Autoriteit Persoonsgegevens, tenzij het nietwaarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen.
3. De melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven inonderdeel 7.
4. Een datalek dat gemeld is aan de Autoriteit Persoonsgegeven wordt eveneens gemeld aan de betrokkenen indien het een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, tenzij inmiddels passende maatregelen zijn genomen dat het hoge risico heeft afgewend.

9 - Melding datalekken aan de Autoriteit Persoonsgegevens en/of betrokkenen

1. De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de AutoriteitPersoonsgegevens en/of de betrokkene(n).
2. Melding geschiedt zo spoedig mogelijk na de ontdekking en uiterlijk binnen 72 uur na ontdekkingvan het datalek.
3. Het is enige andere werknemer dan de interne verantwoordelijke niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) te melden.
4. Als een werknemer het niet eens is met de beslissing van de interne verantwoordelijke omtrent het dan niet melden van het datalek aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dankan hij zijn grieven kenbaar maken aan de directie.
5. Indien daartoe verzocht, verleent een werknemer alle medewerking aan de verantwoordelijke omde getroffen personen conform artikel 34 AVG te kunnen informeren omtrent het datalek.

10 - Gevolgen melding datalekken

- Indien het datalek negatieve gevolgen heeft voor betrokkenen, dan doet de interneverantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.
- Afhankelijk van de aard en de omvang van het datalek voor betrokkenen bepaalt de interneverantwoordelijke:

    - Op welke wijze betrokkenen worden geïnformeerd (waaronder in ieder geval de mededelingen worden gedaan welke soorten persoonsgegevens getroffen zijn, wat de mogelijke gevolgen zijn, welke maatregelen SMT Zorg B.V. neemt en op welke wijzebetrokkenen zelf de schade kunnen voorkomen of beperken
    - Welke nazorg betrokkenen krijgen
    - Welke acties in het belang van de organisatie noodzakelijk zijn

3. Indien een datalek heeft plaatsgevonden - ongeacht of deze is gemeld of niet - worden zo spoedigmogelijk adequate technische en/of organisatorische maatregelen getroffen om toekomstige gelijksoortige datalekken te voorkomen.

11 - Bijhouden register datalekken

De interne verantwoordelijke houdt een register bij van alle datalekken, waarin alle gegevensrondom het datalek worden geregistreerd, zoals:

- Een omschrijving van het incident

- Datum en tijdstip van het datalek
- Datum en tijdstip ontdekking van het datalek
- Omschrijving van de soort gelekte persoonsgegevens
- Omschrijving van de categorie(en) van betrokkenen die zijn getroffen
- Omschrijving aantal betrokkenen (bij benadering)
- Of ook gegevens van personen in andere EU-landen zijn gelekt
- Of het incident is gemeld aan de Autoriteit Persoonsgegevens en zo ja datum en tijdstipmelding
- Of het incident is gemeld aan de betrokkenen en zo ja, datum en tijdstip melding
- Op welke wijze betrokkenen zijn geïnformeerd
- De gevolgen van het datalek, met indien mogelijk vermelding van datum en tijdstip
- Welke technische en/of organisatorische maatregelen zijn getroffen na het datalek, metvermelding van datum en tijd.

<u>Stappenplan:</u> kom in actie bij een datalek. Wanneer wij als SMT Zorg te maken hebben met een datalek, komen we snel in actie. Hieronder ziet u het stappenplan dat wij hiervoor hanteren.

Stap 1: zorg voor overzicht

Analyseer onmiddellijk de situatie. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Indien gegevens zijn gelekt, onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Deze informatie heeft u nodig voor de vervolgstappen.

Stap 2: Beperk de schade!

Bepaal op basis van stap 1 of er maatregelen zijn die u meteen kunt nemen om het datalek te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Bijvoorbeeld door een gestolen laptop op afstand te wissen. Maak tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert (stap 3).

Stap 3: Wel/niet melden bij de AP

Bepaal of u het datalek verplicht moet melden bij de Autoriteit Persoonsgegevens (AP). Zo ja, zorg dat u dit ***binnen 72 uur*** nadat u het lek heeft ontdekt doet. U moet een datalek melden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Heeft u bij de eerste melding nog niet alle informatie over het datalek?
Doe dan een eerste melding binnen 72 uur en doe later een vervolgmelding.

Naar het meldloket datalekken
Zie ook: voorbeeldlijst 'datalek wel/niet melden bij AP en betrokkenen'

Stap 4: Wel/niet melden aan de betrokken personen

Bepaal of u het datalek verplicht moet melden aan de betrokken personen. Zo ja, zorg dat u dit zo snel mogelijk doet. U moet een datalek melden aan de betrokken personen wanneer er sprake is van een *hoog* risico voor de rechten en vrijheden van de betrokken personen.

Stap 5: Registreer het datalek

Registreer het datalek in uw verplichte datalekregister. Ook wanneer u het datalek niet meldt aan de AP.

Zie ook: 10 praktische tips voor betere datalekregistratie

Hieronder 10 punten om een datalek te voorkomen.
Deze punten zijn zowel van toepassing op het registreren van datalekken die wij verplicht zijn te melden bij de Autoriteit Persoonsgegevens (AP).

Omschrijf incidenten, de gevolgen en de corrigerende maatregelen **duidelijk en volledig.**

Maak expliciet onderscheid tussen **corrigerende en preventieve maatregelen**. Leg corrigerende maatregelen altijd vast in het datalekregister. Het kan nuttig zijn deze maatregelen mee te nemen in de plan-do-check-learn-act cyclus.

Voorkom versnippering van registraties: maak **één overzichtelijke registratie** die voor elk organisatieonderdeel tot op hetzelfde detailniveau wordt ingevuld. Overweeg bijvoorbeeld om de registratie inzichtelijk te maken voor alle medewerkers zodat zij het overzicht kunnen checken voordat zij zelf iets registreren.

Heeft uw organisatie een **functionaris gegevensbescherming** (FG)? Neem dan per incident op of de FG betrokken is en, zo ja, in welke mate.

Neem per incident op of het datalek is **gemeld bij de AP en de betrokken personen** en motiveer waarom dat wel of niet is gebeurd.

Wees **transparant naar de getroffen personen** als er een datalek is geweest. Communiceer hier duidelijk en tijdig over. Bewaar het bewijs van die communicatie en neem deze op in de registratie.

Stel een handleiding op of verzorg een training voor de **medewerkers die de datalekregistratie invullen.** Deze instructie kan onderdeel uitmaken van een gedocumenteerde meldingsprocedure voor de meldplicht datalekken.

Leg vast welke **andere organisaties** betrokken zijn geweest bij een inbreuk. Bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of subverwerkers. Dit is handig als een organisatie nieuwe verwerkersovereenkomsten sluit met de desbetreffende verwerkers.

Overweeg om de datalekken in te delen naar **aard, gevolgen en betrokkenen en mogelijke maatregelen.**

Bespreek de datalekregistratie regelmatig op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check-learn-act cyclus. Zo kunnen organisaties leren van fouten. De FG of privacycontactpersoon van uw organisatie kan bij deze besprekingen een actieve rol vervullen.