PROTOCOL DATALEKKEN FOCUS'07

Overwegingen:

- Focus'07 hecht belang aan een goede beveiliging van haar (elektronische) systemen waarin persoonsgegevens zijn opgeslagen en worden verwerkt.
- Het valt desalniettemin nooit volledig te voorkomen dat er een datalek zal plaatsvinden
- Focus'07 is op grond van de Algemene verordening gegevensbescherming (AVG) verplicht om (ernstige) datalekken te melden aan de Autoriteit Persoonsgegevens en aan betrokkene(n).
- Focus'07 wenst aan haar wettelijke verplichtingen te voldoen
- Focus'07 heeft daarom een beleid geformuleerd om zo adequaat mogelijk te handelen indien er onverhoopt toch een datalek plaatsvindt.

1. Definitie data

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 ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

2. Interne verantwoordelijke melding datalekken

a. Focus'07 heeft een interne verantwoordelijke voor de verwerking van datalekken aangesteld die verantwoordelijk is voor de melding van een datalek:
   Verantwoordelijke: Functionaris Persoonsgegevens
   E-mail: fg@focus07.nl
   Hierna te noemen: "*interne verantwoordelijke*"

3. Interne melding bij ontdekking van een datalek

a. Degene die een datalek bij Focus'07 ontdekt, meldt dit per omgaande aan de interne verantwoordelijke.
b. Indien mogelijk, zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelekte gegevens meteen op afstand worden gewist of ontoegankelijk gemaakt.
c. Degene die een datalek bij Focus'07 ontdekt, verstrekt geen informatie aan derden omtrent het datalek.

4. Onderzoek door de interne verantwoordelijke

a. De interne verantwoordelijke onderzoekt onder meer:
   - Of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden;
   - Wie of welke afdelingen binnen de organisatie betrokken zijn bij het datalek; en
   - Of er een verwerker betrokken is bij het incident.
b. Kan het incident betrekking hebben op persoonsgegevens, dan stelt de interne verantwoordelijke (zowel binnen als buiten werktijd) de voorzitter van Focus'07 onmiddellijk telefonisch en per e-mail op de hoogte via: voorzitter@focus07.nl

5. Bestrijding datalek

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

6. Vaststelling van de gevolgen van een datalek

De interne verantwoordelijke onderzoekt de mogelijke gevolgen van het datalek aan de hand van de aard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen van de betrokkene(n) kan zijn.

7. Medewerking verstrekking gegevens omtrent het datalek

Degene die een datalek bij Focus'07 ontdekt, biedt alle medewerking aan de interne verantwoordelijke door zo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:

- Wat is er gebeurd? (Omschrijving dan 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 dat gebeurd?
- Wat zijn de mogelijke gevolgen voor de betrokkene(n)?
- Welke groep(en) personen is/zijn hierdoor getroffen?
- Hoeveel personen zijn hierdoor (bij benadering) getroffen?
- Zijn er ook gegevens van personen in andere EU-landen getroffen door het datalek?
- Konden er l technische en/of organisatorische maatregelen worden getroffen naar aanleiding van het incident?

8. Beschikbaarheid personeel na ontdekking datalek

De interne verantwoordelijke alsook 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 eerste 24 uur na ontdekking van het datalek beschikbaar voor overleg en voor zo ver nodig het uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

9. Beslissing melding datalekken

a. De interne verantwoordelijke beslist zo spoedig mogelijk doch in elk geval binnen 60 uur na ontdekking van het datalek of het datalek dient te worden gemeld aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).
b. Een datalek wordt in principe altijd gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene(n).
c. De melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven in onderdeel 7.
d. Een datalek dat gemeld is aan de Autoriteit Persoonsgegevens wordt eveneens gemeld aan de betrokkene(n) indien het een hoog risico inhoudt oor de rechten en vrijheden van natuurlijke personen, tenzij inmiddels passende maatregelen zijn genomen dat het hoge risico heeft afgewend.

10. Melding datalekken aan de Autoriteit Persoonsgegevens en/of betrokkene(n)

a. De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).
b. Melding geschiedt zo spoedig mogelijk na de ontdekking en uiterlijk binnen 72 uur na ontdekking van het datalek.
c. Het is enige andere vrijwilliger/lid dan de interne verantwoordelijke niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) te melden.
d. Als een vrijwilliger/lid het niet eens is met de beslissing van de interne verantwoordelijke omtrent het al dan niet melden van het datalek aan de Autoriteit Persoonsgegevens en/of betrokkene(n), dan kan hij zijn grieven kenbaar maken aan het bestuur.
e. Indien daartoe verzocht, verleent een vrijwilliger/lid alle medewerking aan de interne verantwoordelijke om de getroffen personen conform artikel 34 AVG te kunnen informeren omtrent het datalek.
f. Het bestuur stelt een communicatieplan op voor eventuele vragen van betrokkene(n), de media en overige derden. Er wordt een woordvoerder aangewezen voor externe communicatie. Lijkt het datalek te leiden tot media-aandacht, bereid dan ook een persverklaring voor.

11. Gevolgen melding datalekken

a. Indien het datalek negatieve gevolgen heeft voor betrokkene(n), dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.
b. Afhankelijk van de aard en de omvang van het datalek voor betrokkene(n) bepaalt de interne verantwoordelijke:
    - 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 Focus'07 neemt en op welke wijze betrokkene(n) zelf de schade kunnen voorkomen of beperken).
    - Welke nazorg betrokkene(n) krijgen
    - Welke acties in het belang van de organisatie noodzakelijk zijn
c. Indien een datalek heeft plaatsgevonden – ongeacht of deze is gemeld of niet – worden zo spoedig mogelijk adequate technische e/of organisatorische maatregelen getroffen om toekomstige gelijksoortige datalekken te voorkomen.

12. Bijhouden register datalekken

De interne verantwoordelijke houdt een register bij van alle datalekken, waarin alle gegevens rondom 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 tijdstip van de melding
- Of het incident is gemeld aan de betrokkene(n) en zo ja datum en tijdstip van de melding
- Op welke wijze betrokkene(n) is/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, met vermelding van datum en tijdstip.

13. Evaluatie

De voorzitter en interne verantwoordelijke evalueren na afronding van het datalek gezamenlijk de wijze waarop Focus'07 het incident is afgehandeld en stellen van deze evaluatie een schriftelijk verslag op. Waar nodig worden nieuwe maatregelen geïmplementeerd en wordt dit protocol aangepast.