W :: www.spixels.nl
E :: info@spixels.nl
T :: 06-54964375
A :: Tuimelaar 10
2673 CK NAALDWIJK

PROTOCOL MELDPLICHT DATALEKKEN

Overwegingen:

- Spixels 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
- Spixels is op grond van de Algemene verordening gegevensbescherming (AVG) verplicht om (ernstige) datalekken te melden aan de Autoriteit Persoonsgegevens en aan de betrokkenen
- Spixels wenst aan haar wettelijke verplichtingen te voldoen
- Spixels heeft daarom een beleid geformuleerd om zo adequaat mogelijk te handelen indien 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 van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

2 - Interne verantwoordelijke melding datalekken

1. Spixels heeft een interne verantwoordelijke voor de verwerking van datalekken aangesteld die verantwoordelijk is voor de melding van een datalek.
2. Deze verantwoordelijke is: Sven Kersten, telefoonnummer: 06 - 54 964 375; e-mailadres: sven@spixels.nl , hierna te noemen: '**interne verantwoordelijke**'.

3 - Interne melding bij ontdekking van een datalek

1. Degene die een datalek bij Spixels ontdekt, meldt dit per omgaande aan de interne verantwoordelijke.
2. Indien mogelijk, zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelekte gegevens meteen op afstand worden gewist of ontoegankelijk gemaakt.

4 - Onderzoek door de interne verantwoordelijke

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
- 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 noodzakelijke maatregelen om het datalek zo goed mogelijk te bestrijden.

Spixels
ONLINE MARKETING

W :: www.spixels.nl
E :: info@spixels.nl
T :: 06-54964375
A :: Tuimelaar 10
2673 CK NAALDWIJK

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 betrokkenen kan zijn.

7 - Medewerking verstrekking gegevens omtrent het datalek

De ontdekker/melder van het datalek biedt alle medewerking aan de interne verantwoordelijk door zo 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 dat gebeurd?
- 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 naar aanleiding van het incident?

8 - Beschikbaarheid personeel na ontdekking datalek

De verantwoordelijke van de afdeling vanuit waar het datalek heeft plaatsgevonden 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 1e 24 uur na ontdekking van het datalek beschikbaar voor overleg met de interne verantwoordelijke c.q. eventueel door hem aangewezen experts en voor het zo nodig uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

9 - 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 vanuit waar 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 niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen.

W :: www.spixels.nl
E :: info@spixels.nl
T :: 06-54964375
A :: Tuimelaar 10
2673 CK NAALDWIJK

3. De melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven in onderdeel 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.

10 - Melding datalekken aan de Autoriteit Persoonsgegeven en/of betrokkenen

1. De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).
2. Melding geschiedt zo spoedig mogelijk na de ontdekking en uiterlijk binnen 72 uur na ontdekking van 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 al dan niet melden van het datalek aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan kan hij zijn grieven kenbaar maken aan de directie.
5. Indien daartoe verzocht, verleent een werknemer alle medewerking aan de verantwoordelijke om de getroffen personen conform artikel 34 AVG te kunnen informeren omtrent het datalek.

11 - Gevolgen melding datalekken

1. Indien het datalek negatieve gevolgen heeft voor betrokkenen, dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.
2. Afhankelijk van de aard en de omvang van het datalek voor betrokkenen 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 Spixels neemt en op welke wijze betrokkenen 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 spoedig mogelijk adequate technische en/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

Spixels
ONLINE MARKETING

W :: www.spixels.nl
E :: info@spixels.nl
T :: 06-54964375
A :: Tuimelaar 10
2673 CK NAALDWIJK

- 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 melding
- 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, met vermelding van datum en tijdstip

Dit protocol meldplicht datalekken is opgemaakt op 02 januari 2020.