World of Travel – datalek policy – 21 mei 2018

Dit is het datalekken beleid van World of Travel bvba.

Dit beleid geeft een stappenplan weer dat dient gevolgd te worden in het geval van een datalek.

Een datalek of "een inbreuk in verband met persoonsgegevens" kan als volgt worden gedefinieerd: "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."

Hieronder volgt een niet-limitatieve opsomming van mogelijke data lekken:
- hacking van computersystemen;
- een ransomware (cryptolocker) die data versleutelt;
- verlies van laptop, smartphone, USB-stick met persoonsgegevens, (…);
- onvoldoende beveiliging van dossiers;
- black out van servers;
- verlies van gegevens ten gevolge van een brand in het datacentrum terwijl er geen back-up beschikbaar is;
- (…)

In geval van een datalek dient u contact op te nemen met één van of de volgende contactpersonen binnen de organisatie:

Contactgegevens

Functie	Naam	Email	Tel.nr.
AVG-verantwoordelijke	Patrick De Vos	patrick.devos@worldoftravel.be	0032/56243882
IT-verantwoordelijke	Conxion	support@conxion.be	0032/56731121

Stappenplan

a. Identificatie van het datalek

Een datalek (of een vermoeden ervan) kan op verschillende manieren worden opgemerkt, bijvoorbeeld door automatische computersystemen, door een werknemer binnen de eigen onderneming zelf of door een melding van buitenaf.

Van zodra iemand binnen de organisatie kennis heeft van een datalek maakt deze hiervan onmiddellijk melding bij de AVG-verantwoordelijke. Bij afwezigheid van deze persoon, wordt melding gedaan bij de IT-verantwoordelijke.

De melding dient per email te gebeuren (zie tabel contactgegevens) en maakt melding van volgende informatie in zoverre deze reeds beschikbaar is:

- de aard van het datalek:
    - verlies of beschadiging van data,
    - vermindering of wegvallen van toegankelijkheid, en/of
    - inbreuk op de vertrouwelijkheid van data;
- de betrokken data;
- de impact op de organisatie; en
- de vermoedelijke oorzaak.

Na elke melding van een datalek houdt de persoon van melding zich steeds ter beschikking van de AVG-verantwoordelijke voor verdere opvolging van de procedure.

b. Analyse door de AVG-verantwoordelijke binnen de organisatie voor de behandeling van datalekken

Een analyse zal steeds dienen te gebeuren om te concluderen of het datalek überhaupt gemeld moet worden aan de toezichthoudende autoriteit. Zo is een melding niet verplicht indien het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene. Elk incident dient echter wel intern te worden beschreven, met een beoordeling van het risico voor de betrokken persoon volgens de geijkte methodes. Deze beoordeling zal gemaakt worden door de AVG-verantwoordelijke binnen de organisatie voor de behandeling van datalekken.

Volgende situaties kunnen zich dan voordoen:

- er is geen sprake van een datalek met betrekking tot persoonsgegevens of het datalek houdt geen risico's in op de rechten en vrijheden van de betrokkenen. De AVG-verantwoordelijke zal dit rapporteren aan het Management en hij of zij gaat over tot een opname in het register van datalekken indien het een datalek met betrekking tot persoonsgegevens betreft;
- er is sprake van een datalek met persoonsgegevens wat vermoedelijk een risico inhoudt op de rechten en vrijheden van één of meerdere betrokkenen evenwel is het beperkt in omvang en impact. De AVG-verantwoordelijke zal zelf overgaan tot afhandeling van het incident, rapporteert dit aan het Management en registreert het datalek in het Register van Datalekken.

- er is sprake van een datalek met persoonsgegevens met een vermoedelijk risico op de rechten en vrijheden van één of meerdere betrokkenen, en één of meerdere van hierna opgesomde vereisten zijn voldaan:
    - er is een vermoeden van impact op de IT-infrastructuur;
    - er is een vermoeden van kwaadwillig opzet;
    - er is een vermoeden van impact op gevoelige gegevens;
    - er is een vermoeden van impact op een grote set van data;
    - er is een vermoeden van impact op data van een groot aantal betrokkenen;
    - iedere andere situatie die ernstig genoeg is om het Crisis Team mee te betrekken in de evaluatie;

De AVG-verantwoordelijke zal zonder uitstel het Crisis Team samenroepen.

c. Samenroepen van een Crisis Team

Indien noodzakelijk zal de AVG-verantwoordelijke een Crisis Team samenroepen.

Deze bestaat uit volgende personen naargelang de omvang en de specifieke omstandigheden van het datalek:

Functie	Naam
AVG-verantwoordelijke	Patrick De Vos
IT-verantwoordelijke	Conxion
Melder van het datalek	
Zaakvoerder	Hilde De Vos
Websitebeheerder	Ewaut Van Gerrewey – Code d'Or

Indien een persoon binnen de organisatie wordt opgeroepen, maar niet aanwezig kan zijn, wordt een vervanger aangeduid. Het Crisis Team zal het incident altijd aan een analyse onderwerpen. Ieder lid zal in het kader van zijn of haar functie, met de nodige kennis en expertise bijdragen tot de analyse van het datalek.

Het Crisis Team stelt een verslag op van elke bijeenkomst hetwelk gedocumenteerd wordt in een intern register.

d. Evaluatie van het datalek door de AVG-verantwoordelijke en/of het Crisis Team

De AVG-verantwoordelijke en desgevallend het Crisis Team gaan over tot de analyse van het datalek en onderzoeken de aard ervan. Ook volgende punten zullen worden besproken:

- de categorieën en aantal betrokkenen bij het datalek
- de categorieën en aantal gegevens bij het datalek
- de eventuele impact van het datalek op de onderneming
- een inschatting van de impact op de rechten en vrijheden van de betrokkenen
- eventuele gevolgen van het datalek

- maatregelen die het datalek moeten verhelpen en de gevolgen ervan moeten vermijden of minstens verminderen
- maatregelen die datalekken in de toekomst kunnen vermijden.

e. Melding aan de toezichthoudende autoriteit (CBPL)

Indien de AVG-verantwoordelijke of het Crisis Team een risico detecteren op de schending van de rechten en vrijheden van natuurlijke personen moeten zij dit melden aan de toezichthoudende autoriteit, zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur na kennisname van de inbreuk. Daarbij maakt het niet uit of het datalek veroorzaakt is door een fout of overmacht.

Een datalek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig) maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig), bijvoorbeeld financiële gegevens of medische gegevens.

Bij deze melding moet er tenminste kennis worden gegeven van volgende wettelijk verplichte informatie ingevolge artikel 33 AVG:

- de aard van de inbreuk;
- indien mogelijk, de categorieën van betrokkenen en persoonsgegevens in kwestie;
- indien mogelijk, het aantal betrokkenen en het aantal persoonsgegevens in kwestie;
- de naam en contactgegevens van de AVG-verantwoordelijke (indien deze aangesteld werd);
- de waarschijnlijke gevolgen van het datalek; en
- maatregelen die worden genomen om het datalek aan te pakken en om de eventuele nadelige gevolgen ervan te beperken.

Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, dient zij vergezeld te zijn van een motivering voor de vertraging.

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging gefaseerd worden verstrekt aan de toezichthoudende autoriteit.

De melding aan de toezichthoudende autoriteit wordt steeds onmiddellijk gedaan door de AVG-verantwoordelijke. Er wordt steeds naar gestreefd om meldingen aan de toezichthoudende autoriteit uit te voeren binnen de wettelijke termijn van 72 uur volgend op de ontdekking van het datalek. Indien de termijn van 72 uur niet kan worden gehaald, zal de informatie zonder uitstel en zo snel als mogelijk worden overgemaakt aan de toezichthoudende autoriteit.

Indien het gedetecteerde risico als laag wordt beoordeeld door de AVG-verantwoordelijke en geen melding bij de toezichthoudende autoriteit vereist is, dient overgegaan te worden naar de stap ‘Aanvullen van het Datalekken Register’.

f. Melding aan de betrokkenen (natuurlijke personen)

Niet elk beveiligingsincident moet worden meegedeeld aan de betrokkene. Dit geldt enkel voor beveiligingsincidenten die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen (artikel 34 AVG).

De AVG somt een aantal gevallen op waarin mededeling aan de betrokkene toch niet vereist is:

- de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermings- maatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het beveiligingsincident betrekking heeft (bv. versleuteling);
- de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou onevenredige inspanningen vergen. In dit geval moet een openbare mededeling gebeuren van het beveiligingsincident of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd (zie stap 'Publieke mededeling' hieronder).

Indien de AVG-verantwoordelijke een hoog risico detecteert op de schending van de rechten en vrijheden van de betrokkene, meldt hij of zij dit zo snel mogelijk aan de betrokkenen in een duidelijke en eenvoudige taal.

De melding naar de betrokkene moet de aard van de inbreuk op de persoonsgegevens omschrijven en bevat ten minste volgende informatie:

- de naam en contactgegevens van de AVG-verantwoordelijke of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek; en
- maatregelen die voorgesteld zijn of genomen werden om het datalek aan te pakken en in voorkomend geval, de maatregelen ter beperking van de eventueel nadelige gevolgen daarvan.

g. Publieke mededeling

Indien een melding aan de betrokkene verplicht is, doch onevenredig hoge inspanningen zou vereisen, dient een publieke mededeling of soortgelijke maatregel te gebeuren waarbij de betrokkenen op een even doeltreffende wijze worden geïnformeerd.

De inhoud van de mededeling moet worden afgestemd met de AVG-verantwoordelijke en/of Crisis Team. Alleszins moet er steeds over gewaakt worden dat iedere publieke mededeling:

- aangeeft dat de nodige maatregelen worden genomen;
- geen melding doet van persoonsgegevens zelf; en
- contactgegevens meedeelt waar meer informatie kan worden bekomen.

h. Implementatie maatregelen en uitvoeren actieplan

De AVG-verantwoordelijke ziet toe dat de voorgestelde maatregelen worden geïmplementeerd en het eventueel opgestelde actieplan ten uitvoer wordt gebracht. Vooropgestelde acties kunnen bestaan in het feit dat de oorzaken van het incident worden ingedijkt, defecten worden hersteld, mogelijke infecties worden verwijderd en de systemen worden hersteld in hun oorspronkelijke toestand van voor het datalek.

De AVG-verantwoordelijke ziet toe op correcte uitvoering van de maatregelen en zorgt voor de opvolging. De AVG-verantwoordelijke stelt hiervan een verslag op.

i. Afsluiting van de procedure en opmaak van het rapport

De procedure voor de behandeling van het datalek wordt afgesloten door de AVG-verantwoordelijke indien:

- de situatie onder controle is (of binnen aanvaardbare proporties is herleid);
- de geïmplementeerde maatregelen het gewenste effect bereiken;
- geen risico op schending van rechten en vrijheden van betrokkene meer bestaat; én
- aan wettelijke verplichtingen tijdig werd voldaan.

De afsluiting van de procedure zal intern worden gecommuniceerd aan alle betrokkenen bij de behandeling van het datalek.

Indien de situatie onder controle is op basis van tijdelijke maatregelen maar een definitieve maatregel noodzakelijk is voor het afsluiten van het incident, kan de AVG-verantwoordelijke om het incident onder voorbehoud van implementatie van de definitieve maatregel af te sluiten.

Bij afsluiting van de procedure wordt een rapport opgesteld door de AVG-verantwoordelijke. Hierin worden alle relevante documenten, communicatie en verslagen opgenomen. In het rapport moet duidelijk vermeld worden wat de aard van het datalek was, de wijze waarop gehandeld werd, de genomen maatregelen, de betrokken personen en de aanbevelingen naar de toekomst toe.

Het verslag zal eerst worden overgemaakt aan alle betrokkenen bij de procedure die 5 werkdagen de tijd krijgen eventuele opmerkingen te formuleren die desgevallend zullen worden toegevoegd aan het verslag, waarna de AVG-verantwoordelijke het rapport zal finaliseren.

Het definitieve verslag wordt overgemaakt aan het bestuur.

j. Aanvullen van het Datalekken Register

Elk vastgesteld datalek dient door de AVG-verantwoordelijke in het Datalekken Register te worden opgenomen, waarbij volgende gegevens dienen te worden vermeld:

- de aard van het datalek en de feitelijke omstandigheden;
- de effecten van het datalek op de organisatie en op de rechten en vrijheden van de betrokkenen;

- de genomen maatregelen; en
- eventuele aanbevelingen naar de toekomst toe