

DATALEKPROTOCOL

1. Inleiding

Dit document beschrijft de verschillende stappen die binnen Nettt Interactieve Media BV genomen worden bij een datalek, die valt onder de Meldplicht Datalekken.

2. Verantwoordelijkheden

Functionaris	Verantwoordelijkheden
Directie	Aannemen en registreren van meldingen van datalekken
Directie	Melden van datalek bij Autoriteit Persoonsgegevens
Directie	Beoordelen en vastleggen van gevolgen en te nemen maatregelen
Directie	Fiatteren van maatregelen
Directie	Melden van datalekken van persoonsgegevens

Beschrijving procedure

De meldplicht datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en treedt in werking met ingang van 1 januari 2016. Bij een datalek is er sprake van inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen ontstaan door:

- Moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting);
- Technisch falen (ICT-storingen);
- Menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- Calamiteiten (brand datacentrum, wateroverlast);
- Verloren USB stick of laptop;
- Verzenden van email met emailadressen van alle geadresseerden;
- Het onrechtvaardig verwerken van gegevens;

3.1 Melden bij Autoriteit persoonsgegevens

3.1.1 Autoriteit persoonsgegevens

Een datalek moet onverwijld (binnen 2 dagen) nadat de verantwoordelijke binnen Nettt Interactieve Media BV er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens gemeld worden. Het datalek moet ook worden gemeld bij de betrokkenen met behulp van de opdrachtgever. In het geval van Nettt Interactieve Media BV zijn dit over het algemeen de gebruikers van de systemen van de opdrachtgever van het specifieke project. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer. Een verwerker is verplicht om een datalek te melden bij de verantwoordelijke.

1. Verantwoordelijke: directie Nettt Interactieve Media BV. De verantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De verantwoordelijke heeft de regierol (regie over het beheer en privacy in de keten);
2. Verwerker: degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen (ook extern). De verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. De verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens ect.

3.2 Stappenplan intern melden

3.2.1 Melden van datalek

Alle datalekken van persoonsgegevens moeten intern worden gemeld aan directie en worden gedocumenteerd door directie. De melding kan door iedere medewerker en iedere verwerker worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van Nettt Interactieve Media BV. De melding moet direct worden gedaan bij de directie en schriftelijk worden vastgelegd.

De directie legt vast:

- Naam van de melder;
- Datum en tijd van de melding;
- Aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- Welke persoonsgegevens vallen onder de melding;
- Om welk aantal en/of gegevensrecords gaat het;
- Welke (groepen) personen zijn betrokken bij de melding;
- Welke maatregelen zijn of worden door de melder getroffen;
- Welke gevolgen zij er volgens de melder voor de betrokkenen;
- De contactpersoon voor de melding;

3.2.2 Inventariseren gevolgen en te nemen maatregelen

Na ontvangst van een melding datalek wordt door de directie van Nettt Interactieve Media BV beoordeeld en vastgelegd:

- De noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- Hetgeen gemeld gaat worden bij de Autoriteit Persoonsgegevens door directie (naast aard inbreuk, welke persoonsgegevens, welke betrokken persoon/records);
- De mogelijke gevolgen voor de betrokkenen;
- De maatregelen die Nettt Interactieve Media BV neemt en/of kan nemen om de schade voor de betrokkenen te verkleinen;
- De maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
- Contactgegevens voor betrokkenen;
- De wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en teamleider(s);
- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsplicht is geschonden, of in strijd meteen contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- Het al dan niet doen van aangifte en vaststellen of er sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit Nettt Interactieve Media BV of wanneer er onvoldoende maatregelen zijn getroffen om ongeregelheden te voorkomen. Indien gewenst vindt overleg plaats met een juridisch adviseur;
- Hetgeen intern gecommuniceerd wordt, op welk moment;
- Hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld op de pers geïnformeerd moet worden;
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd worden;
- Op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;
- Of eventuele schade is gedekt door de verzekeringspolis.

3.2.3 Fiasering

De directie accordeert de uit te voeren activiteiten, zoals vastgesteld, of stelt de uit te voeren activiteiten bij. De door de directie vastgestelde activiteiten worden uitgevoerd.

3.2.4 Melding bij de Autoriteiten Persoonsgegevens

De directie meldt binnen 2 dagen het datalek bij de Autoriteit Persoonsgegevens. In ieder geval zal gemeld moeten worden:

- Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- Beschrijving van de verwachten gevolgen;
- Getroffen en/of voorgestelde maatregelen;
- Informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- Contactgegevens van de betrokkene;

3.2.5 ontvangst bevestiging van Autoriteit Persoonsgegevens

Is er een melding gedaan, dan ontvangt Nettt Interactieve Media BV een ontvangstbevestiging.

Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met Nettt Interactieve Media BV om de herkomst van de melding te verifiëren.