Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Procedure Datalek

Competentie Thermometer respecteert uw privacy en al uw gegevens worden vertrouwelijk behandeld. De verwerking van persoonsgegevens geschiedt altijd op een manier die in overeenstemming is met de eisen die de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679, hierna AVG) en eventuele andere wet- en regelgeving daaraan stelt. In deze Procedure Datalek wordt in meer detail uiteengezet hoe Competentie Thermometer (CT) in onverhoopt geval met het verlies van dergelijke gegevens omgaat.

Dit document beschrijft de verschillende stappen die binnen CT genomen worden bij een datalek, die valt onder de Meldplicht Datalekken. De Meldplicht Datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en is met ingang van 1 januari 2016 in werking getreden. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking. Een datalek moet onverwijld (binnen 2 dagen) nadat de verantwoordelijke persoon binnen CT er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens (voorheen CBP) gemeld worden.

Het datalek moet ook worden gemeld bij de betrokkenen. In het geval van CT zijn dit over het algemeen klanten (gebruikers van de software) of medewerkers. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.

De Verwerker is verplicht om een datalek te melden bij de Verwerkingsverantwoordelijke.

1. **Verwerkingsverantwoordelijke (klant CT)** - De Verwerkingsverantwoordelijke 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 Verwerkingsverantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten), zoals staat beschreven in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG);
2. **Verwerker (Competentie Thermometer BV)** - De organisatie die de gegevens ten behoeve van de Verwerkingsverantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. De Verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Verwerkingsverantwoordelijke. 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, zoals tevens staat beschreven in de tussen Verwerkingsverantwoordelijke en Verwerker overeengekomen Bewerkersovereenkomst.

COMPETENTIE THERMOMETER

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Mogelijke oorzaken van een datalek:

- Moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- Technisch falen (fouten of bugs in software, verlate updates, storingen);
- Menselijk falen (onzorgvuldige omgang gebruikersnaam of wachtwoord, nalatigheid);
- Verloren of gestolen hardware (externe harde schijf, USB-stick, server-apparatuur of laptop);
- Verzenden van e-mail naar meerdere gebruikers met openbaring van e-mailadressen;
- Calamiteit (brand datacentrum, wateroverlast).

Melding

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door de Data Protection Officer (DPO). De melding kan door iedere gebruiker en iedere medewerker of derde partij worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van CT. De melding moet direct en telefonisch worden gedaan bij de DPO en schriftelijk worden vastgelegd. Deze meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.

De Data Protection Officer legt vast:

- Naam van de melder;
- Contactpersoon voor de melding;
- Datum en tijd van de melding;
- Aard van de inbreuk en risico op verlies of onrechtmatig gebruik gegevens;
- Welke persoonsgegevens vallen onder de melding;
- Aantal gegevensrecords;
- Welke (groepen) personen zijn betrokken bij de melding;
- Welke maatregelen zijn of worden door de melder getroffen;
- Welke gevolgen zijn er volgens de melder voor de betrokkenen.

Escalatie bij afwezigheid

Bij afwezigheid van de Data Protection Officer wordt diens rol ingevuld door de directeur CT. Als deze ook afwezig is, wordt diens rol ingevuld door de Privacy Officer. Buiten kantoortijden en in het weekend wordt de melding gedaan bij de DPO. Bij het niet kunnen bereiken van de DPO, wordt de melding gedaan bij de directeur CT.

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Analyse

De Data Protection Officer en de Privacy Officer beoordelen of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats door de DPO.

Is dit wel het geval, dan voert de DPO de acties uit zoals beschreven in het Calamiteitenplan van CT:

1. Telefonisch informeren directeur CT;
2. Tijdens kantooruren onmiddellijk bijeenroepen van het Responseteam Datalek, bestaande uit:
    a. **Data Protection Officer (DPO)** – Marten Wilmink
    Verantwoordelijk voor het Risico Management Programma en voorzitter RMT;
    b. **Directeur Competentie Thermometer BV** – Daniel Hoopman
    Verantwoordelijk voor Competentie Thermometer BV;
    c. **Privacy Officer** (indien noodzakelijk) – Extern
    Juridisch adviseur wet en regelgeving op het gebied van privacy en IT.

De DPO neemt overdag telefonisch contact op met de Privacy Officer. Als het mogelijk is, wordt een eventueel benodigd overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is, wordt zoveel als mogelijk telefonisch en elektronisch overleg gevoerd.

Responseteam Datalek

Het Responseteam Datalek wordt met hoge prioriteit bijeengeroepen door de DPO. De bijeenkomst wordt voorgezeten door de DPO. Het responseteam bespreekt en legt vast:

- De gegevens die door de DPO zijn vastgelegd bij het aannemen van de melding;
- De noodzakelijke vervolgacties met betrekking tot het datalek (lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- De melding die opgesteld moet worden voor de Autoriteit Persoonsgegevens door de DPO. Naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records:
    - De mogelijke gevolgen voor de betrokkenen;
    - De maatregelen die CT neemt en/of kan nemen om de schade voor 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 manager(s);
- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd), of een onrechtmatige daad;

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

- Of het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit CT zelf, een klant, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de Privacy Officer;
- Wat er intern wordt gecommuniceerd over het incident;
- Wat er extern wordt gecommuniceerd over het incident en vaststellen of de pers geïnformeerd moet worden;
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden;
- Of er individuen, klanten, leveranciers geïnformeerd moeten worden;
- Op welke wijze er intern wordt gerapporteerd;
- Of eventuele schade is gedekt door de verzekeringspolis.

Afhandeling

De DPO rapporteert aan de directeur CT de uitkomsten van het overleg van het Responseteam Datalek. De directeur CT accordeert de uit te voeren activiteiten, zoals vastgesteld door het Responseteam Datalek, of stelt de uit te voeren activiteiten bij. De door de directeur CT vastgestelde activiteiten worden uitgevoerd.

Melding bij de Autoriteit Persoonsgegevens

De DPO meldt binnen 2 dagen volgens de aangewezen methode het datalek via het Meldpunt Datalek van de Autoriteit Persoonsgegevens (https://datalekken.autoriteitpersoonsgegevens.nl/).
In ieder geval zal gemeld moeten worden:

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

Ontvangstbevestiging Autoriteit Persoonsgegevens

Is er een melding gedaan, dan ontvangt CT een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met CT om de herkomst van de melding te verifiëren.

Terugkoppeling betrokken

Na de melding bij de Autoriteit Persoonsgegevens en eventuele getroffen maatregelen zal terugkoppeling plaatsvinden bij de betrokkenen. Hierna zal het incident worden afgesloten en zullen de getroffen maatregelen worden geëvalueerd binnen de PDCA-cyclus van het Risico Management Programma.