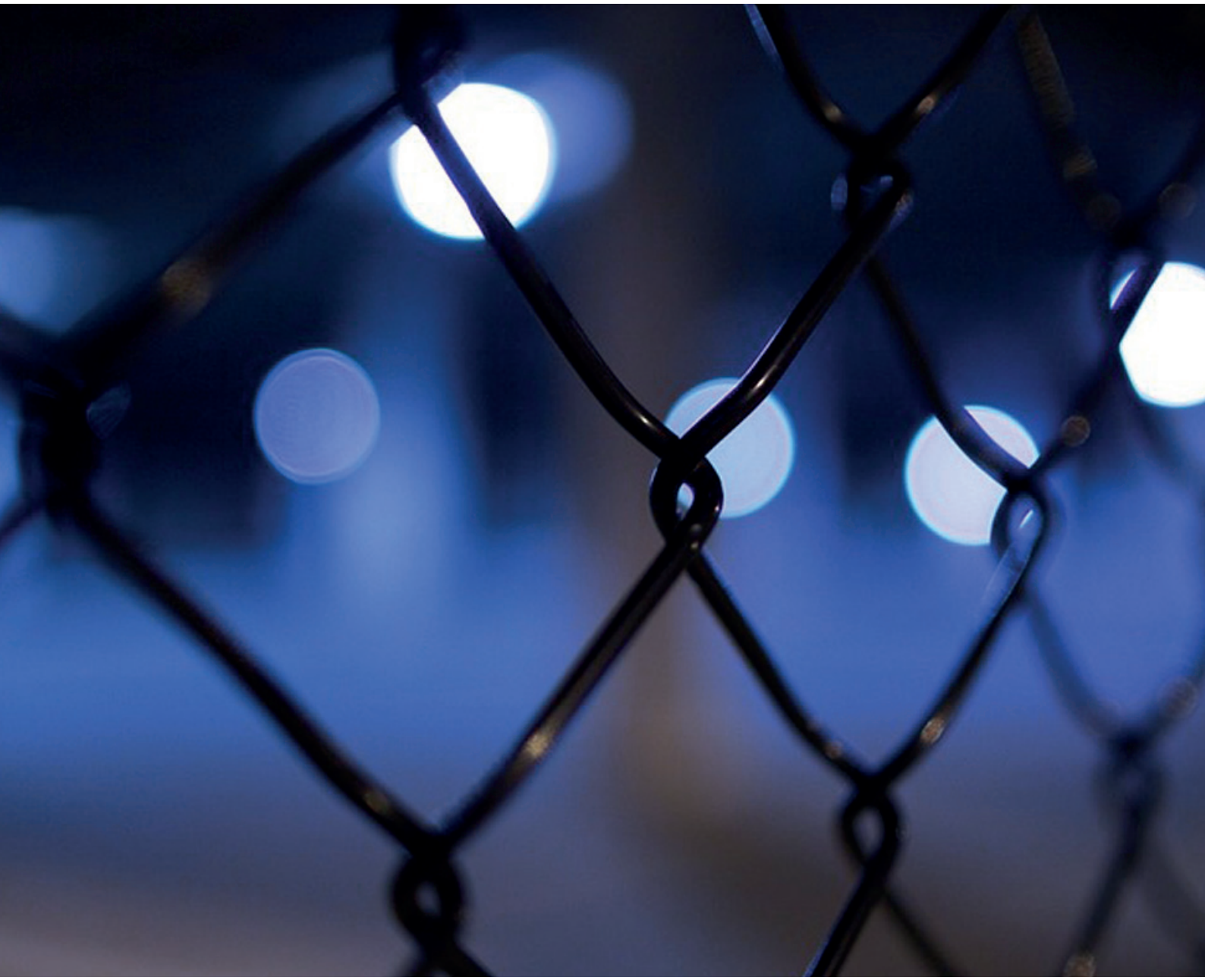
r@to
internetburo



Datalekprotocol binnen Reto

Versie: 01-05-2018

meer @ffect!

Datalekprotocol binnen Reto

1. INLEIDING

Dit document beschrijft de verschillende stappen die binnen Reto genomen worden bij een datalek, die valt onder de Meldplicht Datalekken.

Let op: Bij een Verwerkersovereenkomst tussen Reto en haar opdrachtgevers/sub-processors zijn aparte afspraken gemaakt omtrent het Datalekprotocol zoals vermeld in de desbetreffende documenten: 'Verwerkersovereenkomst' en 'Specificatie persoonsgegevens en betrokkenen'.

2. VERANTWOORDELIJKHEDEN

FUNCTIONARIS	VERANTWOORDELIJKHEDEN
DIRECTIE	Aannemen en registreren van meldingen van datalekken
DIRECTIE	Melden van datalek bij Autoriteit Persoonsgegevens (AP)
DIRECTIE	Beoordelen en vastleggen van gevolgen en te nemen maatregelen
DIRECTIE	Fiatteren van maatregelen
DIRECTIE	Melden van datalekken van persoonsgegevens

Zie bij artikel **5**, pagina **7** een stroomschema voor de privacy inbreuk.

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 een 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 bijvoorbeeld ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van gebruikersnaam/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB-stick of laptop;
- verzenden van e-mail met e-mailadressen van alle geadresseerden;
- het onrechtmatige verwerking van gegevens.

3. MELDEN BIJ AUTORITEIT PERSOONSGEGEVENS

3.1

Autoriteit Persoonsgegevens (AP)

Een datalek moet onverwijld (binnen twee dagen) nadat de verantwoordelijke binnen Reto 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 Reto zijn dit over het algemeen de gebruikers van de systemen van de opdrachtgever van het specifieke project. 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. Een verwerker is verplicht om een datalek te melden bij de verantwoordelijke.

1. **Verantwoordelijke**: functionaris Reto. 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 van 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 etc.

3.2 STAPPENPLAN INTERN MELDEN

3.2.1

Stap 1: Melden van datalek

Alle datalekken van persoonsgegevens moeten intern worden gemeld aan de Verantwoordelijke en worden gedocumenteerd. 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 Reto. De melding moet direct worden gedaan bij de Verantwoordelijke en schriftelijk worden vastgelegd. Buiten kantoortijden is de Verantwoordelijke bereikbaar.

De Verantwoordelijke 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 zijn er volgens de melder voor de betrokkenen;
- de contactpersoon voor de melding.

3.2.2

Stap 2: Inventariseren gevolgen en te nemen maatregelen

Na ontvangst van een melding datalek wordt door de Verantwoordelijke van Reto 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 Verantwoordelijke (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):
- de mogelijke gevolgen voor de betrokkenen;
- de maatregelen die Reto 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 teamleider(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 onrechtmatige daad;
- 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 Reto of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de juridisch adviseur;
- hetgeen intern gecommuniceerd wordt, op welk moment;
- hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden;
- of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden;
- op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;
- of eventuele schade is gedekt door de verzekeringspolis.

3.2.3

Stap 3: Fiattering

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

3.2.4

Stap 4: Melding bij Autoriteit Persoonsgegevens

De Verantwoordelijke meldt binnen twee 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 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.

3.2.5

<u>Stap 5</u>: Ontvangstbevestiging Autoriteit Persoonsgegevens

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

4. MEER INFORMATIE

Mocht er na het doorlopen van dit protocol meer informatie gewenst zijn, neem dan contact op met de Verantwoordelijke.

Jaarlijks zullen alle Reto medewerkers opnieuw op de hoogte worden gebracht van dit protocol. In het Reto-handboek welke elke medewerker heeft zit altijd de meest recente versie.

5. STROOMSCHEMA PRIVACY INBREUK