DATALEKKEN PROTOCOL

Protocol informatiebeveiligingsincidenten en datalekken

QWASP B.V.

Monseigneur Borretstraat 63
5375 AB Reek

Inhoudsopgave

I. Inleiding 3

II. Wet- en regelgeving datalekken 4

III. Werkwijze 5

3.1 Uitgangssituatie 5

3.2 De vier rollen 5

3.3 De zeven stappen 5

3.3.1 Ontdekken 5

3.3.2 Inventariseren 5

3.3.3 Beoordelen 6

3.3.4 Repareren 6

3.3.5 Melden 7

3.3.6 Vastleggen 7

3.3.7 Informeren betrokkene 7

IV. Monitoring beveiligingsincidenten en datalekken 8

V. Communicatie 8

I. Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Qwasp B.V. (hierna ook: Qwasp).

Dit protocol biedt een handleiding voor de melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van Qwasp.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Dit document is opgesteld in juli 2023. Het versienummer is 2023.07

II. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn verwerkingsverantwoordelijken verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van deelnemers, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens. Voor de persoonsgegevens die met de registratiemodule worden verwerkt, is de gemeente verwerkingsverantwoordelijke en Qwasp verwerker. In de door de gemeente en Qwasp afgesloten verwerkersovereenkomst (standaardverwerkersovereenkomst 2.1 VNG) is dit afgesproken:

Artikel 5 Inbreuk in verband met Persoonsgegevens

1. *Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.*
2. *In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.*
3. *Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.*
4. *Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke* waar nodig bij de *melding aan de toezichthoudende autoriteit en/of Betrokkene.*

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

In het geval er sprake is of kan zijn van een datalek bij de persoonsgegevens die bij de niveautoetsen worden verwerkt, is degene verantwoordelijk die doel en middelen bepaalt. Wanneer dat de gemeente is, geldt het bovenstaande. Wanneer de verwerkingsverantwoordelijke een andere organisatie is (een opleidingsinstituut of een taalinstelling bijvoorbeeld), gelden de afspraken die met de betreffende verwerkingsverantwoordelijke zijn gemaakt.

In het Data Pro Statement is het volgende opgenomen: *Qwasp zal opdrachtgever zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) inbreuk. Qwasp zal zelf geen meldingen doen aan de Autoriteit Persoonsgegevens of aan betrokkene(n). Wel of niet melden blijft de verantwoordelijkheid van opdrachtgever. Qwasp zal opdrachtgever desgewenst ondersteunen bij het meldproces*.

III. Werkwijze

3.1 Uitgangssituatie

Er is een actueel gegevensbeschermingsbeleid. Zie hiervoor onze website voor het actuele Beleid Bescherming Persoonsgegevens.

3.2 De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming** of **privacy officer)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security officer/ict coördinator)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

3.3 De zeven stappen

3.3.1 Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via privay@qwasp.eu.

3.3.2 Inventariseren

Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
    - Omschrijving van de groep betrokkenen
    - Aantal betrokkenen
    - Type persoonsgegevens in kwestie
    - Worden de gegevens binnen een keten gedeeld

3.3.3 Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

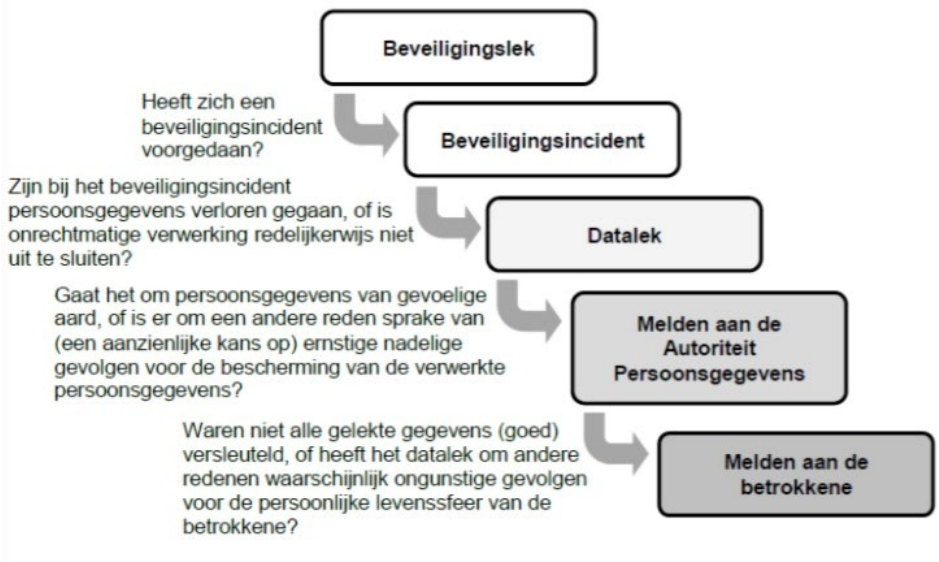
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', hou je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene.

De onderstaande beslisboom wordt gebruikt:



3.3.4 Repareren

De interne Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus kan zich bij zijn onderzoek laten bijstaan door medewerkers van Copaco BV[1] en legt onderstaande vast:

[1] Copaco B.V. is een bedrijf dat ondersteuning levert bij de integratie en opslag van data bij professionele clouddiensten zoals Microsoft Azure.

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

3.3.5 Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken. Een link naar het meldloket vindt u op deze pagina: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplichtdatalekken?qa=meldloket.

3.3.6 Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

3.3.7 Informeren betrokkene

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. In principe kan ervan worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

IV. Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van Qwasp maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Op de website van Qwasp wordt een verslag geplaatst van de analyse.

V. Communicatie

De hiervoor bedoelde analyse wordt per mail gedeeld met de contactambtenaren van de partners van Qwasp.