Procedure
Informatiebeveiligingsincidenten en datalekken

Versie:	0.1
Versiedatum	29-05-2018
V-Classificatie:	Intern document / bedrijfsvertrouwelijk

Inhoud

1. Inleiding

Met deze procedure geeft het GBT uitvoering aan het vastgestelde Privacybeleid.

In de Algemene Verordening Gegevensbescherming (AVG), de wet die het omgaan met persoonsgegevens reguleert, is een onderdeel inzake meldplicht datalekken opgenomen. De meldplicht verplicht een verwerkingsverantwoordelijke melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens en bij betrokkenen (in bepaalde gevallen). Bovendien is het registreren van incidenten en datalekken aan strengere eisen gebonden. Het nalaten van een melding en/of adequate registratie kan leiden tot een (hoge) boete.

Deze procedure beschrijft hoe er binnen het GBT om moet worden gegaan met een incident of datalek als daar persoonsgegevens bij betrokken zijn. De procedure is van toepassing op de gehele organisatie van het GBT.

Gebruikte termen:

- **Beveiligingsincident**: een beveiligingsincident is een gebeurtenis die er voor 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 informatiebeveiligingsincident, waarbij sprake is van een inbreuk op de beveiliging van persoonsgegevens door blootstelling aan verlies of onrechtmatige verwerking (opgeslagen, aangepast, verzonden, kwijtraken, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene:** de persoon van wie de persoonsgegevens zijn gelekt.
- **Verwerkingsverantwoordelijke:** een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of lidstatelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

2. Wet- en regelgeving inzake datalekken (art. 33 AVG) [1]

Een datalek is een informatiebeveiligingsincident waarbij sprake is van een inbreuk op de beveiliging van persoonsgegevens door blootstelling aan verlies of onrechtmatige verwerking. Bij een datalek is dus de eerste vraag altijd of er sprake is van een beveiligingsincident, als dit niet zo is dan is er ook geen sprake van een datalek. De constatering dat de beveiliging van persoonsgegevens in een bepaald geval niet helemaal in orde is of het versturen van persoonsgegevens via mail is dus niet meteen een datalek. Er is wel sprake van een datalek als persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en niet geautoriseerde toegang tot deze persoonsgegevens. Er is dus niet alleen sprake van een datalek bij een inbraak door een hacker. Ook het kwijtraken van een USB-stick, de diefstal van een laptop, het verzenden van gevoelige gegevens naar een onjuist e-mailadres of het verlies van gegevens bij

[1] 2018_IBD_Factsheet_Meldplicht_Datalekken_v1.1

een brand in het datacentrum terwijl er geen back-up beschikbaar is, zijn voorbeelden van een datalek.

Melding aan Autoriteit Persoonsgegevens
Indien er sprake is van een ernstig datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, moet de verantwoordelijke het datalek melden aan de Autoriteit Persoonsgegevens.

Volgens de wet moet een 'ernstig' datalek, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, worden gemeld aan de Autoriteit Persoonsgegevens. Lukt dat niet, dan moet een verklaring worden gegeven van de vertraging, schriftelijk en beargumenteerd.

Een lek kan ernstig zijn indien er persoonsgegevens van gevoelige aard zijn gelekt, bijvoorbeeld: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen of gegevens die betrekking hebben op gezondheid. Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. De aard en omvang van het datalek spelen hierbij dus een belangrijke rol.

De verwerkingsverantwoordelijke hoeft geen melding aan de Autoriteit Persoonsgegevens te maken indien daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.

Als ten onrechte geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete door de Autoriteit Persoonsgegevens.

Melding aan Betrokkene
Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens direct mee. Zowel de aard van de inbreuk als aanbevelingen over hoe de verantwoordelijke mogelijke negatieve gevolgen kan beperken, moet aan betrokkene gemeld worden.

Een melding aan betrokkene is niet nodig wanneer het GBT passende maatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn gemaakt.
Een melding kan ook achterwege gelaten worden als achteraf maatregelen zijn genomen door de verwerkingsverantwoordelijke om te zorgen dat de hoge risico's voor de rechten en vrijheden van betrokkene zich waarschijnlijk niet meer voor zullen doen óf als de mededeling onevenredige inspanning vergt.

3. Verantwoordelijkheid

Wanneer GBT verwerkingsverantwoordelijk is, geldt de meldplicht voor het GBT. Een leverancier of externe partij die persoonsgegevens in opdracht van het GBT gebruikt is een verwerker. Er kan worden afgesproken dat een verwerker namens het GBT de melding doet. Dit gebeurt alleen op verzoek en onder verantwoordelijkheid van het GBT en moet vooraf schriftelijk zijn overeengekomen.

Het GBT is aansprakelijk voor de eventuele schade die ontstaat bij een datalek en moet hiervan melding doen aan de Autoriteit Persoonsgegevens en eventueel bij de betrokkenen.

4. Afspraken met verwerkers

Het GBT moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers of andere externe partijen als zij persoonsgegevens van ons ontvangen. Afspraken over datalekken vallen daar ook onder. In een verwerkersovereenkomst wordt o.a. antwoord gegeven op de volgende vragen:

- Hoe informeren het GBT en haar relaties elkaar over datalekken, en zorgen zij voor bereikbaarheid?
- Wie doet de melding bij de Autoriteit Persoonsgegevens?
- Welke informatie moet de verwerker geven bij een datalek over de persoonsgegevens?
- Welke informatie is nodig voor het doen van een melding en welke afspraken zijn gemaakt over het, over en weer informeren van partijen over de melding?
- Binnen welke tijd leveren de verwerkers de gegevens aan?
- Wie neemt de communicatie met de betrokkenen voor haar rekening als dat nodig is?

5. Werkwijze

Binnen het GBT onderscheiden wij vier rollen om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker**: degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt. Dit kan ook de verwerker zijn.
2. **Melder (CISO/Privacy Officer):** degene die namens het GBT verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Tevens is de melder degene die adviseert over de ernst en de omvang.
3. **Technicus (ICT-coördinator):** degene die de technische oorzaak van het datalek kan (laten) vinden en kan (laten) repareren. Tevens is de technicus degene die adviseert over de technische ernst en omvang.
4. **Functionaris gegevensbescherming:** evalueert periodiek de beveiligingsincidenten en /of datalekken en bespreekt ze met de medewerkers.

Let op: een datalek moet wel na kennisneming door verwerkingsverantwoordelijke binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens!

5.1 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 zo spoedig mogelijk bij de Melder via datalekken@email.nl.

5.2 Inventariseren

De Melder bepaalt 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 in een register van incidentmeldingen en datalekken:

- Samenvatting van het beveiligingsincident, wat is de oorzaak van het lek, wat is er met de gegevens gebeurd, wat voor een soort gegevens het betreft (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;
- Indien gemeld aan de betrokkene: ook de tekst van kennisgeving;
- Type persoonsgegevens in kwestie;
- Worden de gegevens binnen een keten gedeeld.

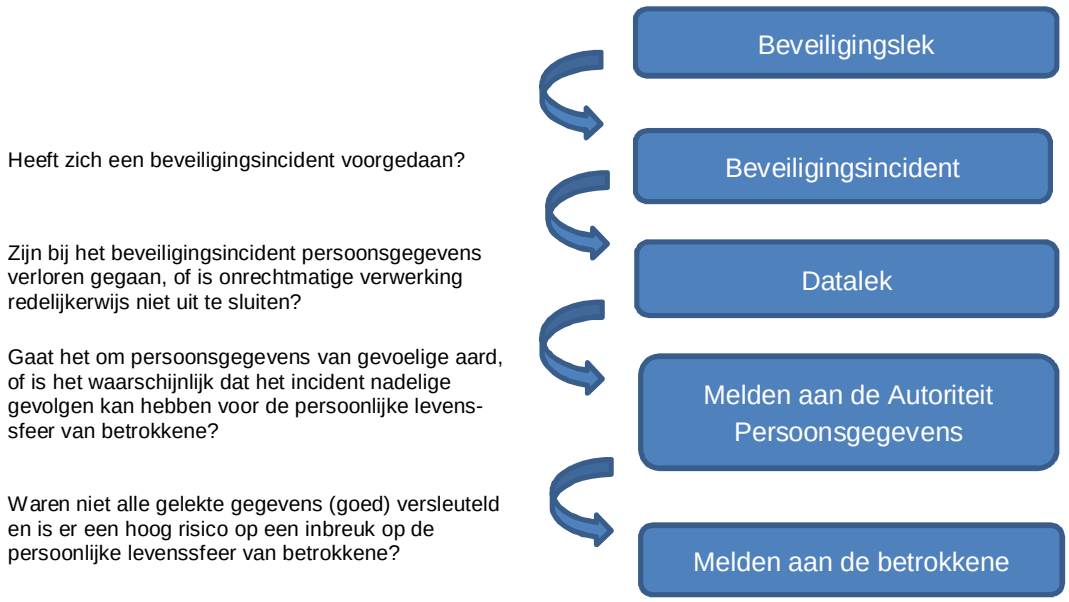
5.3 Beoordelen

De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
Naast de bovenstaande informatie wordt tevens de volgende informatie vastgelegd in het 'register incidentmeldingen en datalekken':

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen;
- Wordt het datalek binnen 72 uur gemeld aan de Autoriteit Persoonsgegevens? Wanneer het antwoord 'nee' is, wordt er uitleg gegeven waarom niet.
- Wordt het datalek aan betrokkenen gemeld?
  Wanneer het antwoord 'nee' is, wordt er uitleg gegeven waarom niet.
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek' wordt er rekening gehouden met het type gegevens en met de hoeveelheid gegevens. Een datalek hoeft niet gemeld te worden bij de Autoriteit Persoonsgegevens, indien het niet waarschijnlijk is dat de inbreuk, in verband met de persoonsgegevens, een risico inhoudt voor de rechten en vrijheden van betrokkene.

De onderstaande beslisboom kan hiervoor in beginsel gebruikt worden:



5.4 Repareren

De Technicus wordt, voor zover van toepassing, gevraagd te achterhalen wat de technische oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Technicus van het GBT geeft vervolgens de volgende informatie door aan de Melder voor vastlegging in het 'register incidentmeldingen en datalekken':

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen (voor zover de oorzaak bekend is).
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Indien het antwoord 'ja' is, wordt aangegeven op welke wijze de gegevens onbegrijpelijk zijn gemaakt (versleuteld).

5.5 Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens, dan zal de Melder dit binnen 72 uur na ontdekking doen. Lukt dat niet, dan moet schriftelijk en beargumenteerd een verklaring worden gegeven van de vertraging. Tevens wordt de directie en het bestuur periodiek van de meldingen aan de Autoriteit Persoonsgegevens op de hoogte gesteld.

De melding aan de Autoriteit Persoonsgegevens bevat de volgende informatie:

- De melder van het datalek;
- Degene met wie de Autoriteit Persoonsgegevens contact op kan nemen voor nadere informatie over de melding;
- En samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan;
- Het tijdstip van de inbreuk;
- De aard van de inbreuk;
- Het type persoonsgegevens waarover het gaat;
- De gevolgen die de inbreuk kunnen hebben voor de persoonlijke levenssfeer van de betrokkenen;
- De technische en organisatorische maatregelen die het GBT heeft getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen;
- Of het GBT het datalek gemeld heeft aan de betrokkenen en zo niet, of het GBT van plan is dit te gaan doen:
    - Zo ja, de inhoud van de melding aan de betrokkenen.
    - Zo nee, de reden waarom het GBT afziet van het melden van het datalek aan de betrokkenen.
- Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

Het lek wordt gemeld bij het meldloket datalekken:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
Daar staat een formulier waar alle beschreven informatie ingegeven dient te worden.

Het zou kunnen zijn dat niet alle informatie gelijktijdig verstrekt kan worden. In dat geval is het mogelijk de informatie in stappen te verstrekken (artikel 33 AVG).

Let op: bij het melden van een datalek wordt een registratienummer afgegeven. Dit nummer moet worden vastgelegd en wordt gebruikt in mogelijke correspondentie met de Autoriteit Persoonsgegevens, zoals bijvoorbeeld bij een vervolgmelding.
Als de melding voor het Autoriteit Persoonsgegevens gereed is wordt ook de mogelijkheid gegeven een kopie van de melding uit te printen voor de eigen administratie. Melder archiveert een kopie van de melding in het 'dossier'.

5.6 Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Melder (en de Technicus), zoals hierboven aangegeven. De verwerkings-verantwoordelijke (het GBT) is onder de AVG verplicht alle inbreuken te documenteren, met inbegrip van de feiten over de inbreuk, de gevolgen en de genomen corrigerende maatregelen (artikel 33, vijfde lid AVG). Hierdoor is de Autoriteit Persoonsgegevens in staat naleving van de AVG te controleren.

NB: dit moet ook gebeuren als het incident niet gemeld hoeft te worden aan de Autoriteit Persoonsgegevens. De AVG schrijft in dat geval voor dat er beargumenteerd en gedocumenteerd moet zijn vastgelegd waarom er niet gemeld is.

De Melder informeert interne betrokkenen (inclusief de Ontdekker) over de genomen maatregelen.

5.7 Informeren betrokkene

Houdt het datalek een hoog risico in voor de rechten en vrijheden van natuurlijke personen, dan deelt de Melder[2] de betrokkene de inbreuk in verband met persoonsgegevens direct mee. In principe kan er van worden uitgaan dat lekken van gegevens van gevoelige aard altijd gemeld moet worden bij de betrokkenen.

De melding aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en tenminste:

- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

NB: als er persoonsgegevens zijn gelekt maar deze zijn beveiligd of versleuteld, en de gelekte data is onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

6. Monitoring beveiligingsincidenten en datalekken

De Functionaris Gegevensbescherming van het GBT maakt tenminste één keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
Bestuur, MT en de OR worden geïnformeerd over de uitkomsten van de analyse.

[2] Dan wel op verzoek van de Melder, de klachtencoördinator of andere medewerker van het GBT.