v.18-1

PROCEDURE MELDING DATALEKKEN

DEZE PROCEDURE VOORZIET IN EEN GESTRUCTUREERDE WIJZE VOOR HET MELDEN VAN DATALEKKEN IN HET KADER VAN DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG).

Definities

Het kan gebeuren dat persoonsgegevens van Bisbee toegankelijk worden voor mensen die geen recht hebben op kennisname van die gegevens (datalek). Een persoonsgegeven is elk gegeven van een persoon waarbij de identiteit van die persoon redelijk eenvoudig kan worden vastgesteld. Bijvoorbeeld namen, klantnummers, (e-mail)adressen.

Het gaat om een inbreuk op de beveiliging, die (een aanzienlijke kans op) ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Deze inbreuken dienen onverwijld te worden gemeld aan de Autoriteit Persoonsgegevens.
Ook alle betrokkenen (is degene wiens persoonsgegevens zijn gelekt) moeten in kennis gesteld worden indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker die direct of indirect kennis krijgt van een privacylek, is verplicht dit direct te melden aan de directie;
2. De directie is verantwoordelijk voor het onderzoeken van het incident en het ondernemen van preventieve en repressieve acties.

Uitvoering

1. De medewerker (waaronder ook verstaan medewerkers van verwerkers) die direct of indirect kennis krijgt van een incident inzake het lekken van privacygegevens meldt dit direct aan de directie;
2. De directie, eventueel in samenwerking met de medewerker Automatisering, onderzoekt het incident. Hierbij is aandacht voor de volgende aspecten:
   a. wat is de aard van het privacylek;
   b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
   c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
   d. is de organisatie verwijtbaar;
   e. kan de schade van het datalek voor betrokkenen door maatregelen beperkt worden;
   f. van het incident wordt een verslag gemaakt en in Afas vastgelegd;
3. De directie neemt indien nodig contact op met de Autoriteit Persoonsgegevens en/of meldt het datalek direct via het Meldloket Datalekken;
4. Eventuele aanwijzingen van de Autoriteit Persoonsgegevens worden vastgelegd en opgevolgd;
5. De directie informeert indien nodig de betrokkenen alsmede de relevante medewerkers.

Interne controle

Een datalek wordt in de AVG gedefinieerd als een "inbreuk op de beveiliging" (artikel 83 AVG). Voor de meldplicht datalekken geldt dat er sprake moet zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft.

Te denken valt aan:
- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum;
- onbeveiligde e-mails (intern/extern) die privacygevoelige informatie bevatten.

Zijn er persoonsgegevens van gevoelige aard gelekt met (een aanzienlijke kans op) ernstige nadelige gevolgen?

Er moet gekeken worden naar de aard van de getroffen gegevens:
Bij persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits-)fraude. Voorbeelden hiervan zijn persoonsgegevens over iemands godsdienst of levensovertuiging, ras, e.d., gebruikersnamen en wachtwoorden, gegevens over de financiële of economische situatie van de betrokkene (salaris- en betalingsgegevens of gegevens die kunnen worden misbruikt voor (identiteits-) fraude zoals kopieën van identiteitsbewijzen en het burgerservicenummer (bsn).

Er moet gekeken worden naar de aard en de omvang van de inbreuk:
Zo kunnen beveiligingslekken in de omvangrijke verwerking van persoonsgegevens soms zeer grote gevolgen hebben voor de betrokkenen. Voorbeelden zijn veel persoonsgegevens per persoon, gegevens van een grote groep betrokkenen of betrokkenheid van kwetsbare groepen.

Hoe wordt een datalek aan de Autoriteit Persoonsgegevens gemeld?

De Autoriteit Persoonsgegevens heeft een digitaal Meldloket Datalekken. De directie is verantwoordelijk voor het tijdig melden van een datalek. Na melding dient een ontvangstbevestiging te worden uitgedraaid.

Wanneer moet het datalek aan de Autoriteit Persoonsgegevens gemeld worden?

Een datalek moet onverwijld gemeld worden. Wel mag er, na het ontdekken van een mogelijk datalek, enige tijd genomen worden voor nader onderzoek teneinde een onnodige melding te voorkomen. Als richtlijn geldt dat er gemeld wordt binnen 48 uur nadat Bisbee op de hoogte raakt van een incident waarbij persoonsgegevens kunnen zijn blootgesteld

aan verlies of onrechtmatige verwerking. Eventueel kan de melding naderhand nog worden aangevuld of ingetrokken.

Om datalekken tijdig te kunnen melden zullen goede afspraken moeten worden gemaakt met de verwerkers die worden ingeschakeld, zodat zij Bisbee tijdig en adequaat informeren over alle relevante incidenten.

Welke gegevens moeten worden vastgelegd over het datalek?

De directie houdt een overzicht bij van alle datalekken, dus ook die niet onder de meldplicht vallen.

Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent:

- de aard van de inbreuk;
- de oorzaak van de inbreuk;
- het soort gelekte persoonsgegevens;
- het aantal personen waarbij gegevens zijn gelekt;
- een omschrijving van de groep personen waarbij gegevens zijn gelekt;
- het moment van ontdekking;
- de datum waarop het lek heeft plaatsgevonden;
- het bekende of te verwachten gevolg;
- de voorgestelde oplossing;
- genomen maatregelen ter beperking van de gevolgen;
- de wijze waarop het lek gedicht is.

Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen.

De wet schrijft niet voor hoe lang het overzicht moet worden bewaard. Uitgegaan kan worden van een bewaartermijn van minimaal een jaar. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren.

Moet het datalek aan de betrokkene worden gemeld?

Wanneer is vastgesteld dat het betreffende datalek gemeld moet worden bij de Autoriteit Persoonsgegevens dient tevens beoordeeld te worden of het datalek aan betrokkene moet worden gemeld. Zo kan kennisgeving aan betrokkene bijvoorbeeld achterwege blijven wanneer de technische beschermingsmaatregelen die zijn genomen voldoende bescherming bieden, of wanneer een datalek waarschijnlijk geen ongunstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkene. De directie is verantwoordelijk voor het melden van een datalek aan de betrokkene.

Korte checklist datalek:

1. Zijn de gelekte gegevens persoonsgegevens zoals namen, klantnummers, e-mailadressen?
2. Zijn persoonsgegevens verloren geraakt of onrechtmatig verwerkt zoals verloren laptop, brand?
3. Zijn er een groot aantal of gevoelige gegevens gelekt zoals 1.000 gegevens, bankrekening, inlog?

Bij 3x ja moet er via de directie melding plaatsvinden bij de Autoriteit Persoonsgegevens.

4. Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van de personen, zoals identiteitsfraude?
5. Zijn de gelekte persoonsgegevens onvoldoende beveiligd zodat ze gelezen kunnen worden?

Bij 2x ja moet via de directie ook de betrokkene geïnformeerd worden over het datalek.