Procedure rondom (mogelijke) datalekken bij Finenzo Zaanstad

Inhoudsopgave

1. Doel

Met ingang van 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) gehandhaafd. Hierbij geldt een meldplicht voor bepaalde datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken bepaalde datalekken moeten melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.
De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de meldplicht valt.
Deze procedure beschrijft hoe te handelen binnen Finenzo Zaanstad, indien er sprake is van een datalek of wanneer een datalek vermoed wordt. De meldplicht is eveneens van toepassing op Finenzo Zaanstad, als het datalek bij een verwerker is ontstaan.
Per datalek behoudt Verantwoordelijke de vrijheid om te beoordelen of de procedure gevolgd wordt, danwel afwijking van deze procedure gerechtvaardigd is.
Het doel van deze procedure is vast te leggen, welke stappen genomen moeten worden door Finenzo Zaanstad bij het vermoeden van of kennis nemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek.

Het volgende resultaat wordt hiermee nagestreefd:
- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van Finenzo Zaanstad, de betrokkene dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk) datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde (mogelijk) datalek.

2. Toepassingsgebied
Deze procedure wordt gehanteerd bij het melden en afhandelen van (mogelijke) datalekken bij Finenzo Zaanstad, dan wel van (mogelijke) datalekken die buiten Finenzo Zaanstad hebben plaatsgevonden, doch waarvoor Finenzo Zaanstad als Verantwoordelijke de eindverantwoordelijkheid draagt (bv. bij een verwerker).

3. Instellen Datalekken Team
Er wordt een Datalekken Team benoemd bestaande uit de volgende personen:
- Baldwin Stuvel (directeur)
- Ilona van Tol (ondersteuning)
- Brenda van Drunen (adviseur)

4. Procedure
4.1 Intern melden van een datalek
- De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij een van de aangewezen personen genoemd bij punt 3. Het teamlid Datalekken dient dan onverwijld Baldwin Stuvel in kennis te stellen van het datalek. De melding moet direct en telefonisch worden gedaan bij Baldwin Stuvel en schriftelijk worden vastgelegd in het CRM pakket: Invice.

Een medewerker is te allen tijde bevoegd zelfstandig een melding te doen aan de directeur!

De procedure Meldplicht Datalekken wordt dan gestart. Noot: Ook (de medewerker van) een Verwerker kan een datalek constateren en melden aan de directeur van Finenzo Zaanstad / Baldwin Stuvel. De directeur is de datalek coordinator tevens de verantwoordelijke.

4.2 Beoordeling aard/ernst incident; datalek ja/nee

- De datalek coördinator draagt zo spoedig mogelijk zorg voor de volledige en juiste informatie die is vereist voor het melden van een datalek.
- De datalek coördinator nodigt het Datalekken Team onverwijld uit.
- Op basis van de verkregen informatie en bij vermoeden van een datalek wordt in het Datalekken Team zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek.
- Tevens kan in dit overleg worden beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen.
- Het Datalekken Team beoordeelt of er sprake is van een incident, dat gemeld moet worden aan de AP.

Bij deze beoordeling spelen o.a. een rol:

- is er sprake van verlies van persoonsgegevens; dit houdt in dat Finenzo Zaanstad deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
- is er sprake van onrechtmatige verwerking van persoonsgegevens; hier onder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging;
- kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid;
- zijn er persoonsgegevens van gevoelige aard gelekt:
    - ❖ bijzondere persoonsgegevens conform artikel 9 AVG;
    - ❖ gegevens over de financiële of economische situatie van de betrokkene;
    - ❖ gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
    - ❖ gebruikersnamen, wachtwoorden en andere inloggegevens;
    - ❖ gegevens die kunnen worden gebruikt voor (identiteits) fraude;
- de aard en de omvang van de inbreuk;

- In geval geoordeeld wordt, dat sprake is van een (mogelijk) datalek, wordt tevens het communicatietraject richting betrokkene(n) en indien van toepassing de verwerker besproken;

4.3 Melden aan de Autoriteit Persoonsgegevens (AP)

- Indien het datalek meldingsplichtig is verzorgt de datalek coördinator zonder onredelijke vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) een elektronische melding bij de AP volgens het online meldingsformulier van de AP. Dit met inachtneming van richtlijnen van de AP terzake.
- De datalek coördinator zorgt voor de volledige en juiste informatie.
- De datalek coördinator fungeert als contactpersoon inzake de communicatie naar de AP. Dit geldt ook ingeval nog niet duidelijk is dat het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken.
- De AP zal na het melden van een datalek een ontvangstbevestiging sturen.
  Alleen indien de melding daartoe aanleiding geeft zal de AP contact opnemen.
- Bij een datalek als gevolg van een hack ligt naast melding bij de AP, ook aangifte bij de politie in de rede in verband met de opsporing van de daders. Aangifte loopt via een eventueel beschikbare contactfunctionaris richting politie.

4.4 Beoordeling of datalek gemeld dient te worden aan de betrokkene(n)

- Indien een datalek is gemeld aan de AP dient tevens vastgesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat.
- Dit ter beoordeling van en advisering door het Datalekken Team.
- Bij de beoordeling speelt onder meer een rol:
    - Of Finenzo Zaanstad passende technische en organisatorische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Bij twijfel hierover dient het datalek gemeld te worden aan de betrokkene(n).

- Of Finenzo Zaanstad achteraf maatregelen heeft genomen, waardoor er waarschijnlijk geen hoog risico meer is voor de rechten en vrijheden van betrokkene(n).
- Of de melding onevenredige inspanningen zou vergen.

4.5 Rapporteren aan de betrokkene(n)

- In opdracht van de Verantwoordelijke stelt het Datalekken Team een kennisgeving aan betrokkene(n) op.
- Het Datalekken Team bepaalt wat aan de betrokkene(n) wordt gemeld.
- De melding bevat in ieder geval de aard van de inbreuk, contactgegevens waar de betrokkene(n) meer informatie over de inbreuk kan krijgen, en de maatregelen die Finenzo Zaanstad de betrokkene(n) aanbeveelt te nemen om de negatieve gevolgen van de inbreuk te beperken.
- De betrokkene(n) worden individueel geïnformeerd.
- Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit houdt in dat Finenzo Zaanstad, na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat Finenzo Zaanstad de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Wel dient hierbij rekening gehouden te worden dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het datalek.
- In de melding aan de AP is al aangegeven of Finenzo Zaanstad het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer Finenzo Zaanstad dat gaat doen. De termijn die Finenzo Zaanstad in de melding aan het AP aangeeft, moet Finenzo Zaanstad ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat Finenzo Zaanstad dit aan de AP weten door middel van een aanpassing van de melding.

5. Rapportage Datalekken Team

- Naar aanleiding van het onderzoek en (al dan niet) de melding richting AP en de betrokkene(n) maakt het Datalekken Team een conceptrapport op van zijn bevindingen.
- Het Datalekken Team stelt in deze rapportage tevens verbetermaatregelen op.

6. Slotbijeenkomst in geval van een datalek: bespreking rapport en vaststellen verbetermaatregelen

- De datalek coördinator plant een slotbijeenkomst ter bespreking van het conceptrapport van het datalekken Team.
- Voor de slotbijeenkomst worden uitgenodigd de Verantwoordelijke, de leden van het Datalekken Team en de directeur in wiens domein de verbetermaatregelen liggen.
- De genodigden ontvangen een afschrift van het conceptrapport.

7. Implementeren verbetermaatregelen

- De directeur in wiens domein de verbetermaatregelen liggen is verantwoordelijk voor de implementatie van de vastgestelde verbetermaatregelen, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering, en rapporteert over de voortgang aan de Verantwoordelijke.
- Indien bij een verwerker verbetermaatregelen nodig zijn, is de directeur die opdrachtgever is van deze verwerker daartoe verantwoordelijk.
- De datalek coördinator bewaakt de voortgang, onder eindverantwoordelijkheid van de Verantwoordelijke.

8. Sluiten melding en vastlegging

De datalek coördinator informeert de Verantwoordelijke, de betrokken organisatorisch directeur, de direct bij de calamiteit betrokkenen en het Datalekken Team op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.

- De leden van het Datalekken Team vernietigen de nog in bezit zijnde documentatie.
- Het datalekdossier wordt digitaal door de datalek coördinator gearchiveerd.