Provincie Antwerpen

Dienstnota van de provinciegriffier

Nummer:	**DAB– 23 - 2022**
Onderwerp:	**Melden van beveiligingsincidenten**
Inhoudelijk contactpersoon:	Katty Scholdis (DPO)
Samenvatting:	In deze nota lichten we toe wat je moet doen als je een beveiligingsincident opmerkt.
Bronnen:	Algemene Verordening Gegevensbescherming Intranetpagina datalekken
Van toepassing op	Medewerkers van de centrale administratie

Deze dienstnota treedt in werking op **20/6/2022**

Deze dienstnota vervangt dienstnota DAB–23/2020

Inhoudstafel

1 Wat is een beveiligingsincident en of vermoedelijk datalek?

We verwachten van onze medewerkers dat ze de (persoons)gegevens die ze verwerken zo goed mogelijk beveiligen.

Maar soms gaat er iet mis. Je hebt bijvoorbeeld zelf geen toegang meer tot je gegevens of persoonsgegevens vallen in handen van derden die geen toegang tot die gegevens zouden mogen hebben. In dit geval is er sprake van een beveiligingsincident.

Indien het incident gevolgen heeft voor de privacy van de personen waarvan je de gegevens verwerkte, dan spreken we over een datalek.

De administratieve afhandeling van een datalek verschilt van de afhandeling van een ander beveiligingsincident. We verwachten echter niet van jou om deze verschillende behandelingen te kennen. We vragen je enkel om ingeval van een beveiligingsincident (incl. datalekken) zo snel mogelijk een melding te doen bij één van de meldpunten. Achter de schermen zullen de verschillende meldpunten informatie uitwisselen met de data protection officer (DPO) om in geval van een datalek te voldoen aan de wettelijke verplichtingen.

We spreken van een datalek als er toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens was zonder dat dit de bedoeling is.

Voorbeelden hiervan zijn een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Een datalek kan ook al ontstaan door gevoelige informatie naar de verkeerde persoon te e-mailen of door de naïviteit van onszelf, door bijvoorbeeld te makkelijke wachtwoorden te gebruiken. Het wachtwoord 123456 staat al jaren met stip op nummer één als meest gebruikt.

Dit zijn allemaal voorbeelden van datalekken. Maar, als er alleen sprake is van een zwakke plek in de beveiliging, dan spreken we van een beveiligingslek en niet van een datalek. Een beveiligingslek hoeft dus niet verplicht gemeld te worden bij de autoriteiten.

2 Waarom moet je het melden?

Van belang is dat iedere medewerker elk incident, van welke aard dan ook, tijdig meldt.
Op deze manier kunnen de nodige maatregelen getroffen worden om eventuele negatieve gevolgen zoveel mogelijk te beperken.

Bij het meldpunt zal het incident verder opgevolgd worden. Indien het incident een datalek betreft zal de DPO door het meldpunt op de hoogte worden gesteld zodat het datalek verder geanalyseerd kan worden. Het kan zijn dat de melder nog gecontacteerd wordt om bijkomende informatie te bezorgen.

Ingeval van een datalek zijn we gebonden aan wettelijke verplichtingen (GDPR). In sommige gevallen zal een melding nodig zijn van het datalek bij de bevoegde toezichthouder, de Gegevensbeschermingsautoriteit (GBA) en de Vlaamse Toezichtcommissie (VTC). Deze melding moet binnen de 72 uur na het ontdekken van het datalek gebeuren. Indien het datalek grote gevolgen heeft voor de personen op wie de gegevens betrekking hebben, moeten ook zij geïnformeerd worden zodat ze zelf maatregelen kunnen nemen.

3 Voorbeelden van incidenten

Enkele voorbeelden van wat mogelijk incidenten kunnen zijn (deze lijst is niet exhaustief):

- Je verliest een informatiedrager met gevoelige gegevens, of deze wordt gestolen. Voorbeelden van zo'n informatiedragers zijn: jouw provinciale laptop, een USB-stick, jouw persoonlijke smartphone die je ook deels gebruikt voor het werk (bv. lezen van provinciale mails in e-mail app).

- Jouw provinciale computer raakt besmet met een virus, of je hebt een vermoeden hiervan (bv. omwille van vreemd gedrag of ongekende programma's).

- Je vermoedt dat jouw logingegevens, of die van een collega, werden misbruikt door derden.
- Je vermoedt dat één van de provinciale informatiesystemen werd gehackt (bv. omdat er een vreemde boodschap staat op de startpagina).
- Je ontvangt een phishing telefoon waarin onbekenden vragen om je provinciale computer over te nemen omdat je zogezegde besmette bestanden op je computer hebt gedownload.
- Je treft een bezoeker of leverancier aan in een gelimiteerde zone zonder toegangsbadge en zonder begeleiding van een provinciale collega en je vermoed dat deze toegang heeft gehad tot persoonsgegevens.
- Omwille van een technisch defect kan iedereen zonder toegangsbadge (een deel van) het gebouw in- en uitgaan.
- Je vermoedt dat een bezoeker op een oneigenlijke manier gevoelige persoonsgegevens gegevens heeft verzameld.
- Je treft een bezoeker aan die zonder toestemming op een provinciale laptop aangemeld is (bijvoorbeeld tijdens de lunchpauze op een laptop die niet correct afgesloten werd of niet in slaapstand stond).
- Een e-mail met gevoelige gegevens komt bij de verkeerde persoon terecht.
- Een poststuk met gevoelige gegevens komt niet aan bij de ontvanger of komt geopend terug.
- Op een externe website staan gevoelige provinciale gegevens (bv. persoonsgegevens van provinciale medewerkers) en het is niet duidelijk of hiervoor wel toestemming is gegeven.
- Een particulier laat je weten dat zijn persoonsgegevens voor andere doeleinden worden aangewend dan diegene waarvoor hij toestemming heeft verleend.
- Iemand laat een vertrouwelijk document bij de printer liggen.
- Je ontvangt een valse factuur.
- Een geprinte klantenlijst werd gestolen.

4 Waar moet je het melden?

Binnen het provinciebestuur kunnen incidenten via verschillende kanalen worden gemeld.

- **ICT – Servicegroep (03/240.52.20 of via ICT-ticket)**

  Meldpunt voor ICT beveiligingsincidenten. Je kan hier op werkdagen terecht van 7u30 tot 17u30. Bij dringende ICT beveiligingsincidenten kan je buiten deze uren terecht bij het departementshoofd ICT (rechtstreeks of via je eigen departementshoofd).

- **Team beveiliging en bewaking (03/240.65.02)**

  Meldpunt voor inbreuk op de fysieke beveiliging van een gebouw of zijn apparatuur, bereikbaar op werkdagen van 7 tot 23u.

- **DPO (03/240.51.25) of provinciegriffier (03/240.58.37)**

  Incidenten met een vertrouwelijke en/of privacy gevoelige impact kunnen rechtstreeks bij de DPO of de provinciegriffier gemeld worden. Bij deze personen kan je terecht tijdens de normale kantooruren.

- **Noodnummer (03/240 50 22)**

  In geval van een ernstig en acuut incident – zie voorgaande voorbeelden – tijdens en buiten de werkuren in het provinciehuis, Parkhuis, Lozanagebouw [1] dien je het noodnummer 03 240 50 22 te contacteren. De telefoon van een apart noodtoestel rinkelt dan bij de bewaking in het provinciehuis.

  Je gebruikt het noodnummer enkel in geval van nood: bij brand, bij een zware technische storing of eender welke rampspoedige gebeurtenis, na een oproep naar de 100 (of 112), bij ontvangst van een bommelding of bij het aantreffen van een verdacht pakje.
  Verder kan je het noodnummer gebruiken om dringend onregelmatigheden en incidenten te melden aan de bewaking (bijvoorbeeld een ongenode of agressieve bezoeker of een ernstig en acuut ICT beveiligingsincident).

5 Welke informatie moet je melden?

We verwachten dat je als melder van een incident o.a. volgende informatie bezorgt aan het meldpunt:

- Contactgegevens van de melder.
- Datum en tijdstip van het incident.
- Korte beschrijving van het incident.
- Wat ben je verloren (laptop, tablet, mobiele telefoon, usb-stick, etc.)?
- Welke (mogelijke) gegevens zijn er verloren gegaan?
- Hoe werden de gegevens beveiligd (kan je op afstand gegevens wissen, is de data voorzien van encryptie)?

Je hoeft niet te wachten tot al deze gegevens gekend zijn alvorens het incident te melden. Hoe meer informatie er op het moment van melden aanwezig is hoe beter. Ontbrekende gegevens zullen opgevraagd worden indien nodig.

6 Wat zijn de gevolgen als je een datalek niet meldt?

Het is misschien een instinctieve reactie om een incident te willen toedekken en niet te melden bij een meldpunt.

Echter, zolang we niet op de hoogte zijn van een incident kunnen we geen maatregelen treffen om negatieve gevolgen voor de bedrijfsprocessen zoveel mogelijk te beperken.

[1] In geval van nood op andere locaties kunnen andere regels van toepassing zijn.

Daarbovenop, als het gaat om een datalek, zijn we gebonden aan wettelijke verplichtingen om in sommige gevallen een melding te doen bij de bevoegde toezichthouder.
De melding van een datalek op zich brengt niet automatisch sancties met zich mee. Dit is wel het geval indien het gaat om grove nalatigheid of opzet.
Indien een datalek echter niet gemeld wordt en nadien komt het datalek toch uit creëert dit niet alleen reputatieschade voor de organisatie maar kan dit ook een sanctie opleveren van de bevoegde toezichthouder.

Wanneer een datalek niet gemeld wordt bij de DPO kunnen, indien nodig, de betrokkenen van wie de gegevens gelekt zijn niet gecontacteerd worden. Bijgevolg kunnen deze personen niet het nodige doen om hun gegevens te beschermen (zoals aanpassen van wachtwoorden ed.). Claims en rechtszaken brengen opnieuw negatieve publiciteit en kosten ook geld.

7 Toepassingsgebied

De principes en voorbeelden die in deze dienstnota worden uiteengezet zijn ook van toepassing op medewerkers van buitendiensten, APB's en EVAP's.

De invulling van de verschillende meldingskanalen waar je een incident kan melden zullen in sommige gevallen afwijken als het gaat om een buitendienst, APB of EVAP. Het is dan ook nodig om aparte afspraken te maken en te communiceren naar de medewerkers zodat duidelijk is bij welke meldpunten ze terecht kunnen. Ook intern dienen er afspraken gemaakt te worden zodat ingeval van een datalek de bevoegde DPO tijdig betrokken wordt.

8 Eigenaar van het document

Het onderhoud, de opvolging en de herziening van deze dienstnota vallen onder de verantwoordelijkheid van de DPO van provinciebestuur Antwerpen.

Maarten Ronny Puls
De Provinciegriffier

23/06/2022