&AP

AUTORITEIT PERSOONSGEGEVENS

Nieuwsbrief voor de FG / 19 december 2019

Deze nieuwsbrief voor functionarissen gegevensbescherming (FG's) verschijnt minstens 4 keer per jaar. Gepubliceerde nieuwsbrieven vindt u op onze website. U kunt zich ook abonneren om de nieuwsbrief per e-mail te ontvangen.

Hoera, een datalek

Een uitspraak die je misschien niet verwacht van de Autoriteit Persoonsgegevens (AP). Maar onlangs lazen wij een blog van een privacy adviseur met deze titel. De boodschap? Wanneer er binnen een organisatie veel beveiligingsincidenten worden gemeld, is dat een teken dat medewerkers privacybewust zijn. Ieder gemeld incident is namelijk een kans om de organisatie veiliger te maken. En dat is ook een van de gedachtes achter de meldplicht datalekken uit de Algemene verordening gegevensbescherming (AVG).

Maar of iedere bestuurder dit ook zo ziet? In deze nieuwsbrief aandacht voor de rol van de FG bij datalekken.

Interview met Barend Bon over het melden van datalekken: "*Zorg dat je als FG hebt vastgelegd wat jouw advies was.* "

“Waarom zou ik mezelf aangeven?” Een reactie die sommige FG’s krijgen wanneer zij hun bestuurder adviseren om een geconstateerd datalek te melden bij de AP. Het is een van de dilemma’s waar FG’s in de praktijk mee te maken hebben. In gesprek met Barend Bon, coördinator datalekken bij de AP.

Wel of niet melden?
Barend: "*Ik vind het oprecht jammer wanneer organisaties het idee hebben dat een datalek melden een soort schuldbekentenis is. Een datalek kan namelijk iedereen overkomen. Wanneer je het datalek op tijd aan de AP meldt, en je de betrokkenen informeert als dat nodig is, heb je over het algemeen niets te vrezen. Wel is het belangrijk dat je laat zien dat je er alles aan doet om de schade te beperken en dat je herhaling wilt voorkomen. Het is vooral belangrijk om binnen 72 uur te melden. Zodat de AP kan controleren of je de juiste stappen en maatregelen hebt genomen.*"

De AP heeft als hulpmiddel een lijst met voorbeelden van 'wel- en niet-meldplichtige' datalekken gepubliceerd. Daarnaast wordt ons vaak gevraagd om in concrete gevallen advies te geven over het al dan niet melden van een datalek. Barend: "*Wij laten als toezichthouder deze afweging juist bij de verantwoordelijken zodat de FG de ruimte heeft de AVG-normen toe te passen op de specifieke situatie. De FG kent de organisatie en de aard van de gegevens als geen ander en kan de risico's dus veel beter inschatten. Zonder onderzoek kunnen wij daar geen uitspraken over doen. Dat is bij uitstek de expertise van de FG.*"

Werk aan de winkel
Voor FG's is er dus nog werk aan de winkel om het principe van de meldplicht in organisaties te verduidelijken. Barend: "*Ja, bestuurders moeten zich realiseren dat wij ook onderzoek doen naar niet gemelde datalekken. We kunnen er ook op andere manieren achter komen dat een datalek niet is gemeld, terwijl dat wel had gemoeten. En dat rekenen wij een verwerkingsverantwoordelijke wél standaard zwaar aan.*"

Leg je advies vast
Maar wat als een bestuurder besluit om een datalek – ondanks het advies van de FG - niet te melden? Barend: "*Zorg dan dat je als FG hebt vastgelegd wat jouw advies was. De verwerkingsverantwoordelijke blijft namelijk verantwoordelijk voor de uitvoering van het privacybeleid. Dat mag de FG niet worden aangerekend.*"

Wie doet de melding?
Een ander dilemma waar FG's mee te maken hebben, is wie het datalek meldt bij de AP. Barend: "*Wat we vaak zien is dat FG's een datalek bij ons melden. Ik kan me wel voorstellen hoe dat in de praktijk gaat. Door gebrek aan capaciteit kan het zo zijn dat de FG de enige medewerker is met verstand van de AVG. Overigens mág je als FG wel een datalek melden namens je bestuur, maar het zou beter zijn om die dubbele pet te voorkomen. De verantwoordelijkheid voor het melden van een datalek ligt immers bij de verwerkingsverantwoordelijke en niet bij de FG.*"

Het is een boodschap die de AP vaker geeft. Als FG ben je niet verantwoordelijk voor de uitvoering van het privacybeleid. Je adviseert een organisatie over wat een gezond privacybeleid is en houdt daar toezicht op. Dat is een wezenlijk verschil.

Barend: "*Ik raad daarom aan om bij het opstellen van een intern datalekproces duidelijk vast te laten leggen wie de afweging maakt of een datalek gemeld moet worden, en wie de melding uiteindelijk doet.*"

Het is niet zo dat ieder gemeld datalek reden is voor een feestje. Maar een 'hoera' voor organisaties die hun verantwoordelijkheid nemen bij een datalek is wel op zijn plaats. Het betekent dat organisaties steeds privacybewuster worden. Bestuurders mogen dus minder huiverig zijn om een datalek bij de AP te melden. En dat is een schone taak voor de FG.

10.000 FG's

In het derde kwartaal was het zover: meer dan 10.000 organisaties hebben hun FG bij de AP aangemeld. In dat kader nodigden wij een FG uit op het kantoor van de AP. Cecile Schut, directeur Systeemtoezicht, Beveiliging & Technologie bij de AP ging in gesprek met Annerine Blufpand over de dilemma's waar je als FG tegenaan loopt.

Op de foto Annerine Blufpand (links) en Cecile Schut (rechts)

Annerine is door de gemeente Katwijk ingehuurd als FG. Met een aanstekelijk enthousiasme vertelt ze over haar werkwijze. Ze benadrukt vooral hoe belangrijk het is om samen te werken met anderen binnen de gemeente. En dat de medewerkers haar kennen, ze is benaderbaar.

Tips van en voor FG's
Uit Annerines verhaal lichten we graag nog 3 hartenkreten voor FG's uit:

1) "Wissel ervaringen uit met andere FG's. Ik schuif regelmatig aan bij kennissessies met FG's van andere gemeentes in de regio. Ook zit ik nog in een werkgroep 'Ethiek' met vakgenoten die ik ken van een leergang voor FG's."
2) "Doe als FG een datalekmelding niet zelf. Je kunt dan in een lastige situatie terechtkomen omdat jij adviseert maar niet verantwoordelijk bent."
3) "Als FG kun je niet alles zelf doen. Wij hebben bijvoorbeeld een extern adviseur ingehuurd voor een bewustwordingssessie over privacy voor het bestuur. Dat heeft enorm geholpen."

AP-website uitgelicht

De AP werkt continu aan het uitbreiden en verduidelijken van de informatie op haar website. Bijvoorbeeld naar aanleiding van de actualiteit of door vragen van FG's.

Recent hebben wij onder meer de volgende content geplaatst of aangevuld op onze website:

Voorbeeldlijst wel/niet melden datalek (pdf)
Hoe zorg ik dat mijn organisatie snel kan handelen bij een datalek? (incl. stappenplan)
Wat doet de Autoriteit Persoonsgegevens met mijn melding van een datalek?
Wanneer mag u zich baseren op de grondslag gerechtvaardigd belang? (incl. normuitleg)
Wat mag ik wél vragen en registreren als mijn werknemer zich ziek meldt?

FG-congres 2020

Zoals ook in de vorige nieuwsbrief aangekondigd, organiseren we in 2020 weer een FG-congres. Zet 25 mei 2020 dus alvast in je agenda! Nadere informatie volgt via onze website, LinkedIn- en Twitteraccount.

Toestemming bij tracking cookies

De AP heeft een controle uitgevoerd bij circa 175 websites van onder meer webshops, gemeenten en media of zij voldoen aan de eisen die aan het plaatsen van tracking cookies worden gesteld. Bijna de helft van de websites die gebruik maken van tracking cookies voldoet niet aan de toestemmingsvereisten.

→ LEES VERDER

Focus AP

De AP legt de komende jaren in het toezichtwerk extra nadruk op drie focusgebieden: datahandel, digitale overheid en artificiële intelligentie en algoritmes.

LEES VERDER

RSS-feed AP

Wilt u direct een melding ontvangen wanneer de AP een nieuwsbericht heeft gepubliceerd op de website? Abonneert u zich dan op de RSS-feed. Dat kan eenvoudig via de knop bovenaan de pagina die u bereikt via deze link: autoriteitpersoonsgegevens.nl/nl/rss

Feedback welkom

De AP werkt continu aan het verbeteren van haar informatie. Heeft u tips of ideeën om onze communicatie met FG's te verbeteren? Laat het ons weten via fg@autoriteitpersoonsgegevens.nl

Over de Autoriteit Persoonsgegevens

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Meer informatie vindt u op autoriteitpersoonsgegevens.nl.