Vereniging Privacyrecht Advocaten (VPR-A)
Hamerstraat 19
1021 JT Amsterdam

Vereniging Privacyrecht (VPR)
Postbus 21695
3001 AR Rotterdam

Autoriteit Persoonsgegevens
t.a.v. de heer mr. A. Wolfsen
Postbus 93374
2509 AJ DEN HAAG

Datum 8 november 2021
Inzake Meldingen datalekken via het meldloket – aanbevelingen voor verbetering

Geachte heer Wolfsen,

Namens de Vereniging Privacyrecht Advocaten (**VPR-A**) en de Vereniging Privacyrecht (**VPR**) richten wij ons hierbij tot de Autoriteit Persoonsgegevens (**AP**) met het verzoek aan de AP om een aantal belangrijke verbeteringen in de meldingsprocedure en het meldloket voor datalekken door te voeren. We hopen dat de AP onze aanbevelingen in overweging neemt en ook implementeert, zodat het melden en opvolgen van datalekken wordt verbeterd.

Als toezichthoudende instantie in Nederland voor het melden van datalekken (onder meer in de zin van artikel 33 AVG), heeft de AP ervoor gekozen een online meldloket in te richten om het melden van relevante datalekken aan de AP te faciliteren. Op 1 juni 2021 heeft de AP haar meldprocedure aangepast in die zin dat zij het oude webformulier op haar website heeft vervangen door een nieuw interactief webformulier die voor drie verschillende situaties kan worden gebruikt, te weten voor het doen van (i) een (initiële) melding, (ii) een vervolgmelding, en (iii) om een melding in te trekken. Bij het publiceren van het nieuwe meldformulier heeft de AP aangegeven dat het doel van de wijzigingen is om een datalek sneller en makkelijker in te kunnen dienen.

Het is prijzenswaardig dat de AP het melden van datalekken probeert te vereenvoudigen. In de praktijk zien wij evenwel dat het nieuwe meldformulier maar ten dele daarin geslaagd is. Op belangrijke punten heeft het nieuwe meldformulier ook tot verslechteringen geleid en staat het formulier zelfs op gespannen voet met de verplichtingen die op de AP als toezichthouder rusten. Ter ondersteuning van het doel van de AP om het doen van datalekmeldingen te vereenvoudigen, geven wij hierbij daarom graag aan de AP een aantal aanbevelingen in overweging op basis van de ervaringen die wij daarmee hebben opgedaan. Deze aanbevelingen zien alleen op de belangrijkste en meest noodzakelijke verbeteringen, zowel in relatie tot het indienen van een datalekmelding alsook de opvolging daarvan. Wij zijn uiteraard graag beschikbaar voor nadere toelichting.

1 Vermelde tijdsduur voor het invullen van de formulieren wekt onterechte verwachtingen

1.1 De AP geeft in haar instructie op het meldformulier aan dat de melding binnen ongeveer een kwartier en/of halfuur voltooid is. Wanneer een organisatie een (nieuw) datalek moet melden, wordt zij echter geconfronteerd met een uitgebreide lijst met gedetailleerde vragen waarop nauwkeurig, soms met exacte aantallen, moet antwoorden. Voor zover de gevraagde informatie al in een vroeg stadium beschikbaar is in verband met de termijn waarbinnen organisaties een (initiële) melding moeten indienen, is bovendien de gevraagde gedetailleerde informatie over het datalek vaak alleen

verspreid bekend bij verschillende personen werkzaam bij de meldende organisatie of bij derden. In de praktijk blijkt dan ook dat de tijd die nodig is om alle informatie te vergaren, de vragen volledig in te vullen en de melding in te dienen veel ruimer is dan de gestelde termijn. Dat geldt ook voor de vervolgmelding.

1.2 Door de tijdsduur van het indienen van de melding op deze manier te schetsen, wekt de AP bij organisaties de verwachting dat het indienen van een melding relatief eenvoudig en snel kan plaatsvinden. Dit heeft tot gevolg dat organisaties te laat worden geconfronteerd met de complexiteit en tijd die nodig is om het meldformulier naar behoren in te vullen en tijdig in te dienen. Onvermijdelijk zullen organisaties dan genoodzaakt zijn om onder tijdsdruk alsnog gehaast het meldformulier aan de AP te versturen, hetgeen afbreuk doet aan de volledigheid en kwaliteit van de melding.

1.3 Omdat het in algemeen belang is dat de informatie zo accuraat en volledig mogelijk wordt ingevuld op het meldformulier, doen wij de volgende aanbevelingen:

1.3.1 We raden aan om organisaties nadrukkelijker bij het meldloket - in aanvulling op de relevante richtsnoeren en gepubliceerde stappenplan - te informeren over de benodigde voorbereiding om het meldformulier goed in te kunnen vullen, waaronder welke gegevens vergaard moet worden en welke mogelijk substantiële tijd nodig kan zijn om deze informatie (binnen de eigen organisatie of bij derden) op te halen.

1.3.2 We raden aan om ook realistischer te informeren over de tijd die nodig zal zijn om het meldformulier volledig en nauwkeurig in te vullen wanneer alle benodigde voorbereidingen eenmaal hebben plaatsgevonden. Naar onze mening is een tijdsbeslag van omstreeks driekwartier tot een uur, nadat de voorbereiding heeft plaatsgevonden, realistischer dan de aangegeven kwartier tot halfuur.

1.3.3 We raden aan om het volledige meldformulier als downloadbaar PDF- en Word-document beschikbaar te stellen. Publicatie daarvan is cruciaal om organisaties te helpen in de voorbereiding op de melding, maar ook voor het voorkomen en detecteren van datalekken, dus als onderdeel van een interne datalekprocedure.

2 Volledig overzicht van het formulier noodzakelijk voor kenbaarheid

2.1 Een veelgehoord punt van kritiek op het oude meldformulier was dat dit statisch was, in die zin dat altijd alle vragen te zien waren en beantwoord moesten worden ongeacht of deze relevant waren voor het datalek. We zien dat de AP deze kritiek met het nieuwe interactieve meldformulier ter harte heeft genomen door te dwingen dat het meldformulier vraag-voor-vraag moet worden ingevuld, aan de hand van verschillende opties en context afhankelijke vervolgvragen. Men zou nu kunnen denken dat het invullen van het formulier daarmee efficiënter en overzichtelijk is geworden, omdat alleen de relevante vragen zichtbaar zijn en moeten worden ingevuld.

2.2 Helaas leidt de wijze waarop dit is geïmplementeerd tot significante problemen, waaronder het gebrek aan kenbaarheid. Zowel voorafgaand aan het invullen van het meldformulier, zoals in de voorbereiding daarop, als tijdens het invullen van het meldformulier is het erg lastig om een volledig overzicht te hebben, inclusief alle (alternatieve) keuzeopties en vervolgvragen. Een dergelijk volledig overzicht is evenwel zeer nuttig en ook noodzakelijk. Vooral in de voorafgaande fase

waarin een organisatie bezig is met het voorbereiden van de melding (en anticiperend daarop het opnemen van een volledige overzicht in een interne datalekprocedure) is de kenbaarheid van het gehele meldformulier cruciaal, zodat organisaties van te voren in staat worden gesteld om te weten wat precies van hen wordt verwacht bij het doen van datalekmeldingen en het uiteindelijk invullen en indienen van het meldformulier daadwerkelijk nauwkeuriger, sneller en efficiënter kan plaatsvinden. Zonder deze noodzakelijke transparantie werpt de AP een te grote drempel op voor organisaties om op een goede en efficiënte manier, zonder kostbare bijstand, invulling te geven aan de meldplicht.

2.3 Aanvullend moet opgemerkt worden dat het tussentijds opslaan van de conceptmelding door het downloaden van een .cas-bestand behulpzaam kan zijn, maar geen redelijk alternatief vormt. Een gedownload .cas-bestand geeft geen volledig overzicht en is niet direct eenvoudig uit te lezen binnen organisaties. Daarmee zorgt het niet voor meer transparantie en vereenvoudigt het niet de uitwisseling van (alle mogelijk relevante) vragen en (concept) antwoorden om tijdig tot een zo volledig en nauwkeurig mogelijke melding te kunnen komen. Ook werkt het opnieuw uploaden van het .cas-bestand geregeld niet. Hoewel dit laatste mede afhankelijk kan zijn van de geïmplementeerde beveiligingsmaatregelen binnen de beveiligde omgeving van organisaties zelf, is het goed als de AP zich hiervan bewust is en daarmee rekening houdt.

2.4 Wij doen de volgende aanbevelingen:

2.4.1 Zoals hierboven ook al aangegeven, raden we aan om het volledige meldformulier als downloadbaar PDF- en Word-document beschikbaar te stellen.

2.4.2 Voor het geval het meldformulier op enig moment wordt aangepast, raden we aan een gepaste waarschuwing op te nemen bij de te downloaden documenten en, indien er daadwerkelijk een wijziging plaatsvindt, de specifieke wijziging duidelijk te communiceren op de website van de AP.

2.4.3 Wij raden aan om tijdens het invullen van het meldformulier, naast het overzicht van de ingevulde vragen, de mogelijkheid te geven om een overzicht te hebben van het gehele meldformulier, inclusief de nog komende vragen en de verschillende keuzeopties. Hierbij raden we aan een duidelijk zichtbaar onderscheid te maken tussen de al ingevulde, niet ingevulde, en niet relevante vragen.

3 Geen (tijdelijke) opslag op de servers van de AP

3.1 De AP informeert op haar website dat bij het invullen van het meldformulier (dus gedurende de actieve browsersessie) gegevens tijdelijk op servers van de AP worden opgeslagen, dus voordat de melding daadwerkelijk is ingediend. De AP geeft aan dat dit nodig is voor de goede werking van het meldformulier, om precies te zijn de uiteindelijke verzending van het meldformulier en het genereren van een .cas-bestand. De AP informeert tevens dat de servers zodanig zijn afgeschermd dat de medewerkers van de AP die datalekken behandelen, deze gegevens niet kunnen inzien.

3.2 Het zal de AP niet bevreemden dat deze werkwijze vragen oproept over de beveiliging van het meldloket en de vertrouwelijkheid van (concept) meldingen. Organisaties moeten erop kunnen vertrouwen dat zij in alle vertrouwelijkheid een melding kunnen voorbereiden, de vertrouwelijkheid

van die voorbereiding en de ingediende melding steeds wordt gewaarborgd, en dat geen onnodige gegevens worden verwerkt of bewaard die deze vertrouwelijkheid in gevaar kunnen brengen. Door de keuze van de AP voor een oplossing die werkt aan de zijde van de AP (server-side), in plaats van een oplossing die werkt aan apparaat zijde (client-side), zijn echter onnodige beveiligingsrisico's geïntroduceerd. Daarmee kan afbreuk worden gedaan aan de te verwachten vertrouwelijkheid. De toezegging van de AP dat zij intern maatregelen heeft getroffen, zodat medewerkers die datalekken behandelen niet bij de gegevens kunnen, neemt legitieme zorgen omtrent deze beveiligingsrisico's niet weg.

3.3 Gelet op de significante belangen die spelen bij de vertrouwelijkheid van (concept) meldingen, raden we de AP met klem aan om te onderzoeken of het meldformulier niet (meer) client-side ingericht kan worden en het (tussentijds) opslaan van een conceptmelding op andere wijze plaatsvindt dan het downloaden van een .cas-bestand, zodat daarvoor geen gegevens naar de servers van de AP hoeven te worden gestuurd voordat daadwerkelijk op de "verstuur" knop is gedrukt.

4 Makkelijker melden namens verwerkingsverantwoordelijke

4.1 In de Q&A op de website van de AP staat vermeld op welke manier een verwerker namens de verwerkingsverantwoordelijke een datalek kan melden. Dit vereist echter een aantal stappen bij het indienen van de melding die niet geheel duidelijk en efficiënt zijn. Bovendien zijn deze stappen in het meldformulier zelf niet op transparante wijze verwerkt. De administratieve complexiteit voor het indienen van datalekmeldingen door verwerkers neemt verder toe wanneer een verwerker namens meerdere verwerkingsverantwoordelijken hetzelfde datalek wil melden. Blijkens de Q&A van de AP dient de verwerker dan voor iedere verwerkingsverantwoordelijke een aparte melding in te dienen. Dit maakt het indienen van een datalekmelding door een verwerker namens meerdere verwerkingsverantwoordelijken ondoenlijk, helemaal indien het een groot datalek betreft dat alle klanten (verwerkingsverantwoordelijken) van de verwerker treft

4.2 Wij menen dat het bovenstaande een gemiste kans is om op efficiënte wijze datalekken af te handelen die met name in de sfeer van de verwerker liggen, een grotere groep verwerkingsverantwoordelijken treffen, waarbij soortgelijke persoonsgegevens worden verwerkt, en het informeren van de betrokkenen door de verwerker namens de verwerkingsverantwoordelijken plaatsvindt. De AP zou sneller op de hoogte zijn van de omvang van dergelijke datalekken en de kosten voor organisaties zouden beter beheersbaar zijn indien verwerkers wel transparant en eenvoudig een datalek namens (meerdere) verwerkingsverantwoordelijke(n) zouden kunnen indienen.

4.3 Om het melden van datalekken door verwerkers eenvoudiger te maken, stellen wij voor om in het meldformulier een optie te integreren waar een verwerker gemakkelijk, bijvoorbeeld door middel van het aanvinken van een vakje, aan kan geven dat het datalek namens een verwerkingsverantwoordelijke gemeld wordt en, door middel van een extra optionele invulvelden, namens welke verwerkingsverantwoordelijke(n) de melding wordt gedaan en of, en zo ja, wie de getroffen betrokkenen zal informeren over het datalek. De AP behoudt daarmee inzicht in de omvang het datalek en of de verwerkingsverantwoordelijken ook andere verplichtingen voldoende in acht hebben genomen.

5 Meer ruimte in invulvelden bieden

5.1 Wij kunnen ons goed voorstellen dat de AP omwille van de efficiëntie van de beoordeling van ingediende datalekken de informatie die daadwerkelijk ingevuld kan worden op het meldformulier waar mogelijk wil beperken. Zeker bij complexere datalekmeldingen is voor bepaalde informatie evenwel meer ruimte nodig in de invulvelden en zijn het toegestane maximum aantal tekens te laag. Zo is de ruimte om een samenvatting te geven van het datalek en de informatie die wordt of is verstrekt aan de betrokkenen te summier. Het uploaden van bijlagen, zoals de brief gericht aan de getroffen betrokkenen, voldoet niet (altijd) als alternatief. Hoewel dit mede afhankelijk kan zijn van de geïmplementeerde beveiligingsmaatregelen binnen de beveiligde omgeving van organisaties zelf, is het goed dat de AP zich bewust is van de onmogelijkheid om aanvullende documenten bij te sluiten voor veel organisaties, en daarmee genoegzaam rekening houdt. De mogelijkheid om verduidelijking te verschaffen over de gebeurtenissen omtrent het datalek is hierdoor sterk verminderd en is het evenwicht tussen bondigheid en voldoende volledige meldingen om onnodige vervolgvragen en ander vervolgwerk van de AP te voorkomen ons inziens te ver doorgeslagen naar het streven naar bondigheid.

5.2 Om dit evenwicht te herstellen, raden wij aan om het maximaal aantal tekens voor invulvelden opnieuw te evalueren en waar nodig te verruimen, waaronder met betrekking tot de samenvatting over het datalek en de brief gericht aan de getroffen betrokkenen.

6 Aantal gegevensrecords

6.1 Een punt waar veel organisaties in de praktijk ook tegenaan lopen is dat van hen verwacht wordt dat zij bekend zijn met het aantal gegevensrecords dat (potentieel) geraakt is door het incident. In de eerste plaats is het voor veel organisaties veelal onduidelijk wat hieronder moet worden verstaan, zodat het goed zou zijn om hierover een nadere toelichting te verschaffen. In de tweede plaats is het aantal gegevensrecords bij de (initiële) melding niet bekend, zonder dat het formulier de mogelijkheid biedt om geen antwoord op die vraag te geven. Wij raden aan om die mogelijkheid wel te bieden in het (initiële) formulier.

7 Informatie over vervolgprocedure en opvolging van meldingen door de AP is wenselijk

7.1 Op het meldloket van de AP is momenteel geen informatie opgenomen over de vervolgprocedure en opvolging van datalekken door de AP. In de Q&A op haar website, heeft de AP hierover slechts summier iets opgenomen, hetgeen erop neerkomt dat de AP zorgvuldig kijkt naar alle meldingen, maar dat zij gelet op het grote aantal meldingen niet alle meldingen even uitgebreid onderzoekt en meestal geen reactie geeft aan de meldende organisatie. Deze aanpak, die afwijkt van andere collega toezichthouders, zorgt voor een gebrek aan transparantie over hoe datalekken worden opgevolgd en leidt onnodig tot onzekerheid bij organisaties die een datalek hebben gemeld.

7.2 Wij hebben uiteraard begrip voor het feit dat de AP kampt met capaciteitsproblemen in combinatie met het grote aantal datalekken dat jaarlijks worden gemeld, maar ons inziens zou de AP transparanter kunnen optreden en tegelijkertijd efficiënt kunnen omgaan met haar beperkte middelen. Wij doen daarom graag de volgende concrete aanbevelingen om het proces van het melden en de opvolging van datalekken duidelijker en transparanter te maken:

7.2.1 Wij raden aan dat de AP bijvoorbeeld in de introductietekst op het meldloket aangeeft (i) wat de AP met een melding doet, (ii) in welke gevallen zij in beginsel contact zal opnemen met de meldende organisatie, en (iii) op welke termijn de opvolging gewoonlijk zal plaatsvinden.

7.2.2 Wij raden aan om de beleidsregels, logica en (geautomatiseerde) wijze van beoordeling van ingediende datalekken bekend te maken. Wij begrijpen uit de toelichting op de website van de AP dat zij alle datalekken onderzoekt. Gezien de zeer beperkte hoeveelheid medewerkers van de AP die daadwerkelijk (eerstelijns) onderzoek doen naar datalekken, lijkt het ons onvermijdelijk dat de AP intern beleidsregels en logica hanteert voor het (automatisch) beoordelen, categoriseren en/of opvolgen van ingediende datalekmeldingen. Wij kunnen ons tevens voorstellen dat dit mede reden voor de AP is geweest om gebruik te maken van een interactieve meldformulier waarin precieze selecties en aantallen moeten worden ingevuld, zodat de (geautomatiseerde) opvolging wordt bevorderd. Transparantie over deze beleidsregels en logica zou goed zijn om de kwaliteit van datalekmeldingen, die uiteraard steeds naar waarheid dienen te worden gedaan, te verbeteren en te voorkomen dat de AP onnodig tijd moet besteden aan de opvolging daarvan.

7.2.3 Wanneer uit de eerstelijns beoordeling van een ingediende datalek volgt dat deze (momenteel) niet verder opgevolgd zal worden door de AP, raden we aan dat de AP (geautomatiseerd) een (standaard) mededeling hiervan stuurt aan de organisatie die het datalek heeft gemeld. Voor zover met deze mededeling niet uitgesloten kan worden dat de AP het datalek opnieuw zal beoordelen afhankelijk van vervolgmeldingen, signalen of klachten, kan de AP dat uiteraard in haar standaard reactie opnemen.

8 Betrouwbaarheid en fouten meldformulier

8.1 We hebben gemerkt dat de AP sinds de lancering van het nieuwe meldformulier verschillende stabiliteits-, beschikbaarheids-, en andere inhoudelijke fouten van het meldformulier heeft verholpen. Eén blijvende punt willen we echter toch expliciet benoemen. Wanneer het formulier volledig is ingevuld en vervolgens op de knop "laatste vraag" (dus niet "verstuur") wordt geklikt, wordt de melding meteen ingediend bij de AP en volgt de gebruikelijke bevestigingsscherm. Wij nemen aan dat deze werking van de knop "laatste vraag" niet intentioneel is. Hoe dan ook kan deze werking niet afgeleid worden uit de naamgeving van de knop. We raden dan ook aan om dit zo spoedig mogelijk te corrigeren.

9 Formulier ook in het Engels

9.1 Begrijpelijkerwijs bevat het meldformulier ruimte om grensoverschrijdende datalekken te melden. Desondanks is het meldformulier alleen in de Nederlandse taal beschikbaar. Voor het melden van grensoverschrijdende datalekken zou het meldformulier ook (tenminste) in de Engelse taal beschikbaar moeten zijn. Dit vergemakkelijkt de afhandeling van grensoverschrijdende datalekmeldingen hoofdzakelijk op twee manieren:

9.1.1 Bedrijven die in het Engels werken hoeven (ter voorbereiding van de melding) de vragen niet steeds heen en terug te vertalen tussen het Nederlands en Engels. Bovendien is het dan makkelijker om een melding in te dienen bij andere toezichthouders, bijvoorbeeld wanneer geen gebruik kan worden gemaakt van het one-

stop-shop mechanisme. Het beschikbaar stellen van het meldformulier vergroot ook de transparantie voor niet-Nederlandse organisaties die bijvoorbeeld door de ruime territoriale toepassingsgebied van de AVG (ook) in Nederland een datalekmelding moeten doen.

9.1.2 De AP kan de datalekmelding gemakkelijker delen met haar collega toezichthouders.

9.2 Mede gelet op de positie van Nederland met relatief veel (Europese) hoofdkantoren van grensoverschrijdend opererende organisaties, raden wij daarom aan om het meldformulier ook in het Engels beschikbaar te maken.

10 Uniforme aanpak in de EU

Ten slotte hopen wij dat de AP de bovenstaande aanbevelingen in overweging neemt en implementeert, zodat het melden en opvolgen van datalekken wordt verbeterd, en daarbij ook gezamenlijk optrekt met haar collega-toezichthouders verenigd in de EDPB. Momenteel houdt iedere toezichthouder zijn eigen manier aan voor het faciliteren van datalekmeldingen, waaronder de inhoud en werking van meldformulieren, als ook de opvolging van een ingediende melding. Dit is onoverzichtelijk en leidt tot significante kosten en onnodige aanvullende tijdsdruk voor organisaties bij de opvolging van (grensoverschrijdende) datalekken, terwijl de middelen dan beter geconcentreerd zouden kunnen worden in het mitigeren van het datalek zelf. Een op EU-niveau afgestemde uniforme werkwijze zou daarom welkom zijn voor veel organisaties die te maken hebben met toezichthouders van verschillende landen.

Deze brief zal worden verstuurd aan alle leden van de VPR-A en de VPR. Gelet op het publieke belang van dit onderwerp zullen wij deze reactie tevens als openbare brief publiceren in diverse media, zoals het tijdschrift Privacy & Informatie.

U kunt uw reactie richten aan bestuur@vpr-a.nl

Hoogachtend,
Mede namens de besturen en leden van VPR-A en VPR

Elisabeth Thole en Özer Zivali, advocaten bij Van Doorne N.V.

Bestuur VPR-A	**Bestuur VPR**
Gerrit-Jan Zwenne (Voorzitter)	Hester de Vries (Voorzitter)
Ard Jan Dunnik	Hendrik Jan Bolte
Olaf van Haperen	Marta Borrat i Frigola
Cathérine Jakimowicz	Huib Gardeniers
Jeroen Koëter	Cathérine Jakimowicz
Quinten Kroes	Mark Jansen
Elisabeth Thole	Jeroen Terstegge
Hester de Vries	Nynke M. Wisman
	Gerrit-Jan Zwenne