Jaar	Datum en tijd van de datalek (schending/ breach)	Melding bij FG	Melding noodzakelijk naar Autoriteit Persoonsgegevens (binnen 72 uur), indien lek resulteert in een risico voor de rechten en vrijheden van individuen.	Als eerste kennisgeving onvolledig is, dan reden voor vertraging aangeven om aan te tonen dat vertraging bij de rapportage gerechtvaardigd en niet buitensporig is	Melding nodig naar getroffen personen (binnen 72 uur), alleen geactiveerd waar dit waarschijnlijk een groot risico voor hun rechten en vrijheden zal opleveren	Aard van de inbreuk in verband met persoonsgegevens	Categorieën	Geschatte aantal betrokken datasubjecten (degenen wier persoonsgegevens worden verwerkt)	Geschatte aantal betrokken persoonsgegevens records	Naam & contactgegevens functionaris gegevens-bescherming of een ander contactpunt voor meer informatie	Waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens	Maatregelen die de voor de verwerking verantwoordelijke heeft genomen of heeft voorgesteld om de inbreuk in verband met persoonsgegevens aan te pakken	In voorkomend geval maatregelen om de mogelijke negatieve gevolgen te beperken
2019	dinsdag 15 januari 2019 14:13	woensdag 16 januari 2019 12:04	Nee	nvt	Nee	Datalek met bedrijfsnamen (handelsnamen), waaronder bedrijven waarvan de naam van een natuurlijk persoon deel uitmaakt van de bedrijfsnaam.	nvt	nvt	nvt	Arian van Balen, fg@maas.nl	Geen. In het bestand staan bedrijfsnamen (SoldtoName) waarvan de naam van een natuurlijk persoon deel uitmaakt van de bedrijfsnaam. Dit is een openbaar gegeven conform de Handelsregisterwet. Het Handelsregister is een openbaar register met adressen en andere gegevens van ondernemingen en rechtspersonen. Iedereen kan deze gegevens raadplegen. In het Handelsregister staan vestigingsadressen maar ook privéadressen. Het vestigingsadres is de plaats waar de activiteiten van je bedrijf worden uitgevoerd en is altijd openbaar. Het privéadres is je woonadres. Dat privéadres kan overigens gelijk zijn aan het vestigingsadres. Dat is het geval als het bedrijf vanuit het woonadres wordt uitgeoefend. In sommige gevallen is dit privéadres openbaar. Dat is afhankelijk van de rechtsvorm. Dit is zo geregeld in de Handelsregisterwet	nvt	nvt
2020	10 september 03.00 uur	donderdag 10 september 2020	Ja	Eerste mitigatie maatregelen uitgevoerd met First Response Team	Nee	Bij de ransomware aanval zijn data versleuteld. Deze inbreuk gaf gevolgen voor personen, aangezien dit een (tijdelijk) verlies van beschikbaarheid van data geeft.	Gewone persoonsgegevens	4500	4500	Arian van Balen, fg@maas.nl	MAAS heeft nagegaan of de inbreuk een hoog risico oplevert voor de betrokkenen. Daarbij is onder andere gekeken of de inbreuk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Dit is momenteel niet het geval, maar kan niet geheel uitgesloten worden.	Cyber hunter, nieuwe en sterkere wachtwoorden en restore van schone backup's	idem
2022	Zondag 17 maart 2022	Dinsdag 12 april 2022	Nee	nvt	Nee	Voor de klanttevredenheidsonderzoeken die MAAS uitvoert bij klanten, werken we samen met een externe partij Growpromoter. Dit is gekoppeld aan ons CRM systeem SAGE als volgt; • In Sage wordt door Front Office Medewerker (FOM) de taak NPS enquête afgerond, wat zorgt voor een Trigger naar GrowPromoter om de enquête naar de klant te verzenden • Zodra de enquête is ingevuld, wordt het resultaat via GrowPromoter in Sage verwerkt op de klantpagina Afgelopen maand (17/3) is voor een batch van 841 adressen een enquête verzonden, die niet voor hen bedoeld was. Ik loop vast bij Sage en GrowPromoter over de verantwoordelijkheid van dit incident, en met name waardoor dit is gekomen en hoe dit in de toekomst voorkomen kan worden.	Gewone persoonsgegevens	841	841	Arian van Balen, fg@maas.nl	Geen. Elke adressant alleen een email op het individuele email adres ontvangen.	Indien er niets contractueel is vastgelegd, dan zijn MAAS, GrowPromoter en SAGE zelfstandig verwerkingsverantwoordelijke.	nvt
2022	Maandag 27 juni 2022	Maandag 27 juni 2022	Nee	nvt	Nee	Potentieel security- en privacy-risico's bij (tijdelijk) verlies van USB-stick. In dit geval een USB-stick voor monteurs.	nvt	nvt	nvt	Arian van Balen, fg@maas.nl	Geen. Op de sticks die door diverse mensen gebruikt wordt staan automaat specifieke instellingen van automaten. Verder staat er op de stick door welke laptop (geen persoon) de stick is gemaakt. In een van de bestanden kan tevens staan voor welke klant de bestanden gemaakt zijn.	nvt	nvt
2023	Donderdag 11 augustus 2023	Donderdag 11 augustus 2023	Nee	nvt	Formeel niet nodig, maar de verwerker heeft de klanten waar dit betrekking op heeft zelf direct aansluitend in kennis gesteld van het feit dat dit is gebeurd.	Via CRM-systeem Sage een mailing uitgestuurd naar 60 klanten. Echter, bij 1 badge de emailadressen per ongeluk in de "AAN" regel geplakt i.p.v. de "BCC" regel. Betreft een generieke mail over: *Prijsaanpassingen MAAS per 1 september 2023* . Daarvan betreft het bij 7 geen persoonsgegeven (admin, credadm, facilities, facilitair, info, inkoop, SECR)	Gewone persoonsgegevens	53	53	Arian van Balen, fg@maas.nl	MAAS is nagegaan of de inbreuk een hoog risico oplevert voor de betrokkenen. Daarbij is onder andere gekeken of de inbreuk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Het is in dit specifieke geval niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokkenen.	De verwerking verantwoordelijke heeft geen aanvullende maatregelen genomen of voorgesteld.	nvt
2023	Woensdag 23 augustus 2023	Woensdag 23 augustus 2023	Nee	nvt	Nee	Systemen van onze hosting provider (Leaseweb) gehackt geweest. Dit houdt in dat momenteel alle SAP systemen van onze klanten plat liggen. De hack heeft plaatsgevonden op infrastructuur niveau (VM Ware) en uit een eerste onderzoek komt naar voor dat er, voor zover we momenteel kunnen analyseren, geen impact is op data of applicatie niveau.	Gewone persoonsgegevens	4500	4500	Arian van Balen, fg@maas.nl	Op basis van analyse Leaseweb en Delaware nagegaan of de inbreuk een hoog risico oplevert voor de betrokkenen. Daarbij onder andere gekeken of de inbreuk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Het is in dit specifieke geval niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokkenen.	Momenteel is Leaseweb alle systemen terug aan het opzetten waarna Delaware dan stap-voor-stap de SAP omgeving terug kunnen opbouwen (waarschijnlijk vanuit de snapshots, backups).	nvt
2024	Zondag 25 februari 2024	Vrijdag 15 maart 2024	Nee	nvt	Nee	Miko/ MAAS systeembeheerder constateerde 14 maart een recente wachtwoordreset voor het wachtwoord van de oude BI Manager op Office 365. Dit is niet gedaan door de resterende BI Manager. Voorstel Miko/ MAAS systeembeheerder om het wachtwoord voor de zekerheid te resetten. Dit zou naar geen invloed hebben op de Power BI-verbindingen. De verbindingen worden namelijk tot stand gebracht tussen de on-premises server en de MS Power BI-servers zelf.	Gewone persoonsgegevens	1	1	Arian van Balen, fg@maas.nl	Op basis van info BI Manager nagegaan of de inbreuk een hoog risico oplevert voor de betrokkenen. Daarbij onder andere gekeken of de inbreuk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Het is in dit specifieke geval niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokkenen.	De resterende Bi manager en de oud BI mananger waren beide user administrators op Office365. Miko/MAAS Systeembeheer heeft 14 maart 2023 deze rechten verwijderd, omdat de resterende BI manager al een globale beheerder is in de Office 365-omgeving van Maas. Met deze rechten heeft de BI manager al toegang tot alles.	nvt
2024	Donderdag 31 oktober 2024	Donderdag 31 oktober 2024	Nee	nvt	Nee	HR medwerker ben in AFAS Insite (Personeelssysteem) bezig geweest om VOG declaraties goed te keuren. Hierbij heeft een medewerker een mhtml.zip file ingeleverd die ons doorverwijst naar zijn privé MAAS mail waarop zijn hele inbox te zien is. Inderdaad een datalek: Leidinggevende en HR onbedoeld inzage (kunnen hebben) in persoonsgegevens in de privé MAAS mail die niet voor leidinggevende of HR bestemd zijn.	Gewone persoonsgegevens	1	1	Arian van Balen, fg@maas.nl	Op basis van info HR mewerker nagegaan of de inbreuk een hoog risico oplevert voor de betrokken medewerker. Daarbij onder andere gekeken of de inbreuk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkene. Zoals: discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Het is in dit specifieke geval niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken medewerker.	HR heeft de desbetreffende medewerker al op de hoogte gebracht dat we door de link in zijn mailbox kunnen en dat hij in het vervolg beter een jpeg, jpg en/of pdf bestand door moet sturen om datalekken te voorkomen.	De vog2024.mhtml.zip bijlage uit AFAS verwijderen. In plaats daarvan alleen als bijlage het *.jpeg-, *.jpg- en/of *.pdf-bestand van de betreffende VOG-declaratie.

2024	Donderdag 28 november 2024	Donderdag 28 november 2024	Nee	nvt	Nee	Ik heb per ongeluk een mail met adresgegevens van een medewerker naar de verkeerde externe contactpersoon gestuurd. Ik stuur een bericht naar de desbetreffende persoon met de vraag of ze de mail wil verwijderen en deleted items. Is er verder nog iets wat ik kan doen?	Gewone persoonsgegevens	1	1	Arian van Balen, fg@maas.nl	Op basis van info HR medewerker nagegaan of de inbreuk een hoog risico oplevert voor de betrokken medewerker. Daarbij onder andere gekeken of de inbreuk kan leiden tot fysieke, materiële of immateriële schade voor de betrokkene. Zoals: discriminatie, (identiteits-) fraude, financiële schade en reputatieschade. Het is in dit specifieke geval niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken medewerker.	HR heeft email laten verwijderen. Medewerker ging ervan uit dat het mailadres al in het adresboek stond, maar dit was dus niet het geval. Medewerker zal voortaan beter letten op wat achter de @ komt.	Ja, de onjuist geadresseerde externe contactpersoon heeft bevestigd dat deze de mails ging verwijderen.
2025	Dinsdag 18 maart 2025	Dinsdag 18 maart 2025	Nee	nvt	Nee	Titel van het rapport: MAAS.DWHV2 Auto. Testversie is gedeeld met Operations Controller en de Chief Operations Officer (COO), dit is vervolgens gedeeld met Senior Business Controller en die heeft weer gedeeld met een Commercial Contract Manager. Bestand bevat persoonsgegevens (namen van de operators) en de kosten van hun leasewagens. Vraag is of er een grondslag is voor Contractmanagement om specifiek deze persoonsgegevens te gebruiken. In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens: a. U heeft toestemming van de persoon om wie het gaat – niet van toepassing b. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren: Ja: COO: Operators vallen allen onder de Operating afdeling binnen Operations; Ja: Operational Controller binnen Finance apart verantwoordelijk voor o.a. controle Operators. Apart van Financial Accounting en van Contractmanagement; Nee: Niet van toepassing voor het beoogde gebruik (alleen de kosten per klant) door Contractmanagement c. Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent – niet van toepassing d. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen - – alleen te gebruiken indien het essentieel is voor iemands leven of gezondheid e. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang uit te voeren / openbaar gezag uit te oefenen – niet van toepassing f. Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen –vereist altijd een expliciete toetsing of het recht om persoonsgegevens te verwerken – omdat je een gerechtvaardigd belang hebt om dit te doen – zwaarder weegt dan het recht van mensen op	Gewone persoonsgegevens	330	330	Arian van Balen, fg@maas.nl	Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. In dit geval dus het ongewenst verstrekken van persoonsgegevens. Of MAAS een datalek wel of niet moet melden bij de AP is afhankelijk van de mogelijke impact van het datalek op de slachtoffers. Ook de vraag of MAAS de slachtoffers moet informeren over het datalek, hangt af van het risico dat zij lopen door het datalek. In dit geval geen grote impact verwacht, dus geen melding naar AP of informatie aan de "slachtoffers" vereist.	IT BI heeft alle gebruikersautorisaties voor delen en inzien van het rapport verwijderd, behalve leesrechten voor de Operations Controller en de COO.	BI gaat de autorisatie structuur nog zorgvuldiger inrichten.
2025	Woensdag 24 jui 2025	Donderdag 25 juli 2025	Nee	nvt	Nee	Mail met 1 verkeerde contactpersoon erin (externe contact met zelfde voornaam als intern contact).	Gewone persoonsgegevens	1	1	Arian van Balen, fg@maas.nl	Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. In dit geval dus het ongewenst verstrekken van persoonsgegevens. Of MAAS een datalek wel of niet moet melden bij de AP is afhankelijk van de mogelijke impact van het datalek op de slachtoffers. Ook de vraag of MAAS de slachtoffers moet informeren over het datalek, hangt af van het risico dat zij lopen door het datalek. In dit geval geen grote impact verwacht, dus geen melding naar AP of informatie aan het "slachtoffer" vereist.	Niet te snel alleen op basis van voornaam selecteren.	Geen negatieve gevolgen voor gemailde persoon verwacht.
2025	12 februari 2026	Dinsdag 10 maart 2026	Nee	nvt	Nee	Cyberaanval waar Odido door getroffen is, omdat wij 2 nummers actief hebben bij Odido deze melding ontvangen!	Gewone persoonsgegevens	2	2	Arian van Balen, fg@maas.nl	Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. In dit geval dus het ongewenst verstrekken van persoonsgegevens. Of MAAS een datalek wel of niet moet melden bij de AP is afhankelijk van de mogelijke impact van het datalek op de slachtoffers. Ook de vraag of MAAS de slachtoffers moet informeren over het datalek, hangt af van het risico dat zij lopen door het datalek. In dit geval geen grote impact verwacht, dus geen melding naar AP of informatie aan het "slachtoffer" vereist.	Beveiliging versterkt – Na de ontdekking van de aanval is de onbevoegde toegang tot ons systeem direct afgesloten. Odido heeft direct extra beveiligingsmaatregelen genomen. Regelgeving & transparantie - Odido heeft het datalek gemeld bij de Autoriteit Persoonsgegevens (AP). Ondersteuning - Odidio heeft speciale informatiepagina geopend.	Geen negatieve gevolgen voor gemailde persoon verwacht.
2026	18/05/2026	18/05/2026	Nee	nvt	Nee	Het geaggregeerd rapporteren van gegevens is in principe toegestaan, bijvoorbeeld door ze voorafgaand aan de rapportage tot groepsniveau te aggregeren. Hiertoe volstaan groepen vanaf tien medewerkers, al vindt de AP groepen vanaf vijf personen soms al acceptabel. Voor kleine groepen (minder dan 5-10 personen) is er een verhoogd risico op herleidbaarheid. Vermijd daarom rapportages over groepen kleiner dan 5-10 personen. Bevinding: Er zijn 10 groepen < 10 personen uitgenodigd, daarvan 2 minder dan 5. Anonimiteit is in MTO 2025 presentatie voor een aantal kleine afdelingen daarom niet gewaarborgd.	Gewone persoonsgegevens	5 tot 61	5 tot 61	Arian van Balen, fg@maas.nl	Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. In dit geval bij de zeer kleine groepen alleen herleidbaar dat de meeste personen deelgenomen hebben. In dit geval daarmee geen grote impact verwacht, dus geen melding naar AP of informatie aan slachtoffers vereist.	Bij het invullen van het MTO konden medewerkers zelf aangeven onder welke afdeling zij zichzelf plaatsten ('overige' of een willekeurige andere afdeling was ook mogelijk). Hierdoor is dit niet rechtstreeks herleidbaar naar individuele medewerkers. Daarnaast zijn de resultaten van de individuele groepen niet bekeken, de kleinst bekeken groep is 'staf' in totaliteit. Kortom: niet herleidbaar op individueel niveau.	Geen negatieve gevolgen voor repondenten verwacht.