Odido bewaart klantgegevens langer dan afgesproken, blijkt na datalek

Anouk Gras

In het kort

- Ook oud-klanten van telecombedrijf Odido zijn betrokken bij het datalek, sommigen zijn al tien jaar weg.
- Experts wijzen op een gebrek aan adequaat beheer van klantdata en mogelijke AVG-schending.
- Elke organisatie wordt geacht zich aan de eigen privacyverklaringen te houden, zegt waakhond AP.

Odido bewaart oude klantgegevens langer dan afgesproken volgens eigen privacyregels, blijkt na datalek. Foto: Robin Utrecht/ANP

Telecombedrijf Odido bewaart de persoonsgegevens van overgestapte klanten langer dan het zelf toezegt. De mobiele provider stelt in zijn privacystatement gegevens tot maximaal twee jaar na het einde van een contract te bewaren. Toch kregen oud-klanten die al vijf of tien jaar geleden overstapten een mail met het bericht dat hun gegevens zijn buitgemaakt bij de grote cyberaanval van afgelopen week.

Odido maakte het datalek donderdag bekend, nadat de aanvallers in het weekend van 7 en 8 februari hadden toegeslagen. De criminelen kregen toegang tot 6,2 miljoen klantaccounts en konden onder meer bij namen, rekeningnummers en adressen. Het is een van de grootste datalekken ooit in Nederland. Het bedrijf zei dat er geen wachtwoorden, belgegevens of factuurgegevens zijn gelekt.

Odido liet maandag weten meer tijd nodig te hebben om na te gaan hoe het komt dat gegevens langer dan twee jaar worden bewaard. Ook kon het bedrijf nog niet aangeven om hoeveel klanten het gaat.

‘Datamanagement niet op orde’

‘Als data die al verwijderd hadden moeten zijn nog bij Odido liggen, gaat dat verder dan alleen het datalek’, zegt advocaat IT-recht Jop Fellinger. ‘Zo’n lek kan gebeuren en is verschrikkelijk, maar hier is achterliggend ook nog iets aan de hand: dat je als bedrijf je

eigen datamanagement niet op orde hebt. Dat klinkt niet goed en is niet AVG-compliant.' Fellinger doelt op de Europese privacywet Algemene verordening gegevensbescherming.

De AVG schrijft voor dat je gegevens kunt bewaren voor zolang dat noodzakelijk is, legt privacyadvocaat Daniëlle Molenkamp uit. 'Odido acht het noodzakelijk voor een periode van twee jaar, daarna zouden de gegevens verwijderd moeten worden. Het ziet ernaar uit dat dat niet is gebeurd, dat er geen deugdelijk proces is ingericht waarbinnen het bedrijf de bewaartermijnen ook echt handhaaft.'

De privacywaakhond Autoriteit Persoonsgegevens (AP) houdt de zaak in de gaten, zegt een woordvoerder. Elke organisatie wordt geacht zich aan de eigen privacyverklaringen te houden.

De Odido-casus staat niet op zich, zegt Molenkamp. 'We zien vaker dat er geen goed proces voor bewaartermijnen is ingericht, dus dit verbaast me niet.' Hoe lang gegevens bewaard mogen worden, verschilt per soort persoonsgegeven en per doel. Zo geldt voor factuurgegevens een termijn van zeven jaar na de beëindiging van het contract. Dat is een wettelijke verplichting.

Verzoeken van toezichthouders

Telecomproviders hebben er wel last van dat ze af en toe dwingende verzoeken krijgen van toezichthouders of het Openbaar Ministerie, zegt IT-advocaat Fellinger. Het kan zijn dat data op basis van een bevel van een autoriteit bewaakt moest worden. 'Die slag om de arm wil ik nog wel houden, maar zelfs in dat geval moet je je op een gegeven moment afvragen: kunnen we dit doen of moeten we ophouden omdat het in strijd is met de eigen privacyregels en AVG?'

Hij wijst daarbij op de zogeheten 'dataminimalisatie' van de privacywet. De default optie is dat er altijd het minimale aan gegevens bewaard moet worden. 'Het hangt van de aard van de gelekte gegevens af of het nodig was om te bewaren of niet.'

Volgens Odido kregen de aanvallers vorige week toegang tot Iban-nummers, geboortedata en identificatiegegevens, zoals de geldigheidsdatum van paspoort of rijbewijs. Klanten en oud-klanten krijgen verschillende e-mails over hoeveel en welke gegevens zijn buitgemaakt.

'Geen grote schoonmaak'

Het datalek van afgelopen week betreft data van klanten van Odido en Ben. T-Mobile Nederland en Tele2 Mobiel gingen in 2023 samen verder onder de naam Odido. Ben en Simpel horen daar ook bij, maar die namen bleven bestaan. 'Wat ik vooral opmerkelijk vind', zegt advocaat Molenkamp, 'is dat er geen grote schoonmaak heeft plaatsgevonden toen T-Mobile samenging in Odido. Ze hadden moeten zien wat ze overdroegen, dus die gegevens hadden allang verwijderd moeten worden.'

Molenkamp merkt op dat de onduidelijkheid rond zo'n lek mensen snel bang maakt. Ze ziet dat gezamenlijke acties vanuit consumenten worden opgezet om een bedrijf aansprakelijk te stellen en schade vergoed te krijgen. 'Maar de vraag blijft: is er daadwerkelijk schade? Als er in strijd met de AVG is gehandeld, betekent dat niet vanzelfsprekend dat er daardoor schade is ontstaan die voor vergoeding in aanmerking komt.'

De advocaat denkt wel dat het goed is dat bedrijven zich er met dit soort initiatieven bewust van blijven dat de AVG moet worden gehandhaafd en welke risico's kunnen ontstaan als daar niet aan wordt voldaan. 'De AVG is nu al bijna acht jaar van kracht, maar het blijkt moeilijk voor bedrijven om gegevens adequaat te blijven beschermen. En er zijn steeds meer technologische mogelijkheden voor criminelen om systemen binnen te treden, waardoor steeds scherpere maatregelen getroffen moeten worden.'