

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2367

Vragen van het lid **Van der Lee** (GroenLinks-PvdA) aan de Minister van Financiën over *rekeninggluren* (ingezonden 28 juni 2024).

Antwoord van Minister **Heinen** (Financiën) (ontvangen 29 augustus 2024)

Vraag 1

Bent u bekend met het NRC-artikel «Bunq-werknemers keken stiekem in klantrekeningen: «Het was te verleidelijk»»¹?

Antwoord 1

Ja, daar ben ik mee bekend.

Vraag 2

Deelt u de opvatting dat het bekijken van gegevens van klanten van banken, zonder daar toestemming of een gegronde reden voor te hebben, een schending van de privacy is?

Antwoord 2

Bankgegevens bevatten veel persoonlijke informatie van klanten. Daar moeten banken zeer zorgvuldig mee omgaan. Gegevens van klanten zouden niet ongehinderd door iedere bankmedewerker moeten kunnen worden ingezien zonder goede reden. Ik ga er dan ook vanuit dat Bunq dit tot de bodem uitzoekt en indien nodig actie onderneemt.

Vraag 3, 4, 5 en 6

Herkent u het beeld dat Bunq-bank verzaakt?

Herkent u het beeld dat rekeninggluren bij Bunq-bank wijdverspreid is, dat privacyschendingen geen prioriteit hebben en waarschuwingen hierover zijn genegeerd door de top?

Wat vindt u ervan dat de situatie al sinds 2022 bekend is bij de bank en dat de situatie nog steeds bestaat? Wat vindt u ervan dat het monitoren van de inzage van gegevens gewoon mogelijk was, maar dat dit niet is gebeurd?

Deelt u de opvatting dat Bunq-bank zelf ook een verantwoordelijkheid heeft, in plaats van deze te leggen bij de individuele medewerkers?

¹ NRC.nl, 26 juni 2024, «Bunq-werknemers keken stiekem in klantrekeningen: «Het was te verleidelijk»» (<https://www.nrc.nl/nieuws/2024/06/26/bunq-werknemers-keken-stiekem-in-klantrekeningen-het-was-te-verleidelijk-a4857800>).

Antwoord 3, 4, 5 en 6

Ik kan niet ingaan op de exacte omstandigheden van individuele gevallen. Het is aan de onafhankelijke toezichthouder om te beoordelen of een bank aan haar wettelijke verplichtingen voldoet, en als dat niet zo is, om daar op te handhaven. Wel kan ik in het algemeen aangeven dat zowel banken als bankiers op grond van op hen rustende wettelijke verplichtingen de verantwoordelijkheid hebben om rekeninggluren te voorkomen, dan wel na te laten. Banken zijn op grond van de privacywetgeving en het Besluit prudentiële regels Wft verplicht om, onder andere, veiligheidssystemen in te richten om dit soort privacyschendingen door werknemers te voorkomen. Deze organisatorische verplichtingen volgen uit het Besluit prudentiële regels Wft, op grond van de artikelen 3:10 en 3:17 Wet op het financieel toezicht (Wft). Betaalgegevens zijn daarnaast persoonsgegevens in de zin van artikel 4, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG) en deze persoonsgegevens worden door Bunq in het kader van hun dagelijkse bedrijfsvoering verwerkt. Bij het verwerken van persoonsgegevens dienen een aantal beginselen, zoals doelbinding en integriteit en vertrouwelijkheid, in acht te worden genomen (zie artikel 5 AVG). Een instelling dient dus passende technische of organisatorische maatregelen te nemen om de bankgegevens op een dusdanige manier te verwerken dat een passende beveiliging ervan gewaarborgd is en dat de bankgegevens voldoende beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking.

Daarnaast hebben banken vaak ook een eigen gedragscode, die voorschrijft dat medewerkers persoonlijke informatie met de grootste zorgvuldigheid en in overeenstemming met de privacywetten behandelen. Ik heb begrepen dat Bunq over een dergelijke gedragscode beschikt. Tot slot is elke bank wettelijk verplicht ervoor te zorgen dat al hun medewerkers de bankierseed of -belofte afleggen en zich onderwerpen aan tuchtrecht. Met de bankierseed of -belofte verklaren medewerkers van banken om hun werkzaamheden integer en zorgvuldig uit te oefenen, waarbij ze de belangen van de klant centraal stellen. Als er aanwijzingen zijn dat medewerkers van banken handelen tegen de eigen gedragscode of de bankierseed of -belofte, dan kan iedereen een melding doen bij de Stichting Tuchtrecht Banken (STB). Daarnaast ziet De Nederlandsche Bank (DNB) erop toe dat banken hun systemen zorgvuldig inrichten en dat banken ervoor zorgen dat al hun medewerkers de bankierseed of -belofte afleggen en zich onderwerpen aan tuchtrecht. Indien nodig kan DNB maatregelen treffen.

Bunq heeft in gesprekken met mijn ministerie aangegeven dit probleem serieus aan te pakken. DNB staat daarnaast ook in contact met Bunq. Ook heeft de STB Bunq om opheldering gevraagd.²

Vraag 7, 8, 9 10 en 11

Wat gaat u, samen met de toezichthouders (DNB en de Autoriteit Persoonsgegevens), doen om te voorkomen dat dit nog een keer kan gebeuren?

Kunt u bij antwoord 7 de maatregelen betrekken die in het NRC-artikel worden genoemd, namelijk het hanteren van strikte interne veiligheidssystemen, het registreren van wat werknemers aan privacygevoelige klantgegevens inzien, het hanteren van het principe «zero trust and the principle of least privilege» en het toegang geven aan zo min mogelijk werknemers tot een zo klein mogelijk aantal klantgegevens?

Welke andere maatregelen zijn mogelijk en wilt u, samen met de toezichthouder, inzetten of verplicht stellen? Wat kan er bijvoorbeeld geleerd worden van andere sectoren, zoals de zorgsector, waar in het verleden een vergelijkbare situatie speelde.

Deelt u de opvatting dat er snel verbetering moet plaatsvinden?

Welke maatregelen gaat u of de toezichthouder nemen als de situatie niet verbetert? Op welk moment wordt er ingegrepen?

Antwoord 7, 8, 9 10 en 11

DNB is wettelijk verplicht tot geheimhouding over de vertrouwelijke gegevens die zij in het kader van haar toezichttaak ontvangt en verwerkt. Over specifieke instellingen kan zij daarom geen uitspraken doen. Voorts is DNB

² <https://www.tuchtrechtbanken.nl/actueel/tuchtrecht-banken-vraagt-bunq-om-opheldering-over-rekeninggluren/>

onafhankelijk, gaat zij over haar eigen handhavingsbeleid en beoordeelt zij een individuele casus onafhankelijk en zonder politieke inmenging. DNB heeft wel aangegeven dat zij in algemene zin het van groot belang vindt dat integriteits- en zorgvuldigheidsnormen worden nageleefd.

DNB hanteert een risicogebaseerde aanpak en betreft onder meer incidentmeldingen en andere signalen bij haar prioriteitstelling. Om vast te stellen of een bank voldoet aan de genoemde Wft-vereisten wordt enerzijds nagegaan of de *compliance*-functie en de *audit*-functie van de bank controleren dat de regelingen worden nageleefd. Anderzijds wordt door DNB via uitvragen en/of onderzoek ter plaatse nagegaan of de regelingen worden nageleefd. Indien DNB vaststelt dat de Wft-vereisten onvoldoende door een bank worden nageleefd, zal DNB handhavende maatregelen overwegen met inachtneming van het eigen handhavingsbeleid.

Zowel DNB als de Autoriteit Persoonsgegevens (AP) houden toezicht op het zorgvuldig omgaan met persoonsgegevens door banken en beschikken over voldoende bevoegdheden om handhavend op te treden indien zij dit constateren. Daarnaast heeft de AP in dit verband een melding ontvangen van Bunq over een mogelijk datalek.³ Het is vervolgens aan de AP om de melding te beoordelen en al dan niet een onderzoek te starten.

Zoals ik in mijn antwoord op deze vragen en mijn antwoord 4, 5 en 6 heb uiteengezet bestaat er een helder wettelijk kader om rekeninggluren te voorkomen en, in voorkomende gevallen, te handhaven dan wel sanctioneren, zowel bij de bank waar dit gebeurt als bij de individuele bankier die zich hier schuldig aan maakt. Daarnaast is er voldoende toezicht op de naleving van dit kader en beschikken de toezichthouders over een handhavingsinstrumentarium om in te grijpen indien dat nodig is. Tot slot ga ik ervanuit dat de signalen uit het NRC-artikel serieus worden genomen en de aandacht hebben van betrokken partijen. Ik heb daarom geen aanleiding te veronderstellen dat aanvullende maatregelen nodig zijn op dit vlak.

Vraag 12

Zijn er andere banken met dezelfde problematiek? Wat gaat u eraan doen om dit in kaart te brengen?

Antwoord 12

Uit de openbaar te raadplegen uitspraken van de STB blijkt dat enkele zaken per jaar over rekeninggluren aan de STB worden voorgelegd en dat in de betreffende zaken sancties worden opgelegd, zoals een beroepsverbod.⁴ Mede gelet hierop en het toezicht van DNB op de bedrijfsvoering van banken zie ik geen aanleiding voor het nader in kaart brengen hiervan.

³ NOS.nl, 27 juni 2024, «Tuchtrecht Banken wil opheldering van Bunq over gluren naar rekeningen» (<https://nos.nl/artikel/2526363-tuchtrecht-banken-wil-opheldering-van-bunq-over-gluren-naar-rekeningen>)

⁴ Te raadplegen via: <https://www.tuchtrechtbanken.nl/uitspraken-zoeken-met-zoekopdracht-«raadplegen-rekeninggegevens-zonder-zakelijke-aanleiding»>.