AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Sociale verzekeringsbank (Raad van bestuur)
t.a.v. de voorzitter
de heer drs. S.T. Sibma
Postbus 1100
1180 BH AMSTELVEEN

Datum
19 januari 2023

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot boeteoplegging

Geachte heer Sibma,

De Autoriteit Persoonsgegevens (hierna: AP) heeft besloten om aan de Sociale verzekeringsbank (hierna: SVB) een bestuurlijke boete van **€ 150.000,--** op te leggen voor overtreding van artikel 32, eerste en tweede lid, van de Algemene verordening gegevensbescherming (hierna: AVG). Dit, omdat de SVB onvoldoende passende maatregelen heeft genomen om een op het risico afgestemd beveiligingsniveau te waarborgen met betrekking tot het verwerken van persoonsgegevens in het kader van telefonisch klantcontact met AOW-verzekerden.

In dit besluit wordt de bestuurlijke boete toegelicht. Hiertoe wordt achtereenvolgens ingegaan op (1) de aanleiding en het procesverloop, (2) de vastgestelde feiten, (3) de door de SVB genomen verbetermaatregelen, (4) de overtreding en (5) de hoogte van de boete. Tot slot volgt (onder 6) het dictum.

Datum
19 januari 2023

Ons kenmerk
[VERTROUWELIJK]

1. Aanleiding en procesverloop

1 Op 1 november 2109 heeft de AP een klacht ontvangen over een beweerdelijke inbreuk in verband met persoonsgegevens bij de SVB. Klaagster gaf te kennen dat een familielid persoonlijke informatie over haar zou hebben ontvangen van een medewerker van de SVB, terwijl zij de SVB geen toestemming had gegeven voor het delen van die informatie. Op diezelfde dag heeft de SVB deze gebeurtenis als datalek gemeld bij de AP. De SVB heeft in die melding onder andere verklaard dat er onbevoegd mondeling persoonsgegevens zijn gedeeld met een onbevoegde ontvanger.

2 Bij besluit van 15 november 2019 heeft de AP aan klaagster medegedeeld geen nader onderzoek te doen naar deze gebeurtenis. Tegen dit besluit heeft klaagster bezwaar gemaakt. Naar aanleiding van het bezwaarschrift van klaagster heeft de AP besloten om (alsnog) een onderzoek te starten. Dit onderzoek richtte zich op de naleving door de SVB van artikel 5, eerste lid, aanhef en onder f, in samenhang met artikel 32 van de AVG voor de periode vanaf 25 mei 2018.

3 Dit onderzoek heeft ertoe geleid dat de Directie Klantcontact en Controlerend Onderzoek van de AP op 4 november 2021 een rapport van bevindingen heeft vastgesteld (hierna: onderzoeksrapport). In het onderzoeksrapport is geconcludeerd dat de SVB op grond van artikel 32, eerste en tweede lid, van de AVG passende technische en organisatorische maatregelen diende te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen met betrekking tot het verwerken van persoonsgegevens in het kader van telefonisch klantcontact met AOW-verzekerden en dat de beveiligingsmaatregelen onvoldoende waren afgestemd op de beveiligingsrisico's. De Directie Klantcontact en Controlerend Onderzoek van de AP is tot de conclusie gekomen dat de SVB vanaf 25 mei 2018 tot de datum van ondertekening van het onderzoeksrapport in strijd met artikel 32, eerste en tweede lid, van de AVG geen passende technische en organisatorische maatregelen had genomen.

4 Bij brief van 11 november 2021 heeft de AP aan de SVB een voornemen tot handhaving verzonden. De SVB heeft op 10 december 2021 een schriftelijke zienswijze ingediend over dit voornemen en het daaraan ten grondslag gelegde onderzoeksrapport, alsmede aanvullende informatie aan de AP verstrekt. Op 18 januari 2022 heeft een zienswijzezitting plaatsgevonden waarbij de SVB zijn schriftelijke zienswijze mondeling nader heeft toegelicht. Na de zienswijzezitting heeft de SVB op verschillende momenten nadere informatie aan de AP verstrekt.

2. Feitelijke bevindingen in het onderzoeksrapport

5 Hierna volgt een samenvatting van de in het onderzoeksrapport neergelegde feitelijke bevindingen. In zijn zienswijze heeft de SVB de bevindingen uit het onderzoeksrapport erkend.

2.1 Betrokken organisatie en taken

6 De SVB is ingesteld op grond van artikel 3, eerste lid, van de Wet structuur uitvoeringsorganisatie werk en inkomen (hierna: Wet SUWI). De SVB is een zelfstandig bestuursorgaan[1] met eigen rechtspersoonlijkheid[2].

7 De SVB is verantwoordelijk voor het uitvoeren van verschillende wetten en regelingen die verband houden met sociale zekerheid, onder andere de Algemene Ouderdomswet (hierna: AOW), de Algemene nabestaandenwet en de Algemene kinderbijslagwet.[3] De SVB draagt er zorg voor dat klanten weten waarop zij – op basis van de verschillende wetten en regelingen – recht hebben en dat zij eventuele vergoedingen ook daadwerkelijk ontvangen. Ter vervulling van deze taak verwerkt de SVB persoonsgegevens van onder andere verzekerden, pensioengerechtigden, nabestaanden en andere uitkeringsgerechtigden.[4] De SVB heeft in totaal elf vestigingen in Nederland. Het hoofdkantoor is gevestigd in Amstelveen.

8 De SVB bestaat uit verschillende directies en afdelingen. Eén van deze directies is de directie 'Dienstverlening Sociale Verzekeringen' (hierna: DSV). DSV is onder meer verantwoordelijk voor het beoordelen van aanvragen van sociale verzekeringen, waaronder de AOW. Medewerkers van DSV (hierna: "servicemedewerkers") zijn ook het (telefonische) aanspreekpunt voor klanten met vragen over sociale verzekeringen. Er werken circa 1500 servicemedewerkers bij de SVB. De servicemedewerkers werken verspreid over tien locaties binnen Nederland.

9 Er bellen gemiddeld zo'n 20.000 mensen per week naar de SVB met vragen over sociale verzekeringen.

2.2 Werking en inhoud van systemen bij het telefonisch contact tussen de SVB en klanten.

10 Een servicemedewerker gebruikt tijdens het telefonische klantcontact verschillende systemen/applicaties: het [VERTROUWELIJK]-systeem, het Document Management Systeem en het systeem [VERTROUWELIJK].

[VERTROUWELIJK] -systeem

11 Het [VERTROUWELIJK]-systeem is de belangrijkste applicatie voor de uitvoering van de sociale regelingen bij de SVB. Het [VERTROUWELIJK]-systeem is onderverdeeld in een aantal deelsystemen, waaronder cliëntenadministratie [VERTROUWELIJK]. De SVB krijgt gegevens over burgers via de Basisregistratie Personen (hierna: BRP). Vanuit de BRP komen deze gegevens in [VERTROUWELIJK] terecht. [VERTROUWELIJK]

[1] Artikel 4, eerste lid, Wet Suwi.
[2] Artikel 3, tweede lid, en artikel 4, eerste lid, Wet SUWI.
[3] Artikel 34, eerste lid, Wet SUWI.
[4] Artikel 35 Wet SUWI.

Document Management Systeem (hierna: "DMS)

12 In het DMS zijn alle persoonsgebonden documenten opgenomen, zoals alle verstuurde en ontvangen brieven, telefoonnotities en interne notities (waaronder rapporten van telefoongesprekken). Het DMS is gekoppeld aan het [VERTROUWELIJK]-systeem.

[VERTROUWELIJK]

13 De [VERTROUWELIJK] is de applicatie die sinds 2016 door servicemedewerkers wordt gebruikt om onder andere de dossiers van AOW-klanten[5] op te zoeken tijdens telefonisch klantcontact. [VERTROUWELIJK] is de front-end oftewel de gebruikersomgeving van het [VERTROUWELIJK]-systeem.

14 In onderstaande afbeelding is het [VERTROUWELIJK]-scherm afgebeeld waarin servicemedewerkers in de gebruikersomgeving de dossiers van AOW-klanten kunnen opzoeken. In het blauwe kader is zichtbaar welke zoekcombinaties servicemedewerkers kunnen gebruiken om klanten op te zoeken in [VERTROUWELIJK].

[VERTROUWELIJK]

15 Hierna wordt, gezien de overlap, het onderscheid tussen het [VERTROUWELIJK]-systeem en de gebruikersomgeving [VERTROUWELIJK] losgelaten en wordt voor beide systemen de term [VERTROUWELIJK] gebruikt.

2.3 Autorisaties in [VERTROUWELIJK]

16 Autorisatie is het proces waarin een persoon bepaalde rechten krijgt binnen een systeem.[6] Hoe meer personen toegang hebben tot gegevens, hoe groter het risico op datamisbruik. Een systeem waar veel personen bepaalde toegangsrechten hebben tot veel gegevens brengt dus (veel) beveiligingsrisico's met zich.

17 In het onderzoeksrapport is geconstateerd dat alle 1500 servicemedewerkers van de SVB zijn geautoriseerd om alle dossiers van [VERTROUWELIJK] AOW-klanten te raadplegen [VERTROUWELIJK].

[5] In de wet- en regelgeving wordt niet gesproken over klanten, maar over verzekerden, omdat de AOW een sociale verzekering is. Binnen de SVB wordt echter gesproken over AOW-klanten. In dit besluit wordt daarom ook de term 'AOW-klanten' gebruikt.
[6] Denk hierbij aan toegangsrechten, leesrechten en mutatierechten.

2.4 (Persoons)gegevens raadplegen, delen en wijzigen

18 In [VERTROUWELIJK] staat een verscheidenheid aan (persoons)gegevens opgeslagen. Het gaat onder andere om NAW-gegevens, mailadres, gegevens over nationaliteit, verblijfstitel, leefsituatie, burgerlijke staat, hoogte van de uitkering, werkgeversgegevens zoals loonheffingennummer, inkomen, rekeninggegevens, BSN en studies van klanten. Ook is gebleken dat indien een servicemedewerker toegang heeft tot het [VERTROUWELIJK]-systeem (en dus [VERTROUWELIJK]) en het DMS, deze ook toegang heeft tot strafrechtelijke gegevens in deze systemen, te weten: gegevens van klanten over een veroordeling tot detentie en de start- en einddatum daarvan, gegevens over (een vermoeden van) sociale verzekeringsfraude en gegevens over de status als uitreiziger. Aangezien alle 1500 servicemedewerkers toegang hebben tot deze systemen, hebben zij dus toegang tot al deze persoonsgegevens.

19 Uit het voorgaande blijkt dat servicemedewerkers tijdens het telefonisch contact met AOW-klanten het gehele dossier van deze klanten kunnen raadplegen in [VERTROUWELIJK].

20 De SVB had verschillende werkinstructies die in een online omgeving [VERTROUWELIJK] beschikbaar waren voor servicemedewerkers.

21 Uit het onderzoeksrapport en de daaraan ten grondslag liggende stukken volgt dat het vastgesteld beleid voorschreef dat indien servicemedewerkers op juiste wijze de identiteit van (een gemachtigde van) een klant hadden vastgesteld, zij alle klant- en rechtsgegevens[7] mochten verstrekken en wijzigen, met uitzondering van gegevens waarvoor een schriftelijke vorm is vereist. Verder blijkt uit [VERTROUWELIJK] dat het BSN nooit telefonisch aan (gemachtigden van) klanten wordt verstrekt. Ook stond in [VERTROUWELIJK] dat servicemedewerkers adresgegevens, bankgegevens en bedragen enkel telefonisch mochten delen na het stellen van controlevragen.

2.5 Authenticatie

22 Authenticatie is het proces waarbij de vermeende identiteit van een persoon wordt geverifieerd. Een goede authenticatieprocedure kan bijdragen aan een passend beveiligingsbeleid omdat het helpt ongeoorloofde toegang en –verstrekking van gegevens te voorkomen.

<u>Beleid over vaststelling identiteit klanten aan de telefoon</u>

23 In het onderzoeksrapport is vastgesteld dat de SVB twee werkinstructies in [VERTROUWELIJK] had staan waarin werd weergegeven hoe servicemedewerkers de identiteit van (AOW-)klanten tijdens het telefonisch contact dienden te controleren.[8]

[7] Dit zijn gegevens van klanten met betrekking tot hun recht op uitkering van volksverzekeringen, zoals de AOW, die de SVB uitvoert.
[8] [VERTROUWELIJK]

24 In het onderzoeksrapport is geconcludeerd dat deze werkinstructies inhoudelijk van elkaar verschillen met betrekking tot de werkwijze voor het vaststellen van de identiteit van de klant aan de telefoon, en dat dit zorgt voor onduidelijkheid bij de servicemedewerkers. Ook is in het onderzoeksrapport geconcludeerd dat veel van de voorgeschreven controlevragen in deze werkinstructies betrekking hadden op relatief eenvoudig te achterhalen informatie. In een van de werkinstructies werden servicemedewerkers zelfs ontmoedigd om naar heel specifieke informatie te vragen, zoals de datum van de laatste betaling of het nettobedrag van de uitkering. Daarnaast is in het onderzoeksrapport geconstateerd dat uit het voorgeschreven beleid niet duidelijk was op te maken welke specifieke controlevragen in ieder geval moeten worden gesteld of hoeveel verschillende controlevragen er minimaal moeten worden gesteld. In één van de documenten in [VERTROUWELIJK] werd bepaald dat in ieder geval naar het SVB-registratienummer [VERTROUWELIJK] of BSN moet worden gevraagd, terwijl dat in het andere document niet werd voorgeschreven. In dat document werd echter niet ingegaan op de situatie waarin de beller deze gegevens niet wil of kan verstrekken. Ook bood het beleid geen duidelijkheid over de vraag wat te doen in geval nog twijfel bestaat over de identiteit en welke (aanvullende) controlevragen vervolgens gesteld moesten worden.

Controle beleid door de SVB

25 Voor wat betreft de controle op de naleving van het authenticatiebeleid is in het onderzoeksrapport geconstateerd dat de SVB geen toereikende manier had om te waarborgen dat servicemedewerkers in overeenstemming met het beleid de identiteit van klanten aan de telefoon controleerden. Zo werd door middel van door servicemedewerkers opgestelde telefoonnotities via een collegiale toets c.q. steekproef gecontroleerd of de identiteit van klanten werd vastgesteld in overeenstemming met het beleid. In geen van de aan de AP overgelegde telefoonnotities was echter informatie opgenomen over de vraag hoe de identiteit van de beller in het telefoongesprek was vastgesteld. Ook waren er geen vaste formats voor het opstellen van deze notities. De SVB heeft tijdens het onderzoek voorts verklaard dat indien de identiteit van de beller op onjuiste wijze is vastgesteld de klant waarschijnlijk een klacht zal indienen bij de SVB en het aannemelijk is dat deze klacht wordt besproken in door de SVB ingerichte leercirkels. Ook heeft de SVB tijdens het onderzoek verklaard bezig te zijn met een Europese aanbesteding waarmee de SVB-organisatie (dus ook op het vlak van de uitvoering van de AOW) zou worden voorzien van onder andere het automatisch vastleggen van telefoongesprekken in tekst en het opnemen van die gesprekken, teneinde de telefonische authenticatie te optimaliseren.

Naleving beleid in de praktijk

26 In het onderzoekrapport wordt geconcludeerd dat het enerzijds ontbreken van eenduidig, helder beleid en het anderzijds ontbreken van een geschikte manier voor de controle op de naleving van dit beleid ertoe heeft geleid dat servicemedewerkers de voorgeschreven instructies in de praktijk niet (in alle gevallen) volgden. Servicemedewerkers verklaarden aan medewerkers van de AP verschillend over welke controlevragen ze wanneer stellen tijdens het telefonisch klantcontact. Ook blijkt uit de verklaringen van servicemedewerkers dat ze de voorgeschreven (van elkaar verschillende) werkwijzen in

[VERTROUWELIJK] niet precies volgden, bijvoorbeeld als het aankomt op de vraag hoe om te gaan met klanten die het SVB-registratienummer of BSN niet konden verstrekken. De wijze waarop de identiteit van de bellende AOW-klanten werd gecontroleerd, werd derhalve kennelijk voor een belangrijk deel overgelaten aan de eigen beoordeling en inzichten van de servicemedewerker, zo is een van de conclusies in het onderzoeksrapport.

2.6 Op het risico afgestemd beleid

Totstandkoming en evaluatie beleid

27 Op de vraag van de Directie Klantcontact en Controlerend Onderzoek van de AP hoe het beleid met betrekking tot controlevragen tot stand is gekomen en in hoeverre dit een op het (beveiligings)risico afgestemd beleid is, heeft de SVB twee notities uit 2006 en 2007 overgelegd, waarin dit beleid behandeld wordt en waarvan de SVB op dat moment vond dat daarin een risicoafweging wordt gemaakt.

28 In het onderzoeksrapport wordt geconcludeerd dat de SVB in 2006 het risico heeft gesignaleerd dat een persoon telefonisch verzoekt tot wijziging van een betaaladres, terwijl deze persoon niet de klant is. De SVB heeft toen besloten om over te gaan tot het stellen van checkvragen. Op een later moment, in 2007, is een interne SVB-notitie opgesteld, waarin is benadrukt dat het stellen van checkvragen een minder sterke vorm van authenticatie is dan een constructie waarbij het authenticatiemiddel onder controle staat van de klant. In die notitie wordt ook gewaarschuwd dat bij het stellen van checkvragen enige zorg op zijn plaats is; ten behoeve van authenticatie kan volgens die notitie geen gebruik worden gemaakt van de identiteitsgegevens en ook niet van gegevens die door een derde eenvoudig te achterhalen zijn, zoals naam, adres, postcode en telefoonnummer. Vervolgens wordt in het onderzoeksrapport geconcludeerd dat het beleid sinds 2006 niet meer was gewijzigd en dat er tussentijds geen evaluaties hadden plaatsgevonden.

2.7 Bewustwording

29 Net als authenticatie is bewustwording een beveiligingsmaatregel die door de SVB is ingezet om persoonsgegevens te beschermen tijdens het telefonisch klantcontact. Bewustwording kan ervoor zorgen dat medewerkers zich meer bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en handelen met inachtneming van hun verantwoordelijkheden.

30 In het onderzoeksrapport wordt geconstateerd dat de SVB zijn medewerkers op verschillende manieren bewust probeert te maken van de regels en risico's van het werken met persoonsgegevens, waarvan de meeste bewustwordingsmethodes een vrijblijvend karakter hebben. Zo waren er werkinstructies te vinden in [VERTROUWELIJK], al wisten de meeste medewerkers met wie de AP-onderzoekers hebben gesproken niet precies welke werkinstructies er over welke processen in [VERTROUWELIJK] staan. Verder zijn op het intranet van de SVB verschillende pagina's gewijd aan informatiebeveiliging. Ook heeft de SVB een gedragscode met daarin een onderdeel over informatiebeveiliging, die door medewerkers bij

indiensttreding wordt ondertekend. Bij overtreding van de gedragscode kunnen disciplinaire maatregelen worden getroffen. Ook worden medewerkers aangesproken die bij een datalek betrokken zijn. Voorts is in het onderzoeksrapport geconstateerd dat de SVB enkele opleidingen aanbiedt waar de regels en risico's van het werken met (persoons)gegevens behandeld worden. In deze opleidingen komen ook de regels over het telefonisch klantcontact aan bod. Hoewel deze opleidingen eenmalig verplicht waren voor zittende en nieuwe medewerkers, werden ze niet regelmatig herhaald.

3. Maatregelen SVB na vaststelling van het onderzoeksrapport

31 In zijn zienswijze heeft de SVB, zoals hiervoor is opgemerkt, de bevindingen van de AP in het onderzoeksrapport erkend. D SVB benadrukt dat privacybescherming voor hem van groot belang is. De afgelopen jaren heeft de SVB stevig geïnvesteerd in het neerzetten van een goede privacy-organisatie en -cultuur. De SVB acht zichzelf een risicomijdende organisatie en zet in dat kader in op strenge beveiliging van de gegevens van zijn klanten. Zo heeft de SVB zich in 2021 geconcentreerd op digitale weerbaarheid en het voorkomen van cybercriminaliteit vanwege zich voortdurend ontwikkelende cyberrisico's. De SVB heeft zich daarbij vooral gericht op het voorkomen van aanvallen waarin op grote schaal persoonsgegevens kunnen worden onttrokken.

32 De SVB onderkent dat het onderzoeksrapport inderdaad constateert dat de bescherming van persoonsgegevens van burgers niet voldoende was gewaarborgd bij de telefonische dienstverlening. In zijn zienswijze heeft de SVB verklaard in het onderzoeksrapport de noodzaak en de kans te zien om de telefonische dienstverlening naar zijn klanten aanzienlijk te verbeteren.

33 Onmiddellijk nadat de AP het onderzoeksrapport naar de SVB had verzonden, op 4 november 2021, is de SVB gestart met het uitvoeren van een risico-inventarisatie en het opstellen van een plan van aanpak. Al op 9 december 2021 – vijf weken na de vaststelling van het onderzoeksrapport – heeft de SVB een uitgebreide, specifiek op de telefonische dienstverlening gerichte risico-inventarisatie aan de AP overgelegd. In die risico-inventarisatie is ook neergelegd welke (aanvullende) maatregelen getroffen kunnen worden. De SVB heeft de risico-inventarisatie overigens niet beperkt tot AOW, maar uitgebreid naar alle onder de SVB ressorterende sociale zekerheidswetten.

34 Eveneens op 9 december 2021 heeft de SVB een door hem vastgestelde plan van aanpak aan de AP verstrekt. In dat plan is een pakket van door te voeren verbetermaatregelen vastgelegd om tegemoet te komen aan de in het AP-onderzoeksrapport neergelegde bevindingen. Dit pakket is gericht op, samengevat, het aanscherpen van de instructies, de controle op de naleving van de instructies en verbetering van bewustwording bij zijn medewerkers.

35 De SVB heeft vervolgens – conform het plan van aanpak – al in de eerste helft van 2022 de volgende verbetermaatregelen daadwerkelijk en concreet doorgevoerd.

* Aanpassing/herijking van de werkinstructies

Op 31 mei 2022 heeft de SVB herijkte werkinstructies aan de AP verstrekt. Deze werkinstructies zijn eind juni 2022 operationeel geworden en toen ook in [VERTROUWELIJK] geplaatst en worden 2-jaarlijks geëvalueerd. Onder ander de volgende onderwerpen zijn verwerkt in de werkinstructie:
- met welke controlevragen de servicemedewerker moet starten;
- welke aanvullende controlevragen de servicemedewerker moet stellen. De servicemedewerker moet gegeven de specifieke situatie beoordelen welke controlevragen passend zijn (maatwerk), maar de werkinstructie heeft geen vrijblijvend karakter. Zo is bijvoorbeeld voorgeschreven welke vragen de servicemedewerker in ieder geval moeten stellen en hoeveel controlevragen hij (minimaal) moet stellen.
- wanneer de servicemedewerker aanleiding heeft om te twijfelen aan de identiteit van de beller;
- wat de servicemedewerker moet doen als de twijfel niet wordt weggenomen;
- dat de servicemedewerker moet vastleggen op welke wijze de identiteit is gecontroleerd en welke controlevragen zijn gesteld;
- welke persoonsgegevens door de servicemedewerker niet via de telefoon mogen worden verstrekt.[9]

Bovendien heeft de SVB besloten de werkinstructies voor het gehele terrein van onder hem ressorterende sociale zekerheidswetten te herijken, dus niet alleen voor de AOW (scope onderzoek AP).
Ook zullen de werkinstructies periodiek (2 jaarlijks) worden geëvalueerd.

* Gestructureerd vastleggen controlevragen (systeemondersteuning)

Zoals in paragraaf 2.5 is opgemerkt heeft de SVB al tijdens het lopende AP-onderzoek verklaard bezig te zijn met een Europese aanbesteding waarmee de gehele SVB (en dus ook met betrekking tot de uitvoering van de AOW) zou worden voorzien van onder andere het automatisch vastleggen van telefoongesprekken in tekst en het opnemen van die gesprekken, teneinde de telefonische authenticatie te optimaliseren. Het is de bedoeling dat het terugluisteren van de door servicemedewerkers gestelde controlevragen een doorlopend karakter krijgt en dat deze worden geanalyseerd; de zogeheten feedbackloop.
In mei 2022 heeft de SVB, ter bevordering van de bewustwording en om controle op de naleving van de werkinstructie mogelijk te maken, een invulveld in het (naar de AP aanneemt: [VERTROUWELIJK]) systeem geïncorporeerd. Hierin moeten servicemedewerkers – als input voor hun telefoonnotitie – de gestelde controlevragen ter vaststelling van de identiteit van de beller invullen.

* Periodieke inzet van mystery callers (bewustwording, toetsing en borging)

Vanaf het tweede kwartaal van 2022 maakt de SVB gebruik van zogeheten mystery callers. Deze mystery callers bellen in opdracht van de SVB met een servicemedewerker en koppelen aan de SVB terug op welke wijze de servicemedewerker de identiteit heeft gecontroleerd. De SVB evalueert het gesprek met de

[9] Daarbij moet worden gedacht aan BSN, strafrechtelijke gegevens en bijzondere persoonsgegevens (gezondheid, nationaliteit, etniciteit).

servicemedewerker en deelt de leerpunten (in algemene zin) met andere medewerkers. Dit is een vast onderdeel geworden van de leercurve van de servicemedewerkers.

* Doorlopende campagne (bewustwording)
Om de bewustwording te vergroten heeft de SVB de bevindingen van de AP onder de aandacht gebracht van zijn servicemedewerkers. Daarnaast heeft de SVB in zijn plan van aanpak opgenomen voortdurend aandacht te besteden aan privacybescherming tijdens telefonisch klantcontact, bijvoorbeeld via het SVB-intranet, in interne nieuwsbrieven en organisatiebrede bijeenkomsten.

* Aanpassing van de telefoontraining (vakmanschap)
Vanaf het eerste kwartaal van 2022 heeft de SVB zijn bestaande telefoontraining aangepast. De bewustwording wordt vergroot op het gebied van identificatie en authenticatie van de beller en het delen van informatie via de telefoon. Deze aanpassing komt in alle telefonietrainingen terug en wordt gefaseerd aangeboden aan zowel nieuwe als ervaren servicemedewerkers. De SVB monitort de (verplichte) deelname en naleving van de trainingen en organiseert daarnaast - ter voorkoming van kennisvervaging - opfriscursussen.

4. Beoordeling

4.1 Reikwijdte AVG

36 Ingevolge artikel 2, eerste lid, van de AVG is deze verordening van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

37 Ingevolge artikel 3, eerste lid, van de AVG is deze verordening van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

4.2 Verwerking van (strafrechtelijke) persoonsgegevens en verwerkingsverantwoordelijkheid

4.2.1 Juridisch kader

38 Op grond van artikel 4, aanhef en onder 1, van de AVG wordt onder persoonsgegeven verstaan alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als een identificeerbaar natuurlijk persoon moet worden beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd.

39 Onder de AVG gelden meer waarborgen voor het verwerken van strafrechtelijke gegevens, omdat deze gegevens betrekking hebben op gedragingen die aanleiding geven tot maatschappelijke afkeuring, zodat

het feit dat toegang wordt verleend tot dergelijke gegevens de betrokkene kan stigmatiseren en aldus op ernstige wijze inbreuk kan maken op zijn privé-of beroepsleven.[10] Artikel 10 van de AVG omschrijft strafrechtelijke gegevens als persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

40 Artikel 4, aanhef en onder 2, van de AVG bepaalt dat onder het verwerken van persoonsgegevens wordt verstaan een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

41 In overweging 15 van de AVG is vermeld dat om te voorkomen dat een ernstig risico op omzeiling zou ontstaan, de bescherming van natuurlijke personen technologieneutraal dient te zijn en niet afhankelijk mag zijn van de gebruikte technologieën. De bescherming van natuurlijke personen dient te gelden bij zowel geautomatiseerde verwerking van persoonsgegevens als handmatige verwerking daarvan indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand.

42 Artikel 4, aanhef en onder 7, van de AVG bepaalt dat onder verwerkingsverantwoordelijke wordt verstaan een natuurlijke persoon of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze worden aangewezen.

43 Artikel 35, eerste lid, van de Wet SUWI bepaalt dat de SVB de verwerkingsverantwoordelijke is voor de verwerking van gegevens over verzekerden en uitkeringsgerechtigden in de zin van de volksverzekeringen en over bij de verzekerden behorende personen in de verzekerdenadministratie.

4.2.2 Beoordeling

Persoonsgegevens

44 In paragrafen 2.2 en 2.4 van dit besluit is uiteengezet dat de SVB in [VERTROUWELIJK] van [VERTROUWELIJK] AOW-klanten, verschillende categorieën persoonsgegevens heeft opgeslagen, zoals NAW-gegevens, werkgeversgegevens, BSN, geboortedatum of burgerlijke staat. Ook zijn in [VERTROUWELIJK] en DMS in voorkomende gevallen gegevens van klanten opgeslagen over een veroordeling tot detentie en over de start- en einddatum daarvan, gegevens over (een vermoeden van) sociale verzekeringsfraude en gegevens over de status als uitreiziger.

45 De gegevens met betrekking tot detentie kwalificeren als gegevens betreffende strafrechtelijke veroordelingen, aangezien detentie het gevolg is van een strafrechtelijke veroordeling of een gegronde

[10] HvJEU 22 juni 2021,C-439/19, ECLI:EU:C:2021:504 (*Latvijas Republikas Saeima (Point de pénalité)*), r.o. 75.

verdenking van een strafbaar feit. Gegevens over uitreizigers en sociale verzekeringsfraude kunnen eveneens kwalificeren als gegevens betreffende strafbare feiten, aangezien het gegevens betreft over gegronde verdenkingen van strafbare feiten, respectievelijk sociale verzekeringsfraude[11] en de deelneming aan een terroristische organisatie[12].

46 De AP concludeert op grond van het voorgaande dat in [VERTROUWELIJK] en DMS zowel reguliere persoonsgegevens zijn opgeslagen als persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 4, aanhef en onder 1, van de AVG en artikel 10 van de AVG.

Verwerking

47 Hiervoor heeft de AP geconcludeerd dat de SVB in [VERTROUWELIJK] en DMS verschillende categorieën persoonsgegevens van AOW-klanten heeft opgeslagen. De persoonsgegevens die in [VERTROUWELIJK] zijn opgeslagen, worden door de SVB veelvuldig gebruikt, geraadpleegd, bijgewerkt, gewijzigd of ter beschikking gesteld in het kader van het telefonisch contact dat servicemedewerkers hebben met AOW-klanten en derden. De AP concludeert daarom dat sprake is van verwerking van persoonsgegevens in de zin van artikel 4, aanhef en onder 2, van de AVG.

Verwerkingsverantwoordelijke

48 Zoals volgt uit randnummer 43 van dit besluit, is de SVB verwerkingsverantwoordelijke bij de verwerking van persoonsgegevens bij de uitvoering van volksverzekeringen. De AOW is een van die volksverzekeringen, zodat de AP concludeert dat de SVB kwalificeert als verwerkingsverantwoordelijke voor het verwerken van persoonsgegevens in het kader van de AOW.

4.3 Beveiligingsverplichting

4.3.1 Juridisch kader

49 Artikel 32, eerste lid, van de AVG luidt, voor zover hier relevant: “Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen (…).”

50 Artikel 32, tweede lid, van de AVG luidt: “Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico’s, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.”

[11] Zie artikel 84 van de Wet SUWI.
[12] Zie o.a. artikel 140a van het Wetboek van Strafrecht.

51 Bij het bepalen van passende maatregelen dient rekening te worden gehouden met het risico voor de rechten en vrijheden van personen. In overweging 15 van de AVG is vermeld dat het qua waarschijnlijkheid en ernst uiteindelijke risico voor de rechten en vrijheden van natuurlijke personen kan voortvloeien uit persoonsgegevensverwerking die kan resulteren in ernstige lichamelijke, materiële of immateriële schade, met name:
"- waar de verwerking kan leiden tot discriminatie, identiteitsdiefstal of –fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde gegevens, ongeoorloofde ongedaanmaking van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel;
- wanneer de betrokkene hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;
- (…) bij de verwerking van (…) strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
- (…);
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heef voor een groot aantal betrokkenen."

52 Ten aanzien van het bepalen van passende maatregelen is in overweging 83 van de AVG vermeld dat die maatregelen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid dienen te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Bij de beoordeling van de gegevensbeveiligingsrisico's dient aandacht te worden besteed aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden.

53 Artikel 41, eerste lid, van de Kaderwet zelfstandige bestuursorganen bepaalt dat een zelfstandig bestuursorgaan op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorgdraagt voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van gegevens.

54 Voorschriften voor de nodige technische en organisatorische voorzieningen ter beveiliging van gegevens binnen de overheid zijn neergelegd in de Baseline Informatiebeveiliging Overheid (hierna: BIO). De Directie Klantcontact en Controlerend Onderzoek van de AP heeft de volgende bepalingen uit de BIO betrokken bij haar onderzoek:
- Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen (BIO-norm 7.2);
- De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie

(BIO-norm 7.2.1); en
- Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie (BIO-norm 7.2.2).

4.3.2 Beoordeling risico-inventarisatie

55 Naar het oordeel van de AP beschikte de SVB ten tijde van de ondertekening van het onderzoeksrapport, 4 november 2011, niet over een toereikende risico-inventarisatie. Voor zover al sprake was van een risico-inventarisatie, was deze gedateerd en onvolledig.

56 Tijdens het onderzoek van de AP heeft de SVB desgevraagd twee notities uit 2006 en 2007 aan de AP overgelegd, waarin dit beleid wordt behandeld en waarvan de SVB vond dat daarin een risicoafweging wordt gemaakt.[13]

57 Deze twee notities kunnen echter niet worden aangemerkt als (deugdelijke) risico-inventarisatie. Deze notities waren ten tijde van de ondertekening van het onderzoeksrapport 14 jaar oud en derhalve zeer gedateerd. Voorts stelt de AP vast dat – kennelijk – tussentijds geen herbeoordeling van de risico's heeft plaatsgevonden.

58 Ook inhoudelijk kunnen deze twee notities naar het oordeel van de AP niet worden aangemerkt als risico-inventarisatie waarbij de specifieke risico's worden geïdentificeerd en beoordeeld op basis van de waarschijnlijkheid van optreden daarvan en de ernst van de nadelige gevolgen voor de betrokken personen. In beide notities wordt het risico aangekaart dat iemand naar de SVB belt die zich ten onrechte voordoet als klant, maar daarbij wordt niet ingegaan op (de ernst van) de nadelige gevolgen voor de klant of op de waarschijnlijkheid dat dit risico optreedt. In de notities worden bovendien niet alle risico's genoemd. Zo wordt geen aandacht besteed aan het feit dat alle 1500 servicemedewerkers toegang hebben tot alle persoonsgegevens van [VERTROUWELIJK] AOW-klanten, waaronder BSN, financiële en strafrechtelijke gegevens, en de risico's die dergelijke grootschalige toegang met zich brengt.

4.3.3 Beoordeling risico

59 De AP is van oordeel dat de risico's voor de rechten en vrijheden van natuurlijke personen die gepaard gaan met de telefonische dienstverlening, mede gelet op de omvang van de verwerking, de aard van de verwerkte gegevens, het grote aantal geautoriseerde medewerkers en de frequentie waarmee klanten telefonisch contact opnemen met de SVB, als hoog moeten worden aangemerkt.

60 Vast staat dat er van een zeer grote groep betrokkenen, namelijk [VERTROUWELIJK] AOW-klanten, persoonsgegevens zijn opgeslagen in de systemen van de SVB. Vastgesteld is dat de SVB beschikt over een breed scala aan persoonsgegevens van deze AOW-klanten, zoals NAW-gegevens, telefoonnummer,

[13] Zie paragraaf 2.6 van dit besluit.

geboortedatum, geboorteland, BSN, bankrekeningnummer, gegevens over een eventuele partner, hoogte van de uitkering en werkgeversgegevens. Daarbij komt dat de SVB in voorkomende gevallen ook beschikt over persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Dit zijn zeer gevoelige gegevens die in het bijzonder beschermd moeten worden. De gevolgen van (onrechtmatige) openbaarmaking van dergelijke gegevens kunnen zeer verstrekkend zijn.[14]

61 Daarnaast staat vast dat alle 1500 servicemedewerkers de gegevens van [VERTROUWELIJK] AOW-klanten kunnen inzien. Een dergelijk 'open' autorisatiesysteem brengt onmiskenbaar beveiligingsrisico's met zich. Hoe meer mensen toegang hebben tot dit systeem, hoe groter het risico op datamisbruik.

62 Ook staat vast dat de SVB een beleid voert waarbij (AOW-)klanten onder andere informatie kunnen opvragen en mutaties kunnen doorgeven en dat er wekelijks gemiddeld 20.000 mensen met de SVB bellen.[15] Zonder passende beveiligingsmaatregelen kan dit ertoe leiden dat telefonisch onrechtmatig persoonsgegevens worden verstrekt of gewijzigd.

63 De kans dat derden op grote schaal telefonisch via servicemedewerkers van de SVB toegang proberen te krijgen acht de AP evenwel niet waarschijnlijk. Wel bestaat de kans dat derden contact opnemen met de SVB om informatie te verkrijgen over iemand die ze kennen en die zij niet vertegenwoordigen. De in randnummer 1 van dit besluit genoemde klacht is ook voor de AP aanleiding geweest om een onderzoek te starten.

64 Gelet het voorgaande beoordeelt de AP de risico's van deze gegevensverwerkingen voor de individuele AOW-klant als hoog. Zo kunnen persoonlijke gegevens gedeeld of gewijzigd worden met of door een onbevoegde, wat in bepaalde gevallen ernstige gevolgen kan hebben voor de betrokkene. In individuele gevallen is ernstige materiële en immateriële schade denkbaar. Hierbij kan gedacht worden aan het risico van schade door ongeoorloofd gebruik van gegevens. [VERTROUWELIJK]. Dit kan grote gevolgen hebben voor de betrokkene, niet alleen financiële. Daarnaast bestaat er een reëel risico dat bekenden van AOW-klanten om persoonlijke redenen bij de SVB informatie proberen te achterhalen of te wijzigen, wat zou kunnen leiden tot bijvoorbeeld stalking of afpersing. Tot slot is er het risico op (reputatie)schade bij het delen van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

4.3.4 Beoordeling passende veiligheidsmaatregelen ten tijde van de ondertekening van het onderzoeksrapport

65 De AP is van oordeel dat – gelet op de hiervoor beschreven risico's – de maatregelen die SVB ten tijde van de vaststelling van het onderzoeksrapport had genomen op het vlak van authenticatie en bewustwording ontoereikend waren c.q. dat die maatregelen de beveiligingsrisico's onvoldoende mitigeerden om tot een op die risico's afgestemd beveiligingsniveau te komen. De AP licht dit toe.

[14] Zie pararaaf 2.4 van dit besluit.
[15] Zie paragrafen 2.1 en 2.4 van dit besluit.

Beleid telefonische authenticatie

66 Weliswaar had de SVB beleid opgesteld aangaande het controleren van de identiteit van bellers door middel van (controle)vragen, maar de AP heeft vastgesteld dat dit beleid in twee afzonderlijke werkinstructies beschikbaar was [VERTROUWELIJK] die bovendien elk een verschillende werkwijze beschrijven.[16] Het beleid was dan ook niet eenduidig, waardoor het voor de servicemedewerkers ook niet duidelijk was welke van de twee instructies de juiste was en gevolgd moest worden.

67 Daarnaast had meer dan de helft van de controlevragen betrekking op eenvoudig te achterhalen gegevens. Uit het interne SVB-beleid volgde bijvoorbeeld dat gevraagd kon worden naar een combinatie van adres en geboortedatum van de betrokkene, hetgeen een laag beschermingsniveau voor de beveiliging biedt omdat NAW-gegevens voor een groot aantal mensen beschikbaar zijn. Zo zijn deze gegevens bijvoorbeeld vaak bekend bij vrienden, familie en (voormalig) collega's. Bovendien zijn deze gegevens eenvoudig te achterhalen via openbare bronnen, waaronder sociale media.

68 Verder schreef slechts één van de [VERTROUWELIJK] pagina's voor dat servicemedewerkers dienen te vragen naar ofwel het SVB-registratienummer [VERTROUWELIJK] ofwel het BSN. Voor deze nummers geldt dat het beschermingsniveau hoger is dan bij NAW-gegevens, omdat deze identificatienummers in het algemeen slechts bereikbaar zullen zijn voor een selecte kring rondom de betrokkene. Servicemedewerkers werden in deze instructie echter vrij gelaten in hun keuze welke aanvullende controlevragen, wanneer gesteld moesten worden. Ook gaf deze werkinstructie niet aan of er gegevens verstrekt of gewijzigd mogen worden als de klant zijn of haar SVB-registratienummer [VERTROUWELIJK] of BSN niet kan noemen, zodat het voor servicemedewerkers onduidelijk was wat ze in dat geval moesten doen.[17]

69 Weliswaar volgde uit het beleid dat indien de servicemedewerkers na de eerste vragen nog twijfelden aan de identiteit van de beller, de medewerkers aanvullende controlevragen dienden te stellen. Het beleid bood echter geen duidelijkheid over de vraag in welke situaties nog twijfel zou moeten bestaan over de identiteit en welke (aanvullende) controlevragen in dat geval gesteld moesten worden.[18]

70 Tot slot is geconstateerd dat de servicemedewerkers het beschikbare beleid niet nauwgezet en op consistente wijze naleefden.[19] Servicemedewerkers hadden, ervaarden of namen in de uitvoering van hun werkzaamheden kennelijk een bepaalde mate van vrijheid.

Controle van het beleid telefonische authenticatie

71 De SVB had ten tijde van de ondertekening van het onderzoeksrapport ook geen toereikende manier om te controleren dat servicemedewerkers in overeenstemming met het beleid de identiteit van de klanten aan

[16] Zie paragraaf 2.5 van dit besluit.
[17] Ibid.
[18] Ibid.
[19] Ibid.

de telefoon controleerden. Zoals hiervoor is opgemerkt werd weliswaar door middel van door servicemedewerkers opgestelde telefoonnotities via een collegiale toets c.q. steekproef gecontroleerd of de identiteit van klanten werd vastgesteld in overeenstemming met het beleid, maar was in geen van de aan de AP overgelegde telefoonnotities informatie opgenomen over hoe de identiteit van de beller in het telefoongesprek was vastgesteld. Ook waren er geen vaste formats voor het opstellen van deze notities.[20] Daardoor bestond er voor servicemedewerkers geen enkele prikkel die ervoor zorgde dat zij in hun telefoonnotities opnamen hoe zij de identiteit van de beller vaststelden. Weliswaar heeft de SVB tijdens het AP-onderzoek verklaard bezig te zijn met een Europese aanbesteding waarmee de gehele SVB (en dus ook AOW) zou worden voorzien van onder andere het automatisch vastleggen van telefoongesprekken in tekst en het opnemen van gesprekken waardoor de praktijk rondom telefonische authenticatie zou worden verbeterd, maar dit aanbestedingstraject was nog niet afgerond waardoor ten tijde van de ondertekening van het onderzoeksrapport de hiervoor genoemde omissies nog bestonden.

72 Zoals in randnummer 25 van dit besluit is weergegeven, heeft de SVB tijdens het onderzoek voorts verklaard dat indien de identiteit van de beller op onjuiste wijze is vastgesteld de klant waarschijnlijk een klacht zal indienen bij de SVB en het aannemelijk is dat deze klacht wordt besproken in door de SVB ingerichte leercirkels.[21] Als een controlemiddel is gebaseerd op een dergelijke aanname, dan is dat naar het oordeel van de AP per definitie ontoereikend. Er vindt dan immers enkel een controle plaats in het geval een klant zich ervan bewust is dat een andere persoon onbevoegd informatie over hem of haar heeft verkregen en die klant bovendien daadwerkelijk een klacht indient bij de SVB.

Bewustwording

73 Verwerkingsverantwoordelijken dienen ervoor te zorgen dat hun medewerkers zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en handelen met inachtneming van die verantwoordelijkheden.

74 De SVB zet verschillende bewustwordingsmethodes in. In deze zaak acht de AP met name de werkinstructies in [VERTROUWELIJK] en de door de SVB aangeboden opleidingen relevant, aangezien daar specifiek wordt genoemd hoe servicemedewerkers moeten omgaan met het verwerken van persoonsgegevens in het kader van telefonisch contact met klanten.

75 Naar het oordeel van de AP waren ten tijde van de vaststelling van het onderzoeksrapport ook de organisatorische maatregelen die de SVB had getroffen op het vlak van bewustwording ter beveiliging van persoonsgegevens ontoereikend.

76 Weliswaar had de SVB eenmalig verplichte opleidingen waar de regels en risico's van het werken met (persoons)gegevens bij telefonisch klantcontact werden behandeld, maar de frequentie van de opleidingen was laag. Daarnaast geldt voor de werkinstructies [VERTROUWELIJK] dat deze te allen tijden beschikbaar

[20] Ibid.
[21] Ibid.

waren, maar dat het aan de medewerkers was om deze werkinstructies (periodiek) te raadplegen. Resultaat hiervan was dat de medewerkers niet altijd op de hoogte waren van de (meest) recente instructies. Ook is gebleken dat de werkwijze van servicemedewerkers met enige regelmaat afweek van de werkwijze die werd voorgeschreven in de verschillende bewustwordingsmethodes. Een regelmatige bijscholing van de regels en procedures met betrekking tot beveiliging van persoonsgegevens in het kader van telefonisch klantcontact ontbrak, met het risico dat meer ervaren medewerkers geleidelijk konden afwijken van het beleid – wat in de praktijk ook daadwerkelijk gebeurde.

4.3.5 Conclusie beveiligingsmaatregelen

77 De AP herhaalt haar conclusie dat de SVB ten tijde van de vaststelling van het onderzoeksrapport (nog) geen toereikende risico-inventarisatie had uitgevoerd. Voor zover al sprake was van een risico-inventarisatie, was deze gedateerd en onvolledig. Daarnaast moeten naar het oordeel van de AP de risico's die gepaard gaan met de telefonische dienstverlening, mede gelet op de omvang van de verwerking ([VERTROUWELIJK] AOW-klanten), de aard van de verwerkte gegevens (onder andere financiële en strafrechtelijke gegevens), het grote aantal geautoriseerde medewerkers (alle 1500 servicemedewerkers) en de frequentie waarmee mensen telefonisch contact opnemen met de SVB (gemiddeld 20.000 keer per week[22]), als hoog worden aangemerkt. Gelet op dit hoge risico, waren naar het oordeel van de AP de maatregelen die de SVB had genomen op het vlak van authenticatie van de beller en bewustwording ontoereikend.

78 Met betrekking tot het oordeel of de beveiligingsmaatregelen passend zijn, dient onder andere rekening te worden gehouden met de uitvoeringskosten van die maatregelen. Naar het oordeel van de AP zijn er geen grote uitvoeringskosten gemoeid met het (substantieel) verbeteren van de beveiligingsmaatregelen. Dat geldt bijvoorbeeld voor het opstellen van een goede, eenduidige werkwijze met betrekking tot het controleren van de identiteit van de beller. Ook aan het verhogen van de nalevingsgraad van het beveiligingsbeleid voor telefonisch klantcontact zijn geen disproportionele uitvoeringskosten verbonden.

79 Gelet op het voorgaande concludeert de AP dat SVB de beveiligingsmaatregelen van de SVB niet passend waren ten opzichte van de beveiligingsrisico's bij de verwerking van persoonsgegevens bij het telefonisch klantcontact met AOW-klanten. Hieruit concludeert de AP dat de SVB heeft gehandeld in strijd met artikel 32, eerste en tweede lid, van de AVG.

4.4 Duur van de overtreding

80 In het op 4 november 2021 ondertekende onderzoeksrapport is geconcludeerd dat de SVB vanaf 25 mei 2018 geen passende technische en organisatorische maatregelen had getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen met betrekking tot het telefonisch klantcontact met AOW-

[22] Het betreft hier het totaal aantal vragen per week ten aanzien van alle sociale zekerheidswetten. Het is de AP niet bekend welk percentage daarvan ziet op AOW, maar aangezien volgens de SVB ongeveer 63% van de populatie AOW-gerechtig is, kan worden aangenomen dat een substantieel deel van de telefonische vragen ziet op de AOW.

klanten. De SVB erkent dit. Zoals hiervoor in hoofdstuk 3 van dit besluit is uiteengezet heeft de SVB zodra het onderzoeksrapport van de AP bekend werd onmiddellijk en voortvarend gewerkt aan de verbetering van de beveiliging van de verwerking persoonsgegevens tijdens het telefonisch klantcontact.

81 De SVB heeft al op 9 december 2021 een uitgebreide, specifiek op de telefonische dienstverlening gerichte risico-inventarisatie aan de AP overgelegd. Deze risico-inventarisatie heeft zich niet beperkt tot de AOW, maar is gericht op alle onder de SVB ressorterende sociale zekerheidswetten. Naar het oordeel van de AP zijn in deze inventarisatie de (specifieke) risico's die gepaard gaan met het verwerken van persoonsgegevens in het kader van telefonisch klantcontact in toereikende mate geïdentificeerd en beoordeeld op basis van de waarschijnlijkheid dat die risico's zich voordoen.

82 In december 2021 heeft de SVB tevens een plan van aanpak vastgesteld waarin een pakket van verbetermaatregelen is opgenomen om de risico's die gepaard gaan met zijn telefonische dienstverlening te beperken. Onmiddellijk na de vaststelling van dit plan van aanpak is de SVB gestart met de implementatie ervan, hetgeen erin heeft geresulteerd dat in juni 2022 een groot aantal verbetermaatregelen daadwerkelijk en concreet is doorgevoerd op het gebied van vastlegging, systeemondersteuning, toetsing en borging, vakmanschap en bewustwording.

83 Zo heeft de SVB zijn beleid ten aanzien van telefonische authenticatie aangepast door de twee oude werkinstructies te vervangen door één nieuwe, eenduidige, heldere en voor de servicemedewerkers centraal toegankelijke werkinstructie die de procedure voorschrijft bij telefonische authenticatie van bellers. De wijze waarop de identiteit van de bellende AOW-klanten wordt gecontroleerd wordt in aanzienlijk mindere mate overgelaten aan de eigen beoordeling en inzichten van de servicemedewerker. De werkinstructie maakt duidelijk met welke controlevragen een servicemedewerker moet starten, welke aanvullende controlevragen een servicemedewerker moet stellen, welke vragen een servicemedewerker in ieder geval moeten stellen, hoeveel controlevragen een servicemedewerker (minimaal) moet stellen, wanneer een servicemedewerker aanleiding heeft om te twijfelen aan de identiteit van de beller en wat een servicemedewerker moet doen als de twijfel niet wordt weggenomen. Ook is duidelijker wat servicemedewerkers moeten doen als klanten het [VERTROUWELIJK]-nummer of BSN niet kunnen of willen verstrekken. Servicemedewerkers zijn derhalve minder vrij in hun keuze welke (aanvullende) vragen zij wanneer kunnen stellen en wat zij moeten doen in geval nog twijfel bestaat over de identiteit van de beller. Voorts heeft de AP geconstateerd dat de controlevragen niet enkel zien op gemakkelijk te achterhalen gegevens. Deze instructies dragen daarom ook bij aan een verhoogd bewustwordingsniveau van de servicemedewerkers. Bovendien maakt een periodieke (tweejaarlijkse) evaluatie door de SVB een vast onderdeel van het proces, hetgeen een positieve bijdrage levert aan het beveiligingsniveau van de telefonische dienstverlening.

84 Ook leggen servicemedewerkers voortaan in hun telefoonnotities – via een invulveld in [VERTROUWELIJK] – gestructureerd vast welke controlevragen zij tijdens een telefoongesprek hebben gesteld ter verificatie van de identiteit van de beller. Op die manier kan de SVB de bewustwording binnen

zijn organisatie vergroten. Bovendien kan de SVB hierdoor controleren hoe de verificatie van de identiteit van bellers in de praktijk verloopt, hierover een oordeel vormen en eventueel verdere verbetermaatregelen treffen. De introductie van een periodieke inzet van mystery callers, waarbij de SVB tevens het door de mystery caller gevoerde gesprek evalueert met de servicemedewerker en de leerpunten in algemene zin deelt met andere medewerkers, bevordert zowel de controle als het bewustwordingsniveau nog verder.

85 Daarnaast heeft de SVB in zijn plan van aanpak een doorlopende bewustwordingscampagne opgenomen waarin met regelmaat aandacht wordt besteed aan privacybescherming tijdens telefonisch klantcontact, bijvoorbeeld via het SVB-intranet, in interne nieuwsbrieven en organisatie-brede bijeenkomsten.

86 Daarenboven is relevant dat de SVB zijn bestaande (voor servicemedewerkers verplichte) telefoontraining heeft aangepast om de bewustwording op het gebied van authenticatie van de beller en het delen van informatie via de telefoon nog verder te vergroten. Deze aanpassing wordt aangeboden aan zowel nieuwe als ervaren servicemedewerkers. Tevens organiseert de SVB opfriscursussen.

87 Naar het oordeel van de AP heeft de SVB met de invoering van deze verbetermaatregelen in elk geval al in juni 2022 passende en organisatorische maatregelen getroffen die een op het risico afgestemd beveiligingsniveau waarborgen.

4.5 Conclusie

88 Gelet op het voorgaande is de AP van oordeel dat, hoewel de SVB verbetermaatregelen heeft ingevoerd, de SVB niettemin artikel 32, eerste en tweede lid, van de AVG heeft overtreden. Die overtreding bestaat eruit dat de SVB heeft nagelaten passende technische en organisatorische maatregelen op een op het risico afgestemd beveiligingsniveau te waarborgen met betrekking tot het verwerken van persoonsgegevens in het kader van telefonisch klantcontact met AOW-klanten. Deze overtreding heeft geduurd vanaf 25 mei 2018 tot juni 2022.

5. Boete

5.1 Inleiding

89 Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Ter voorkoming dat organisaties met verwerkingen van persoonsgegevens inbreuk maken op de privacy van burgers is het van groot belang dat zij een op risico afgestemd beveiligingsniveau toepassen.

90 De SVB heeft in strijd gehandeld met artikel 32, eerste en tweede lid, van de AVG. Hierdoor heeft de SVB niet in overeenstemming gehandeld met de basisbeginselen van de verwerking van persoonsgegevens zoals bedoeld in artikel 5 AVG. De AP maakt daarom gebruik van haar bevoegdheid om aan de SVB een boete op te leggen. Omdat de SVB deze overtreding inmiddels voortvarend ongedaan heeft gemaakt en er

gelet op de door de SVB getroffen verbetermaatregelen geen vrees bestaat voor herhaling van deze overtreding, is het opleggen van een last onder dwangsom niet meer aan de orde.

5.2 Boetebeleidsregels Autoriteit Persoonsgegevens 2019

91 Ingevolge artikel 58, tweede lid, aanhef en onder i en artikel 83, vierde lid en zevende lid, van de AVG, gelezen in samenhang met artikel 18, eerste en tweede lid, van de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG), is de AP bevoegd aan de SVB in geval van een overtreding van artikel 32 van de AVG een bestuurlijke boete op te leggen tot € 10.000.000.

92 Ter invulling van voornoemde boetebevoegdheid heeft de AP boetebeleidsregels vastgesteld[23] (hierna: de Boetebeleidsregels). De systematiek van de Boetebeleidsregels is als volgt.

93 De overtredingen waarvoor de AP een boete kan opleggen tot het hierboven vermelde bedrag, zijn in de Boetebeleidsregels ingedeeld in drie boetecategorieën. Deze categorieën zijn gerangschikt naar zwaarte van de overtreding van de genoemde artikelen, waarbij categorie I de minst zware overtredingen bevat en categorie III de zwaarste overtredingen. Aan de categorieën zijn in hoogte oplopende geldboetes verbonden. Dit volgt uit artikel 2, onder 2.1 en 2.3 van de Boetebeleidsregels.

Categorie I	Boetebandbreedte tussen € 0 en € 200.000	Basisboete: € 100.000
Categorie II	Boetebandbreedte tussen € 120.000 en € 500.000	Basisboete: € 310.000
Categorie III	Boetebandbreedte tussen € 300.000 en € 750.000	Basisboete: € 525.000

94 Overtreding van artikel 32 van de AVG (beveiliging van de verwerking) is, blijkens bijlage I bij de Boetebeleidsregels, ingedeeld in categorie II. Zoals volgt uit de tabel hiervoor, geldt voor deze categorie een boetebandbreedte tussen minimaal € 120.000 en maximaal € 500.000, met een basisboete van € 310.000.

95 De basisboete geldt als neutraal uitgangspunt, en dient te worden verhoogd of verlaagd voor zover de in artikel 7 van de Boetebeleidsregels vermelde factoren daartoe aanleiding geven. De uiteindelijke hoogte van de boete dient evenredig te zijn en afgestemd op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten.[24]

[23] Boetebeleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019), Stcrt. 2019, 14586, 14 maart 2019.
[24] Vergelijk artikel 49, derde lid van het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest) en de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht.

5.3 Boetehoogte

96 Naar het oordeel van de AP leiden enkele boeteverlagende omstandigheden en evenredigheid tot aanzienlijke verlaging van de (basis)boete. De mate van verwijtbaarheid van de gedraging geeft geen aanleiding tot verdere aanpassing van de boete.

5.3.1 Boeteverlagende omstandigheden

97 De in artikel 7, aanhef en onder a en c van de Boetebeleidsregels vermelde factoren geven aanleiding om de basisboete te verlagen.

98 Vast staat dat de SVB verschillende categorieën persoonsgegevens verwerkt van zeer veel betrokkenen.[25] Zoals in paragraaf 4.3.3 van dit besluit is uiteengezet kan dit grote gevolgen hebben voor de betrokkenen. Hoewel de kans bestaat dat derden telefonisch contact opnemen met de SVB met het doel informatie te verkrijgen over iemand die ze kennen en die zij niet vertegenwoordigen, kan daar in dit geval tegenover worden gesteld dat die derden in dat contact direct in aanraking komen met een servicemedewerker, hetgeen een zekere drempel opwerpt. Daarnaast had de SVB in zijn beleid al maatregelen getroffen ten aanzien van informatieverstrekking tijdens telefonisch klantcontact, die de AP als risico beperkend beschouwt. Zo mochten servicemedewerkers in het geval zij op juiste wijze de identiteit van (een gemachtigde van) een klant hadden vastgesteld, geen gegevens verstrekken en wijzigen waarvoor een schriftelijke vorm is vereist. Ook mochten servicemedewerkers adresgegevens, bankgegevens en bedragen enkel telefonisch verstrekken na het stellen van (aanvullende) controlevragen. Het BSN mochten servicemedewerkers nooit aan (gemachtigden van) klanten verstrekken. Zodoende bestond telefonisch toegang tot een beperkter aantal persoonsgegevens. Ook bij de invoering van het nieuwe telefonische authenticatiebeleid heeft de SVB nog een lijst opgesteld waarin is geëxpliciteerd dat de volgende gegevens niet via de telefoon mogen worden verstrekt: het BSN, strafrechtelijke gegevens (zoals gegevens over – het zich onttrekken aan – detentie) en bijzondere persoonsgegevens, zoals gegevens over de gezondheid van een persoon, nationaliteit en etniciteit (bijvoorbeeld het geboorteland, land van herkomst).

99 Hoewel gevallen van ongeoorloofde toegang via telefonisch klantcontact niet altijd (direct) door de SVB zullen worden opgemerkt, is het wel zeer aannemelijk dat het aantal door het oude telefonische authenticatiebeleid getroffen betrokkenen gering is. Anders dan vaak het geval is bij bijvoorbeeld een inbraak in een computersysteem van een verwerkingsverantwoordelijke, is bij telefonisch klantcontact geen sprake van ongeoorloofde toegang tot complete klantenbestanden. Derden kunnen namelijk slechts steeds in individuele gevallen informatie verkrijgen van een specifieke betrokkene door het voeren van vaardige gesprekken met een servicemedewerker.

[25] De SVB heeft in [VERTROUWELIJK] van [VERTROUWELIJK] AOW-klanten, verschillende categorieën persoonsgegevens opgeslagen, zoals NAW-gegevens, werkgeversgegevens, BSN, strafrechtelijke gegevens geboortedatum of burgerlijke staat.

100 Uit door de SVB verstrekte informatie blijkt ook dat er gemiddeld zo'n 20.000 mensen per week naar de SVB bellen met vragen over sociale verzekeringen. Dit, terwijl de SVB in de periode 2018 tot en met 2021 slechts tien datalekken heeft geconstateerd in relatie tot het verstrekken van gegevens aan een onbevoegde persoon via telefonische dienstverlening. Bovendien hadden maar drie van die datalekken betrekking op AOW-klanten en zag slechts één datalek – het datalek dat aanleiding vormde voor het onderhavige onderzoek van de AP – op telefonische authenticatie. De SVB heeft met die betrokkene bovendien overeenstemming bereikt over een schadeloosstelling.[26]

101 Gelet op het voorgaande ziet de AP op grond van artikel 7, aanhef en onder a en c, van de Boetebeleidsregels aanleiding om en het basisbedrag van de boete te verlagen.

5.3.2. Verwijtbaarheid en evenredigheid

102 Op grond van artikel 5:46, tweede lid, van de Algemene wet bestuursrecht (hierna: Awb) houdt de AP bij het opleggen van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten. Artikel 32 van de AVG bevat geen opzet of schuld als bestanddeel. Zoals onder meer volgt uit de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 27 maart 2013, ECLI:NL:RVS:2013:BZ7467, mag dan in beginsel van de verwijtbaarheid van de overtreding worden uitgegaan. Indien een verwerkingsverantwoordelijke betoogt dat hem ter zake van die overtreding geen enkel verwijt valt te maken, zal hij dit aannemelijk moeten maken.[27]

103 De SVB is verplicht om door middel van passende technische en organisatorische maatregelen een op risico afgestemd beveiligingsniveau te waarborgen. Het is aan de SVB te verwijten dat hij niet aan deze verplichting heeft voldaan. De AVG, maar ook de BIO waaraan de SVB moet voldoen, heeft ten aanzien van de beveiliging van de verwerking van persoonsgegevens nadrukkelijk beschreven dat organisaties een op risico afgestemd beveiligingsniveau moeten waarborgen. Van de SVB mag worden verwacht dat het zich van de voor hem geldende normen vergewist en daarnaar handelt. Nu de overtreding de SVB ten volle kan worden verweten, geeft de mate van verwijtbaarheid van de overtreding geen aanleiding om het boetebedrag te verlagen.

104 Tot slot beoordeelt de AP ingevolge artikel 49, derde lid van het Handvest en de artikelen 3:4 en 5:46 van de Awb of de toepassing van haar beleid voor het bepalen van de hoogte van de boetes gezien de omstandigheden van het concrete geval, niet tot een onevenredige uitkomst leidt.

[26] Verslag van de zienswijzezitting van 18 januari 2022, blz. 10.

[27] Vergelijk de uitspraken van de Afdeling bestuursrechtspraak van de Raad van State van 29 augustus 2018 (ECLI:NL:RVS:2018:2879, ow. 3.2) en 5 december 2018 (ECLI:NL:RVS:2018:3969, ow. 5.1). Vergelijk ook de uitspraken van het College van Beroep voor het bedrijfsleven van 29 oktober 2014 (ECLI:NL:CBB:2014:395, ow. 3.5.4), 2 september 2015 (ECLI:NL:CBB:2015:312, ow. 3.7) en 7 maart 2016 (ECLI:NL:CBB:2016:54, ow. 8.3). Zie tot slot *Kamerstukken II* 2003/04, 29 702, nr. 3, p. 134.

105 De AP acht het in het licht van de evenredigheid van de op te leggen boete van belang dat de SVB zeer proactief aan de slag is gegaan met de bevindingen uit het AP-onderzoeksrapport. Al vijf weken na de ondertekening en verzending van het onderzoeksrapport heeft de SVB aan de AP een uitgebreide risico-inventarisatie en een plan van aanpak overgelegd. Vervolgens heeft de SVB geheel uit eigener beweging heel snel een groot aantal verbetermaatregelen daadwerkelijk en concreet uitgevoerd op het gebied van vastlegging, systeemondersteuning, toetsing en borging, vakmanschap en bewustwording. Al deze acties hebben ertoe geleid dat de SVB de overtreding al binnen een half jaar na ondertekening van het onderzoeksrapport heeft beëindigd, zonder dat daaraan een handhavingsbesluit van de AP ten grondslag lag. Daarnaast weegt mee dat de SVB al in december 2021 zelfstandig (zonder tussenkomst van de AP) heeft besloten om de herijkte werkinstructies voor niet alleen voor de AOW, maar voor het gehele terrein van onder hem ressorterende sociale verzekeringen door te voeren. Alle getroffen maatregelen en de snelheid ervan tonen in ieder geval de bereidwilligheid van de SVB om serieus met de beveiliging in de organisatie aan de slag te gaan.

106 Gezien het voorgaande ziet de AP aanleiding het bedrag van de boete op grond van de evenredigheid verder te verlagen tot een bedrag van € 150.000.

5.4 Conclusie

107 De AP stelt het boetebedrag voor de overtreding van artikel 32, eerste en tweede lid, van de AVG, gelet op het voorgaande vast op € 150.000.

Datum
19 januari 2023

Ons kenmerk
[VERTROUWELIJK]

6. Dictum

De AP legt aan de Sociale verzekeringsbank wegens overtreding van artikel 32, eerste en tweede lid, van de AVG een bestuurlijke boete op ten bedrage van: **€ 150.000,--** (zegge: honderdvijftigduizend euro).[28]

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

mr. A. Wolfsen
voorzitter

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Ingevolge artikel 38 van de UAVG schort het indienen van een bezwaarschrift de werking van de beschikking tot oplegging van de bestuurlijke boete op. De AP zal pas tot invordering overgaan, nadat het besluit onherroepelijk is geworden.[29] Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Bezwaar maken tegen een besluit, onderaan de pagina onder de kop Contact met de Autoriteit Persoonsgegevens. Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, postbus 93374, 2509 AJ Den Haag.
Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'.
Schrijf in uw bezwaarschrift ten minste:
- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer); of een kopie van dit besluit bijvoegen;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

[28] De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB). De boete dient overeenkomstig artikel 4:87, eerste lid, van de Awb binnen zes weken te worden betaald. Voor informatie en/of instructie over de betaling kan contact opgenomen worden met de eerder vermelde contactpersoon bij de AP.
[29] De AP zal de vordering alsdan uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).