Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

> Retouradres Postbus 450 9700 AL Groningen

PER KOERIER
Vodafone Libertel B.V.
[VERTROUWELIJK]

Rijksinspectie Digitale Infrastructuur

Bezoekadres
Emmasingel 1
9726 AH Groningen

Postadres
Postbus 450
9700 AL Groningen

T +31 (0)088 04 16 000

Contactpersonen
[VERTROUWELIJK]

Ons kenmerk
[VERTROUWELIJK]

Uw kenmerk
-

Bijlagen
1. Juridisch kader
2. Verslag hoorzitting
3. Persbericht
4. Publieksversie besluit

Datum 21 mei 2024
Betreft Beschikking tot oplegging bestuurlijke boete en publicatie

Geachte [VERTROUWELIJK],

1. Inleiding

Hierbij informeer ik Vodafone Libertel B.V. (hierna: Vodafone) dat ik aan Vodafone een bestuurlijke boete als bedoeld in artikel 15.4, eerste lid, van de Telecommunicatiewet (hierna: Tw) van € 2.250.000,- (twee miljoen tweehonderdvijftig duizend euro) opleg. De reden voor de oplegging van de bestuurlijke boete is dat Vodafone als aanbieder van openbare telecommunicatie-netwerken en -diensten in de periode 5 oktober 2021 tot 15 december 2022 onvoldoende zorg heeft gedragen voor het treffen van noodzakelijke beveiligingsmaatregelen om kennisneming van LI-gegevens[1] door onbevoegden te voorkomen. Daarmee heeft Vodafone een overtreding begaan van de artikelen 2, 3, 4 en 8 van het Besluit beveiliging gegevens telecommunicatie (hierna: Bbgt) in samenhang gelezen met de artikelen I, II, III en V van de bijlage bij het Bbgt.

Daarnaast besluit ik een publieksversie van dit besluit alsmede een persbericht op de website van de RDI te publiceren.

Mijn overwegingen treft u hieronder aan.

2. Samenvatting: kern van het boetebesluit

Een belangrijke kerntaak van de overheid is het garanderen van een veilig land waarin in vrijheid kan worden geleefd en de democratische rechtsorde is gewaarborgd.[2] Een essentieel onderdeel is het werk dat de inlichtingendiensten, de politie en het Openbaar Ministerie verrichten om de samenleving te beschermen tegen dreigingen. Zonder effectief optreden van deze diensten kunnen bijvoorbeeld dreigingen in het fysieke of cyberdomein niet tijdig worden onderkend of de inzet van de krijgsmacht in die domeinen niet afdoende worden ondersteund, met mogelijk ingrijpende gevolgen. Ook zouden bijvoorbeeld

[1] Gegevens die betrekking hebben op Lawful Interception, dat wil zeggen het bevoegd aftappen of opnemen van telecommunicatie.
[2] Bijvoorbeeld: De Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023, p. 2.

(pogingen tot) de ontvreemding van hoogwaardige technologische kennis, bedrijfsvertrouwelijke informatie, persoonsgegevens, vitale economische informatie en staatsgeheimen onopgemerkt kunnen blijven.

Daartoe hebben de inlichtingendiensten onder meer de bevoegdheid om communicatie te onderscheppen. Ten behoeve van de opsporing van zware criminaliteit komt ook de officier van justitie dit middel toe. Van groot belang is de voorwaarde dat inzet van de bevoegdheid heimelijk kan geschieden, zonder dat een betrokkene daarvan op de hoogte is. Geheimhouding en beveiliging tegen onbevoegde kennisneming zijn hierbij ook van het grootste belang.

In hoofdstuk 13 van de Tw is de uitwerking van de bovengenoemde bevoegdheden opgenomen. Aanbieders van openbare communicatiediensten en -netwerken dienen gehoor te geven aan de bevoegd gegeven lasten om communicatie te onderscheppen. De aanbieder dient gegevens die verband houden met bevoegd aftappen geheim te houden. De Tw en het daarop gebaseerde Bbgt verplichten de aanbieders daartoe de LI-gegevens behoorlijk te beveiligen tegen onbevoegde kennisname. Zonder een goede beveiliging kan de vertrouwelijkheid en daarmee ook de effectiviteit van het onderscheppen van communicatie niet worden gegarandeerd.

De toezichthouder heeft geconstateerd dat de beveiliging door Vodafone van LI-gegevens op meerdere punten tekortschoot. Deze tekortkomingen waren zowel op organisatorisch als technisch vlak aanwezig. Het gaat om de volgende overtredingen.

Overtreding 1

Artikel 3 van het Bbgt vereist dat de aanbieder zorg draagt voor een beveiligingsplan, waarin hij aangeeft op welke wijze uitvoering is gegeven aan zijn beveiligingsplicht. Dat plan dient ten minste aan te geven op weke wijze uitvoering is gegeven aan de maatregelen genoemd in de bijlage. Bij Vodafone was dit plan niet volledig en bovendien sterk verouderd.

Overtreding 2

Onderdelen van het proces van bevoegd aftappen kan een aanbieder buiten zijn organisatie beleggen. Artikel 8 van het Bbgt vereist in geval van uitbesteding de derde zich verplicht LI-gegevens te beveiligen tegen kennisneming door onbevoegden, dat geheimhouding met betrekking tot die gegevens wordt betracht en dat de ingevolge het Bbgt gestelde maatregelen worden nageleefd. Vodafone heeft onderdelen van haar LI-proces aan derden uitbesteed. Vodafone heeft daarbij de vereiste afspraken niet afdoende volledig en concreet met al haar leveranciers gemaakt.

Overtreding 3

Artikel 4, tweede lid, van het Bbgt vereist – kort en goed – dat de medewerking aan taplasten uitsluitend mag worden verleend door personen aan wie een VOG is verstrekt. In artikel II van de bijlage bij het Bbgt zijn voorts concrete beveiligingseisen ten aanzien van personeel opgenomen. Zo is daarin bepaald dat in de functiebeschrijving van personeel dat belast is met de verwerking van LI-gegevens de verantwoordelijkheid voor de beveiliging daarvan is beschreven (a), dat personeel dat in aanraking komt met LI-gegevens een geheimhoudingsverklaring tekent (b), en dat uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van LI-gegevens toegang tot die gegevens heeft.

De beveiligingseisen van Vodafone ten aanzien van het personeel waren onvoldoende:

a. Personeel dat niet was belast met verwerking van LI-gegevens had toegang tot de LI-gegevens;
b. Er ontbraken Verklaringen Omtrent Gedrag (VOG's) of daarmee gelijk te stellen documenten van personeel dat belast is met het verwerken van LI-gegevens;
c. Er ontbraken functieomschrijvingen van personeel belast met het verwerken van LI-gegevens;
d. Er ontbraken geheimhoudingsverklaringen van personeel belast met het verwerken van LI-gegevens.

Overtreding 4

In artikel III van de bijlage bij het Bbgt staan concrete vereisten met betrekking tot de fysieke beveiliging en beveiliging van de omgeving waarin LI-gegevens zich bevinden opgenomen.

De fysieke beveiliging van de ruimte waarin LI-gegevens aanwezig waren was onvoldoende:

a. Er kon eenvoudig toegang door onbevoegden tot de fysieke ruimte waarin LI-gegevens aanwezig waren worden verkregen;
b. Toegang tot die fysieke ruimte was niet uitsluitend toegestaan voor geautoriseerde personen voor zover dit voor hun functie noodzakelijk was;
c. Tijdens het onderzoek is gebleken dat er voor onderhoud door niet-geautoriseerde personen geen begeleiding was van een geautoriseerd persoon;
d. Er was geen gecontroleerde en achteraf herleidbare toegang op individueel niveau;
e. Er was geen detectie van toegang tot de fysieke ruimte en ook ontbrak de mogelijkheid tot het tijdig interveniëren.

Overtreding 5

In artikel V van de bijlage bij het Bbgt staan concrete maatregelen met betrekking tot toegangsbeveiliging van geautomatiseerde informatiesystemen opgenomen.

De toegangsbeveiliging tot geautomatiseerde systemen waarin LI-gegevens worden verwerkt was onvoldoende:

a. Op drie systemen was geen sprake van een deugdelijke beveiliging, onder meer doordat persoonsgebonden authenticatie ontbrak;
b. Op drie systemen zat geen blokkering bij overschrijding van drie foutieve inlogpogingen;
c. Op drie systemen was geen externe logging en detectie geactiveerd;
d. Handelingen met betrekking tot de verwerking van de LI-gegevens werden niet persoonsgebonden vastgelegd om onderzoek mogelijk te maken.

Ik verwijs naar hoofdstuk 6 van dit besluit voor een uitgebreide uiteenzetting van de overtreden normen.

Deze overtredingen acht ik niet alleen afzonderlijk, maar zeker ook in onderlinge samenhang bezien ernstig. Een adequate beveiliging bestaat namelijk uit een combinatie van maatregelen op het gebied van preventie en detectie alsook administratieve en personele maatregelen. Hierbij heeft de toezichthouder vastgesteld dat de beveiliging van de LI-keten van Vodafone conceptueel, zoals dient te worden vastgelegd in het beveiligingsplan, als in de daadwerkelijke uitvoering ernstig tekort schoot. Ik licht dat in hoofdstuk 7 van dit besluit verder toe. In dit besluit leg ik Vodafone daarom een bestuurlijke boete op voor elk van de vijf hoofdovertredingen. Daarnaast heb ik besloten een publieksversie van het besluit met een begeleidend persbericht openbaar te maken.

3. Inhoudsopgave

4. Wettelijk kader

Het relevante wettelijk kader is opgenomen in bijlage 1. Deze bijlage maakt deel uit van dit besluit.

5. Onderzoek van de toezichthouder

De RDI staat voor een veilig verbonden Nederland en houdt onder andere toezicht op de naleving van de Tw en het bepaalde in het Bbgt en de bijlage bij het Bbgt. Uit artikel 13.5 van de Tw volgt dat iedere aanbieder van openbare telecommunicatienetwerken en -diensten aan het Bbgt dient te voldoen.

5.1 Verloop procedure

Op 5 oktober 2021 is de toezichthouder een onderzoek gestart naar de naleving van het Bbgt door Vodafone. Dit onderzoek is afgerond op 15 oktober 2022. Voor een volledige weergave van het procesverloop gedurende de inspectiefase verwijs ik naar hoofdstuk 2 van het Rapport van bevindingen (hierna: Rvb).

Per brief van 26 juli 2023, met kenmerk [VERTROUWELIJK], heb ik mijn voornemen om een bestuurlijke boete aan Vodafone en mijn voornemen een publieksversie van dit boetebesluit te publiceren kenbaar gemaakt aan Vodafone. Als bijlage aan dit voornemen was het Rvb gehecht. Ik heb Vodafone in de gelegenheid gesteld een zienswijze te geven op mijn voornemen. De termijn hiervoor liep tot 1 september 2023.

Op 26 juli 2023 heb ik het verzoek van Vodafone ontvangen om de zienswijze termijn uit te stellen tot 29 september 2023. Dit verzoek heb ik per e-mailbericht van 26 juli 2023 gehonoreerd.

Op 21 augustus heb ik het verzoek van Vodafone ontvangen om de zienswijze termijn uit te stellen tot vier weken na 29 september 2023. Dit verzoek heb ik per brief, met kenmerk [VERTROUWELIJK], van 29 augustus 2023 gehonoreerd.

Op 3 oktober 2022 heeft Vodafone telefonisch verzocht om nader uitstel van de zienswijze termijn. Op 3 oktober 2023 heeft een van mijn medewerkers dit verzoek telefonisch en per e-mailbericht gehonoreerd.

Op 8 november 2023 heb ik de zienswijze van Vodafone tijdig ontvangen.

Op 29 november 2023 heeft Vodafone, bijgestaan door haar gemachtigden, een mondelinge toelichting gegeven op haar zienswijze. Het verslag van de hoorzitting is als bijlage 2 aan dit besluit toegevoegd.

Per e-mailbericht van 7 december 2023 heb ik Vodafone verzocht schriftelijk te reageren op mijn vragen die ik haar tijdens de hoorzitting heb gesteld.

Op 21 december 2023 heb ik de antwoorden van Vodafone op de vragen naar aanleiding van de hoorzitting per e-mailbericht tijdig ontvangen.

5.2 Resultaten onderzoek

5.2.1 Hoedanigheid Vodafone

De toezichthouder heeft zijn onderzoek gericht op Vodafone en haar groepsmaatschappijen als bedoeld in artikel 2:24b Burgerlijk Wetboek voor zover zij aanbieder zijn van openbare telecommunicatienetwerken en openbare telecommunicatiediensten in de zin van artikel 1.1 van de Tw.

Vodafone is in het handelsregister van de Kamer van Koophandel ingeschreven onder het nummer 14052264 en is gevestigd op de Avenue Ceramique 300 te Maastricht. Vodafone is per 20 juli 2004 geregistreerd bij de Autoriteit Consument en Markt als aanbieder van openbare elektronische communicatienetwerken of -diensten.

5.2.2 Reikwijdte en afbakening onderzoek

De toezichthouder heeft van 5 oktober 2021 tot en met 15 december 2022 onderzoek naar de naleving van het Bbgt door Vodafone verricht. Voor het verloop van het onderzoek verwijs ik naar hoofdstuk 2 van het door mijn toezichthouder opgestelde Rvb van 15 december 2022 en de daarbij behorende bijlagen.

De toezichthouder heeft zijn onderzoek gericht op de drie systemen van Vodafone waarin de gegevens die in het kader van een taplast aan Vodafone worden verstrekt om een taplast uit te kunnen voeren, worden verwerkt.[3] Ik verwijs naar paragraaf 5.2.4 van dit besluit voor een uitgebreidere omschrijving van deze systemen en een visuele weergave hiervan.

De toezichthouder heeft geen onderzoek gedaan naar de beveiliging van de zogeheten Mobile Core, dat wil zeggen de omgeving waar alle zendmasten van Vodafone samenkomen en het mobiele internet- en telefonieverkeer wordt afgehandeld.

5.2.3 Onderzoeksbevindingen

De minimumnormen die in de bijlage bij het Bbgt zijn gesteld, beschermen de integriteit van strafvorderlijke onderzoeken en staatsgeheime informatie. Voorgeschreven zijn maatregelen die zoveel mogelijk beogen te voorkomen dat ongeautoriseerde toegang plaatsvindt, maatregelen die toegang registreren en maatregelen die een tijdige detectie van ongeautoriseerde toegang mogelijk maken.

[3] Rvb, p. 5.

Het Rvb bevat een volledige beschrijving van de vastgestelde feiten waarop ik mijn bevindingen baseer. Het Rvb moet hier als herhaald en ingelast worden beschouwd. In het hiernavolgende beschrijf ik mijn bevindingen, onder verwijzing naar het Rvb.

5.2.4 Inrichting LI-proces Vodafone

De toezichthouder heeft geconstateerd dat Vodafone contracten heeft gesloten met partijen waaraan zij diensten uitbesteedt op het gebied van LI-gegevens.[4]

Bij het onderzoek is een aantal leveranciers van Vodafone betrokken. Deze worden hieronder kort toegelicht:

- [VERTROUWELIJK] is een leverancier van een LI-systeem die een administratieve rol vervult in de LI-keten;
- [VERTROUWELIJK] is een leverancier van een LI-systeem die een technische rol vervult in de LI-keten;
- [VERTROUWELIJK] is een leverancier van een LI-systeem die een technische rol vervult in de LI-keten;
- [VERTROUWELIJK] is een leverancier die eerste aanspreekpunt (eerstelijns support) is voor diverse LI-systemen;
- [VERTROUWELIJK] is een leverancier van een LI-systeem ten behoeve van vaste verbindingen[5];
- [VERTROUWELIJK] is de leverancier van één van de datacenters waarin Vodafone haar LI-systemen onderbrengt.

Vodafone heeft het proces van voldoen aan een tapverzoek schematisch als volgt ingericht:

[4] Rvb, p. 21.
[5] Dit systeem is niet door de toezichthouder onderzocht.

De toezichthouder heeft op basis van het onderzoek, diverse gesprekken, documenten en onderzochte systemen (en diens functionaliteiten) het LI-proces bij Vodafone uitgewerkt in bovenstaand schema en onderstaande stappen. Het proces voor bevoegd aftappen bestaat, verkort weergegeven, uit de volgende stappen[6]:

1. Elk tapproces begint met een daartoe strekkende bijzondere last tot aftappen (tapverzoek) van een bevoegde autoriteit, doorgaans zijnde de Officier van Justitie, de AIVD en de MIVD.

[6] Rvb, p. 23.

6. De afgetapte informatie wordt door [VERTROUWELIJ] en het [VERTROUWELIJK]-systeem aangeboden aan de bevoegde autoriteit in het afgesproken bestandstype. De overgedragen informatie betreft zowel de inhoud van de telefoongesprekken als de bijbehorende metadata.

6. Overtredingen

In het Bbgt en de bijlage daarvan zijn nadere regels gesteld met betrekking tot de beveiliging van LI-gegevens. Hierin wordt onder meer bepaald welke beveiligingsmaatregelen een aanbieder in ieder geval moet nemen om kennisneming van LI-gegevens door onbevoegden te voorkomen. Deze maatregelen richten zich onder andere op de beveiliging van geautomatiseerde systemen die LI-gegevens bevatten, op te treffen beveiligingsmaatregelen ten aanzien van personeel dat in aanraking komt met LI-gegevens en op de beveiliging van de fysieke ruimte waarin de LI-gegevens zich bevinden.

De maatregelen die een aanbieder op basis van het Bbgt in ieder geval moet treffen, zien daarmee op de gehele LI-keten. De toezichthouder heeft daarom de getroffen beveiligingsmaatregelen ten aanzien van de gehele LI-keten van Vodafone onderzocht, te weten de logische beveiliging van de drie LI-systemen, de getroffen beveiligingsmaatregelen ten aanzien van personeel dat belast is met de verwerking van LI-gegevens en de beveiliging van de fysieke ruimte waarin de LI-gegevens zich bevinden. Ook heeft de toezichthouder onderzoek gedaan naar het door Vodafone opgestelde beveiligingsplan.

Op basis van het onderzoek heeft de toezichthouder zes overtredingen vastgesteld.

In de hiernavolgende paragrafen worden de constateringen van de toezichthouder besproken per onderdeel waar de norm van het Bbgt op ziet.

---

[7] Technische identificatie gegevens zijn gegevens die de LI-systemen nodig hebben om de tap technisch mogelijk te maken, bijvoorbeeld het telefoonnummer.
[8] Deze 'retourstroom' maakt geen deel uit van het onderzoek.

6.1 Ondeugdelijk beveiligingsplan

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 3, eerste lid van het Bbgt. In dit artikel is de plicht opgenomen dat de aanbieder zorg draagt voor een beveiligingsplan, waarin hij aangeeft op welke wijze door hem uitvoering is gegeven aan zijn beveiligingsplicht. In het beveiligingsplan wordt ten minste aangegeven op welke wijze uitvoering is gegeven aan de maatregelen die genoemd staan in de bijlage bij het Bbgt.

Artikel 3, eerste lid, van het Bbgt luidt als volgt:

> 1. *De aanbieder draagt zorg voor een beveiligingsplan, waarin hij aangeeft op welke wijze door hem uitvoering is gegeven aan zijn beveiligingsplicht. In het beveiligingsplan wordt ten minste aangegeven op welke wijze uitvoering is gegeven aan de maatregelen, bedoeld in de bijlage.*

De nota van toelichting van het Bbgt zegt over het beveiligingsplan het volgende:

> *"De door de aanbieder te treffen c.q. getroffen maatregelen dienen te worden vastgelegd in een beveiligingsplan. In het beveiligingsplan dienen alle beveiligingsaspecten welke aan de orde zijn ten aanzien van de bedrijfsprocessen waaraan de gegevens en informatie zijn onderworpen op een gestructureerde wijze te worden behandeld.(…)"*[9]
>
> *"Ingevolge artikel 2, tweede lid, onder d, van het besluit dient de aanbieder daartoe beveiligingsmaatregelen te treffen; in de bijlage bij het besluit is een aantal van deze maatregelen reeds geëxpliciteerd (vergelijk onderdeel V, onder b en e). De door de aanbieder getroffen maatregelen dienen in het in artikel 3 bedoelde beveiligingsplan te worden vastgelegd."*[10]
>
> *'In het beveiligingsplan moet worden aangegeven op welke wijze uitvoering is gegeven aan de bescherming en beveiliging van de gegevens die worden verstrekt ten behoeve van het onderzoeken, opsporen of vervolgen van strafbare feiten en de gegevens die in het belang van de nationale veiligheid worden verstrekt aan de inlichtingen- en veiligheidsdiensten. Daarbij dient specifieke aandacht te worden besteed aan het onderscheid in de verschillende beveiligingsregimes, omdat dezelfde gegevens gebruikt kunnen worden ten behoeve van zakelijke doeleinden van de aanbieders als ten behoeve van het voldoen aan een vordering op grond van de artikelen 13.2b en 13.4 van de Tw.'*[11] *(onderstreping JZ)*

Vodafone moet als aanbieder aan artikel 3, eerste lid van het Bbgt voldoen en een beveiligingsplan hebben. Uit de wettekst, in samenhang gelezen met de nota van toelichting daarbij, zoals hierboven is opgenomen, blijkt duidelijk dat in het beveiligingsplan minimaal moet zijn opgenomen op welke wijze de aanbieder

[9] *Stb*. 2003, 472, p. 10.
[10] *Stb*. 2003, 472, p. 13.
[11] *Stb.* 2009, 350, p. 6 en 7.

uitvoering geeft aan zijn beveiligingsplicht, waarbij de aanbieder ten minste moet aangeven hoe uitvoering wordt gegeven aan de maatregelen genoemd in de bijlage bij het Bbgt.

De bijlage bij het Bbgt bevat zes categorieën van de te treffen beveiligingsmaatregelen, 1) zijnde een algemene beveiligingseis, 2) beveiligingseisen ten aanzien van het personeel, 3) fysieke beveiliging en de beveiliging van de omgeving, 4) beheer van communicatie- en bedieningsprocessen, 5) toegangsbeveiliging van geautomatiseerde informatiesystemen en 6) de ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen. Deze maatregelen, met uitzondering van de algemene beveiligingseis, richten zich elk op een afzonderlijk aspect van de beveiliging van LI-gegevens.

Daarnaast vermeldt de nota van toelichting dat alle beveiligingsaspecten welke aan de orde zijn ten aanzien van de bedrijfsprocessen waaraan LI-gegevens zijn onderworpen op een gestructureerde wijze moeten worden behandeld.[12] Bovendien volgt uit de nota van toelichting dat hierbij specifieke aandacht besteed moet worden aan het onderscheid in de verschillende beveiligings-regimes.[13]

De toezichthouder heeft van Vodafone het beveiligingsplan, in de zin van artikel 3 van het Bbgt, opgevraagd. De toezichthouder heeft het beveiligingsplan op 12 oktober 2021 van Vodafone ontvangen.[14] In paragraaf 4.3.2 van het Rvb heeft de toezichthouder een volledig verslag opgenomen van het onderzoek naar het beveiligingsplan. Samengevat blijkt daaruit het volgende.

Het beveiligingsplan bevat volgens de toezichthouder enkel een opsomming met generieke maatregelen of een verwijzing daarnaar. In het beveiligingsplan ontbreekt een specifieke omschrijving van de wijze waarop uitvoering is gegeven aan de maatregelen die in de zes artikelen van de bijlage bij het Bbgt zijn opgenomen. In de opsomming van LI-systemen ontbreekt het [VERTROUWELIJK] -systeem, terwijl uit het onderzoek van de toezichthouder blijkt dat dit wel een LI-systeem is dat Vodafone gebruikt waarin LI-gegevens worden verwerkt en waarop de maatregelen derhalve betrekking dienen te hebben.[15] Ook ontbreekt een beschrijving van het 4G-tapproces, terwijl dit voor 2G en 3G wel beschreven is.[16] Daarnaast zijn de maatregelen ten aanzien van de fysieke beveiliging niet gerelateerd aan maatregelen die Vodafone zou moeten treffen volgens de bijlage bij het Bbgt.[17] De toezichthouder heeft verder geconstateerd dat bij de getroffen maatregel camera-observatie niet wordt vermeld op welke wijze die maatregel uitvoering geeft aan de betrokken normen in de bijlage bij het Bbgt onder III. In

[12] *Stb*. 2009, 350, p. 10.
[13] *Stb.* 2009, 350, p. 7.
[14] Beveiligingsplan VodafoneZiggo 2021.pdf.
[15] Rvb, p. 27.
[16] Beveiligingsplan VodafoneZiggo 2021.pdf.
[17] Paragraaf 4.3.2 van het Rvb en Beveiligingsplan VodafoneZiggo 2021, p. 14 t/m 20.

het beveiligingsplan staat verder dat [VERTROUWELIJK]

Ook heeft de toezichthouder vastgesteld dat in het beveiligingsplan niet in de aanstelling van de in artikel I van de bijlage bij het Bbgt bedoelde functionaris is voorzien. Ook blijken de verantwoordelijkheden en bevoegdheden van de Bbgt-functionaris anderszins niet uit het beveiligingsplan van Vodafone.

De toezichthouder heeft verder vastgesteld dat het beveiligingsplan van Vodafone sterk verouderd is; de versies 0.1 en 1.1 stammen uit respectievelijk 2008 en 2010.[20] De eerstvolgende en tevens laatste versie van het beveiligingsplan, versie 2.0, stamt uit 2021. De toezichthouder heeft vastgesteld dat deze versie geen inhoudelijke aanpassingen bevat ten opzichte van de versie 1.1 uit 2010. Ook heeft de toezichthouder vastgesteld dat het beveiligingsplan op meerdere punten niet aansluit op het in de praktijk aangetroffen en onderzochte LI-proces van Vodafone.[21] Daarnaast wordt er in het beveiligingsplan verwezen naar verouderde wetgeving, namelijk het Besluit beveiliging gegevens aftappen telecommunicatie (BBGAT). Dit is de voorloper van het Bbgt, dat uit het jaar 2009 stamt. Deze vaststelling ondersteunt de vaststelling dat het beveiligingsplan van Vodafone verouderd is. Dit geldt zowel voor de maatregelen ten aanzien van de deugdelijke logische beveiliging van geautomatiseerde systemen als de fysieke beveiliging hiervan.

Verder bevat het beveiligingsplan een opsomming van interne beveiligings-standaarden van Vodafone. Vastgesteld is dat deze niet aan het Bbgt gerelateerd is. De fysieke beveiligingseisen behelzen slechts een klein gedeelte van de LI-keten. Overige afspraken over de beveiliging van de fysieke ruimte waarin geautomatiseerde LI-systemen zich bevinden, ontbreken in het beveiligingsplan.

Wat betreft de duur van de overtreding overweeg ik als volgt. Uit het verslag van een gesprek tussen de toezichthouder en Vodafone, dat heeft plaatsgevonden op 14 juni 2022, blijkt dat de aanpassingen van het beveiligingsplan hebben geleid tot een 0.7 versie van het beveiligingsplan op 7 juni 2022. Uit het gespreksverslag blijkt dat de fysieke beveiligingsmaatregelen [VERTROUWELIJK] nog ontbreken. De toezichthouder heeft Vodafone de dringende suggestie gedaan dat artikel 6 en artikel 8 van het Bbgt explicieter meegenomen moeten worden. Daarnaast volgt uit het gespreksverslag van de bespreking tussen Vodafone en RDI die plaats heeft gevonden op 14 juni 2022 dat de 1.0 versie van het Beveiligingsplan naar verwachting eind 2022 klaar zou zijn.[22]

[18] Beveiligingsplan VodafoneZiggo 2021, p. 12.
[19] Rvb, p. 27 en 28.
[20] Zie paragraaf 4.3.2 van het Rvb en Bijlage 2 van het Rvb.
[21] Paragraaf 4.3.2 van het Rvb.
[22] Verslag AT – VZ 14 juni 2022_DEF, ad. 4.

Op grond van bovenstaande stel ik vast dat Vodafone artikel 3, eerste lid van het Bbgt heeft overtreden in ieder geval in de periode van 5 oktober tot en met 15 december 2022.

6.2 Beveiligingsfunctionaris

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 2, eerste lid, onder a, in samenhang gelezen met artikel 2, tweede en derde lid, van het Bbgt en artikel I van de bijlage bij het Bbgt.

Artikel 2, eerste lid, onder a, in samenhang gelezen met artikel 2, tweede en derde lid, van het Bbgt en artikel I van de bijlage bij het Bbgt verplichten de aanbieder een beveiligingsfunctionaris te hebben, die is belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen. Hiertoe dient de functionaris regelmatig controles uit te voeren en de resultaten daarvan vast te leggen.

Voor een volledige weergave van dit onderzoek verwijs ik naar hoofdstuk 4.3.2 van het Rvb. Samengevat blijkt daaruit het volgende.

De functieomschrijving van de [VERTROUWELIJK] beschrijft slechts op zeer summiere, algemene wijze de verantwoordelijkheid ten aanzien van de naleving van geldende wet- en regelgeving. Ook is er gedurende het onderzoek door Vodafone een vacature opengesteld voor de functie van functionaris. Deze functie is vervuld en de nieuwe functionaris is per 1 december 2022 gestart.[23]

De verplichting op grond van artikel I van de bijlage bij het Bbgt is tweeledig. Allereerst dient de aanbieder een beveiligingsfunctionaris te hebben. Daarnaast dient deze beveiligingsfunctionaris regelmatig controles uit te voeren en de resultaten daarvan vast te leggen.

De toezichthouder heeft niet kunnen vaststellen dat de betreffende functionaris de op grond van artikel I van de bijlage van het Bbgt verplichte controles heeft uitgevoerd, dan wel de resultaten daarvan heeft vastgelegd.

In de door Vodafone gegeven zienswijze zie ik aanleiding om van mijn voornemen om op basis van deze overtreding tot boeteoplegging over te gaan af te wijken. Hoewel er aanwijzingen zijn dat de verplichte controles niet regelmatig zijn uitgevoerd dan wel dat de resultaten hiervan niet zijn vastgelegd door de functionaris, acht ik het op grond van de door Vodafone aangevoerde zienswijze niet overtuigend bewezen dat Vodafone geen beveiligingsfunctionaris had aangesteld gedurende het onderzoek. Vodafone heeft hiertoe aangevoerd dat de per 1 december 2022 aangestelde functionaris is aangetreden als gevolg van een interne governance wijziging bij Vodafone. Op basis hiervan kan niet buiten

[23] Bijlage 20221026: Status aanpassingen Vodafone.pdf, p. 2.

redelijke twijfel worden vastgesteld dat de betreffende functionaris voor die tijd niet was aangesteld.

Ik wijk daarom af van mijn voornemen en ga niet tot boeteoplegging over wegens overtreding van artikel 2, eerste lid, onder a, in samenhang gelezen met artikel 2, tweede en derde lid, van het Bbgt en artikel I van de bijlage bij het Bbgt.

6.3 Gesloten overeenkomsten met derden met betrekking tot LI-gegevens

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 8 van het Bbgt door Vodafone. Onderzocht zijn de overeenkomsten die Vodafone heeft gesloten met derden waaraan zij werkzaamheden heeft uitbesteed en waarbij die derde kennis neemt of kan nemen van LI-gegevens.

Artikel 8 van het Bbgt luidt als volgt:

1. *Indien de aanbieder de uitvoering van werkzaamheden uitbesteedt aan een derde en in dat kader de derde kennis neemt of kan nemen van gegevens en informatie als bedoeld in artikel 2, eerste lid, draagt de aanbieder er zorg voor dat de derde zich verplicht:*
   a. *de desbetreffende gegevens en informatie te beveiligen tegen kennisneming door onbevoegden;*
   b. *met betrekking tot de desbetreffende gegevens en informatie geheimhouding te betrachten;*
   c. *de ingevolge dit besluit gestelde maatregelen na te leven;*
   d. *alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.*
2. *De verplichtingen van de derde als bedoeld in het eerste lid worden geregeld in een schriftelijke overeenkomst tussen aanbieder en derde. Op een daartoe strekkend verzoek van de bevoegde autoriteit wordt inzage verleend in de overeenkomst.*
3. *De aanbieder is verantwoordelijk voor de naleving door de derde van de verplichtingen, bedoeld in het eerste lid.*

In paragraaf 4.3.7 van het Rvb heeft de toezichthouder een volledig verslag opgenomen van het onderzoek naar de contracten die Vodafone heeft gesloten met derden met betrekking tot de beveiliging van LI-gegevens. Uit het onderzoek van de toezichthouder blijkt samengevat het volgende.

De toezichthouder heeft geconstateerd dat de uitvoering van werkzaamheden aan derden is uitbesteed door Vodafone. De toezichthouder heeft daarnaast vastgesteld dat medewerkers van de betreffende derde partijen, te weten [VERTROUWELIJK] , kennis konden nemen van LI-gegevens. Met het oog hierop heeft de toezichthouder de met deze partijen gesloten overeenkomsten opgevraagd. De toezichthouder heeft de overeenkomsten die hij van Vodafone heeft ontvangen onderzocht. Uit het onderzoek van de toezichthouder is gebleken dat geen van de onderzochte documenten afspraken bevat zoals voorgeschreven in artikel 8, eerste lid en onder a tot en met d, van het Bbgt.

Vodafone heeft op verzoek van mijn toezichthouder op 26 oktober 2022 een overzicht van actualisaties op Bbgt-gebied gegeven.[24] Vodafone geeft daarin onder meer te kennen dat zij haar overeenkomst met leveranciers [VERTROUWELIJK] heeft aangevuld met een 'Bbgt-schedule'. Echter blijkt uit het document dat Vodafone met leverancier [VERTROUWELIJK] nog steeds hetzelfde contract hanteert. Die overeenkomst bevat niet de in artikel 8 van het Bbgt vereiste inhoud. Ditzelfde geldt voor de overeenkomst met [VERTROUWELIJK]. Een wijziging of aanvulling van die overeenkomst wordt niet genoemd. Vodafone heeft de overtreding derhalve op 26 oktober 2022 nog niet (volledig) hersteld. Ik kom dan ook tot de conclusie dat de overtreding in ieder geval tot en met 26 oktober 2022 heeft voortgeduurd.

Ik stel op grond van het bovenstaande vast dat Vodafone artikel 8, eerste en tweede lid, van het Bbgt in ieder geval in de periode van 5 oktober 2021 tot en met 26 oktober 2022 heeft overtreden.

6.4 Beveiligingseisen ten aanzien van personeel

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 4, tweede lid, Bbgt in samenhang gelezen met artikel 2, tweede en derde lid, Bbgt en onderdeel II, onderdeel a, b en c van de bijlage bij het Bbgt, gericht op het treffen van noodzakelijke beveiligingsmaatregelen ten aanzien van personeel.

Artikel 4, tweede lid, van het Bbgt luidt als volgt:

> *2. De aanbieder draagt er zorg voor dat aan de uitvoering van de in artikel 13.2, eerste en tweede lid, van de wet bedoelde bevoegd gegeven bijzondere last en de in de artikelen 13.2b en 13.4 van de wet neergelegde verplichting tot het verstrekken van informatie, de medewerking uitsluitend wordt verleend door personen, die aan hem een verklaring omtrent het gedrag als bedoeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag hebben overgelegd. De eerste volzin is niet van toepassing, indien de betrokken persoon een vertrouwensfunctie uitoefent als bedoeld in het eerste lid.*

In artikel II van de bijlage bij het Bbgt staan, voor zover relevant, de navolgende concrete maatregelen ten aanzien van personeel:

> *II. Beveiligingseisen ten aanzien van personeel*
> *a. In de functiebeschrijving van personeel dat belast is met de verwerking van de informatie en gegevens wordt de verantwoordelijkheid voor de beveiliging daarvan beschreven.*
> *b. Personeel dat in aanraking komt met de informatie en gegevens tekent een geheimhoudingsverklaring.*
> *c. Uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van de informatie en gegevens heeft toegang tot de informatie en de gegevens.*

[24] Bijlage: 20221026 Status aanpassingen Vodafone.pdf.

De strekking van deze bepalingen is dat uitsluitend personeel dat belast is met de verwerking van LI-gegevens en dat beschikt over een toereikende functieomschrijving, VOG en dat een geheimhoudingsverklaring heeft getekend, toegang mag hebben tot LI-gegevens, LI-gegevens mag verwerken of daarmee in aanraking mag komen. Onbevoegde toegang, dat wil zeggen toegang door personen die aan voormelde eisen niet voldoen, is verboden.

a. Onbevoegde toegang

De toezichthouder heeft vastgesteld dat 72 medewerkers van [VERTROUWELIJK] [25] onbedoelde toegang tot [VERTROUWELIJK] . Vodafone heeft desgevraagd verklaard dat deze 72 personen toegang hadden tot deze [VERTROUWELIJK] .[27] Daarbij heeft Vodafone ook aangegeven dat deze groep personen onbedoelde toegang had tot LI-gegevens.[28] Dit levert een overtreding op van artikel II, onderdeel c, van de bijlage bij het Bbgt.

b. Geen VOG

De toezichthouder heeft vastgesteld dat negen [VERTROUWELIJK] -medewerkers geautoriseerde toegang hebben tot het [VERTROUWELIJ] -systeem en het [VERTROUWELIJK] -systeem. Daarnaast heeft één [VERTROUWELIJK] -medewerker toegang tot het [VERTROUWELIJ] -systeem. Uit hoofde van hun functie hebben deze medewerkers toegang tot en zijn zij belast met de verwerking van LI-gegevens.[29] Zij verlenen daarmee medewerking aan de uitvoering van taplasten. De toezichthouder heeft bij Vodafone een kopie of inzage van de vereiste VOG's gevorderd. Aangaande de [VERTROUWELIJK] -medewerker heeft de toezichthouder geconstateerd dat de VOG van na de aanvang van zijn inspectie is gedateerd. Vodafone heeft voor de overige medewerkers echter geen kopieën verstrekt of inzage in relevante documenten geboden. De toezichthouder heeft ook anderszins bij Vodafone of haar leverancier geen enkel bewijs van aanwezigheid van de VOG's vastgesteld. Daarop heeft de toezichthouder geconcludeerd dat de VOG's voor [VERTROUWELIJK] -medewerkers en de [VERTROUWELIJK] -medewerker van het [VERTROUWELIJ] -systeem en het [VERTROUWELIJK] -systeem niet aanwezig waren.[30] Dit levert een overtreding op van artikel 4, tweede lid, van het Bbgt.

[25] [VERTROUWELIJK]
[26] [VERTROUWELIJK]

[27] Toelichting Bbgt HR-vordering 27 september 2022 def.pdf.
[28] Rvb, p. 36.
[29] Rvb, p. 36.
[30] Rvb, p. 34, 36 en 43.

c. Geen functieomschrijving

De toezichthouder heeft van Vodafone één functieomschrijving ontvangen die zou gelden voor de hiervoor genoemde negen [VERTROUWELIJK]-medewerkers die belast zijn met de verwerking van LI-gegevens.[31] Er is in deze ontvangen functiebeschrijving geen verantwoordelijkheid beschreven voor de beveiliging van LI-gegevens zoals bedoeld in het Bbgt.

De toezichthouder heeft vastgesteld dat er ten aanzien van het [VERTROUWELIJK]-systeem één [VERTROUWELIJK] medewerker geen functiebeschrijving heeft. Daarnaast hebben acht [VERTROUWELIJK] medewerkers en één [VERTROUWELIJK]-medewerker, eveneens belast met verwerking van LI-gegevens, wel een functiebeschrijving, maar hierin mist de relatie tot bevoegd aftappen, zodat hierin ook niet de verantwoordelijkheid voor de beveiliging van LI-gegevens is beschreven. Verder was er voor één medewerker van [VERTROUWELIJK] geen arbeidsovereenkomst en/of functieomschrijving aanwezig. Drie medewerkers van [VERTROUWELIJK] hebben wel een toereikende functieomschrijving, maar deze dateert van 17 augustus 2022, oftewel na aanvang van de inspectie van mijn toezichthouder.[32] Ook deze personen zijn belast met verwerking van LI-gegevens.[33]

De toezichthouder heeft verder vastgesteld dat voor negen medewerkers van [VERTROUWELIJK] met toegang tot het [VERTROUWELIJK]-systeem de functiebeschrijving ontoereikend is, omdat uit de functiebeschrijving niet blijkt dat die medewerkers belast zijn met de verwerking van LI-gegevens en hierin ook niet de verantwoordelijkheid voor de beveiliging van LI-gegevens is beschreven, terwijl zij wel belast waren met de verwerking van LI-gegevens.[34]

Het voorgaande levert een overtreding op van artikel II, onderdeel a, van de bijlage bij het Bbgt.

d. Geen geheimhoudingsverklaring

De toezichthouder heeft vastgesteld dat er voor het [VERTROUWELIJ]-systeem voor één [VERTROUWELIJK]-medewerker een geheimhoudingsverklaring ontbrak. De geheimhoudingsverklaring van één [VERTROUWELIJK]-medewerker en acht [VERTROUWELIJK] medewerkers zijn bovendien gedateerd na de aanvang van inspectie, namelijk 22 november 2021 respectievelijk 13 oktober 2022.[35]

De toezichthouder heeft vastgesteld dat voor acht [VERTROUWELIJK] medewerkers met toegang tot het [VERTROUWELIJK]-systeem geen geheimhoudingsverklaring aanwezig was.

[31] Rvb, p. 35.
[32] Rvb, p. 43.
[33] Rvb, p. 41.
[34] Rvb, p. 48 en 49.
[35] Rvb, p. 35.

Na aanvang van de inspectie zijn de verklaringen, gedateerd op 13 oktober 2022, toegevoegd.[36]

Voor zeven medewerkers van het team [VERTROUWELIJK] van Vodafone die in aanraking komen met LI-gegevens op het [VERTROUWELIJK]-systeem stelt de toezichthouder vast dat de geheimhoudingsverklaring bij aanvang van het inspectietraject niet aanwezig was. De geheimhoudingsverklaringen zijn opgesteld gedurende het inspectietraject.[38]

De toezichthouder heeft verder geconstateerd dat door negen medewerkers van [VERTROUWELIJK] een zogenoemde 'Code of business Conduct' is getekend. Hierin wordt verwezen naar de interne gedragscode. Dit document betreft geen geheimhoudingsverklaring in de zin van het Bbgt, omdat hierin geen verantwoordelijkheid is beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens.[39]

Het voorgaande levert een overtreding op van artikel II, onderdeel b, van de bijlage bij het Bbgt.

Tussenconclusie

Schematisch heeft de toezichthouder de hierboven beschreven feiten als volgt weergegeven[40]:

	VOG	**Functiebeschrijving[41]**	**Geheimhoudingsverklaring[42]**
[VERTROUWELIJK] 1 medewerker	29 november 2021	Mist relatie tot aftappen*	22 november 2021
[VERTROUWELIJK] 8 medewerkers	Geen	Mist relatie tot aftappen*	13 oktober 2022
[VERTROUWELIJK] 1 medewerker	Geen	Geen	Geen
72 Overige (niet met LI-taak belaste) medewerkers	Geen	Geen	Geen

[36] Rvb, p. 35 en 36.
[37] 'Afdeling/Team dat belast is met de LI-taak binnen Vodafone', zie Rvb, p. 80.
[38] Rvb, p. 49.
[39] Rvb, p. 49.
[40] Rvb, p. 72.
[41] Mist relatie tot aftappen*: Geen verantwoordelijkheden voor de beveiliging van LI-gegevens beschreven zoals bedoeld in Bbgt bijlage II-a
[42] CobC*: Is geen geheimhoudingsverklaring

3 [VERTROUWELIJK] Medewerkers	Aanwezig	17 augustus 2022	Aanwezig
1 [VERTROUWELIJK] medewerker	Aanwezig	Geen	Aanwezig
9 [VERTROUWELIJK] medewerkers	Aanwezig	Mist relatie tot aftappen	CobC is ontoereikend
7 [VERTROUWELIJK] medewerkers	Aanwezig	Aanwezig	6 oktober 2021

Op grond van bovenstaande kom ik tot de volgende conclusie:

a. Ik stel vast dat 72 ongeautoriseerde personen toegang hadden tot LI-gegevens.
b. Daarnaast stel ik vast dat Vodafone niet de vereiste maatregelen heeft genomen ten aanzien van personeel dat de medewerking verleent aan taplasten. Ik stel vast dat Vodafone voor in totaal tien medewerkers die medewerking verleenden aan taplasten geen VOG aanwezig had.
c. Ook stel ik vast dat in de functiebeschrijving van 23 personen met toegang tot het [VERTROUWELIJ] en [VERTROUWELIJK]-systeem geen verantwoordelijkheid voor verwerking en beveiliging van LI-gegevens is genoemd. Verder stel ik vast dat negen medewerkers met toegang tot het [VERTROUWELIJK]-systeem eveneens geen functiebeschrijving hadden waaruit bleek dat zij verantwoordelijkheid hebben voor de verwerking en beveiliging van LI-gegevens.
d. Tot slot stel ik vast dat Vodafone met betrekking tot één medewerker van [VERTROUWELIJK], negen [VERTROUWELIJK]-medewerkers en negen [VERTROUWELIJK]-medewerkers geen (toereikende) geheimhoudingsverklaring aanwezig was.

In oktober 2022 heeft Vodafone inzicht gegeven in de stand van zaken van haar herstelwerkzaamheden. Vodafone geeft aan dat de verplichtingen op grond van het Bbgt ten aanzien van de medewerkers van het LI-team, [VERTROUWELIJK], [VERTROUWELIJK] en [VERTROUWELIJK] sinds oktober 2022 worden nageleefd. Met betrekking tot de medewerkers van [VERTROUWELIJK] deelt Vodafone mee dat zij geheimhoudings-verklaringen heeft laten ondertekenen, maar dat aan de overige verplichtingen (nog) niet is voldaan. Ik stel daarom vast dat Vodafone in ieder geval tot en met 26 oktober 2022 niet voldeed aan de verplichtingen die gelden voor personeel dat (kort gezegd) in aanraking komt met LI-gegevens.

Ik kom tot de conclusie dat Vodafone artikel 4, tweede lid, in samenhang met artikel 2, tweede en derde lid Bbgt en onderdeel II, onder a, b en c van de bijlage

bij het Bbgt heeft overtreden in ieder geval van 5 oktober 2021 tot en met 26 oktober 2022.

6.5 Fysieke beveiliging

De toezichthouder heeft daarnaast onderzoek gedaan naar de naleving door Vodafone van artikel 2, tweede en derde lid van het Bbgt in samenhang gelezen met artikel III van de bijlage bij het Bbgt.

In artikel III van de bijlage bij het Bbgt staan, voor zover relevant, de navolgende concrete maatregelen ten aanzien van fysieke beveiliging en beveiliging van de omgeving.

> *III. Fysieke beveiliging en beveiliging van de omgeving*
> *(…)*
> *b. De ruimte waarbinnen de informatie en de gegevens aanwezig zijn is deugdelijk fysiek beveiligd.*
> *c. De fysieke beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.*
> *d. Toegang tot de ruimte waar de gegevens of de informatie zich bevindt is uitsluitend toegestaan aan daartoe geautoriseerde personen voorzover dit voor hun functie noodzakelijk is.*
> *e. Het binnentreden en verlaten van de ruimte moet zodanig zijn geregeld dat er sprake is van gecontroleerde en achteraf herleidbare toegang op individueel niveau.*
> *(…)*
> *g. Personen belast met onderhouds- en reparatiewerkzaamheden in de ruimte waarin de informatie en de gegevens zich bevinden worden door eigen geautoriseerd personeel begeleid.*

Ik verwijs voor een gedetailleerde en volledige uiteenzetting van dit onderdeel van het onderzoek naar hoofdstuk 4.3.6 van het Rvb. Samengevat is daarin het volgende vastgesteld.

De toezichthouder heeft geconstateerd dat Vodafone in een datacentrum van [VERTROUWELIJK] een ruimte huurt in de vorm van een afgeschermde kooi met daarin een door Vodafone geplaatste kabinetkast. Dit datacentrum huisvest ook servers die gehuurd worden door andere klanten dan Vodafone. [VERTR

Op ten minste één van deze servers, [VERTROUWELIJK] zijn LI-gegevens aanwezig.[43] Deze server met LI-gegevens bevindt zich in een kabinetkast in een afgesloten kooi op een zaal op de tweede verdieping van het datacentrum [VERTROUWELIJK]. Deze kooi is vanaf de openbare ruimte toegankelijk via een beveiligingssluis op de begane grond en via een deur met toegangscontrole op de tweede verdieping.[44]

[43] Rvb, p. 60 e.v.
[44] Zie ook Rvb, p. 52, afbeelding 1 en 2.

De toezichthouder heeft van [VERTROUWELIJK] een lijst ontvangen waarop 280 personen, werkzaam bij 145 klanten van [VERTROUWELIJK], genoemd zijn die permanente toegang tot de tweede verdieping van het datacenter hebben.[45] Ook geeft [VERTROUWELIJK] aan dat deze 145 klanten van [VERTROUWELIJK] elk willekeurig persoon op elk gewenst tijdstip van de dag kunnen aanmelden bij het datacenter voor toegang, waarmee zij door de beveiligingssluis dan wel de deur op de tweede verdieping kunnen komen. Ook heeft [VERTROUWELIJK] te kennen gegeven dat vier van haar eigen leveranciers eveneens zelfstandig personen kunnen aanmelden voor werkzaamheden in [VERTROUWELIJK] en dus ook tot aan de kast met LI-gegevens van Vodafone [VERTROUWELIJK] kunnen komen. Daardoor ligt het werkelijk aantal personen met mogelijkheid tot toegang nog veel hoger dan de 280 personen op de lijst. [VERTROUWELIJK] schat zelf in dat het historisch gaat om 700 tot 900 personen.

De locatie is door de toezichthouder op 6 april 2022 bezocht voor onderzoek naar de staat van de fysieke beveiliging. Uit het onderzoek op de tweede verdieping is onder meer het volgende gebleken.

a. Deugdelijke fysieke beveiliging

De toezichthouder heeft geconstateerd dat de kooi waarin het LI-systeem van Vodafone zich bevindt (en waarin de LI-gegevens zich derhalve bevinden) is afgeschermd met een hekwerk dat niet tot het plafond reikt. Uit door de toezichthouder genomen foto's en beschrijving van de toezichthouder blijkt mij dat de ruimte tussen het plafond en de bovenzijde van het hekwerk voldoende groot is voor een persoon om toegang tot de kooi te verkrijgen.[46]

Mijn toezichthouder heeft verder vastgesteld dat de draaiknoppen aan de binnenzijde van de kooi voor het openen van de toegangsdeur vanaf de buitenzijde te bedienen zijn. Met behulp van gereedschap kon, door het hekwerk heen, aan de knoppen gedraaid worden.[47] De deur kon op deze wijze vanaf de buitenzijde worden geopend.

Omdat in datacenters normaliter onder de vloer een lege ruimte is ingericht voor koelingsluchtstromen, bekabeling en onderhoud, is ook onderzocht in hoeverre via die ondergrondse lege ruimte toegang kan worden verkregen tot de ruimte waarbinnen de LI-gegevens zijn. De toezichthouder heeft gezien dat een ondergrondse wandafscheiding bij de toegangsdeur tot de kooi ontbreekt. Door vloertegels te verwijderen kon via die ondergrondse lege ruimte toegang worden verkregen tot de ruimte waarbinnen de LI-gegevens zijn. Uit het verslag van de toezichthouder en door hem genomen foto's blijkt mij dat deze ruimte voldoende groot is om een persoon toegang te bieden tot de kooi.[48]

[45] Rvb, p. 54.
[46] Rvb, p. 54.
[47] Rvb, p. 56.
[48] Rvb, p. 56.

In de kooi bevindt het LI-systeem zich in een afgesloten kabinetkast. De toezichthouder heeft de kwaliteit van het sluitwerk op de kabinetkast onderzocht. Vodafone heeft desgevraagd geen certificering van het sluitwerk overgelegd. Op basis van het verslag van de toezichthouder stel ik vast dat de deur van de kabinetkast op eenvoudige wijze met handgereedschap kon worden geforceerd.[49] Deze kast is namelijk voorzien van een deur van dun materiaal, die met eenvoudig gereedschap kan worden opengebroken.

Ik ben van oordeel dat de ruimte waarbinnen de LI-gegevens aanwezig zijn niet deugdelijk fysiek beveiligd is. Met relatief eenvoudige hulpmiddelen was het voor in ieder geval 280 ongeautoriseerde personen mogelijk zich toegang te verschaffen tot het (fysieke) LI-systeem in kwestie. Deze personen konden daardoor eenvoudig toegang krijgen tot de LI-gegevens. Ik ben dan ook van oordeel dat Vodafone artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder b, van de bijlage bij het Bbgt heeft overtreden, in ieder geval in de periode van 5 oktober 2021 tot en met 15 december 2022. Daarbij merk ik op dat elk van de hierboven genoemde beveiligingshiaten afzonderlijk maar ook in onderlinge samenhang een overtreding van artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder b, van de bijlage bij het Bbgt opleveren.

b. Geautoriseerde toegang ruimte

Uit een door [VERTROUWELIJK] verstrekt document blijkt dat 39 van haar medewerkers, waaronder twee directieleden, permanente toegang hadden tot de kooi waarin de LI-gegevens zich bevinden.[50]

Met de toezichthouder acht ik de *permanente* toegang van deze personen tot de ruimte niet noodzakelijk voor de (onderhouds)functie die zij vervullen.

Ik stel vast dat Vodafone daarmee artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder d, van de bijlage bij het Bbgt heeft overtreden in ieder geval in de periode van 5 oktober 2021 tot en met 15 december 2022.

c. Begeleiding onderhoudspersoneel door geautoriseerd personeel

Tijdens het bezoek van de toezichthouder op 6 april 2022 te [VERTROUWELIJK] heeft de toezichthouder geconstateerd dat onderhoudswerkzaamheden werden verricht in de kooi waarin de LI-gegevens zich bevinden. Die werkzaamheden werden verricht door twee personen, zonder begeleiding van eigen geautoriseerd personeel.[51] Uit een periodieke toegangsrapportage van [VERTROUWELIJK] blijkt dat de

[49] Rvb, p. 57 e.v.
[50] Rvb, p. 57.
[51] Rvb, p. 58

betrokken personen al twee uur zonder begeleiding van eigen geautoriseerd personeel toegang hadden tot de ruimte waarin LI-gegevens worden verwerkt.[52]

Vodafone heeft daarmee naar mijn oordeel artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder g, van de bijlage bij het Bbgt in ieder geval op 6 april 2022 overtreden.

d. Achteraf herleidbare toegang

De toezichthouder heeft verder geconstateerd dat de camerabeelden van de gangen met kabinetkasten in de betrokken zaal, met daarin ook het LI-systeem, voor Vodafone niet beschikbaar waren.[53] De toezichthouder heeft daarnaast geconstateerd dat toegangspassen voor de kabinetkast waarin het LI-systeem zich bevindt niet persoonsgebonden zijn uitgereikt aan de [VERTROUWELIJK]-medewerkers.[54] Het zijn toegangspassen die telkens door willekeurige [VERTROUWELIJK] medewerkers worden gebruikt wanneer toegang tot een betreffende kabinetskast nodig is. Door Vodafone en/of [VERTROUWELIJK] en/of [VERTROUWELIJK] wordt geen uitgifteadministratie met betrekking tot de passen bijgehouden.

De bovengenoemde feiten leiden tot de conclusie dat achteraf niet te herleiden is welke individuen toegang hebben gehad tot de betrokken ruimte of kabinetkast. Vodafone heeft daarmee naar mijn oordeel artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder e, Bijlage Bbgt overtreden in ieder geval in de periode van 5 oktober 2021 tot en met 15 december 2022.

e. Detectie ongeautoriseerde toegang

De toezichthouder heeft tijdens zijn bezoek op 6 april 2022 te [VERTROUWELIJK] geconstateerd dat het cameratoezicht in de kooi van Vodafone niet is gericht op de toegang van de kooi waarin het LI-systeem zich bevindt. Daarnaast heeft de toezichthouder vastgesteld dat een persoon de camera in de kooi eenvoudig onklaar kan maken zonder in beeld te komen.[55] De toezichthouder heeft vastgesteld dat het cameratoezicht van [VERTROUWELIJK] slechts passief van aard was en tijdige detectie daardoor niet goed mogelijk was. Ook heeft de toezichthouder geen andere detectiemaatregelen aangetroffen bij de kabinetkast.

Op basis van het bovenstaande stel ik vast dat er onvoldoende detectie van ongeautoriseerde toegang plaatsvond. Op relatief eenvoudige wijze kon het cameratoezicht omzeild worden, dan wel kon dit toezicht onklaar worden gemaakt.

[52] Rvb, p. 58.
[53] Rvb, p. 55 e.v.
[54] Rvb, p. 57.
[55] Rvb, p. 55.

Dit leidt tot de conclusie dat Vodafone artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder c, Bijlage Bbgt heeft overtreden.

Tussenconclusie

Vodafone heeft mijn toezichthouder op 27 oktober 2022 een brief toegezonden waarbij zij onder andere de stand van zaken omtrent de fysieke beveiliging van de ruimte in het datacentrum beschrijft.[56]

Vodafone geeft aan dat haar camerasysteem per augustus 2022 naar behoren functioneert. Daarnaast blijkt dat bij [VERTROUWELIJK] de opdracht is gegeven tot het aanbrengen van extra beveiligingsmaatregelen. In Q4 2022 zouden de maatregelen gerealiseerd moeten worden.

Vodafone heeft voor wat betreft het herstel van haar cameratoezicht aangegeven dat dit herstel per augustus 2022 is geschied. Voor het overige stel ik vast dat Vodafone geen concrete herstelmaatregelen in de betrokken brief heeft genoemd. Ik leid daaruit af dat op de overige onderdelen van de fysieke beveiligingsvoorschriften in ieder geval per 27 oktober 2022 nog geen herstel had plaatsgevonden. Ik acht daarmee bewezen dat de overtreding van artikel III onder b, d en e Bijlage Bbgt tot in ieder geval 27 oktober 2022 heeft voortgeduurd.

Ik concludeer dat Vodafone op grond van het bovenstaande artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder c, van de bijlage bij het Bbgt heeft overtreden, in ieder geval in de periode van 5 oktober 2021 tot en met 27 oktober 2022.

6.6 Toegang geautomatiseerde systemen onvoldoende beveiligd

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 2 Bbgt in samenhang gelezen met artikel V van de bijlage van het Bbgt.

Op grond van artikel 2, eerste lid, van het Bbgt draagt de aanbieder zorg voor het treffen van noodzakelijke beveiligingsmaatregelen om kennisneming van LI-gegevens door onbevoegden te voorkomen. Artikel 2, tweede lid, onder c van het Bbgt bepaalt dat de maatregelen, zoals bedoeld in het eerste lid van dit artikel, ten minste dienen te bestaan uit maatregelen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarin de gegevens worden verwerkt. Artikel 2, derde lid, van het Bbgt geeft aan dat tot deze maatregelen in ieder geval de maatregelen genoemd in de Bijlage bij het Bbgt worden gerekend.

[56] 20221026 Status aanpassingen Vodafone.pdf.

Artikel V van de bijlage bij het Bbgt geeft aan welke maatregelen getroffen moeten worden ten aanzien van de toegangsbeveiliging van geautomatiseerde informatiesystemen die LI-gegevens bevatten.

Artikel V van de bijlage bij het Bbgt luidt voor zover relevant als volgt.

> *V. Toegangsbeveiliging van geautomatiseerde informatiesystemen*
> *a. De toegang tot geautomatiseerde informatiesystemen waarin de informatie en de gegevens worden verwerkt is op deugdelijke wijze beveiligd, onder meer door middel van persoonsgebonden authenticatie.*
>
> *b. De logische beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.*
>
> *c. Het aantal foutieve inlogpogingen is beperkt tot drie. Overschrijding van het aantal foutieve inlogpogingen leidt tot definitieve blokkering, welke uitsluitend door de functionaris, bedoeld in onderdeel I van deze bijlage, kan worden opgeheven. Het voorgaande is niet van toepassing op de systeembeheerder, met dien verstande dat bij drie foutieve inlogpogingen een hernieuwde inlogpoging slechts kan plaatsvinden via een voor noodsituaties ingericht account en persoonsgebonden authenticatie voor het gebruik waarvan door de functionaris, bedoeld in onderdeel I van deze bijlage toestemming moet worden verleend.*
> (…)
> *e. Alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem worden persoonsgebonden vastgelegd teneinde onderzoek mogelijk te maken.*
> *(..)*

Uit de nota van toelichting blijkt voorts dat de maatregelen die genomen moeten worden, bij dienen te dragen aan het bewerkstelligen van een minimumniveau van beveiliging van LI-gegevens:

> *"De maatregelen dienen bij te dragen aan het doel van het besluit, te weten het bewerkstelligen van een minimumniveau van beveiliging."*[57]

Ook blijkt uit de nota van toelichting duidelijk dat de wetgever als doel heeft de beveiliging van LI-gegevens en het voorkomen van een inbreuk op de vertrouwelijkheid daarvan. Zie

> *"Het is evident dat in beide gevallen de desbetreffende gegevens en informatie een uiterst gevoelig karakter hebben. Indien de gegevens bekend zouden worden met betrekking tot wie een taplast is afgegeven, komt – al naar gelang het doel waarvoor de taplast is afgegeven – het welslagen van een strafrechtelijk onderzoek of de veiligheid van de staat in ernstige mate in het geding. Dit geldt evenzeer voor de informatie die benodigd is om een taplast op te kunnen stellen;*
> *ook dan wordt immers kenbaar wie in het belang van het strafrechtelijk onderzoek of de veiligheid van de staat de aandacht van de met opsporing en vervolging van strafbare feiten belaste autoriteiten onderscheidenlijk de Algemene Inlichtingen- en*

[57] *Stb.* 2003, 472, p. 9.

> *Veiligheidsdienst (AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft. Het is dan ook noodzakelijk dat ter zake van de hier bedoelde gegevens en informatie wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen en, voor zover een dergelijke inbreuk wel plaats heeft gevonden, in maatregelen waarmee op een snelle en adequate wijze daarop kan worden gereageerd."(onderstreping JZ)*[58]

In de nota van toelichting wordt benadrukt dat het noodzakelijk is dat ter zake van de LI-gegevens wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen.[59] Daaruit vloeit logischerwijs voort dat de te treffen beveiligingsmaatregelen aan moeten sluiten bij de huidige stand van de techniek.

Op grond van deze artikelen dienen LI-systemen logisch deugdelijk beveiligd te zijn en zodanig te zijn ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat hierop tijdige interventie plaatsvindt.

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 2 van het Bbgt in samenhang met artikel V van de bijlage van het Bbgt.

De toezichthouder heeft bij Vodafone drie LI-systemen aangetroffen, te weten het [VERTROUWELIJK] . Deze systemen bevatten LI-gegevens en worden door Vodafone gebruikt bij het bevoegd aftappen in de zin van artikel 13.2 van de Tw. De toezichthouder heeft daarom de logische deugdelijke beveiliging van deze systemen onderzocht.

Voor de volledige beschrijving van de inrichting van het LI-proces bij Vodafone verwijs ik naar paragraaf 5.2.4 van dit besluit en naar paragraaf 4.2 van het Rvb.

Hieronder volgen de feiten zoals die door de toezichthouder zijn vastgesteld, per onderdeel van artikel V van de bijlage bij het Bbgt.

a. Deugdelijke beveiliging, onder meer door persoonsgebonden authenticatie

Artikel V, onder a, van de bijlage bij het Bbgt vereist dat Vodafone een deugdelijke toegangsbeveiliging van geautomatiseerde informatiesystemen heeft, onder meer door middel van persoonsgebonden authenticatie.

De nota van toelichting bij het Bbgt zegt hierover het volgende.

> *"In onderdeel V, onder a, is bepaald dat de beveiliging van geautomatiseerde informatiesystemen onder meer door middel van persoonsgebonden authenticatie dient plaats te vinden. Authenticatie is erop gericht vast te stellen of de betrokkene*

[58] *Stb.* 2003, 472, p. 7.
[59] *Stb.* 2003, 472, p. 7.

> *rechtmatig toegang heeft tot het systeem; uit de eis dat deze persoonsgebonden dient te zijn, vloeit voort dat deze altijd herleidbaar dient te zijn tot een identificeerbare persoon. Voor authenticatie kan bijvoorbeeld gebruik gemaakt worden van een PKI (Public Key Infrastructure)-mechanisme."*[60]

Uit de nota van toelichting volgt dat persoonsgebonden authenticatie erop is gericht om vast te stellen of de betrokkene rechtmatig toegang heeft tot het systeem en dat uit de eis dat deze persoonsgebonden dient te zijn voortvloeit dat deze altijd herleidbaar dient te zijn tot een identificeerbare persoon.

6.6.1 Niet-persoonsgebonden authenticatie

De toezichthouder heeft vastgesteld dat op elk van de drie onderzochte LI-systemen van Vodafone ingelogd kon worden door middel van niet persoonsgebonden accounts.

Het [VERTROUWELIJ]*-systeem*
De toezichthouder heeft vastgesteld dat een werknemer van een van de twee leveranciers van het [VERTROUWELIJ]-systeem via de Commandline interface 'Secure Shell' (hierna: SHH) ongelimiteerde toegang had tot LI-gegevens. Op dit systeem kon ingelogd worden met twee niet-persoonsgebonden accounts. Via een van die twee groepsaccounts kon de medewerker van leverancier [VERTROUWELIJK] rootgebruiker worden.[61] Ook negen medewerkers van [VERTROUWELIJK] konden op dezelfde wijze rootgebruiker worden op het [VERTROUWELIJ]-systeem.[62]

Wanneer iemand rootrechten heeft, de meest verstrekkende rechten op een Linux-server, kan diegene de gehele server naar zijn hand zetten, waaronder het vinden van de wachtwoordsleutel die de database met de aanwezige LI-gegevens kan ontsleutelen.[63]

Het [VERTROUWELIJK]*-systeem*
Het [VERTROUWELIJK]-systeem is uitbesteed aan en wordt tweedelijns beheerd door de onderneming [VERTROUWELIJK]Ten behoeve van eerstelijnssupport worden het inloggen en aflezen van storingen uitgevoerd door [VERTROUWELIJK]. De [VERTROUWELIJK]-medewerker maakte hiervoor gebruik van een niet-persoonsgebonden account, oftewel een groepsaccount, op het [VERTROUWELIJK]-systeem.[64] Ook voor het tweedelijnsbeheer werd door medewerkers van [VERTROUWELIJK] ingelogd met een niet-persoonsgebonden account, oftewel een groepsaccount.[65]

[60] *Stb.* 2003, 472, p. 10.
[61] Zie paragraaf 4.3.3. van het Rvb.
[62] Rvb, p. 30.
[63] Zie voor meer details het Rvb, paragraaf 4.3.1, 4.3.3 en 4.3.5.
[64] Rvb paragraaf 4.3.4, p. 38.
[65] Rvb, p. 39.

Het [VERTROUWELIJK] *-systeem*
De toezichthouder heeft vastgesteld dat een medewerker van [VERTROUWELIJK] via de 'graphical user interface' (GUI) kon inloggen met twee niet-persoonsgebonden accounts.[66] Ook heeft de toezichthouder vastgesteld dat een medewerker van [VERTROUWELIJK] vanaf de 'Secure Shell' kon inloggen met een niet-persoonsgebonden account. Via dit groepsaccount kon de medewerker zichzelf op twee servers van het [VERTROUWELIJK]-systeem rootrechten, de meest verstrekkende rechten op een Linux-systeem, toekennen.[67]

Op grond van bovenstaande stel ik vast dat op elk van de drie LI-systemen van Vodafone ingelogd kon worden door middel van niet-persoonsgebonden accounts. Dat maakt reeds dat de toegang tot geautomatiseerde systemen waarin LI-gegevens worden verwerkt niet op deugdelijke wijze is beveiligd. Dit levert een overtreding op van artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder a, Bijlage Bbgt.

6.6.2 Deugdelijke beveiliging schoot ook op andere punten tekort

De toezichthouder heeft vastgesteld dat de beveiliging van de LI-systemen ook op andere punten tekort schoot. Naast het ontbreken van persoonsgebonden authenticatie als toegangsbeveiliging voor de LI-systemen van Vodafone, ontbraken ook overige maatregelen in het kader van de toegangsbeveiliging van de LI-systemen, zoals artikel 2 Bbgt in samenhang gelezen met artikel V, onder a van de Bijlage bij het Bbgt vereist, of was er sprake van verouderde beveiligingsstandaarden.

In mijn voornemen ben ik uitgegaan van internationaal breed erkende en geaccepteerde standaarden voor logische toegangsbeveiliging van informatiesystemen en -netwerken.[68] Deze standaarden betreffen referentiekaders, welke ruimte bieden voor interpretatie en toepassing in een specifiek beveiligingssysteem. Op welke wijze een aanbieder invulling geeft aan deze normen, staat haar vrij. De aanbieder heeft daarbij vrijheid om deze kaders toe te passen op een wijze die past bij de door haar gebruikte LI-systemen. Echter is het resultaat duidelijk voorgeschreven, namelijk het behalen van het niveau van beveiliging dat het Bbgt vereist. Daarbij is van belang op te merken dat van een professionele marktpartij mag worden verwacht dat zij op de hoogte is van de geldende wet- en regelgeving en zich daaraan houdt. Ook mag van haar worden verwacht dat zij op de hoogte is van de laatste stand van de techniek en deze

[66] Rvb, p. 44.
[67] Rvb, p. 44.
[68] Standaarden voor de inrichting van versleuteling, waaronder de Special Publication 800-52 Revision 2 van het National Institute of Standards and Technology, een wetenschappelijke overheidsinstelling uit de Verenigde Staten die onder meer standaarden in de (informatie)technologie voorschrijft en de standaarden van KeePass, een internationaal geaccepteerde en gerenommeerde wachtwoordkluis die eveneens een standaard hanteert voor versleuteling en wat betreft netwerkzonering de internationaal breed geaccepteerde standaard Special Publication 800-215 Revision 2 van het National Institute of Standards and Technology.

toepast als dat nodig is. Of een aanbieder het op grond van het Bbgt vereiste resultaat heeft bereikt, is aan handhaving onderhevig.

Uit voormelde standaarden volgt dat een adequate beveiliging bestaat uit een aantal essentiële onderdelen, zoals versleuteling van gegevens (encryptie), deugdelijke wachtwoordbeveiliging, netwerkzonering en het tijdig uitvoeren van updates, welke oplossingen voor ontdekte kwetsbaarheden in de beveiliging kunnen bevatten.

In de paragrafen hieronder volgt op welke punten de toegangsbeveiliging van Vodafone tekortschoot.

6.6.2.1 Verouderde versleutelingstechnieken

De toezichthouder heeft vastgesteld dat het [VERTROUWELIJK]-systeem gebruik maakt van versleutelingstechnieken die niet meer voldoen aan internationale standaarden.[69] Op het [VERTROUWELIJK]-systeem worden LI-gegevens versleuteld opgeslagen middels [VERTROUWELIJK] -algoritme.[70] Daarmee maakt het [VERTROUWELIJK]-systeem gebruik van een versleutelingstechniek die niet meer voldoet aan internationale standaarden, omdat zij gebruik maakt van een beveiligingsstandaard, te weten de MD5 hash functie, die al in 2008 als onveilig is aangeduid door de internationale gemeenschap.[71] Ruim twaalf jaar lang heeft Vodafone toch nog gebruik gemaakt van deze onveilige standaard.

De toezichthouder heeft geconstateerd dat binnenkomende tapverzoeken op de MSDR-webserver middels protocollen TLSv1.2, TLSv1.1 en TLSv1 versleuteld konden worden. In onder meer de hiervoor genoemde Special Publication 800-52 Revision 2 van NIST is het gebruik van zowel TLSv1.1 als TLSv1 als onveilig aangeduid. De standaarden van de NIST zijn door de internationale gemeenschap erkend en aanvaard. Van protocollen die als onveilig zijn aangeduid is bekend dat deze een hiaat in de beveiliging vormen. Het valt Vodafone daarom te verwijten dat zij deze protocollen niet uit haar systemen heeft verwijderd.

De toezichthouder heeft vastgesteld dat beide servers van het [VERTROUWELIJK]-systeem niet tijdig zijn geüpdatet.[72] Voor de frontend-server geldt dat ten tijde van de inspectie de laatste systeemupdate drie jaar en vier maanden geleden was uitgevoerd. De laatste systeemupdate van de [VERTROUWELIJK] dateerde ten tijde van de inspectie van twee jaar en vijf maanden geleden. Systeemupdates dienen regelmatig uitgevoerd te worden, om de beveiliging up-to-date te houden. Het valt Vodafone daarom te verwijten dat zij twee servers met daarop LI-gegevens drie jaar en vier maanden respectievelijk twee jaar en vijf maanden niet

[69] Paragraaf 4.3.5 van het Rvb.
[70] Rvb, p. 45.
[71] Zie bijvoorbeeld: MD5 vulnerable to collision attacks, Carnegie Mellon University, d.d. 31-12-2008, (https://www.kb.cert.org/vuls/id/836068). Zie ook Rvb, p. 45.
[72] Rvb, p. 45 en 46.

geüpdatet heeft. Hierdoor was de beveiliging van haar systemen niet up-to-date en werden oplossingen voor eventuele ontdekte kwetsbaarheden in de beveiliging niet doorgevoerd.

De toezichthouder heeft vastgesteld dat de [VERTROUWELIJK] van het [VERTROUWELIJK]-systeem het gebruik van TLS versies TLSv1 en TLSv.1.1 toestaat. Deze protocollen zijn internationaal als onveilig aangeduid in 2011 respectievelijk 2019.[73] Het aanwezig hebben van onveilige protocollen in een LI-systeem van Vodafone verhoogt de kans op ongeoorloofde toegang tot LI-gegevens. Daarbij is niet relevant dat deze protocollen niet standaard worden gebruikt. Het beveiligingsrisico schuilt in het *kunnen* gebruiken van deze protocollen. Het ligt daarom op de weg van Vodafone om deze onveilige protocollen uit haar LI-systemen te verwijderen. Dit heeft Vodafone echter nagelaten, waardoor er een grotere kans was op ongeautoriseerde toegang tot haar LI-systemen.

6.6.2.2 Zwakke wachtwoordkwaliteit en versleuteling

Artikel V, onder a van de bijlage bij het Bbgt vereist deugdelijke toegangsbeveiliging van LI-systemen. Accounts waarmee toegang verkregen kan worden tot een LI-systeem dienen derhalve deugdelijk beveiligd te zijn, onder meer door middel van een kwalitatief sterk wachtwoord. De kwaliteit van het wachtwoord en de frequentie waarmee dit wachtwoord wordt gewijzigd, zijn voor de deugdelijkheid van de beveiliging van LI-systemen bepalend.

Een aanbieder heeft de vrijheid om een eigen invulling te geven aan de wijze waarop zij invulling geeft aan de te nemen beveiligingsmaatregelen die volgen uit het Bbgt. De toezichthouder neemt dan ook de door de aanbieder getroffen maatregelen als uitgangspunt voor het toezicht.

Vodafone maakt gebruik van KeePass als wachtwoordmanager. De toezichthouder heeft de wachtwoordkwaliteit van de wachtwoorden die gebruikt werden voor de groepsaccounts die toegang geven aan de LI-systemen van Vodafone daarom getoetst aan normen die KeePass, een wachtwoordmanager, hanteert.

De toezichthouder heeft vastgesteld dat de wachtwoorden die gebruikt worden voor de onderzochte groepsaccounts om in te loggen op het [VERTROUWELIJ]-systeem, het [VERTROUWELIJK]-systeem en het [VERTROUWELIJK]-systeem zijn aangemerkt als 'zeer zwak' door KeePass. Ook is vastgesteld dat het wachtwoord voor een groepsaccount waarmee ingelogd kon worden op het [VERTROUWELIJK]-systeem op het moment van onderzoek zes jaar en vier maanden niet is gewijzigd.

Het risico op ongeautoriseerde toegang van informatiesystemen is sterk aanwezig, nu er gebruik is gemaakt van zwakke wachtwoorden, die niet frequent werden gewijzigd in combinatie met het gebruik van groepsaccounts, waardoor de

[73] Rvb, p. 46, derde bulletpoint.

gebruikte wachtwoorden bij meerdere personen kenbaar waren, tezamen met de vaststelling dat een groot aantal personen inlogpogingen kon doen op de LI-systemen van Vodafone, zoals is vastgesteld in paragraaf 6.4.

6.6.2.3 Netwerkzonering en onversleutelde overdracht van LI-gegevens

De toezichthouder heeft vastgesteld dat de systemen [VERTROUWELIJ] en [VERTROUWELIJK] in hetzelfde netwerksegment zitten. Er is dus geen netwerkzonering toegepast. Hierdoor kunnen beheerders van de leverancier [VERTROUWELIJK] inlogpogingen doen op het [VERTROUWELIJ]-systeem van Vodafone en vice versa.[74] Voor het [VERTROUWELIJK]-systeem geldt dat er wel een hostbased firewall aanwezig is. Deze firewall staat echter toe dat verbinding wordt gemaakt tussen het [VERTROUWELIJ]-systeem en het [VERTROUWELIJK]-systeem.[75] Hieruit volgt dat personen met toegang tot een van deze systemen ook inlogpogingen konden doen op het andere systeem.

De toezichthouder heeft vastgesteld dat er onversleutelde LI-gegevens verstuurd worden tussen het [VERTROUWELIJK] en het [VERTROUWELIJK]-systeem van Vodafone. Dit maakt het mogelijk dat een ieder met fysieke toegang tot de bekabeling van deze onversleutelde LI-verbinding van het zogeheten [VERTROUWELIJK], die liep tussen [VERTROUWELIJK] , deze gegevens kon afvangen.[76] Ook kon onderschepping via een [VERTROUWELIJK] van netwerkswitches plaatsvinden. Vodafone heeft desgevraagd verklaard dat 72 personen toegang hadden tot deze [VERTROUWELIJK]

In een eerder RDI onderzoek van 2020 tot 2021 naar de NL-Alertdienst van Vodafone is door de toezichthouder gewaarschuwd voor het risico van overdracht over onversleutelde verbindingen.[79] Vodafone heeft dit risico verholpen door versleuteling aan te brengen alvorens de gegevens over de onversleutelde [VERTROUWEL verbinding worden verzonden.[80] Deze maatregel is door Vodafone echter niet voor de LI-keten genomen.

Uit het voorgaande volgt dat de LI-gegevens die verstuurd werden tussen het [VERTR -systeem en het [VERTROUWELIJK]-systeem van Vodafone onversleuteld verzonden werden. Deze verbinding is te onderscheppen op [VERTROUWELIJK] Deze functionaliteit is te gebruiken door 72 personen. Hierdoor was het voor deze 72 personen mogelijk om toegang te krijgen tot onversleutelde LI-gegevens. Deze gegevens zijn daarom niet deugdelijk beveiligd, in de zin van artikel V, onder a van de bijlage bij het Bbgt.

---

[74] Rvb, p. 32.
[75] Rvb, p. 40 en bijlage 10.
[76] Rvb, p. 46.
[77] [VERTROUWELIJK]

[78] List of users with RW access to switches 2022.xlsx.
[79] 20210317 – Gespreksverslag NL-Alert VodafoneZiggo IP-Infra V1.0.docx.
[80] RE_ _External_Definitieve gespreksverslag 24 maart 2021.msg.

6.6.3 Tussenconclusie

Op grond van bovenstaande stel ik vast dat op elk van de drie LI-systemen van Vodafone ingelogd kon worden door middel van niet-persoonsgebonden accounts. Ook stel ik op grond van bovenstaande vast dat overige beveiligingsmaatregelen ten aanzien van de logische beveiliging van de drie LI-systemen tekortschoten.

Ik stel daarom vast dat Vodafone artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder a van de Bijlage van het Bbgt heeft overtreden.

b. Blokkering bij drie foutieve inlogpogingen

Artikel V, onder c Bijlage Bbgt vereist dat het aantal foutieve inlogpogingen is beperkt tot drie. Overschrijding van het aantal foutieve inlogpogingen moet leiden tot definitieve blokkering, die uitsluitend door de functionaris, als bedoeld in onderdeel I van de Bijlage, kan worden opgeheven.

De toezichthouder heeft vastgesteld dat zowel het [VERTROUWELIJK] - als het [VERTROUWELIJK] [83]-systeem een onbeperkt aantal foutieve inlogpogingen toestaan. Het aantal foutieve inlogpogingen is dus niet beperkt tot drie. Er vond geen blokkering plaats.

Ik stel daarom vast dat Vodafone artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt van het Bbgt in samenhang gelezen met artikel V, onder c van de bijlage bij het Bbgt heeft overtreden.

c. Detectie van ongeautoriseerde toegang en pogingen daartoe

Artikel V, onder b Bijlage Bbgt vereist dat de logische beveiliging zodanig is ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

Aan het vereiste uit artikel V, onder b Bijlage Bbgt kan voldaan worden door (ongeautoriseerde) inlogpogingen extern te registreren, door bijvoorbeeld een (geautomatiseerde) lijst aan te leggen met de voor de inlogpoging gebruikte ip-adres, gebruikersnaam en tijd/datum. Vervolgens dient de registratie (geautomatiseerd) gecontroleerd te worden, aan de hand van een lijst van geautoriseerde gebruikers, waarbij de gebruikte gebruikersnaam wordt afgezet tegen geautoriseerde gebruikersnamen. Deze registratie en opvolging daarvan dient direct plaats te vinden op een extern systeem of door middel van een andere organisatorische maatregel. Het doel hiervan is om te voorkomen dat bij ongeautoriseerde toegang de registratie van de ongeautoriseerde toegang direct

[81] Rvb, p. 32.
[82] Rvb, p. 41.
[83] Rvb, p. 47.

verwijderd kan worden door degene die ongeautoriseerde toegang heeft verkregen.

De toezichthouder heeft vastgesteld dat er voor het [VERTROUWELIJ]-systeem[84], het [VERTROUWELIJK]-systeem[85] en het [VERTROUWELIJK]-systeem[86] geen enkele vorm van externe logging is geactiveerd. Ook vond er geen detectie plaats op logging ten aanzien van ongeautoriseerde toegang en pogingen daartoe.[87] Hierdoor konden foutieve inlogpogingen niet worden opgemerkt en in het geval van een dergelijke poging kon evenmin een tijdige interventie plaatsvinden.

Ik stel op grond van bovenstaande vast dat Vodafone artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder b Bijlage Bbgt heeft overtreden.

d. Persoonsgebonden logging en detectie

Artikel V, onderdeel e Bijlage Bbgt vereist dat alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem persoonsgebonden worden vastgelegd teneinde onderzoek mogelijk te maken.

Uit het onderzoek van de toezichthouder blijkt dat handelingen met betrekking tot LI-gegevens op het [VERTROUWELIJ]-systeem[88], het [VERTROUWELIJK]-systeem[89] en het [VERTROUWELIJK] systeem[90] konden worden uitgevoerd met groepsaccounts. De toezichthouder heeft vastgesteld dat op het [VERTROUWELIJ]-systeem, het [VERTROUWELIJK]-systeem en het [VERTROUWELIJK]-systeem van Vodafone alleen lokale registratie in de vorm van logging aanwezig is.[91]

Voor handelingen met betrekking tot de verwerking van LI-gegevens is geen enkele vorm van externe logging geactiveerd. Lokale registratie in de vorm van logging is per definitie onbetrouwbaar, omdat gebruikers met administrator-rechten of rootrechten eigenstandig en ongedetecteerd hun handelingen ten aanzien van LI-gegevens in de loghistorie kunnen aanpassen of verwijderen. Dit levert temeer een risico op, gezien het door de toezichthouder vastgestelde feit dat gebruikers van groepsaccounts van het [VERTROUWELIJK]-systeem- en het [VERTROUWELIJ]-systeem zichtzelf rootrechten kunnen toekennen en gebruikers van groepsaccounts van het [VERTROUWELIJK]-systeem administratorrechten.

[84] Rvb, p. 32 en bijlage 6.
[85] Rvb, p. 40.
[86] Rvb, p. 47.
[87] Respectievelijk paragraaf 4.3.3, 4.3.4 en 4.3.5 van het Rvb.
[88] Rvb, p. 30.
[89] Rvb, p. 39.
[90] Rvb, p. 44.
[91] Zie respectievelijk paragraaf 4.3.3., 4.3.4 en 4.3.5 van het Rvb.

Ik stel op grond van bovenstaande vast dat de LI-systemen van Vodafone niet voldoen aan de vereisten van artikel V, onder e Bijlage Bbgt. Ik stel dan ook vast dat Vodafone artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder e Bijlage Bbgt heeft overtreden.

6.6.4 Duur van de overtreding

Wat betreft de duur van de overtreding overweeg ik als volgt.

Uit een verslag van een gesprek tussen de toezichthouder en Vodafone, dat heeft plaatsgevonden op 14 juni 2022, blijkt dat er nog groepsaccounts aanwezig zijn om in te loggen op het [VERTROUWELIJK]-systeem en groepsaccounts waarmee wordt ingelogd op het [VERTROUWELIJ]-systeem van Vodafone.[92]

Op 27 oktober 2022 heeft mijn toezichthouder van Vodafone een brief ontvangen via het infoportaal, met onderwerp Status aanpassingen Vodafone n.a.v. inspectie Agentschap Telecom.[93] In de bijlage bij deze brief staat een overzicht van de door Vodafone gemaakte aanpassingen.[94] Hieruit volgt dat het LI-team van Vodafone met de invoering van [VERTROUWELIJK] actie heeft ondernomen om alle groepsaccounts op te schonen. Voor het [VERTROUWELIJK]- en het [VERTROUWELIJK]-systeem is deze wijziging reeds doorgevoerd in november/december 2021. Vanwege technische ondersteuningsredenen was voor aanpassing van het [VERTROUWELIJ] systeem meer tijd nodig, ter waarborging van de continuïteit. Uit deze statusupdate blijkt niet dat en/of op welk moment er voor toegang tot het [VERTROUWELIJ] account geen groepsaccounts meer worden gebruikt. Ik trek hieruit de conclusie dat er voor het inloggen op het [VERTROUWELIJ]-systeem nog groepsaccounts aanwezig zijn. het verslag van 14 juni 2022, waarin staat dat er voor het [VERTROUWELIJ]-systeem nog wel groepsaccounts gebruikt worden.[95]

Concluderend overweeg ik dat het gebruik van groepsaccounts voor de LI-systemen [VERTROUWELIJK] en [VERTROUWELIJK] per november/december 2021 is beëindigd door Vodafone. Voor het inloggen op het [VERTROUWELIJ]-systeem zijn nog wel groepsaccounts aanwezig.

Wat betreft de duur van de overtreding overweeg ik daarom als volgt. Indien er met een groepsaccount toegang kan worden verkregen tot een geautomatiseerd informatiesysteem dat LI-gegevens bevat, is er sprake van een overtreding van artikel V, onder a van de bijlage van het Bbgt. Hoewel Vodafone deze overtreding ten aanzien van twee LI-systemen heeft beëindigd, waren er op het [VERTROUWELIJ]-systeem gedurende het onderzoek van de toezichthouder nog groepsaccounts aanwezig. Daarmee is de overtreding van artikel V, onder a van de bijlage bij het Bbgt nog niet beëindigd.

[92] Verslag gesprek AT – VZ 14 juni 2022_Def.pdf.
[93] 20221027 Brief Status Aanpassingen VodafoneZiggo.pdf.
[94] 20221026 Status aanpassingen Vodafone.pdf.
[95] Verslag gesprek AT – VZ 14 juni 2022_Def.pdf, onder ad 5 Risicobeheersing autorisatiemanagement, p. 3.

Uit de status update van Vodafone blijkt dat vanaf september 2022 zowel het [VERTROUWELIJK]-systeem, het [VERTROUWELIJ]-systeem en het [VERTROUWELIJK]-systeem met behulp van de gecentraliseerde [VERTROUWELIJK] OS-loggegevens naar de collector opsturen. Dit betekent dat logbestanden extern realtime worden opgeslagen.[96] De overtreding van artikel V, onder e van de bijlage van het Bbgt heeft daarmee tot september 2022 voortgeduurd.

Ik stel daarom op grond van bovenstaande vast dat, overeenkomstig mijn voornemen, de duur van de overtreding van artikel V van de bijlage bij het Bbgt een periode bestrijkt van 5 oktober 2021 tot en met 15 december 2022.

6.6.5 Concluderend

Op grond van bovenstaande stel ik vast dat Vodafone artikel 2, eerste lid, in samenhang met artikel 2, tweede en derde lid en artikel V, onder a, b, c en e van de Bijlage bij het Bbgt heeft overtreden in de periode van 5 oktober 2021 tot en met 15 december 2022.

7. Handhavingsbevoegdheid van de RDI

Ingevolge artikel 15.4, eerste lid, onder j, van de Tw in samenhang met artikel 15.1 van de Tw ben ik bevoegd een bestuurlijke boete op te leggen ter zake van de overtreding van de voorschriften gesteld bij of krachtens artikel 13.2, derde lid en artikel 13.5, vierde lid van de Tw.

Hieronder overweeg ik of het opleggen van een bestuurlijke boete vanwege de geconstateerde overtredingen passend en geboden is. Ik zal hierbij een belangenafweging maken en daarbij alle relevante omstandigheden van het geval beoordelen, waaronder de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten. Ook neem ik hierbij de door Vodafone naar voren gebrachte zienswijze in aanmerking.

8. Aard, ernst en duur van de overtredingen

8.1 Aard en ernst

Volgens hoofdstuk 13 van de Tw zijn aanbieders van openbare telecommunicatie-netwerken en -diensten verplicht hun medewerking te verlenen aan een, kort gezegd, bevoegd gegeven aftapverzoek. De bevoegde autoriteiten verstrekken de aanbieder bij een dergelijk verzoek LI-gegevens die de af te tappen persoon of organisatie identificeren. De wetgever stelt eisen aan de beveiliging van de verstrekte gegevens en informatie. De Memorie van Toelichting zegt daarover:

[96] 20221026 Status aanpassingen Vodafone.pdf, p. 1.

> *"Gegevens betreffende aftappen en informatieverstrekking die in het belang van de staat geheim moeten worden gehouden, zijn formele staatsgeheimen en worden bij de overheid aan een beveiligingsregime onderworpen. Deze gegevens dienen ook bij aanbieders van openbare telecommunicatienetwerken en openbare diensten op gelijkwaardige wijze en op basis van een wettelijke bepaling te worden beveiligd. De gegevens waar het hier om gaat zijn bijvoorbeeld abonneegegevens en het feit dat er een tap geplaatst is."*[97]

Kennisname van LI-gegevens door onbevoegden moet te allen tijde worden voorkomen. Vanwege de zeer gevoelige aard van de LI-gegevens heeft de wetgever in het Bbgt minimumeisen gesteld aan de informatiebeveiliging. Het Bbgt vormt daarmee een uitwerking van de verplichting om gegevens met een buitengewoon gevoelig karakter te beschermen tegen kennisneming door onbevoegden.[98] De artikelen 2, 3, 4 en 8 van het Bbgt en de bijbehorende Bijlage expliciteren de minimumbeschermingsmaatregelen.

De belangen die met deze beschermende maatregelen zijn gemoeid zijn tweeledig. In de eerste plaats is de veiligheid van de Staat het beschermde belang wanneer de taplast afkomstig is van de AIVD of de MIVD. De verstrekte gegevens en informatie betreffen in dit geval bijzondere informatie waarvan de geheimhouding in het belang van de Staat of zijn bondgenoten is geboden. Beveiliging van een dergelijke taplast dient schade aan deze belangen te voorkomen.

In de tweede plaats dient de beveiliging en vertrouwelijkheid van een bijzondere last afkomstig van de Officier van Justitie of een ander hoofd van een opsporingsdienst, het belang van integriteit en doelmatigheid van onderzoeken naar strafbare feiten. Het bevoegd aftappen en opnemen van telecommunicatie vormt een belangrijk element bij de bestrijding van de georganiseerde en zware criminaliteit. Ook voor de opsporing van strafbare feiten is het van cruciaal belang dat de vertrouwelijkheid wordt gewaarborgd van de vanuit de justitieketen verstrekte tapinformatie en -gegevens. Ik verwijs in dit verband naar de volgende passage uit de Nota van Toelichting bij het Bbgt:

> *"Gaat het bij artikel 13.2 Tw om het verlenen van medewerking aan de daadwerkelijke uitvoering van een taplast, bij artikel 13.4 gaat het om de verplichting tot verstrekking van informatie aan de desbetreffende autoriteiten die zij nodig hebben om een dergelijke taplast op te kunnen stellen dan wel een vordering tot het verstrekken van verkeersgegevens te kunnen doen. Het is evident dat in beide gevallen de desbetreffende gegevens en informatie een uiterst gevoelig karakter hebben. Indien de gegevens bekend zouden worden met betrekking tot wie een taplast is afgegeven, komt – al naar gelang het doel waarvoor de taplast is afgegeven – het welslagen van een strafrechtelijk onderzoek of de veiligheid van de staat in ernstige mate in het geding. Dit geldt evenzeer voor de informatie die benodigd is om een taplast op te kunnen stellen; ook dan wordt immers kenbaar*

[97] Kamerstukken II 1996/97, 25 533, nr. 3, p. 125 (MvT).
[98] NvT bij het Bbgt, *Stb. 2003*, 472, p. 9.

wie in het belang van het strafrechtelijk onderzoek of de veiligheid van de staat de aandacht van de met opsporing en vervolging van strafbare feiten belaste autoriteiten onderscheidenlijk de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft. Het is dan ook noodzakelijk dat ter zake van de hier bedoelde gegevens en informatie wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen en, voor zover een dergelijke inbreuk wel plaats heeft gevonden, in maatregelen waarmee op een snelle en adequate wijze daarop kan worden gereageerd."[99]

Gelet op de hiervoor genoemde belangen, is bescherming van vertrouwelijkheid van LI-gegevens van zeer groot belang. Ieder hiaat in de beveiliging, in het bijzonder in het minimumbeveiligingsniveau, vormt een grote bedreiging van de genoemde belangen. Iedere overtreding van het Bbgt doet afbreuk aan de vertrouwelijkheid van LI-gegevens. Het is dan ook noodzakelijk dat wordt voorzien in adequate beveiligingsmaatregelen om een inbreuk te voorkomen op de vertrouwelijkheid van de LI-gegevens en, voor zover een dergelijke inbreuk heeft plaatsgevonden, hierop op een snelle en adequate wijze kan worden gereageerd.

De verplichting om hiervoor te zorgen ligt bij de aanbieder. Ook is de aanbieder verplicht geheimhouding te betrachten met betrekking tot deze gegevens. De aanbieder is zelf verantwoordelijk voor het treffen van de in het Bbgt voorgeschreven beveiligingsmaatregelen.

Mijn toezichthouder heeft vastgesteld, zoals hierboven weergegeven, dat Vodafone diverse van deze beveiligingsmaatregelen niet heeft getroffen. Over de gehele linie van de beveiliging van LI-gegevens, heeft Vodafone nagelaten adequate beveiligingsmaatregelen te treffen. Vodafone had geen beveiligingsplan dat voldoet aan de eisen van het Bbgt, contractueel verplichte afspraken met derden ontbraken, Vodafone heeft niet voorzien in de vereiste beveiligingsmaatregelen ten aanzien van personen die in aanraking komen met LI-gegevens, de logische beveiliging van de geautomatiseerde systemen schoot te kort, als ook de fysieke beveiliging van de ruimtes waarin zich LI-gegevens bevinden.

Door het aantal geconstateerde overtredingen in de gehele LI-keten van Vodafone acht ik het risico dat er ongeoorloofde toegang plaats heeft kunnen vinden groot. Gelet op de hiervoor beschreven risico's en de belangen die gediend worden met de beveiliging van LI-gegevens, maakt dat ik alle omschreven overtredingen zeer ernstig acht. De overtredingen vormen niet alleen op zichzelf, maar zeker in onderlinge samenhang bezien, een zeer groot risico op ongeautoriseerde kennisname van LI-gegevens.

[99] NvT bij het Bbgt, *Stb.* 2003, 472, p. 7.

8.2 Duur overtredingen

In mijn voornemen ben ik wat betreft de duur van de geconstateerde overtredingen uitgegaan van de onderzoeksperiode van de toezichthouder zoals is vastgelegd in het Rvb, te weten de periode van in elk geval 5 oktober 2021 (het begin van het onderzoek door de toezichthouder) tot en met 15 december 2022.

Ik heb daarbij overwogen dat van zwaarwegend belang is dat Vodafone geen weet had van deze overtredingen, terwijl Vodafone op grond van het Bbgt wel de verantwoordelijkheid heeft om de overtredingen te voorkomen en geacht wordt daarvan op de hoogte te zijn. Daarmee kwalificeren de overtredingen naar mijn oordeel als systeemfouten die geen incidenteel karakter hebben, maar die voor langere tijd en in ieder geval ruim een jaar hebben voortgeduurd.

9. Verwijtbaarheid

Als gevolg van de geconstateerde overtredingen had Vodafone, in de periode van in ieder geval 5 oktober 2021 tot en met 15 december 2022, onvoldoende dan wel ontoereikende maatregelen getroffen ter beveiliging tegen onbevoegde kennisneming en geheimhouding van LI-gegevens. Van Vodafone als aanbieder van openbare telecommunicatiediensten en netwerken mag verwacht worden dat zij op de hoogte is van de geldende wet- en regelgeving en dat zij zorg draagt voor de naleving daarvan. Daarbij weeg ik zwaar mee dat tijdens het onderzoek meermaals is gebleken dat Vodafone zich niet bewust was van de geconstateerde overtredingen. Dit beeld werd versterkt door het feit dat in de overeenkomsten die Vodafone met haar leveranciers heeft gesloten nergens een concrete invulling is gegeven aan de verplichtingen uit het Bbgt, terwijl de verplichting om daarvoor zorg te dragen expliciet in het Bbgt is voorgeschreven. De geconstateerde overtredingen zijn dan ook aan Vodafone te verwijten.

10. Zienswijze Vodafone

Bij brief van 26 juli 2023 heb ik Vodafone in kennis gesteld van mijn voornemen tot het opleggen van een bestuurlijke boete wegens de geconstateerde overtredingen (Voornemen). Vodafone is in de gelegenheid gesteld naar aanleiding hiervan mondeling dan wel schriftelijk een zienswijze naar voren te brengen.

Vodafone heeft op 8 november 2023 een schriftelijke zienswijze gegeven op mijn voornemen om aan haar een bestuurlijke boete op te leggen wegens overtreding van de artikelen 2, 3, 4 en 8 van het Bbgt en de bijbehorende Bijlage en op mijn voornemen om dit besluit te publiceren. Daarnaast heeft Vodafone tijdens de hoorzitting van 29 november 2023 een aanvullende zienswijze gegeven. Vodafone heeft daarbij pleitaantekeningen verstrekt van de door haar voorgedragen zienswijze.

Vodafone betwist primair de overtredingen en meent daarnaast dat het opleggen van een boete niet opportuun is. Subsidiair stelt Vodafone zich op het standpunt dat de voorgenomen boetehoogte disproportioneel is.

Overkoepelend benadrukt Vodafone dat de beveiliging van LI-data voor haar zeer belangrijk is. Zij hecht eraan om op deugdelijke wijze uitvoering te geven aan de beveiligingseisen die in dit verband zijn neergelegd in het Bbgt. Vodafone heeft daarom meegewerkt aan het onderzoek en wijzigingen in de beveiliging van de LI-gegevens op aanwijzen van de inspecteur doorgevoerd. Hierbij benadrukt Vodafone dat RDI vooraf geen guidance heeft gegeven hoe de RDI wenst dat aanbieders invulling geven aan de open normen uit het Bbgt. Vodafone is van mening dat bij gebrek aan guidance niet over kan worden gegaan tot handhaving, voordat RDI kenbaar heeft gemaakt welke specifieke eisen er aan de beveiliging worden gesteld.

Verder voert Vodafone aan dat zij op 26 oktober 2022 een voorlopige feitenverificatie heeft gedeeld met de toezichthouder, waarin verschillende onjuistheden in het Rapport van bevindingen zijn aangewezen. Hierbij verwijst zij naar bijlage 1 van de zienswijze. Vodafone stelt dat de toezichthouder deze feitenverificatie niet heeft meegenomen in haar beoordeling en verzoekt dat alsnog te doen in de nu voorliggende besluitvorming.

Vodafone voert daarnaast aan dat RDI geen sanctiebeleid heeft en dat de voorgenomen boetehoogte op onnavolgbare wijze afwijkt van de vastgestelde boetehoogte bij een vergelijkbare sanctie. Volgens Vodafone bestond er bovendien geen aanleiding voor RDI om een onderzoek te starten. Er heeft zich volgens Vodafone, in tegenstelling tot bij een vergelijkbare sanctie aan een andere partij, bijvoorbeeld geen incident bij Vodafone voorgedaan.

Vodafone voert aan dat de feitelijke motivering van de overtredingen gebrekkig is, en bovendien onjuiste aannames bevatten. Hierdoor wordt de ernst van de overtredingen overschat.

Ik bespreek de zienswijze van Vodafone in de hiernavolgende paragrafen.

10.1 Duidelijkheid normen

Vodafone voert, kort en zakelijk weergegeven, aan dat RDI niet tot handhavend optreden had mogen besluiten, vanwege de aard van de normen uit het Bbgt en de (voorzienbaarheid van de) uitleg die RDI daaraan geeft. Vodafone stelt in dat verband voorop dat het Bbgt bedoeld is als minimumset maatregelen. De uitwerking en implementatie daarvan is volgens Vodafone aan de aanbieder zelf voorbehouden. Het is volgens Vodafone aan RDI als toezichthouder om vervolgens te beoordelen of is voldaan aan de minimumset. Daarvoor dient RDI volgens Vodafone guidance te geven. Zonder die guidance kan volgens Vodafone niet tot handhaving worden overgegaan. Omdat RDI volgens Vodafone geen guidance heeft gegeven over de invulling die volgens RDI aan de minimumeisen uit het

Bbgt dient te worden gegeven, terwijl RDI volgens Vodafone nieuwe, specifieke beveiligingseisen voor LI-data zou introduceren, kan Vodafone zich niet verenigen met het voornemen om handhavend op te treden. Vodafone stelt dat dit voor haar onvoldoende voorzienbaar was.

Vodafone geeft verder aan dat de toezichthouder de door haar op 26 oktober 2022 gedeelde voorlopige feitenverificatie niet heeft meegenomen in de beoordeling en verwijst daarbij naar bijlage 1 van de door haar gegeven zienswijze.

Mijn reactie
In reactie op de stellingen van Vodafone stel ik voorop dat RDI bevoegd is om handhavend op te treden tegen overtredingen van de Tw en de normen uit het Bbgt. Artikel 2, eerste lid, Bbgt, bepaalt in dat verband dat aanbieders moeten zorgdragen voor het treffen van alle noodzakelijke beveiligingsmaatregelen om kennisneming door onbevoegden te voorkomen van de in die bepaling opgenomen gegevens en informatie. Het tweede lid bepaalt vervolgens waaruit de maatregelen als bedoeld in het eerste lid ten minste dienen te bestaan. In het derde lid is voorts bepaald dat tot de maatregelen, bedoeld in het eerste en tweede lid, in ieder geval de maatregelen worden gerekend die in de bijlage bij het Bbgt zijn opgenomen.

In de bijlage bij het Bbgt is zeer uitvoerig en per onderdeel uiteengezet welke maatregelen aanbieders in ieder geval dienen te treffen. RDI meent dan ook dat een professionele marktdeelnemer als Vodafone wist, of in ieder geval behoorde te weten wat van haar werd verwacht ten aanzien van de te treffen beveiligingsmaatregelen met betrekking tot LI-gegevens. RDI heeft hiervoor vastgesteld dat Vodafone hier niet aan heeft voldaan. RDI heeft immers vijf overtredingen van het Bbgt, over alle lagen van de interne organisatie vastgesteld. De bevindingen van RDI laten zien dat Vodafone de minimumbeveiligingseisen volstrekt niet op orde had. Dat Vodafone de invulling die RDI geeft aan de normen uit het Bbgt niet voldoende duidelijk vindt, acht RDI gezien het voorgaande dan ook niet overtuigend: uit (de bijlage bij) het Bbgt blijkt klip-en-klaar welke maatregelen Vodafone minimaal diende te treffen.

Voor zover al sprake zou zijn van open normen, merk ik op dat zelfs het enkele feit dat er open normen zouden zijn, op zich niet maakt dat die normen onduidelijk zijn en al helemaal niet dat beboeting van die normen een schending van het lex certa-beginsel oplevert.[100]

> *"5.4 Het College overweegt verder dat de wetgever goede redenen kan hebben om zich van algemene termen te bedienen (zie de uitspraak van het College van 21 mei 2019, ECLI:NL:CBB:2019:207). In dit verband dient de vraag of een wettelijk voorschrift voldoet aan het lex certa-beginsel mede te worden bezien in het licht van wat de bedoeling van de wetgever met het wettelijk voorschrift is geweest. (…)*

[100] CBb 23 maart 2021, ECLI:NL:CBB:2021:324, r.o. 5.2-5.5.

> *5.5 (…) Zoals de rechtbank terecht heeft overwogen, dient appellante als professioneel pluimveehouder, die wordt bijgestaan door haar dierenarts en een bedrijfsvoorlichter, in staat te zijn om te bepalen welke maatregelen voor haar bedrijfsvoering passend zijn, zodat het dierenwelzijn in stal 4 wordt verbeterd. Anders dan appellante stelt, betekent dit niet dat zij te allen tijde moet voorkomen dat haar dieren ziek worden, maar veeleer dat zij, nadat een dierenarts van de NVWA haar gegevens heeft verstrekt die wijzen op slechte dierenwelzijnsomstandigheden, alert reageert en al naar gelang de omstandigheden op haar bedrijf de maatregelen neemt die nodig zijn om het dierenwelzijn te verbeteren. Daarbij neemt het College tot uitgangspunt dat de passende maatregelen ter verbetering van de dierenwelzijnsomstandigheden moeten resulteren in ten minste een zodanig niveau van dierenwelzijn dat een toezichthoudend dierenarts van de NVWA geen aanleiding vindt voor de conclusie dat sprake is van slechte dierenwelzijnsomstandigheden (waarvoor blijkens de hiervoor onder 5.3 geciteerde Nota van Toelichting indicaties onder meer bestaan uit abnormale niveaus van contactdermatitis, parasitisme en systemische ziektes). Het College is gelet op het voorgaande met de rechtbank van oordeel dat de verplichting van artikel 2.53, eerste lid, van het Besluit een resultaatsverplichting inhoudt en dat van strijd met het lex certa-beginsel geen sprake is."*

Daarbij is van belang op te merken dat van een professionele marktdeelnemer zoals Vodafone mag worden verwacht dat zij op de hoogte is van de geldende wet- en regelgeving en dat zij zich daaraan houdt.

Ik merk hierbij op dat Vodafone niet duidelijk maakt waarom de aan de orde zijnde normen voor haar onduidelijk zouden zijn geweest en welke interpretatie daaraan volgens haar gegeven moest worden. Ook hierom gaan de stellingen van Vodafone niet op. Voor zover Vodafone in haar zienswijze deze stelling wel nader concretiseert, ga ik daar in de hiernavolgende paragrafen verder op in.

Uit bovenstaande volgt de conclusie dat de schending van de normen uit het Bbgt een voorzienbare overtreding van het Bbgt oplevert. Voor zover Vodafone een zienswijze heeft gegeven over door mij aangehaalde normen in relatie tot een specifieke overtreding van het Bbgt, ga ik, indien nodig, daar in hiernavolgende paragrafen verder op in.

In reactie op het standpunt van Vodafone dat ik de door haar aangedragen feitenverificatie niet heb meegenomen in de definitieve versie van het Rvb overweeg ik het volgende. Ik volg Vodafone niet in dit standpunt. Desgevraagd heeft de toezichthouder bevestigd kennis te hebben genomen van de voorlopige feitenverificatie concept Rapport van bevindingen.[101] De door Vodafone aangedragen wijzigingen vormden voor de toezichthouder geen aanleiding om het Rvb te wijzigen, nu de vaststelling van de feiten door de toezichthouder heeft plaatsgevonden naar aanleiding van eigen constateringen. Een enkele ontkenning door Vodafone doet hier niet aan af.

[101] 20220930 [AT] T[VFZ] O[Concept rapport van bevindingen – Inspectie Bevoegd Aftappen Vodafone Libertel B_V_.msg.

10.2 Ondeugdelijk beveiligingsplan

In haar zienswijze merkt Vodafone, kort en zakelijk weergegeven, op dat zij een beveiligingsplan heeft. Daarnaast stelt Vodafone dat zij ten aanzien van het beveiligingsplan niet de cautie heeft gekregen van de toezichthouder. Voorts wijst Vodafone erop dat zij in overleg met de toezichthouder stappen zou hebben gezet om een nieuw beveiligingsplan te maken. De toezichthouder zou hierover volgens Vodafone hebben geconcludeerd dat het plan er veelbelovend is en dat de juiste route is ingeslagen. De feitelijke gang van zaken rond de aanpassing van het beveiligingsplan blijkt niet uit het voornemen. Vodafone stelt zich op het standpunt dat het gezien de bereidheid van Vodafone tot verandering in de rede had gelegen dat RDI zou afzien van handhaving.[102]

Subsidiair stelt Vodafone zich op het standpunt dat ik ten onrechte vaststel dat het beveiligingsplan van Vodafone niet voldoet aan de vereisten uit artikel 3, eerste lid van het Bbgt. Volgens Vodafone volgt uit het Bbgt niet dat zij in het beveiligingsplan de naam van het Bbgt moet opnemen. Het was daardoor volgens Vodafone voor haar niet voorzienbaar dat zij met het niet vermelden van deze verwijzingen een beboetbare overtreding van het Bbgt zou begaan.[103] Voorts stelt Vodafone zich op het standpunt dat haar beveiligingsplan wel aan de vereisten van het Bbgt voldoet. Dit zou onder meer blijken uit pagina 10 van het beveiligingsplan, waarin de VF NL Policies zijn opgesomd, en uit pagina 12, waarin wordt ingegaan op de fysieke beveiliging. Mijn voornemen zou hierom ondeugdelijk motiveren waarom het beveiligingsplan niet voldoet aan de vereisten uit artikel 3, eerste lid van het Bbgt. Vodafone stelt zich voorts op het standpunt dat ik mijn vaststelling baseert op de versiegeschiedenis van het beveiligingsplan. Daaruit zou ik afleiden dat het beveiligingsplan verouderd is. Vodafone wijst er in dit verband op dat het feit dat er meerdere versies van het document zijn, aantoont dat het een dynamisch document is. Daarbij geldt dat het Bbgt volgens Vodafone niet bepaalt hoe vaak het beveiligingsplan moet worden geüpdatet.[104]

Tot slot merkt Vodafone op dat ik ten onrechte in het kader van het vereiste van het hebben van een beveiligingsplan tegenwerp dat Vodafone niet zou hebben voldaan aan de maatregel tot het benoemen van een functionaris.[105]

Vodafone stelt op basis van het voorgaande dat de voorgenomen oplegging van een bestuurlijke boete niet op zijn plaats is en de voorgenomen boetehoogte niet passend en geboden is. Er had volstaan kunnen worden met een waarschuwing.[106]

---

[102] Randnummer 1-3.
[103] Randnummer 4-9.
[104] Randnummer 10-17.
[105] Randnummer 18.
[106] Randnummer 19-20.

Mijn reactie

Zoals ik heb overwogen in paragraaf 6.1 volgt uit de wettekst en de toelichting daarbij duidelijk dat alle maatregelen die in de zes genoemde categorieën beveiligingsmaatregelen in de bijlage bij het Bbgt in het beveiligingsplan aan bod moeten komen. In het beveiligingsplan dient op grond van artikel 3, eerste lid, Bbgt, te worden aangegeven op welke manier door de aanbieder uitvoering is gegeven aan zijn beveiligingsplicht. Met het oog hierop heeft de toezichthouder Vodafone verzocht om het beveiligingsplan. Het geven van een cautie is voor het opvragen van dergelijk wilsonafhankelijk materiaal, niet noodzakelijk.[107] Ik ben daarom van oordeel dat er geen consequenties verbonden hoeven te worden aan het feit dat de cautie niet is gegeven.

Blijkens artikel 3 van het Bbgt dient in het beveiligingsplan ten minste te worden aangegeven op welke wijze uitvoering is gegeven aan de maatregelen bedoeld in de bijlage bij het Bbgt. In geval hier niet aan wordt voldaan levert dit een voorzienbare overtreding van artikel 3, eerste lid, Bbgt op. Het hebben van een adequaat beveiligingsplan vormt een startpunt van een deugdelijke fysieke en digitale beveiliging van LI-gegevens door een aanbieder. Zonder een deugdelijk plan, geeft een aanbieder er immers geen blijk van zich bewust te zijn van het nut en de noodzaak van de te treffen maatregelen en is intern ook niet duidelijk aan welke maatregelen men zich moet houden. De vereisten waaraan het beveiligingsplan moet voldoen, vormen dus niet enkel een vormvoorschrift. Het is dus ook niet zo, zoals Vodafone suggereert, dat haar beveiligingsplan op orde zou zijn als zij daarin naar het Bbgt zou verwijzen. Het beveiligingsplan van Vodafone had moeten aantonen hoe Vodafone uitvoering geeft aan (in ieder geval) de maatregelen bedoeld in de bijlage bij het Bbgt. Daaraan voldoet het beveiligingsplan van Vodafone niet.

In reactie op het standpunt van Vodafone dat het voornemen geen vermelding maakt van de feitelijke gang van zaken rondom de aanpassing van het beveiligingsplan, overweeg ik het volgende.

De toezichthouder heeft de overtreding vastgesteld. Ik erken dat Vodafone werk heeft verricht om de overtreding te beëindigen. Daarbij merk ik op dat uit het door Vodafone aangehaalde gespreksverslag blijkt, dat de aanpassingen van het beveiligingsplan hebben geleid tot een 0.7 versie van het beveiligingsplan op 7 juni 2022. Uit het gespreksverslag blijkt dat de fysieke beveiligingsmaatregelen in [VERTROUWELIJK] nog ontbreken. De toezichthouder heeft Vodafone de dringende suggestie gedaan dat artikel 6 en artikel 8 van het Bbgt explicieter meegenomen moeten worden. Daarnaast volgt uit het gespreksverslag van de bespreking tussen Vodafone en RDI die plaats heeft gevonden op 14 juni 2022 dat

[107] Artikel 5:10a Algemene wet bestuursrecht. Afdeling Bestuursrechtspraak van de Raad van State, 27 juni 2018, ECLI:NL:RVS:2018:2115, r.o. 7.1.

de 1.0 versie van het Beveiligingsplan naar verwachting eind 2022 klaar zou zijn.[108]

Hoewel Vodafone hiermee de juiste weg heeft ingeslagen, laat dat onverlet dat het beveiligingsplan tijdens de overtredingsperiode niet voldeed aan de eisen uit artikel 3, eerste lid van het Bbgt. Bovendien is Vodafone als aanbieder op grond van het Bbgt verplicht om een beveiligingsplan te hebben dat aan de eisen van artikel 3, eerste lid van het Bbgt voldoet. Het beëindigen van een overtreding behoort daarmee ook tot haar wettelijke plicht en staat niet in de weg aan handhaving ten aanzien van een geconstateerde overtreding. Ik ben daarom bevoegd haar een boete op te leggen, ook wanneer zou blijken dat de overtreding inmiddels is beëindigd.

In reactie op het standpunt van Vodafone dat het beveiligingsplan een dynamisch document is dat wordt bijgewerkt wanneer nodig, overweeg ik het volgende. Ik volg Vodafone niet in dit standpunt. Uit de versiegeschiedenis blijkt dat de versie 1.1 uit 2010 stamt en de versie 2.0 uit 2021. De toezichthouder heeft vastgesteld dat de versie 2.0 slechts is veranderd door [VERTROUWELIJK] Bovendien zit er een periode van elf jaar tussen deze updates. De toezichthouder ziet daarnaast in versie 2.0 geen inhoudelijke aanpassingen die tot een actueel, bijgewerkt en deugdelijk beveiligingsplan hebben geleid. Zoals vastgesteld in paragraaf 6.1, ontbreekt een beschrijving van het [VERTROUWELIJK]-systeem en ontbreekt een beschrijving van de 4G technologie. Het beveiligingsplan omvat daarmee niet alle beveiligingsmaatregelen die op basis van het Bbgt worden vereist.

Daarover merk ik verder op, in reactie op het standpunt van Vodafone dat uit p. 10 en 12 van het beveiligingsplan zou blijken dat deze wel aan de vereisten van het Bbgt voldoet op, dat deze policies op p. 12 van het beveiligingsplan generieke maatregelen opsommen, die niet aan het Bbgt gerelateerd zijn. In deze lijst wordt bijvoorbeeld ook de 'Cloud Computing Security Detailed Policy' genoemd. Dit, terwijl in de LI-keten van Vodafone geen enkel cloud aspect is waargenomen. Uit deze opsomming blijkt verder ook niet op welke onderdelen van de LI-keten deze policies van toepassing zijn.[109] Uit deze opsomming volgt dus niet duidelijk welke policies van toepassing zijn op de LI-keten van Vodafone.

Ik volg Vodafone dus niet in haar zienswijze dat het beveiligingsplan aan de vereisten uit het Bbgt voldoet. Ik blijf bij de conclusie die ik in mijn voornemen en in paragraaf 6.1 van dit besluit heb getrokken.

[108] Verslag AT – VZ 14 juni 2022_DEF, ad. 4.
[109] Rvb, p. 27.

10.3 Overtreding functionaris

Vodafone heeft een zienswijze gegeven in reactie op mijn voornemen om aan haar voor de overtreding van artikel 2, eerste lid, onder a, in samenhang gelezen met artikel 2, tweede en derde lid, van het Bbgt en artikel I van de bijlage bij het Bbgt, zijnde het niet aanwezig hebben van een functionaris, een boete op te leggen.

Zoals overwogen in paragraaf 6.2 van dit besluit, heb ik besloten ten aanzien van deze voorgenomen overtreding van mijn voornemen af te wijken. Ik zie daarom geen aanleiding om de door Vodafone gegeven zienswijze ten aanzien van deze voorgenomen overtreding nader te bespreken.

10.4 Overtreding overeenkomsten

Vodafone betwist artikel 8, eerste en tweede lid, van het Bbgt te hebben overtreden. Zij verzoekt mij daarom af te zien van oplegging van een bestuurlijke boete. Daartoe stelt Vodafone, zakelijk weergegeven, onder meer het volgende.

Vodafone stelt voorop dat uit artikel 8 van het Bbgt en de nota van toelichting de verplichting blijkt om overeenkomsten te sluiten met derden waarin wordt ingegaan op de te treffen beveiligingsmaatregelen. Hoe dat moet worden neergelegd, blijkt volgens Vodafone echter niet uit het Bbgt. Daaruit leidt Vodafone af dat het aan haar is om hier zelf invulling aan te geven.[110]

Vodafone licht vervolgens toe welke overeenkomsten met derden zij met RDI heeft gedeeld. In dat verband merkt Vodafone op dat zij de overeenkomst met [VERTROUWELIJK] genaamd [VERTROUWELIJK] per abuis niet eerder met RDI gedeeld heeft. Vodafone verzoekt dit document bij mijn beoordeling te betrekken. Vodafone heeft bij dit document aangegeven op welke manier zij zorg heeft gedragen voor naleving van de normen uit het Bbgt door [VERTROUWELIJK].[111]

Vodafone stelt zich verder op het standpunt dat in het Rvb geen onderbouwing wordt gegeven op welke punten en waarom de inhoud van de onderzochte documenten niet voldoet aan artikel 8, eerste lid, Bbgt. Een algemene constatering dat in geen van de onderzochte documenten de verplichte inhoud van artikel 8, eerste lid, van het Bbgt bevat, is volgens Vodafone een onvoldoende onderbouwing van de constatering van een overtreding. Zowel de toezichthouder in het Rvb als ik in mijn voornemen heb volgens Vodafone nagelaten te specificeren op welke punten de inhoud van de onderzochte documenten niet aan het Bbgt voldoen. Ook is er voorafgaand aan het onderzoek door mij geen *guidance* gegeven over de verplichte inhoud van de overeenkomsten [112]

[110] Randnummers 27 – 30.
[111] Randnummers 31 – 38.
[112] Randnummers 39 – 41, Pleitnota 2.4 - 2.8 en voetnoot 2.

Mijn reactie

Vodafone acht niet voldoende bewezen dat zij artikel 8, eerste en tweede lid, van het Bbgt heeft overtreden. Ik volg Vodafone niet in dit standpunt en licht dat hieronder toe.

Zoals hiervoor is toegelicht, is een aanbieder op grond van artikel 8, eerste lid, van het Bbgt, indien zij de uitvoering van werkzaamheden uitbesteedt aan een derde en die derde in dat kader kennis neemt van LI-gegevens, verplicht er zorg voor te dragen dat de derde zich ertoe verplicht de nodige maatregelen in acht te nemen. De in artikel 8, eerste lid, van het Bbgt bedoelde verplichtingen van de derde moeten blijkens het tweede lid worden vastgelegd in een schriftelijke overeenkomst tussen de aanbieder en de derde. De eisen die aan een overeenkomst tussen een aanbieder en een leverancier worden gesteld zijn voldoende duidelijk en kenbaar. Op grond van artikel 8, eerste lid, van het Bbgt dient een aanbieder met een leverancier in ieder geval het volgende schriftelijk overeen te komen:

(…)

a. *de desbetreffende gegevens en informatie te beveiligen tegen kennisneming door onbevoegden;*
b. *met betrekking tot de desbetreffende gegevens en informatie geheimhouding te betrachten;*
c. *de ingevolge dit besluit gestelde maatregelen na te leven;*
d. *alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.*

Artikel 8 van het Bbgt bepaalt dan ook zeer uitvoerig wat in de overeenkomsten tussen Vodafone en derden aan wie zij werkzaamheden uitbesteedt moet worden opgenomen. Zodoende is op basis van deze bepaling duidelijk wat Vodafone in haar overeenkomsten met derden aan wie zij werkzaamheden uitbesteedt diende op te nemen.

De toezichthouder heeft een grondig onderzoek verricht naar de tussen Vodafone en haar leveranciers bestaande overeenkomsten. De toezichthouder heeft voor de beoordeling van de overeenkomsten elk overgelegd document integraal onderzocht.[113] De toezichthouder heeft reeds op 9 februari 2022 aan Vodafone per e-mailbericht verslag uitgebracht. Het was hem gebleken dat de documenten niet de verplichte inhoud zoals bedoeld in artikel 8, eerste en tweede lid, van het Bbgt bevatten. In hetzelfde e-mailbericht is andermaal verzocht om documenten te verstrekken waaruit de door Vodafone met haar leveranciers overeengekomen verplichting tot naleving van artikel 8, eerste en tweede lid, van het Bbgt blijkt. Uit de reactie per e-mail eveneens op 9 februari 2022 op dit verzoek is door Vodafone aangegeven dat dit verzoek van de toezichthouder voor haar duidelijk

[113] Rvb, p. 63.

is.[114] Zodoende heeft Vodafone voldoende gelegenheid gekregen om de vereiste documentatie aan te leveren.

Alle aangeleverde documenten zijn vervolgens niet alleen door de toezichthouder, maar ook nogmaals door mij onderzocht bij het voornemen tot oplegging van de bestuurlijke boete en ook nu nogmaals bij dit besluit. Met de toezichthouder heb ik de conclusie getrokken dat geen van de documenten de vanwege artikel 8, eerste en tweede lid, van het Bbgt verplichte inhoud bevat. De overeenkomsten bevatten bijvoorbeeld niet een beschrijving van alle relevante in het Bbgt en de bijlage daarbij voorgeschreven maatregelen die door de betrokken leverancier moeten worden nageleefd. Op grond van artikel 8, eerste lid en onder c, van het Bbgt is dit wel vereist.

In dit verband heb ik ook onderzoek gedaan naar de door Vodafone in het kader van de zienswijze verstrekte overeenkomst met [VERTROUWELIJK] en de gegeven toelichting op 21 december 2023. Ten aanzien daarvan concludeer ik als volgt.

Ik breng in herinnering dat artikel 8, eerste en tweede lid, van het Bbgt een aanbieder verplicht met zijn leverancier overeen te komen dat de leverancier de in het Bbgt gestelde maatregelen neemt.[115] Zowel de overeenkomst als de bijlagen (schedules) geven geen blijk van specifieke en volledige verwijzingen naar beveiligingsmaatregelen uit het Bbgt. Zo ontbreken de specifieke verplichtingen die het Bbgt op grond van bijvoorbeeld art. II van de Bijlage aan het personeel stelt. De vastgestelde overtredingen 4, 5 en 6 illustreren het risico van dergelijke generieke contractsbepalingen die ook bij [VERTROUWELIJK] worden gehanteerd. Ook deze overeenkomst voldoet daarom niet aan de eisen die artikel 8 van het Bbgt daaraan stelt.

De zienswijze van Vodafone brengt mij niet tot een ander oordeel. Ik blijf bij de conclusie die ik in mijn voornemen en in paragraaf 6.3 van dit besluit heb getrokken, met dien verstande dat de overtreding tot en met 26 oktober 2022 heeft voortgeduurd.

10.5 Overtreding Bbgt-HR

Zoals hiervoor is toegelicht, heb ik vastgesteld dat Vodafone artikel 4, tweede lid, in samenhang met artikel 2, tweede en derde lid Bbgt en onderdeel II, onder a, b en c Bijlage Bbgt heeft overtreden.

Deze overtreding is opgesplitst in vier onderdelen:
(i) Onbevoegde toegang (paragraaf 10.5.1);
(ii) Ontbreken VOG (paragraaf 10.5.2);
(iii) Ontoereikende functieomschrijving (paragraaf 10.5.3);

[114] 20220209 F[VFZ] T[AT] O[RE_ _EXTERNAL_ Bevoegd Aftappen VodafoneZiggo - uitvraag overeenkomsten LI-specifiek.
[115] Zie ook NvT Bbgt, p. 14.

(iv) Ontbreken van geheimhoudingsverklaringen (paragraaf 10.5.4).

Vodafone heeft haar zienswijze per onderdeel toegelicht. Daarop wordt hierna ingegaan.[116]

10.5.1 Onbevoegde toegang ex artikel II onder c Bijlage Bbgt

Vodafone bestrijdt de vaststelling dat de op pagina 36 van het Rvb genoemde 72 medewerkers toegang hadden tot LI-gegevens. Deze medewerkers waren daarvoor ook niet bevoegd en hadden specifieke commando's moeten invoeren waarvan het gebruik door die medewerkers niet is vastgesteld door de toezichthouder.[117]

Vodafone heeft de stelling dat medewerkers niet beschikken over de URL en inloggegevens om zich toegang tot LI-gegevens te verschaffen mondeling teruggetrokken.[118]

Mijn reactie

Ik kan Vodafone niet volgen in haar standpunt en licht dat als volgt toe. Op grond van artikel II, onder c, van de bijlage bij het Bbgt mag uitsluitend personeel dat overeenkomstig de functieomschrijving belast is met de verwerking van LI-gegevens, toegang tot die gegevens hebben.

De kern van de in dit verband bij Vodafone geconstateerde overtreding van onderdeel II, onder c, Bijlage Bbgt is dat 72 personen, die niet belast waren met de verwerking van LI-gegevens (en die in zoverre onbevoegd waren), toegang hadden tot LI-gegevens.

Over de vraag of de betrokken 72 personen belast waren met verwerking van LI-gegevens en bevoegd waren om hiervan kennis te nemen bestaat tussen mij en Vodafone geen verschil van inzicht. Zij waren hiertoe niet bevoegd.

Anders dan Vodafone ben ik van oordeel dat de bedoelde 72 personen wel degelijk toegang hadden tot LI-gegevens. Door Vodafone is verklaard dat zij werkzaam zijn bij de netwerkafdeling van [VERTROUWELIJK] voor andere dan LI-gerelateerde werkzaamheden.[119] Voor de reguliere beheerwerkzaamheden die worden uitgevoerd door [VERTROUWELIJK] is het nodig om op individuele netwerkapparatuur van Vodafone in te loggen. Met behulp van [VERTROUWELIJK] kon data tussen de [VERTROUWELIJK]

[116] Randnummer 42.
[117] Randnummers 43 – 48.
[118] Pleitnota p. 6.
[119] 20221004-Opgave-lijst-personen-met-toegang.pdf en Toelichting Bbgt HR vordering 27 september 2022 def.pdf.
[120] [VERTROUWELIJK]

[VERTRO-systemen worden onderschept. Ik verwijs naar paragraaf 6.5 van dit besluit voor een uitgebreidere uiteenzetting van deze methode van toegang. De voorgaande wijze van gebruik van [VERTROUWELIJK] in combinatie met de door de toezichthouder geconstateerde aanwezigheid van LI-gegevens in onversleutelde vorm[121], leidt tot de onbevoegde toegang.

10.5.2 Ontbreken VOG

Vodafone geeft aan dat voor het personeel waarvoor door haar geen VOG is overgelegd, niet belast zijn met LI-werkzaamheden. Zij zijn volgens Vodafone uitsluitend belast met onderhoudswerkzaamheden. Vodafone wijst er in dit verband op dat artikel 4, tweede lid, van het Bbgt een specifieke verplichting oplegt aan de aanbieder zelf. Enkel de personen die voor de aanbieder werkzaam zijn en die zijn belast met de uitvoering van de taplast en de verstrekking van informatie aan de bevoegde autoriteiten dienen volgens Vodafone een VOG te hebben. Daaruit blijkt volgens Vodafone dat deze verplichting niet ziet op leveranciers die support leveren en onderhoudswerkzaamheden aan systemen verrichten (de [VERTROUWELIJK] medewerkers). Vodafone wijst er hierbij op dat het Bbgt een aparte voorziening kent voor het geval een aanbieder een deel van zijn werkzaamheden uitbesteedt (artikel 8). Op grond daarvan geldt de VOG-verplichting volgens Vodafone niet voor ingeschakelde derden.[122]

Indien en voor zover een VOG wel vereist zou zijn, merkt Vodafone op dat er in [VERTROUWELIJK] geen VOG bestaat zoals wij die in Nederland kennen. Vodafone hanteert voor de desbetreffende personen een uniform screeningproces. Dat geldt ook voor medewerkers van [VERTROUWELIJK] [VERTROUWELIJK] medewerkers. Vodafone meent hiermee hoe dan ook uitvoering te hebben gegeven aan een proces dat vergelijkbaar is met het Nederlandse VOG screeningproces. Vodafone stelt ten aanzien hiervan dat het haar niet was toegestaan om de documentatie ten aanzien van eventuele criminele achtergronden van de desbetreffende medewerkers aan RDI te verstrekken.[123]

Mijn reactie

Op grond van artikel 4, tweede lid, van het Bbgt mag (kort gezegd) de medewerking aan taplasten uitsluitend worden verleend door personen die beschikken over een VOG. Hiervoor heb ik toegelicht dat Vodafone deze bepaling heeft geschonden, omdat personen belast waren met de uitvoering van LI-taken (het verlenen van medewerking aan taplasten), terwijl zij niet over een VOG beschikten.

---

[121] Zie de overtreding beschreven in paragraaf 6.5.
[122] Randnummers 49 – 53.
[123] Randnummers 54 – 61.

Anders dan Vodafone acht ik de personen genoemd in het Rvb wel op zodanige wijze met uitvoering van de LI-taken belast zijn dat artikel 4, tweede lid, in samenhang met artikel 2, tweede en derde lid Bbgt en onderdeel II, onder a, b en c Bijlage Bbgt op hen van toepassing zijn. Ik licht dat als volgt toe.

Zoals volgt uit paragraaf 6.5 beschreven feiten is van elk van de betrokken personen vastgesteld dat zij toegang hadden tot LI-gegevens. Met uitzondering van de 72 in paragraaf 10.5.1 bedoelde personen betreft dit *geautoriseerde* toegang. Deze medewerkers zijn door Vodafone aangewezen om werkzaamheden ten behoeve van de LI-taak uit te voeren en komen in aanraking met LI-gegevens. Voor deze groep medewerkers gelden onder meer de eisen genoemd in artikel 4, tweede lid, en artikel II van de Bijlage bij het Bbgt. Dit laatste wordt door Vodafone niet bestreden. Voor een ieder die uit hoofde van zijn functie kennis kan nemen van LI-gegevens is volgens de toelichting op de wet *screening* aangewezen.[124] Dit houdt onder meer in dat naar hen een onderzoek voor de verstrekking van een VOG dient te worden uitgevoerd. De veiligheid van de staat of doelmatigheid van OM-onderzoeken kan immers worden geschaad, indien van deze gegevens door onbevoegden kennis wordt genomen.

Ook van het genoemde personeel dat systemen of verbindingen daartussen onderhoudt, heeft de toezichthouder vastgesteld dat zij kennis kunnen nemen van LI-gegevens.[125] De (bedoelde) mogelijkheid tot kennisname van LI-gegevens maakt dat ook zij een VOG dienen te overleggen, een geheimhoudingsverklaring dienen te tekenen en een LI-functiebeschrijving dienen te hebben.

Vodafone is dus wel degelijk gehouden van het [VERTROUWELIJK] -personeel een VOG te overleggen.

Ten aanzien van de stellingen omtrent de inschakeling van derden en de verhouding tussen artikel 4 en artikel 8 van het Bbgt merk ik het volgende op. Uit artikel 8, derde lid, van het Bbgt, gelezen in samenhang met artikel 8, eerste lid, onder c, van het Bbgt, volgt dat een aanbieder verantwoordelijk is voor, onder meer, de naleving door de leverancier van ingevolge het Bbgt gestelde maatregelen op HR-gebied. De eisen die het Bbgt stelt aan personeel dat in aanraking komt en belast is met verwerking van LI-gegevens zijn onderdeel van die maatregelen. Vodafone is dus wel degelijk gehouden om de bedoelde personen een VOG te laten overleggen op grond van artikel 8, eerste lid sub c en derde lid, in samenhang gelezen met artikel 4, tweede lid, van het Bbgt.
In artikel 4, tweede lid, van het Bbgt is geen uitzondering gemaakt voor niet-Nederlandse leveranciers of personen.

Naar mijn oordeel is aan Vodafone om aan te tonen dat zij voor de betrokken medewerkers een met een VOG-onderzoek vergelijkbaar antecedentenonderzoek

[124] NvT bij Bbgt, p. 11.
[125] Zie paragraaf 6.5 van dit besluit.

heeft laten uitvoeren. Vodafone stelt dat het antecedentenonderzoek dat in [VERTROUWELIJK] heeft plaatsgevonden met een VOG-onderzoek gelijkgesteld kan worden. Daaraan heeft Vodafone niet voldaan. Zo zijn geen stukken overgelegd waaruit zou blijken dat de antecedenten zijn gecontroleerd. Ook is niet gesteld of gebleken wat de onderzoeken exact inhielden, bijvoorbeeld voor wat betreft de gehanteerde terugkijktermijnen of screeningsprofielen.

10.5.3 Functieomschrijving

Bij de functieomschrijving is volgens Vodafone niet vereist dat de verantwoordelijkheid voor de beveiliging en/of verwerking van LI-gegevens specifiek moet zijn beschreven. Een *algemene* functieomschrijving is volgens haar voldoende als duidelijk is dat de desbetreffende taak aan de medewerker is toebedeeld.[126] Specifiek voor de directeur van [VERTROUWELIJK] is de toegezonden functieomschrijving niet in het Rvb opgenomen. Zijn functieomschrijving volgt bovendien uit de statuten van [VERTROUWELIJK] Daarbij is het aantal van 81 ontoereikende functieomschrijvingen van medewerkers volgens Vodafone ontoereikend door mij gemotiveerd.[127]

Mijn reactie

Op grond van artikel II, onder a, van de bijlage bij het Bbgt dient in de functiebeschrijving van personeel dat belast is met de verwerking van informatie en gegevens de verantwoordelijkheid voor de beveiliging daarvan te worden beschreven. Ik heb bij Vodafone vastgesteld dat de op dit vlak vastgestelde overtreding tweeledig is. Enerzijds betreft de overtreding het ontbreken van een functieomschrijving (vergelijk artikel II, onder c, van de bijlage bij het Bbgt). Anderzijds betreft de overtreding het hanteren van een algemene functieomschrijving waaruit verantwoordelijkheid voor de LI-taak niet blijkt. Beide gevallen leveren een overtreding op.

Anders dan Vodafone ben ik van oordeel dat een algemene functieomschrijving die de relatie tot bevoegd aftappen mist en waarin de verantwoordelijkheid voor de beveiliging van LI-gegevens niet wordt genoemd niet voldoet aan de eis van onderdeel II, sub a, van de Bijlage bij het Bbgt.

Zowel de tekst van het aangehaalde subonderdeel als de toelichting daarbij maken duidelijk dat een algemene functieomschrijving niet volstaat:

> *"(…)*
> *In onderdeel II van de bijlage worden enkele eisen gesteld met betrekking tot de functiebeschrijving van personeel. Het begrip functiebeschrijving moet hier ruim worden geïnterpreteerd in die zin, dat ingeval*

[126] Randnummers 62 – 69.
[127] Randnummers 70 – 73.

> *personeel op een later tijdstip met werkzaamheden wordt belast in het kader waarvan van de hier bedoelde gegevens en informatie moet worden kennisgenomen, dit niet per se vergt dat een geheel nieuwe functiebeschrijving wordt opgemaakt, maar dat met een aanvulling op de bestaande functiebeschrijving (bijvoorbeeld in de vorm van een aantekening) kan worden volstaan. Duidelijk dient te zijn dat de desbetreffende taak is toebedeeld aan een persoon en dat de taak tot zijn functie behoort.*[128] *(…)"*

Duidelijk dient te zijn dat een LI-taak is toebedeeld aan een medewerker en dat die taak ook tot zijn functie behoort. Het is aan de aanbieder of een nieuwe functiebeschrijving wordt opgesteld of dat een bestaande functiebeschrijving wordt aangevuld met een vermelding van verantwoordelijkheid voor een LI-taak.

Met betrekking tot de directeur van [VERTROUWELIJK] overweeg ik dat de toezichthouder heeft vastgesteld dat er geen functieomschrijving aanwezig was waaruit de verantwoordelijkheid voor de LI-taak blijkt. Zoals ik hiervoor heb overwogen voldoet een algemene functiebeschrijving niet.

Ik volg de zienswijze van Vodafone wél in zoverre dat het aantal ontbrekende functieomschrijvingen in mijn voornemen per abuis op 81 is uitgekomen. In dit besluit, paragraaf 6.4, is het correcte aantal van 23 gehanteerd.

10.5.4 Geheimhoudingsverklaring

Vodafone stelt voorop dat de norm van artikel II, onder b, van de bijlage bij het Bbgt slechts geldt voor personeelsleden die belast zijn met de werkzaamheden ter uitvoering van een bevoegd gegeven bijzondere last dan wel de werkzaamheden ter uitvoering van een bevoegd gegeven bijzondere last dan wel de (daaraan) gerelateerde informatieverstrekking. De norm bevat volgens Vodafone bovendien niet de verplichting dat de geheimhoudingsverklaring specifiek de verantwoordelijkheid beschrijft ten aanzien van geheimhouding van LI-gegevens. Vodafone herhaalt dat haar leveranciers niet zijn belast met uitvoering van tapverzoeken, maar dat zij uitsluitend zorgen voor onderhoud van LI-systemen. Medewerkers van deze leveranciers zijn daarom niet aan geheimhouding uit hoofde van het Bbgt gebonden volgens Vodafone. Uit hoofde van hun functie zijn de betrokken werknemers van de leveranciers contractueel wel tot geheimhouding verplicht. Voor [VERTROUWELIJK]-medewerkers is de Code of business conduct een dergelijke overeenkomst. Hoewel daartoe volgens Vodafone geen verplichting bestaat in het Bbgt, is door Vodafone voor de betrokken medewerkers alsnog een aparte op LI gerichte geheimhoudingsverklaring opgesteld.[129]

[128] NvT bij Bbgt, p. 9 en 10.
[129] Randnummers 74 – 83.

Mijn reactie

Op grond van artikel II, onder b, van de bijlage bij het Bbgt dient personeel dat in aanraking komt met LI-gegevens een geheimhoudingsverklaring te tekenen. Zoals hiervoor reeds is toegelicht, komen de [VERTROUWELIJK] medewerkers van Vodafone wel degelijk in aanraking met LI-gegevens. Ik verwijs daarbij bijvoorbeeld naar pagina 30 en 31 van het Rvb. Voorts geldt dat artikel 8, eerste lid, onder b, Bbgt, gelezen in samenhang met het derde lid, duidelijk maakt dat deze verplichting ook geldt voor medewerkers van een derde waaraan Vodafone werkzaamheden uitbesteedt. Zodoende bestaat ten aanzien van deze [VERTROUWELIJK] medewerkers de verplichting een geheimhoudingsverklaring te laten tekenen.

Ik volg Vodafone voorts niet in haar betoog dat een algemene, niet specifiek op LI gerichte, geheimhoudingsverklaring volstaat.

Uit de nota van toelichting bij Bbgt blijkt dat de geheimhoudingsverplichting een heel traject betreft met de geheimhoudingsverklaring als sluitstuk:

> *"Deze geheimhoudingsplicht, die zich primair richt tot de aanbieder, kan niet los gezien worden van het geheel van te treffen beveiligingsmaatregelen. In artikel 6 van het besluit wordt dan ook bepaald dat de aanbieder er voor zorg dient te dragen dat de personeelsleden die belast zijn met de werkzaamheden ter uitvoering van een bevoegd gegeven bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, Tw alsmede met de werkzaamheden verbonden aan de informatieverstrekking als bedoeld in artikel 13.4 Tw, met betrekking tot deze werkzaamheden en de gegevens en informatie waarvan zij in dat verband kennis nemen, geheimhouding betrachten. Deze zorgplicht kan op verschillende wijzen worden ingevuld. Een adequate voorlichting aan de betrokken personeelsleden waarbij zij worden doordrongen van het gevoelige karakter van de door hen te verrichten werkzaamheden alsmede van de gegevens en informatie waarvan zij in dat kader kennisnemen en de noodzaak ter zake geheimhouding te bewaren is daarbij een allereerste vereiste. In dat verband ware zeker te wijzen op de wettelijke geheimhoudingsverplichtingen die er bestaan; denk daarbij aan de artikelen 98 en 272 van het Wetboek van Strafrecht (schending van geheimen) en – waar het gaat om de veiligheid van de staat – artikel 85 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (een taplast strekt ter uitvoering van de in deze wet neergelegde taak voor de AIVD of MIVD en daarmee ter uitvoering van deze wet, waarvoor de aangescherpte geheimhoudingsverplichting ex artikel 85 geldt). Overigens geldt voor de werkgever, in casu de aanbieder, die een persoon wil belasten met een vertrouwensfunctie, op grond van artikel 4, tweede lid, Wvo de verplichting de betrokken persoon te informeren over de betekenis en de rechtsgevolgen van het feit dat deze voor een veiligheidsonderzoek wordt aangemeld; daartoe behoort op zijn minst ook een aanduiding van de redenen waarom in casu sprake is van een vertrouwensfunctie. Als sluitstuk van het voorlichtingstraject is het wenselijk om de betrokken personeelsleden een geheimhoudingsverklaring te laten ondertekenen."*[130]

[130] NvT bij Bbgt, p. 12.

De aanbieder dient zijn personeel dat belast is met LI-gegevens voor te lichten over het belang van geheimhouding en te wijzen op de gevolgen van schending van deze verplichting. De culminatie van dit bewustwordings- en voorlichtingstraject is het ondertekenen van de geheimhoudingsverklaring met betrekking tot LI-gegevens. Dit proces omvat dus veel meer en verhoudt zich niet tot het hanteren van een algemene geheimhoudingsverklaring waar de LI-taak of -gegevens niet specifiek in worden genoemd.

Met de toezichthouder acht ik ook de door [VERTROUWELIJK] gehanteerde *code of business conduct* geen in onderdeel II, onder b, van het Bbgt bedoelde geheimhoudingsverklaring. In die *code* wordt immers geen geheimhouding beschreven en daarmee wordt al helemaal geen geheimhouding met betrekking tot LI-gegevens beschreven. De enkele stelling dat deze wel zou voldoen, brengt mij derhalve niet tot een ander oordeel.

10.6 Overtreding fysieke ruimte

Vodafone meent dat zij artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel III onder c, Bijlage Bbgt niet heeft overtreden. Daarom kan er geen boete worden opgelegd. De zienswijze van Vodafone ten aanzien van de fysieke beveiliging laat zich onderverdelen in de volgende onderwerpen:

(i) Compleetheid bevindingen (paragraaf 10.6.1);
(ii) Eenvoudige toegang tot data op LI-server (paragraaf 10.6.2);
(iii) Toegang tot afgeschermde kooi (paragraaf 10.6.3);
(iv) Toegang door geautoriseerde personen (paragraaf 10.6.4);
(v) Begeleiding onderhoudspersoneel (paragraaf 10.6.5);
(vi) Achteraf herleidbare toegang (paragraaf 10.6.6);
(vii) Detectie ongeautoriseerde toegang (paragraaf 10.6.7).

10.6.1 Compleetheid bevindingen

Vodafone stelt zich met betrekking tot de fysieke beveiliging in haar zienswijze op het standpunt dat RDI in het Rvb en in het voornemen niet alle bevindingen heeft opgenomen. Daardoor ontstaat volgens Vodafone een verkeerd beeld van de door haar getroffen beveiligingsmaatregelen. Vodafone mist in het voornemen allereerst in dit verband het onderscheid tussen de [VERTROUWELIJK], de beveiligde kooi in die zaal, de kast in de kooi en de server in de kast. Dit onderscheid is relevant voor de vier verschillende beveiligingsmaatregelen tussen deze fysieke plaatsen. De vier beveiligingsmaatregelen betreffen: de toegangscontrole bij binnenkomst, de vingerafdruk-/kaartlezer bij [VERTROUWELIJK] en de kooi en het slot op de kabinetkast met de server. Volgens Vodafone gaat het voornemen er ten

onrechte vanuit dat er twee beveiligingsstappen moeten worden doorlopen in plaats van vier.[131]

Vodafone gaat vervolgens in op het cameratoezicht in de door haar gehuurde zalen. Vodafone wijst er daarbij op dat niet alle bevindingen in het Rvb lijken te zijn opgenomen. Vodafone licht toe dat in het Rvb niet vermeld is dat er in de desbetreffende zalen bewegingssensoren met licht verbonden zijn, waardoor bij iedere beweging licht zichtbaar is op de camera's van [VERTROUWELIJK] in de zaal. Deze camera's worden bekeken door een 24/7 bemande receptie. Daarnaast hangen er camera's van Vodafone in de servergangen. Hoewel deze camera's uit stonden, betekent dat niet dat er geen cameratoezicht is.

De camera's zijn gericht op de ingang van [VERTROUWELIJK] waarbij niet is aangetoond dat de ingang van de kooi niet op camera zichtbaar is. Deze camera's zijn niet onklaar te maken zonder op de camera's zichtbaar te zijn. De camera's kunnen live worden bekeken door de permanent bemande receptie.[132]

De kooi, waarin de kabinetkast met de LI-server staat, is afgeschermd met een hekwerk. De vaststelling van de toezichthouder dat een persoon door de ruimte tussen de bovenzijde van het hekwerk en het plafond kan klimmen is geen gecontroleerde vaststelling. Uit het Rvb of bijgevoegde foto's blijkt niet wat de exacte afmetingen zijn van deze ruimte. Ook blijkt niet uit het Rvb dat er een trap in een openbare ruimte van het datacentrum aanwezig is.[133]

Over de draaiknop waarmee de deur van de kooi aan de binnenzijde kan worden geopend voert Vodafone aan dat niet is aangetoond dat deze vanaf de buitenzijde kan worden gemanipuleerd. Ondanks herhaalde pogingen van de inspecteur is het hem niet gelukt de kooideur op deze manier vanaf de buitenzijde te openen. In het dossier bevindt zich geen foto waarop de inspecteur een kabelkoord van een toegangspas om de knop heeft gehangen.[134]

Vodafone gaat vervolgens in op de autorisaties voor toegang tot het datacentrum. Zij voert aan dat de afgeschermde kooi alleen toegankelijk is voor geautoriseerd personeel of onder begeleiding van dergelijk personeel.

Zo hanteert Vodafone een whitelist voor het datacentrum. Personen die toegang dienen te verkrijgen tot [VERTROUWELIJK] worden door Vodafone opgevoerd. Voor toegang is vereist dat deze personen gecertificeerd zijn, specifiek op het gebied van ESD/VCA. Deze personen mogen rechtens zonder begeleiding in de betrokken zaal zijn. Dit betekent niet dat zij permanente toegang hebben. Bij elk bezoek wordt een toegangsbadge verstrekt en weer ingeleverd. Ook wordt bij ieder bezoek een vingerafdruk afgenomen en identiteitsbewijzen gecontroleerd.

---

[131] Randnummers 92 – 94.
[132] Randnummer 95.
[133] Randnummer 96.
[134] Randnummer 97.

Toegang tot de zalen gebeurt middels een vingerafdruk. De succesvolle en niet-succesvolle toegangspogingen tot de zalen worden daarmee ook bijgehouden.

Naast de personen op de whitelist kunnen ook vier VIP-accounts binnen Vodafone personen aanmelden voor onderhoudswerkzaamheden in de betrokken zalen. Deze personen dienen zich ook aan te melden bij [VERTROUWELIJK], worden op ieder moment begeleid en hebben geen eigen autorisaties, zodat voor iedere toegang de vingerafdruk van de begeleider nodig is.[135]
Ook medewerkers van [VERTROUWELIJK] staan op de whitelist of doorlopen de aanmeldprocedure van onderhoudsmedewerkers en zijn dus als zodanig herleidbaar.[136]

Mijn reactie

Artikel III van de bijlage bij het Bbgt bevat verschillende eisen aan de fysieke beveiliging van LI-gegevens.
Anders dan Vodafone ben ik van oordeel dat de ruimte waarbinnen de LI-gegevens aanwezig zijn niet deugdelijk fysiek beveiligd is. De zienswijze van Vodafone brengt mij niet tot een ander oordeel. Ik licht dat als volgt toe.

Net als Vodafone heeft mijn toezichthouder vier toegangsbeveiligingsmaatregelen en cameratoezicht geïdentificeerd in het datacentrum [VERTROUWELIJK]. Bij zijn onderzoek zijn door de toezichthouder dan ook geen relevante beveiligingsmaatregelen buiten beschouwing gelaten en is de beveiliging in haar totaliteit onderzocht. Per beveiligingsmaatregel zijn naar mijn oordeel echter meerdere eenvoudige manieren om deze te omzeilen. Dat maakt de beveiliging, ook als geheel, niet deugdelijk.

Ik overweeg dat de eerste van de beveiligingsmaatregelen, de toegangscontrole aan de voordeur en de toegangscontrole voor de gang op verdieping 2, minder solide zijn dan Vodafone deze in haar zienswijze doet voorkomen. De overwegingen over het feit dat het betrokken datacentrum niet bij Vodafone in eigendom is en wordt gedeeld met andere huurders hangen hiermee samen. Ik zal dat hieronder uiteenzetten.

Nu een deel van de LI-systemen in een datacentrum is ondergebracht, dient er rekening te worden gehouden met andere huurders. Het is in principe voor een ieder, dus ook voor kwaadwillenden, mogelijk om een serverruimte te huren in [VERTROUWELIJK]. Mijn toezichthouder heeft vastgesteld dat in ieder geval 280 personen toegang hadden tot deze zaal. Deze personen hebben eveneens toegang tot [VERTROUWELIJK] voor de levering van goederen, bijvoorbeeld gereedschap, via de goederenlift in [VERTROUWELIJK]. Voor standaardwerkzaamheden in een datacentrum, zoals het bijplaatsen van servers, is het meenemen van een gereedschapskoffer

[135] Randnummers 98 – 101.
[136] Randnummers 102 – 104.

met divers gereedschap gebruikelijk.[137] Daarnaast loopt de route naar één van de nooduitgangen voor personen in [VERTROUWELIJK] . Voor in elk geval 280 personen, en in potentie ook andere huurders, is het dus mogelijk om [VERTROU][VERTROUWELIJK] te betreden zonder dat zij een beveiligingsmaatregel, te weten de toegangscontrole bij binnenkomst en de vingerafdrukscanner, hoeven te doorbreken. Het startpunt van deze dreiging is de legitieme toegang tot [VERTROUW][VERTROUWELIJK], waarbij ook de aanwezigheid van gereedschap voordehand ligt.

Ik merk aangaande het cameratoezicht op dat de constateringen dat de camera's niet op de ingang van de kooi waren gericht en gemakkelijk onklaar gemaakt konden worden, betrekking hebben op de camera's binnen de kooi van Vodafone. In paragraaf 6.4 van dit besluit is dat verschil verduidelijkt.

Het cameratoezicht dat [VERTROUWELIJK] in de zaalgangen houdt, acht ik geen voldoende deugdelijke beveiligingsmaatregel. Vanuit [VERTROUWELIJK] is aangegeven dat er geen automatische detectie of alarmering plaatsvindt.[138] De waarde van deze beveiligingsmaatregel staat of valt met de oplettendheid van de persoon die de beelden bekijkt. [VERTROUWELIJK] geeft aan dat er geen afspraken zijn gemaakt over waar op gelet wordt.[139] Ook tijdens de hoorzitting is door Vodafone in het midden gelaten of de betrokken medewerker van [VERTROUWELIJK] steeds naar de camerabeelden kijkt. Zelfs een permanent oplettende medewerker dient zijn aandacht te verdelen over meerdere camera's in meerdere zalen en op meerdere verdiepingen. Deze medewerker bemant daarnaast de receptie. Dit voorgaande brengt mee dat aldus ingericht cameratoezicht als detectiemaatregel sterk aan effectiviteit inboet. De omstandigheid dat er lichtsensoren in de zaalgangen aanwezig zijn maakt dat niet anders. Deze lichtsensoren voegen zelfstandig geen waarde toe aan de beveiliging, maar doen dat slechts in combinatie met goed cameratoezicht. De toezichthouder heeft vastgesteld dat de vrije toegang tot [VERTROU][VERTROUWELIJK] is toegestaan voor personen die toegang hebben tot [VERTROUWELIJK]. Personen die serverruimte in [VERTROUWELIJK] huren, kunnen voor aanvoer van goederen gebruikmaken van de lift in [VERTROUWELIJK]. De omstandigheid dat er personen in [VERTROUWELIJK] aanwezig zijn en het licht aanspringt zal geen omstandigheid zijn die tot bijzondere oplettendheid van de bewaker oproept.

Ten aanzien van de door Vodafone aangevoerde stellingen over de toegangsprocedure voor de ruimte waarin het LI-systeem zich bevindt overweeg ik het volgende.

De door Vodafone geschetste procedure houdt in dat gecertificeerde personen, zij doelt specifiek op ESD- en VCA-certificeringen, zonder begeleiding toegang hebben tot de ruimte waarin het LI-systeem zich bevindt. Anders dan Vodafone ben ik van oordeel dat de onderhoudsmedewerkers, bijvoorbeeld de tijdens de

[137] [VERTROUWELIJK]

[138] [VERTROUWELIJK]
[139] [VERTROUWELIJK]

inspectie aangetroffen onbegeleide medewerkers van [VERTROUWELIJK], niet het in artikel III onder g Bbgt bedoelde *eigen geautoriseerd* personeel zijn.

Eigen geautoriseerd personeel in de zin van het Bbgt heeft de autorisatie en screeningstappen van artikel 4, tweede lid 2, en artikel II van de Bijlage van het Bbgt doorlopen. Het plaatsen van personeel op een whitelist kan niet in de plaats treden van de screeningseisen die artikel 4, tweede lid, en artikel II Bijlage van het Bbgt van een aanbieder verwacht. De medewerkers van [VERTROUWELIJK] of andere onderhoudsmedewerkers van het datacentrum komen niet voor op de lijsten met personeel dat geautoriseerde toegang tot LI-gegevens heeft. Daarnaast hebben een VCA[140]- of ESD[141]-certificering niets van doen met de eisen die het Bbgt aan personeel stelt.

Dat de constatering van de toezichthouder geen incident is, zie ik bevestigd in de verklaring namens [VERTROUWELIJK] dat onderhoudspersoneel werkzaamheden aan bijvoorbeeld de airco-installatie laat verrichten. Dat personeel had onder meer toegang tot de kooi van [VERTROUWELIJK] [142] Vanuit [VERTROUWELIJK] is verder verklaard dat het onderhoudspersoneel door een medewerker van [VERTROUWELIJK] worden begeleid naar de kooi, maar dat het zij daarna zelfstandig verder werken in de kooi. Deze werkwijze acht ik niet in overeenstemming met art. III onder g van de Bijlage bij het Bbgt.

Vodafone gaat vervolgens in op de wijze waarop toegang door medewerkers van [VERTROUWELIJK] te herleiden is op het individu via hun vingerafdrukken. Ik onderschrijf de stelling van Vodafone dat toegang tot het datacenter alleen kan plaatsvinden na legitimatie en identificatie bij de receptie, waarna het datacenter een persoonsgebonden authenticatiemethode activeert of uitreikt (vingerafdruk en/of pas). Het gebruik van deze persoonsgebonden authenticatie (bijv. openen van een deur) levert een persoonsgebonden registratie op in het toegangssysteem van het datacenter. Ik volg Vodafone niet in haar argumenten dat door het datacenter persoonsgebonden authenticatiemethode (pas en/of vingerafdruk) sluitend kan worden vastgesteld wie toegang heeft gehad tot de zaal of kooi (de ruimte) waarin het LI-systeem zich bevindt. Zowel de zaaldeur, als de kooideur kan worden geopend door één persoon waarna vervolgens met de deuropening meerdere personen toegang kunnen krijgen. Het betreft hier namelijk geen tourniquet zoals op de begane grond, maar een normale deur waardoor meer dan één persoon tegelijk toegang tot de ruimte kan krijgen.

Toegang tot de ruimte waarin LI-gegevens zich bevonden kon daarom niet met vingerafdrukken achterhaald worden. Voor de [VERTROUWELIJK]-medewerkers geldt dat zij zich met een niet-persoonsgebonden toegangspas, uitgereikt door [VERTROUWELIJK],

[140] VCA-certificering is een algemeen diploma op het gebied van veiligheid: https://www.vca.nl/diplomas-certificaten/vca.
[141] Een ESD-opleiding stelt personen in staat om schade door statische elektriciteit te voorkomen: https://www.esda.org/certification/esd-certificate-of-compliance/.
[142] [VERTROUWELIJK]

de toegang tot de kabinetkast met LI-gegevens konden verschaffen. Ook aan dit laatste toegangsmiddel kon dus geen sluitende persoonsgebonden registratie worden ontleend.

Anders dan Vodafone ben ik van oordeel dat ik in mijn afweging de relevante bevindingen in hun compleetheid heb betrokken. Ik zie in hetgeen Vodafone hiertegen inbrengt dan ook geen reden om op de genoemde onderdelen van mijn voornemen af te wijken.

10.6.2 Eenvoudige toegang tot fysieke ruimte

Vodafone stelt zich op het standpunt dat uit het voornemen lijkt te volgen dat RDI de wens heeft dat datacenters waarin LI-gegevens zich bevinden in eigendom van Vodafone zelf zijn. Volgens Vodafone blijkt evenwel nergens uit het Bbgt dat de LI-server zich moet bevinden in een gebouw, zaal of andere ruimte die enkel toegankelijk is voor Vodafone zelf zelfs in een ruimte in eigendom van Vodafone. Dat zulks een vereiste is, blijkt volgens Vodafone ook niet beleid of een aanwijzing van RDI. Om die reden stelt Vodafone dat haar niet kan worden verweten dat [VERTROUWELIJK] andere klanten heeft die ruimte huren op de tweede verdieping.[143]

Mijn reactie

In reactie op de zienswijze van Vodafone merk ik op dat het geen vereiste is, en ik werp dat ook niet aan Vodafone tegen, dat Vodafone al haar fysieke LI-infrastructuur op eigen locaties onderbrengt. Een dergelijke eis is, zoals Vodafone ook stelt, ook niet op het Bbgt terug te voeren. Als LI-gegevens zich in gedeelde datacentra bevinden, is het evenwel aan Vodafone om te waarborgen dat de LI-systemen tegen ongeautoriseerde toegang zijn beveiligd. Vodafone zal daarbij rekening moeten houden met de aanwezigheid van derden binnen het datacentrum. De geconstateerde overtredingen betreffen ieder concrete hiaten zoals die in paragraaf 6.4 zijn toegelicht waarmee geenszins is volstaan met de opmerking dat LI-data zich in een gedeeld datacentrum bevinden.

10.6.3 Eenvoudige toegang tot de afgeschermde kooi van Vodafone

Vodafone stelt zich vervolgens op het standpunt dat de afgesloten kooi niet eenvoudig toegankelijk is voor ongeautoriseerde personen.[144] Volgens Vodafone zijn de bevindingen die ik hieraan ten grondslag leg 'vergezochte argumenten' en gebaseerd op 'niet getoetste inschattingen'. Daarnaast worden bepaalde onderdelen van de beveiliging van de LI-server volgens Vodafone op diverse plekken onbesproken gelaten.

[143] Randnummers 105 – 109.
[144] Randnummer 110 – 120.

Vodafone wijst er in dat verband dat in het voornemen is opgenomen dat het hekwerk van de kooi niet tot het plafond reikt. Uit het voornemen of Rvb blijkt niet welke afmetingen de ruimte tussen het plafond en het hekwerk heeft en dat een trap aanwezig was. Er is daarom niet aangetoond dat een persoon over het hek kan klimmen.

De draaiknop bij de deur van de kooi kon door de toezichthouder tijdens zijn bezoek niet worden gemanipuleerd vanaf de buitenzijde zodat de deur zou openen. Iedere in het voornemen genoemde vorm van ongeautoriseerde toegang (via de kooideur, onder het hekwerk door of over het hekwerk heen) zou volgens Vodafone op de camera's te zien zijn.[145]

De zuignap voor het weghalen van een tegel om zo toegang te krijgen tot de ruimte onder de vloer is volgens Vodafone niet voor iedereen voorhanden. Ook voor ander (zwaar) gereedschap geldt dat men daarmee eerst langs de beveiligingsmaatregelen, camera's en bewegingssensoren moet. Volgens Vodafone is niet aangetoond hoe een onbevoegd persoon hiermee door de in paragraaf 9.6.1 genoemde beveiligingsmaatregelen komt en onopgemerkt blijft op camera's en bewegingssensoren. Ook zou zelfs na het doorbreken van de beveiliging tot in de kooi nog geen toegang tot LI-gegevens verkregen zijn. Een indringer dient dan nog toegang te krijgen tot de LI-server in de afgesloten kabinetkast.

Met betrekking tot (het sluitwerk) op de kabinetkast merkt Vodafone op dat de ondeugdelijkheid daarvan op aannames berust. Zo betekent het ontbreken van een certificaat voor het slot op de kabinetkast volgens Vodafone niet dat het slot niet deugdelijk is.[146]

Dat de kabinetkast afwijkt van andere servers in de kooi, door de aanwezigheid van een slot [VERTROUWELIJK], is niet aan een overtreding van het Bbgt te relateren.[147]

Mijn reactie

Zoals hiervoor is toegelicht bevat artikel III van de bijlage bij het Bbgt verschillende eisen aan de fysieke beveiliging van LI-gegevens. Ik begrijp het betoog van Vodafone zo dat zij betwist dat zij artikel III sub b van de bijlage bij het Bbgt heeft overtreden. Ik onderschrijf dat betoog niet. Tijdens de inspectie heeft mijn toezichthouder drie manieren geïdentificeerd waarmee de beveiliging door het hekwerk van de kooi kon worden omzeild of doorbroken. Ik wijs daarbij op het waarnemingsverslag en de daarbij gevoegde foto's.[148]

---

[145] Randnummers 110 – 112.
[146] Randnummers 113 – 116.
[147] Randnummers 117 – 118.
[148] [VERTROUWELIJK]

Door de toezichthouder is vastgesteld dat de tegels met eenvoudig gereedschap, bijvoorbeeld een zuignap, vlot zijn te verwijderen. Ook is op de door de toezichthouder genomen foto's te zien dat de ruimte onder de tegelvloer voldoende groot is om onder het hekwerk door toegang te bieden tot de kooi.[149] In hetzelfde verslag blijkt verder dat eenvoudig toegang tot de kooi kan worden verkregen door over het hekwerk te klimmen met behulp van de aanwezige losse trap.[150] Dat er geen trap aanwezig is in het datacentrum is dan ook onjuist. Bovendien kunnen kwaadwillenden een trap ook zelf meenemen als onderdeel van een gereedschapset waarmee in het datacentrum gewerkt kan worden. De ruimte tussen de bovenkant van het hekwerk en het betonnen plafond is hiervoor voldoende groot.[151]

Wat betreft de draaiknop van de toegangsdeur tot de kooi, klopt het dat de toezichthouder deze tijdens zijn inspectie niet heeft kunnen openen. Wel is aangetoond dat een koord vanaf de buitenzijde van de kooi om de draaiknop gewikkeld kon worden. De toezichthouder had tijdens zijn inspectie niet de juiste middelen voorhanden om het slot vervolgens open te draaien. Het is echter de inschatting van de toezichthouder dat met zeer eenvoudig gereedschap, bijvoorbeeld een stuk ijzerdraad, vanaf de buitenzijde van de kooi aan de knop kan worden gedraaid.[152] Een draai van een halve slag opent de deur van de kooi.

Hoewel de voornoemde wijzen van ongeautoriseerde toegang op camera te zien zouden zijn, acht ik het cameratoezicht van [VERTROUWELIJK] niet van afdoende kwaliteit als effectieve detectiemaatregel. Zoals al onder 10.6.1 is overwogen, is in wezen de oplettendheid van de medewerker bij de receptie hetgeen de detectie moet bewerkstelligen.

Wie eenmaal de kooi binnengaat, bevindt zich buiten het zicht van de camera's van [VERTROUWELIJK]. Het cameratoezicht binnen de kooi functioneerde tijdens de inspectie niet. Mijn toezichthouder heeft na zijn inspectie ter plaatse de camerabeelden van deze camera's opgevraagd. Daarop is geantwoord dat Vodafone de camera's beheert, maar dat het systeem niet bekend is en er een onderzoek is gestart naar de camerabeelden.[153] De camerabeelden konden, ook na een herhaald verzoek, echter niet geleverd worden.[154] Ik volg Vodafone daarom niet in haar zienswijze dat dit een eenmalig manco is, nu in ieder geval tot en met 13 september 2022 geen beelden konden worden geleverd.

De toegang tot het systeem dat de LI-gegevens bevat, is vervolgens beveiligd met een slot op de kabinetkast waarin het systeem zich bevindt. Ik stel daarbij voorop

---

[149] [VERTROUWELIJK]
[150] [VERTROUWELIJK]

[151] Foto E8ED7E17-755A-413E-B5CE-C9F75CD77374.
[152] [VERTROUWELIJK]

[153] [VERTROUWELIJK]
[154] [VERTROUWELIJK]

dat het sluitwerk van de kabinetkast door toezichthouder uitgebreid is onderzocht.[155] Daarbij is niet alleen geconstateerd dat het sluitwerk geen certificering heeft. De toezichthouder heeft vanuit zijn expertise ook de kwaliteit van het sluitwerk beoordeeld. Zijn vaststellingen met betrekking tot de beveiliging van de kabinetkast zijn als volgt:

> *(…) dat het gebruikte metaal van de deur erg dun is als het gaat om het grote platte vlak van de deur waaronder het luchtdoorlatende gaasgedeelte valt. Het slot is niet voorzien van enige certificeringsopdrukken zoals gebruikelijk op een slot (bijvoorbeeld SKG-keurmerk). Het uitstekende gedeelte van het slot/paslezer - mechanisme is gemaakt van dun metaal en plasticcomponenten.*[156]

Voor zover Vodafone betoogt dat ik met de opmerking dat het betrokken slot niet is gecertificeerd een nieuwe norm buiten het Bbgt in het leven heb geroepen, onderschrijf ik die stelling niet. Het bewijs voor de vaststelling dat het slot niet aan een deugdelijke fysieke beveiliging bijdraagt, steunt op de feitelijke waarneming van de toezichthouder. De essentie is het hiervoor beschreven gebruik van dun materiaal van de deur en het slot. De afwezigheid van een certificaat ondersteunt slechts de inhoudelijke vaststelling dat de beveiliging van de kabinetskast niet aan de eisen van het Bbgt voldoet.
Naar het oordeel van de toezichthouder is een dergelijke kabinetkast binnen vijf minuten te openen gebruikmakend van eenvoudig gereedschap. Dat oordeel volg ik. Een dergelijke beveiliging van de kabinetkast acht ik niet deugdelijk en daarmee niet in overeenstemming met de eis van artikel III onder b van de bijlage bij het Bbgt.

Met Vodafone ben ik van oordeel dat de [VERTROUWELIJK] van de kabinetkast geen omstandigheid is die de deugdelijke beveiliging beïnvloedt. Ik heb deze constatering in paragraaf 6.4 niet gebruikt als onderbouwing van de overtreding van artikel III onder b van de bijlage bij het Bbgt.

10.6.4 Toegang geautoriseerd personeel

Ongeautoriseerde toegang is volgens Vodafone niet mogelijk door de genoemde beveiligingsstappen. Slechts voor gecertificeerden of onder begeleiding daarvan is toegang mogelijk.

Vervolgens gaat Vodafone in op de toegang tot de kooi door 39 medewerkers van [VERTROUWELIJK]. Het is volgens Vodafone in dat verband ook logisch dat deze medewerkers toegang moesten hebben tot het ventilatiesysteem van het datacenter, dat gelegen is achter de beveiligde kooi van Vodafone. Daardoor moesten deze medewerkers ook toegang tot de kooi van Vodafone verkrijgen. Vodafone stelt zich op het standpunt dat door RDI niet is aangetoond dat deze 39 personen geen toegang nodig zouden hebben voor hun functie. Vodafone merkt

[155] [VERTROUWELIJK]
[156] [VERTROUWELIJK]

hierover verder op dat de medewerkers van [VERTROUWELIJK] geldt geen permanente toegang hadden, maar dat zij per bezoek moeten worden aangemeld.[157]

Mijn reactie

Op grond van artikel III, onder d, van de bijlage bij het Bbgt is toegang tot de ruimte waar de LI-gegevens zich bevinden uitsluitend toegestaan aan daartoe geautoriseerde personen, voor zover dit voor hun functie noodzakelijk is. Ik heb vastgesteld dat Vodafone hier niet aan heeft voldaan, omdat de genoemde 39 personen daartoe op grond van het Bbgt niet *geautoriseerd* zijn en zij daarnaast permanente toegang hebben.

Zoals ik hiervoor onder 10.6.1 heb overwogen dient het begrip 'geautoriseerde persoon' in de zin van het Bbgt gelezen te worden. Eigen geautoriseerd personeel in de zin van het Bbgt heeft de autorisatie en screeningstappen van artikel 4, tweede lid, en artikel II van de bijlage van het Bbgt doorlopen. Voor de betrokken 39 personen van [VERTROUWELIJK] geldt niet dat zij deze stappen hebben doorlopen.

Met permanente toegang wordt bedoeld dat zij, anders dan Vodafone aanvoert, zonder aanmelding toegang hadden tot de kooi in zaal [VERTROUWELIJK].[158] Dit zijn allen medewerkers van [VERTROUWELIJK] die toegang tot de kooi hadden, zelfs als zij op dat moment geen onderhoudswerkzaamheden hoeven uit te voeren.

Dit onderhoudspersoneel dient op grond van artikel III onder d van de bijlage bij het Bbgt te worden geautoriseerd voor zover dat voor hun functie noodzakelijk is of op grond van artikel III onder g van de bijlage bij het Bbgt door geautoriseerde medewerkers begeleid te worden.

10.6.5 Begeleiding onderhoudspersoneel

Vodafone gaat vervolgens in op mijn bevindingen met betrekking tot de begeleiding van onderhoudspersoneel door geautoriseerde bevindingen en meer specifiek op mijn bevinding dat op het moment van de inspectie onderhoudswerkzaamheden werden verricht in de kooi waar het LI-systeem zich bevindt.159 Volgens Vodafone heb ik nagelaten te onderbouwen waarom dit een overtreding van het Bbgtwhitelist staan geen begeleiding nodig binnen het datacenter. Aangezien de desbetreffende monteurs op de whitelist stonden, was begeleiding van (ander) geautoriseerd personeel volgens Vodafone niet nodig.[160]

[157] Randnummers 121 – 126.
[158] [VERTROUWELIJK]
159 Randnummers 127 – 128.
[160] Randnummers 127 – 128.

Mijn reactie

Op grond van artikel III, onder g, van de bijlage bij het Bbgt dienen personen belast met onderhouds- en reparatiewerkzaamheden in de ruimte waarin de LI-gegevens zich bevinden te worden begeleid door eigen geautoriseerd personeel. Deze bepaling heeft Vodafone geschonden, doordat tijdens de inspectie onderhoudspersoneel zonder begeleiding van door Vodafone geautoriseerd personeel rondliep in de ruimte waar zich de LI-gegevens van Vodafone bevinden.

In paragraaf 10.6.1 heb ik al uiteengezet dat het plaatsen van personen op een whitelist niet betekent dat deze daarmee geautoriseerd zijn in de zin van het Bbgt. Niet-geautoriseerd onderhoudspersoneel dient in de ruimte waar zich de LI-gegevens bevinden te worden begeleid door een persoon met de juiste autorisaties. Ik verwijs verder naar mijn reactie onder 10.6.1.

10.6.6 Achteraf herleidbare toegang

Vodafone betwist verder dat achteraf niet herleidbaar is welke personen toegang tot de ruimte hebben.[161] Zij verwijst naar hetgeen in eerdere randnummers is opgenomen. Alleen personen die door Vodafone of leveranciers van [VERTROUWELIJK] zijn aangemeld en door [VERTROUWELIJK] zijn geïdentificeerd, kunnen de ruimte betreden. Zij zijn ofwel zelf gecertificeerd of betreden de ruimte onder begeleiding van een gecertificeerde medewerker. Van eerstgenoemden is toegang herleidbaar via hun vingerafdruk en bij de laatstgenoemden kan eenvoudig worden nagegaan wie zich in de kooi bevonden.

Mijn reactie

Vodafone betwist dat zij artikel III onder e van de bijlage bij het Bbgt heeft overtreden. Zij verwijst daarbij naar hetgeen zij daarvoor, bij randnummers 92 tot en met 104, heeft aangevoerd.

In paragraaf 10.6.1 ben ik al uitvoerig ingegaan op hetgeen Vodafone heeft aangevoerd. Daar heb ik de conclusie getrokken dat Vodafone art. III onder e van de bijlage bij het Bbgt heeft overtreden. Ik volsta hier met een verwijzing naar die overwegingen.

10.6.7 Detectie ongeautoriseerde toegang

Vodafone bestrijdt dat ongeautoriseerde toegang tot de kooi niet wordt gedetecteerd en tijdige interventie plaatsvindt. Zo zijn in de gang van [VERTROU [VERTROUWELIJK] camera's in beide looprichtingen bevestigd waarop de gehele gang zichtbaar is. De toegangsdeur tot de kooi is op deze camera's te zien. Zij verwijst daarbij naar de afbeelding op pagina 32 van haar zienswijze.

[161] Randnummers 129 – 131.

De camera's zijn volgens Vodafone niet onklaar te maken zonder op camera te worden waargenomen. Direct bij binnenkomst in de zaal is men op beide camera's te zien. Vodafone voegt daaraan toe dat niet is toegelicht hoe de camera's binnen de kooi onklaar kunnen worden gemaakt zonder op die camera's zichtbaar te zijn. Voorts is volgens Vodafone niet aangetoond dat zonder detectie toegang tot LI-gegevens kon worden verkregen.[162]

De vaststelling dat Vodafone niet de beschikking heeft over de camerabeelden in de gangen van de kooi en daardoor ongeautoriseerde toegang niet tijdig kan detecteren is volgens haar niet juist. Nu er permanente (realtime) camerabewaking is vanuit de receptie, gecombineerd met het aanspringen van het licht via de bewegingssensoren, is het niet mogelijk ongemerkt de zaal te betreden. Het niet-functioneren van de camera's in de kooi is een ongelukkige momentopname.[163]

Mijn reactie

Vodafone bestrijdt in randnummers 132 tot en met 140 mijn conclusie dat ongeautoriseerde toegang onvoldoende wordt gedetecteerd en daarmee artikel III onder c van de bijlage bij het Bbgt heeft overtreden.

Onder 10.6.1 heb ik uiteengezet waarom met het cameratoezicht dat Vodafone en [VERTROUWELIJK] in de betrokken ruimte houden ongeautoriseerde toegang niet in voldoende mate wordt gedetecteerd. Ik verwijs Vodafone dan ook naar mijn overwegingen daarover. Datzelfde geldt voor de bewegingssensoren die het licht in de zaal doen aangaan.

De zienswijze van Vodafone brengt mij niet tot een ander oordeel. Ik blijf bij de conclusie die ik in mijn voornemen en in paragraaf 6.5 van dit besluit heb getrokken, met dien verstande dat de overtreding tot en met 26 oktober 2022 heeft voortgeduurd.

10.7 Toegangsbeveiliging geautomatiseerde systemen

Vodafone stelt zich op het standpunt dat geen sprake is van een overtreding van artikel V van de bijlage bij het Bbgt, ten aanzien van de toegangsbeveiliging van de geautomatiseerde systemen. De zienswijze van Vodafone is opgesplitst in de volgende onderdelen:

(i) Toegangsbeveiliging geautomatiseerde systemen (paragraaf 10.7.1);
(ii) Persoonsgebonden authenticatie (paragraaf 10.7.2);
(iii) Verouderde versleutelingstechnieken (paragraaf 10.7.3);
(iv) Wachtwoordkwaliteit en versleuteling (paragraaf 10.7.4).

[162] Randnummers 132 – 135.
[163] Randnummers 136 – 140.

10.7.1 Toegangsbeveiliging geautomatiseerde systemen

Vodafone stelt zich in haar zienswijze op het standpunt dat de door RDI gehanteerde maatstaf met betrekking tot de toegangsbeveiliging van geautomatiseerde systemen niet uit het Bbgt, de bijlage of de toelichting op het Bbgt volgt. Daardoor legt RDI volgens Vodafone zonder toereikende (wettelijke) basis internationale standaarden op het gebied van cyberveiligheid, netwerkzonering en updates op aan Vodafone. Hierop kan RDI volgens Vodafone geen overtreding baseren: daarvoor is een basis in het Bbgt vereist.[164]

Mijn reactie

In reactie op de stellingen van Vodafone stel ik voorop dat artikel V van de bijlage bij het Bbgt verschillende, specifieke vereisten stelt aan de toegangsbeveiliging van geautomatiseerde informatiesystemen. Uit de toelichting op het Bbgt blijkt dat de maatregelen die in de bijlage bij het Bbgt zijn voorgeschreven, minimumnormen betreffen. Die maatregelen dienen aanbieders zoals Vodafone dus in ieder geval te treffen met het oog op de beveiliging van LI-gegevens. Uit artikel V, onder a, van de bijlage bij het Bbgt blijkt in dit verband onder andere dat de toegang tot geautomatiseerde informatiesystemen waarin LI-gegevens worden verwerkt op deugdelijke wijze beveiligd dient te zijn. Wat 'op deugdelijke wijze' precies inhoudt, is weliswaar niet voorgeschreven, maar duidelijk is wel, gelet op de aard van de maatregelen en het doel waarvoor deze maatregelen zijn voorgeschreven, dat LI-gegevens dusdanig moeten worden beveiligd dat onbevoegde kennisneming wordt tegengegaan. Hoe hieraan invulling moet worden gegeven, hangt af van de aanbieder zelf (van wat voor soort systemen wordt bijvoorbeeld gebruik gemaakt), maar ook van de technologische ontwikkelingen. Immers, wat 20 jaar geleden een deugdelijke beveiliging van digitale systemen vormde, is dat nu niet meer. Kortom: er zal doorlopend moeten worden nagegaan of de informatiesystemen nog deugdelijk beveiligd zijn.

Om hieraan uitdrukking te geven, is logisch om aan te sluiten bij algemene, in de markt erkende, internationale standaarden. Die standaarden houden immers rekening met de stand van de techniek en zijn daarom bruikbaar voor de beoordeling van de deugdelijke beveiliging. Van een professionele marktpartij als Vodafone, die bovendien werkzaam is binnen de digitale infrastructuren en daar ook haar hoofdactiviteit op richt, mag worden verwacht dat zij van die standaarden op de hoogte is en dat zij die ook in acht neemt.

Dat ik hier in mijn beoordeling van de door Vodafone getroffen maatregelen bij heb aangesloten, is dan ook niet verboden of in strijd met het Bbgt: integendeel. Hiermee geef ik invulling aan het vereiste dat op deugdelijke wijze moet worden voorzien in de beveiliging van LI-gegevens. Ik heb vastgesteld – zoals hiervoor in

[164] Randnummer 142-148.

hoofdstuk 6 is toegelicht – dat Vodafone hier volstrekt in tekort is geschoten, door onder andere gebruik te maken van groepsaccounts, verouderde software updates, verouderde versleutelingstechnieken en onveilige wachtwoorden, welke bovendien niet frequent werden gewijzigd. Hiermee staat hoe dan ook vast dat Vodafone niet had voorzien in een "deugdelijke beveiliging" van de toegang tot geautomatiseerde informatiesystemen waarin LI-gegevens worden verwerkt.

10.7.2 Persoonsgebonden authenticatie

Vodafone stelt zich in haar zienswijze op het standpunt dat de toezichthouder ten onrechte heeft vastgesteld dat kon worden ingelogd op de LI-systemen door middel van niet-persoonsgebonden accounts. Vodafone merkt hierover op dat, alvorens een [VERTROUWELIJK]-medewerker kan inloggen in het [VERTROUWELIJK]-systeem, de medewerker met een persoonsgebonden account dient in te loggen in de [VERTROUW]-omgeving. De toegang voor deze omgeving wordt geregistreerd door [VERTROUW], zodat het volgens Vodafone wel degelijk te achterhalen is welke medewerker met een persoonsgebonden account heeft ingelogd. Vervolgens wordt pas volgens Vodafone met een groepsaccount ingelogd in het [VERTROUWELIJK]-systeem. Voorts wekt RDI volgens Vodafone ten onrechte de suggestie dat [VERTROUWELIJK] medewerkers zelfstandig bij target-informatie kunnen komen.

Voor wat betreft het [VERTROUWELIJ] systeem merkt Vodafone op dat op dit systeem kon worden ingelogd met twee niet-persoonsgebonden accounts. Via één van de twee accounts kon de medewerker van [VERTROUWELIJK] rootgebruiker worden. Ook negen [VERTROUWELIJK] medewerkers konden volgens Vodafone op dezelfde wijze rootgebruiker worden op dit systeem.

Ten aanzien van het gebruik van groepsaccounts voor toegang tot het [VERTROUWELIJK]-systeem voert Vodafone aan dat het [VERTROUWELIJK] account minder rechten bezit en geen toegang heeft tot LI-gegevens. De toegang tot het [VERTROUWELIJK]-systeem vereist een persoonlijk GUI account in combinatie met een persoonlijk door Vodafone verstrekt SSL certificaat. [VERTROUWELIJK]-medewerkers kunnen volgens Vodafone alleen een connectie opzetten via een SSH tunnel vanuit [VERTROUW] naar een intern adres van het [VERTROUWELIJK], met gebruik van een persoonlijk SSH account. Vodafone licht voorts toe dat op het [VERTROUWELIJK] systeem inlogpogingen, inclusief het source IP-adres, te zien waren door middel van audit logging. Daarin worden volgens Vodafone alle gebruikershandelingen binnen de applicatie geregistreerd, inclusief succesvolle en niet-succesvolle inlogpogingen. Bovendien resulteren mislukte inlogpogingen volgens Vodafone in het beperken van de toegang met dat account.[165]

[165] Randnummer 149- 157.

Mijn reactie

Ik volg Vodafone niet in haar standpunt dat om bovenstaande reden geen sprake is van een overtreding. Hieronder licht ik mijn overwegingen toe.

Onderdeel V, onder a van bij bijlage bij het Bbgt schrijft voor dat er sprake moet zijn van een deugdelijke beveiliging van de toegang tot geautomatiseerde informatiesystemen die LI-gegevens bevatten, onder meer door persoonsgebonden authenticatie. Dit betekent dus dat het inloggen op een LI-systeem moet gebeuren door middel van persoonsgebonden authenticatie.

De [VERTROUW]-omgeving is geen geautomatiseerd informatiesysteem waarin LI-gegevens worden verwerkt. Ook medewerkers van Vodafone die geen geoorloofde toegang hebben tot LI-gegevens loggen in op de [VERTROUW]-omgeving. Vanuit de [VERTROUW]-omgeving wordt ingelogd op de LI-systemen van Vodafone. Dat is dus het moment waarop toegang tot LI-gegevens wordt verkregen. De norm van artikel V, onder a van de bijlage bij het Bbgt schrijft voor dat die toegang deugdelijk beveiligd moet zijn, onder meer door persoonsgebonden authenticatie.

Vanuit de [VERTROUW]-omgeving wordt met een groepsaccount ingelogd op het [VERTROUWELIJK]-systeem. De toegang tot dit LI-systeem wordt dus verkregen zonder gebruik te maken van persoonsgebonden authenticatie. Daarmee is de toegang tot LI-gegevens niet op deugdelijke wijze beveiligd, zoals artikel V, onder a van de bijlage bij het Bbgt vereist. Dat via het [VERTROUW]-systeem mogelijk achterhaald kan worden wie er ingelogd heeft, doet niet af aan het feit dat Vodafone niet aan de vereisten voldoet die de Bbgt stelt aan de toegangsbeveiliging.

Ik acht daarom bewezen dat Vodafone op het [VERTROUWELIJK]-systeem geen gebruik maakt van persoonsgebonden authenticatie en daarmee niet voldoet aan de eisten die het Bbgt stelt.

In reactie op het standpunt van Vodafone dat ik volgens Vodafone ten onrechte de suggestie wek dat [VERTROUWELIJK] medewerkers zelfstandig bij target-informatie kunnen komen, overweeg ik het volgende. Mijn toezichthouder heeft vastgesteld dat er een onversleutelde FTP-verbinding tussen het [VERTROUWELIJK] systeem en het [VERTROUWELIJ] systeem aanwezig was, met onversleutelde LI-gegevens.[166] Deze LI-gegevens konden ook door [VERTROUWELIJK] medewerkers worden ingezien vanaf het [VERTROUWELIJK]-systeem, omdat deze medewerkers via hun niet-persoonsgebonden account administratorrechten hadden.[167]

De door Vodafone aangevoerde zienswijze ten aanzien van het [VERTROUWELIJK]-systeem, doet evenmin af aan mijn voornemen en vastgestelde overtreding. Hieronder licht ik mijn overwegingen toe.

---

[166] Rvb, bijlage 5.
[167] Rvb, bijlage 10.

Het onderzoek naar het [VERTROUWELIJK]-systeem heeft op 30 november 2021 via een videogesprek plaatsgevonden door middel van schermdeling van de [VERTROUWELIJK] [VERTROU] medewerker. Van dit onderzoek is een gespreksverslag gemaakt.[168] Daarnaast zijn er gedurende het videogesprek schermafdrukken (ook wel 'screenshots' genaamd) gemaakt. De toezichthouders hebben daarom zelf kunnen waarnemen op welke wijzen toegang tot het [VERTROUWELIJK]-systeem kan worden verkregen. Daarnaast is er tijdens dit onderzoek een door de toezichthouders aangeleverd script met commando's uitgevoerd op zowel de (fysieke) [VERTROUWELIJK] als de daarop geïnstalleerde (virtuele) [VERTROUWELIJK]. Ook hiervan zijn de resultaten vastgelegd en opgenomen in het Rvb.

De toezichthouder heeft, zoals Vodafone aangeeft in haar zienswijze, vastgesteld dat voor een gebruiker van het [VERTROUWELIJK] account geen LI-gegevens zichtbaar zijn in de Graphical User Interface.[169] Echter is uit het onderzoek van de toezichthouder gebleken dat, naast het [VERTROUWELIJK] account, er ook met het zogeheten [VERTROUWELIJK] groepsaccount in de GUI ingelogd kan worden op het [VERTROUWELIJK]-systeem.[170] Voor de gebruiker van dit account zijn wel LI-gegevens zichtbaar in de GUI.[171] Hieruit volgt dus dat dit account toegang heeft tot LI-gegevens en daarom persoonsgebonden authenticatie vereist op grond van artikel V, onder a van de bijlage bij het Bbgt.

Wat betreft de stelling van Vodafone dat toegang tot het [VERTROUWELIJK]-systeem een persoonlijk GUI account in combinatie met een persoonlijk door Vodafone verstrekt SSL certificaat vereist, overweeg ik het volgende.

De toezichthouder heeft op basis van de configuratie vastgesteld dat inloggen op de SSH van zowel de [VERTROUWELIJK] alsook de [VERTROUWELIJK] mogelijk was via het niet-persoonsgebonden account '[VERTROUWELIJK]'. Ook heeft de toezichthouder vastgesteld dat op beide servers ingelogd kon worden met dit account met hetzelfde wachtwoord.[172] De toezichthouder heeft vastgesteld dat de beheerder van [VERTROUWELIJK] bekend was met dit account en het bijbehorende wachtwoord.[173] Uit deze feiten blijkt dat [VERTROUWELIJK] medewerkers konden inloggen met het niet-persoonsgebonden account '[VERTROUWELIJK]' op de [VERTROUWELIJK] om de SSH tunnel op te zetten. Oftewel, de SSH tunnel kon dus worden opgezet met een niet-persoonsgebonden account. Vervolgens kon verbinding gemaakt worden met de GUI, op het niet-persoonsgebonden account [VERTROUWELIJK]. Hiermee konden LI-gegevens ingezien worden.

[168] Rvb, p. 44 en [VERTROUWELIJK]
[169] Rvb, p. 44 en Bijlage 12, onder 7 van het Rvb.
[170] Rvb, p. 44 en Bijlage 12, onder 8 van het Rvb.
[171] Rvb, Bijlage 12, onder 8.
[172] Rvb, Bijlage 13, tweede bullet.
[173] [VERTROUWELIJK]

Op grond van bovenstaande concludeer ik dat er ten aanzien van het [VERTROUWELIJK]-systeem geen sprake is van een deugdelijke beveiliging door middel van persoonsgebonden authenticatie, nu er vanaf de eerste aanraking met het systeem tot de bandering van LI-gegevens een aaneengesloten logisch toegangspad mogelijk was dat bestond uit niet-persoonsgebonden toegang.

Voor wat betreft de stellingen van Vodafone omtrent de logging merk ik het volgende op. Ik stel allereerst overeenkomstig mijn voornemen vast dat er op het [VERTROUWELIJ]-systeem en op het [VERTROUWELIJK]-systeem geen enkele vorm van externe logging is geactiveerd. Hierover heeft Vodafone ook geen zienswijze gegeven. Ook vond er op deze systemen geen detectie plaats op logging ten aanzien van ongeautoriseerde toegang en pogingen daartoe.[174] Hierdoor konden foutieve inlogpogingen niet worden opgemerkt en in het geval van een dergelijke poging kon evenmin een tijdige interventie plaatsvinden.

Ook blijkt uit de zienswijze niet op welke wijze tijdige interventie op ongeautoriseerde toegang(spogingen) plaatsvindt. De toezichthouder heeft geconstateerd dat er geen detectie op logging bij het [VERTROUWELIJK]-systeem plaatsvond.[175] Hierdoor konden foutieve inlogpogingen niet worden opgemerkt en in het geval van een dergelijke poging geen tijdige interventie plaatsvinden.

De stelling van Vodafone dat mislukte inlogpogingen resulteerden in het beperken van de toegang met dat account is niet nader onderbouwd. Zij zet niet uiteen op welke wijze opvolging wordt gegeven aan ongeautoriseerde toegangspogingen en op welke wijze de rechten van dat accounts beperkt zouden worden. Deze stelling kan daarom niet opwegen tegen de bevindingen van de toezichthouder en doet aan bovenstaande niks af.

Wat er verder ook van de audit logging op het [VERTROUWELIJK]-systeem zij, de toezichthouder heeft vastgesteld dat deze logging lokaal geregistreerd wordt. Lokale registratie in de vorm van logging is per definitie onbetrouwbaar, omdat gebruikers met administratorrechten of rootrechten eigenstandig en ongedetecteerd hun handelingen ten aanzien van LI-gegevens in de loghistorie kunnen aanpassen of verwijderen. Dit levert temeer een risico op, gezien het door de toezichthouder vastgestelde feit dat gebruikers van groepsaccounts van het [VERTROUWELIJK]-systeem en het [VERTROUWELIJ]-systeem zichzelf rootrechten kunnen toekennen en gebruikers van groepsaccounts van het [VERTROUWELIJK]-systeem administratorrechten. Hieruit volgt dan ook de conclusie dat deze vorm van logging niet volstaat als logische beveiliging die zodanig is ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

[174] Respectievelijk paragraaf 4.3.3, 4.3.4 en 4.3.5 van het Rvb.
[175] Rvb, p. 47.

10.7.3 Verouderde versleutelingstechnieken
Vodafone stelt zich in haar zienswijze op het standpunt dat uit het Bbgt zelf geen verplichting volgt om een bepaalde versleutelingstechniek te gebruiken. De RDI heeft hierop ook geen beleid uitgevaardigd. Het was daarom volgens Vodafone daarom niet voorzienbaar aan welke standaarden haar versleutelingstechniek volgens de toezichthouder had moeten voldoen. Daarnaast stelt Vodafone dat de vaststelling dat het [VERTROUWELIJK] -systeem gebruik maakt van de protocollen TLSv1.1 en TLSv1 niet correct is. De RDI heeft daarom onvoldoende onderbouwd waarom de wijze van versleuteling onrechtmatig is. Van boeteoplegging kan volgens Vodafone geen sprake zijn.[176]

Mijn reactie

In reactie op de zienswijze van Vodafone, overweeg ik het volgende.

Zoals ik heb overwogen in paragraaf 6.6 volgt uit het Bbgt en de nota van toelichting daarbij duidelijk dat de maatregelen die genomen moeten worden, bij dienen te dragen aan het bewerkstelligen van een minimumniveau van beveiliging van LI-gegevens. Ook blijkt uit de nota van toelichting duidelijk dat de wetgever als doel heeft de beveiliging van LI-gegevens en het voorkomen van een inbreuk op de vertrouwelijkheid daarvan. Daarbij wordt benadrukt dat het noodzakelijk is dat ter zake van de LI-gegevens wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen.[177] Daaruit vloeit logischerwijs voort dat de te treffen beveiligingsmaatregelen aan moeten sluiten bij de huidige stand van de techniek.

Zoals ik heb vastgesteld in paragraaf 6.6.2.1 konden binnenkomende tapverzoeken op de [VERTROUWELIJK] middels protocollen TLSv1.2, TLSv1.1 en TLSv1 versleuteld worden. In onder meer de eerder aangehaalde Special Publication 800-52 Revision 2 van NIST is het gebruik van zowel TLSv1.1 als TLSv1 als onveilig aangeduid. De standaarden van de NIST zijn door de internationale gemeenschap erkend en aanvaard. Van protocollen die als onveilig zijn aangeduid is bekend dat deze een hiaat in de beveiliging vormen. Het aanwezig hebben van onveilige protocollen in een LI-systeem van Vodafone verhoogt de kans op ongeoorloofde toegang tot LI-gegevens. Daarbij is niet relevant dat deze protocollen niet standaard worden gebruikt. Het beveiligingsrisico schuilt in het *kunnen* gebruiken van deze protocollen. Het ligt daarom op de weg van Vodafone om deze onveilige protocollen uit haar LI-systemen te verwijderen, om zo het beoogde doel van het Bbgt, namelijk het bewerkstelligen van een minimumniveau van beveiliging, te bereiken. Dit heeft Vodafone echter nagelaten, waardoor er een grotere kans was op ongeautoriseerde toegang tot haar LI-systemen.

---

[176] Zienswijze, randnummers 158-163.
[177] *Stb.* 2003, 472, p. 7.

Dat ik hierop geen beleid heb uitgevaardigd, is daarbij niet relevant. Van een professionele marktpartij zoals Vodafone mag verwacht worden dat zij op de hoogte is van de geldende wet- en regelgeving en van de maatregelen die genomen moeten worden om het beoogde niveau van beveiliging, zoals het Bbgt dat vereist.

10.7.4 Wachtwoordkwaliteit en versleuteling

Vodafone stelt zich in haar zienswijze op het standpunt dat het onnavolgbaar is dat de toezichthouder de wachtwoorden van het [VERTROUWELIJ]-systeem, [VERTROUWELIJK]-systeem en het [VERTROUWELIJK]-systeem als 'zeer zwak' heeft aangemerkt. Vodafone stelt daartoe dat de toezichthouder niet alle wachtwoorden heeft gecontroleerd en dat bovendien Password Managers wachtwoorden op verschillende manieren kwalificeren. Vodafone stelt daarom dat ik onvoldoende heb aangetoond dat zij op dit punt het Bbgt heeft overtreden.[178]

Mijn reactie

In reactie op de door Vodafone gegeven zienswijze overweeg ik het volgende.

Zoals ik heb overwogen in paragraaf 6.6.2.2 vereist artikel V, onder a van de bijlage bij het Bbgt deugdelijke toegangsbeveiliging van LI-systemen. Accounts waarmee toegang verkregen kan worden tot een LI-systeem dienen derhalve deugdelijk beveiligd te zijn, onder meer door middel van een kwalitatief sterk wachtwoord. De kwaliteit van het wachtwoord en de frequentie waarmee dit wachtwoord wordt gewijzigd, zijn voor de deugdelijkheid van de beveiliging van LI-systemen bepalend.

Naar aanleiding van de door Vodafone gegeven zienswijze, heb ik de motivering in paragraaf 6.6.2.2 aangepast ten opzichte van mijn voornemen, waarbij ik nader gemotiveerd heb welke wachtwoorden zijn gecontroleerd door de toezichthouder en welke bevindingen hieruit voort zijn gekomen. Ik heb vastgesteld dat de wachtwoorden die gebruikt worden voor de onderzochte groepsaccounts om in te loggen op het [VERTROUWELIJ]-systeem, het [VERTROUWELIJK]-systeem en het [VERTROUWELIJK]-systeem zijn aangemerkt als 'zeer zwak' door KeePass. Ook heb ik vastgesteld dat het wachtwoord voor een groepsaccount waarmee ingelogd kon worden op het [VERTROUWELIJK]-systeem op het moment van onderzoek zes jaar en vier maanden niet is gewijzigd.

Daarmee is het risico op ongeautoriseerde toegang van de informatiesystemen die LI-gegevens bevatten sterk aanwezig, nu er gebruik is gemaakt van zwakke wachtwoorden, die niet frequent werden gewijzigd in combinatie met het gebruik van groepsaccounts, waardoor de gebruikte wachtwoorden bij meerdere personen

[178] Zienswijze, randnummers 164-169.

kenbaar waren, tezamen met de vaststelling dat een groot aantal personen inlogpogingen kon doen op de LI-systemen van Vodafone.

Van een deugdelijke logische toegangsbeveiliging van LI-systemen, zoals door artikel V, onder a van de bijlage bij het Bbgt wordt vereist, is daarom geen sprake. De door Vodafone gegeven zienswijze doet mij niet tot een ander oordeel komen.

Concluderend overweeg ik dat de door Vodafone gegeven zienswijze geen aanleiding vormt voor mij om af te wijken van mijn voornemen en het vastgestelde in hoofdstuk 6 van dit besluit.

10.8 Aard, ernst, duur

Vodafone verzoekt om, vanwege de onmiskenbare samenhang tussen verschillende elementen in de zes vermeend zelfstandige overtredingen, volledig af te zien van het Voornemen. Of in ieder geval geen boete van deze omvang op te leggen.[179]

Volgens Vodafone is het Voornemen op diverse plaatsen gebaseerd op niet-onderzochte aannames van de RDI, waarbij overige beveiligingsstappen worden weggelaten. Door dergelijke aannames wordt de potentiële ernst van de vermeende overtredingen ten onrechte substantieel overschat. Vodafone verzoekt de RDI deze punten in het definitieve besluit te corrigeren en deze correcties te betrekken in de vaststelling van de aard en de ernst van de overtredingen en af te zien van het opleggen van en boete, althans de ernst van de overtredingen te heroverwegen.[180]

Vodafone voert in haar pleitaantekeningen aan dat ik de duur van de overtredingen niet goed gemotiveerd heb. De in het voornemen gehanteerde duur is volgens Vodafone geen juiste feitelijke weergave en zou niet aan haar tegengeworpen kunnen worden bij het vaststellen van de boete(hoogte).[181]

Mijn reactie

Allereerst merk ik op dat Vodafone in haar zienswijze niet nader onderbouwt op welke wijze de verschillende elementen in de geconstateerde overtredingen met elkaar samenhangen en waarom deze vermeende samenhang zou moeten leiden tot het volledig afzien van mijn voornemen aan Vodafone een boete voor overtredingen van het Bbgt op te leggen.

Ik overweeg daarom het volgende. In de bijlage bij het Bbgt zijn de beveiligingseisen ten aanzien van LI-gegevens onderverdeeld in verschillende

[179] Pleitaantekeningen, randnummers 2.1 tot en met 2.9.
[180] Pleitaantekeningen, randnummers 4.1 tot en met 4.5.
[181] Zienswijze, randnummers 5.5-5.8.

aspecten, te weten een algemene beveiligingseis in de vorm van het hebben van een beveiligingsfunctionaris, beveiligingseisen ten aanzien van personeel, de fysieke beveiliging van LI-gegevens en de toegangsbeveiliging van geautomatiseerde LI-systemen. Tevens volgen er uit het Bbgt beveiligingseisen ten aanzien van het personeel.

In mijn voornemen ben ik daarom uitgegaan van zes hoofdovertredingen. In dit besluit wordt een boete voor vijf hoofdovertredingen opgelegd. Deze hoofdovertredingen zien elk op een afzonderlijk aspect van de beveiliging van LI-gegevens. Zo heb ik bijvoorbeeld de normen uit onderdeel V van de bijlage bij het Bbgt beoordeeld als één overtreding van het Bbgt. In het geval er samenhang tussen die normen en de geconstateerde feiten zou zijn, wordt dit dus niet aan Vodafone tegengeworpen. Ik zie daarom niet in waarom dit geen zelfstandige overtreding zou zijn, op grond waarvan ik volledig af zou moeten zien van mijn voornemen.

De door Vodafone aangevoerde zienswijze ten aanzien van de ernst van de overtredingen, doet evenmin af aan mijn voornemen.

Voor zover de zienswijze van Vodafone ziet op de feitelijke vaststelling van de overtredingen, ben ik daar op in gegaan in onderdeel 6 van dit besluit. Op de punten waar ik dat nodig achtte, heb ik de motivering ten aanzien van de geconstateerde overtredingen ten opzichte van mijn voornemen aangepast of uitgebreid. Voor het vaststellen van de aard en ernst van de overtredingen in dit besluit, ga ik uit van de in onderdeel 6 vastgestelde overtredingen, waarbij alle relevante feiten en omstandigheden door mij worden meegenomen.

Daaruit rijst overkoepelend het volgende beeld. De beveiliging van de LI-keten van Vodafone voldeed op meerdere onderdelen niet aan de vereisten uit het Bbgt. Zowel organisatorische maatregelen, de beveiligingseisen ten aanzien van personeel, de beveiliging van de fysieke ruimte waarin LI-gegevens zich bevinden als de beveiliging van de geautomatiseerde systemen schoten te kort. De belangen die het Bbgt beoogt de beschermen, de veiligheid van de staat en de integriteit van strafvorderlijke onderzoeken, worden hierdoor ernstig geschaad.

Ik blijf daarom van oordeel dat de geconstateerde overtredingen niet alleen op zichzelf, maar ook in onderlinge samenhang bezien een zeer groot risico vormen voor de vertrouwelijkheid van LI-gegevens. De ernst van de geconstateerde overtredingen acht ik daarom, gelet op de hierboven beschreven belangen, zeer groot.

In reactie op de zienswijze van Vodafone ten aanzien van de duur van de overtredingen overweeg ik het volgende.

Allereerst merk ik op dat Vodafone in haar zienswijze niet vermeld welke consequenties volgens haar verbonden moeten worden aan haar zienswijze ten aanzien van de duur van de overtreding.

Verder merk ik op dat ik in hoofdstuk 6 van dit besluit de duur van de overtreding nader gemotiveerd heb. Ik zie daarom geen aanleiding hier verder in te gaan op de duur van de overtredingen.

10.9 Andere behandeling dan bij vergelijkbare sanctiezaak

Vodafone voert in haar mondelinge zienswijze aan ik geen sanctiebeleid hanteer voor overtredingen van het Bbgt en dat het boetebesluit gericht aan KPN van 30 augustus 2022 het enige haar bekende referentiekader is. Vodafone stelt dat in vergelijking met dit besluit de door mij voorgenomen boetehoogte onnavolgbaar is. Daartoe voert Vodafone het volgende aan.

Vodafone merkt op dat er bij Vodafone, in tegenstelling tot bij KPN, geen aanleiding bestond om een onderzoek te starten.

Vodafone voert aan dat aan KPN een boete is opgelegd voor drie zelfstandige overtredingen, terwijl die overtredingen inhoudelijk vergelijkbaar zijn aan drie van de overtredingen van Vodafone. Ook merkt Vodafone op dat de omvang van het onderzoek bij KPN beperkter lijkt te zijn geweest. Zij noemt hierbij de leveranciers. [182]

Mijn reactie

In reactie op de door Vodafone gegeven zienswijze, overweeg ik het volgende.

Ten aanzien van de stellingen van Vodafone met betrekking tot de aanleiding van het onderzoek merk ik het volgende op. RDI is bevoegd om toezicht te houden op de Tw en het Bbgt. Hierbij mogen toezichtbevoegdheden ingezet worden voor zover dat redelijkerwijs voor de invulling van deze taak nodig is.[183]

Als een van de aanbieders van openbare telecommunicatienetwerken en -diensten is Vodafone daarom onderworpen aan toezicht op de naleving van de Tw en het Bbgt. Toezichthouders van de RDI zetten deze toezichtbevoegdheden ook in bij andere aanbieders van openbare telecommunicatienetwerken en -diensten.

Primair merk ik op dat de stelling van Vodafone dat er zich bij Vodafone geen incident heeft voorgedaan, daarbij niet relevant is. Uit rechtspraak van het CBb blijkt dat toezichthouders beschikken over verschillende bevoegdheden die zij steeds en spontaan kunnen uitoefenen. Daartoe is niet een daaraan voorafgaand en redengevend feit, signaal, grond of vermoeden vereist, zoals volgt uit onderstaande overweging.

[182] Mondelinge zienswijze, randnummers 3.1-3.10.
[183] Artikel 5:11 van de Awb.

> *"Het College volgt niet het standpunt van appellante dat AFM op oneigenlijke gronden en zonder redelijke aanleiding een onderzoek ter plaatste bij appellante heeft ingesteld.*
>
> *Het College overweegt daartoe, onder verwijzing naar zijn uitspraak van 12 oktober 2017 (ECLI:NL:CBB:2017:326), dat AFM en de bij haar werkzame toezichthouders teneinde adequaat toezicht te kunnen uitoefenen op de naleving van de bij en krachtens de Wft gestelde regels, beschikken over verschillende bevoegdheden die zij steeds en spontaan kunnen uitoefenen. Daartoe is niet een daaraan voorafgaand en redengevend feit, signaal, grond of vermoeden vereist."*[184]

De toezichthouder was daarom bevoegd een onderzoek naar de naleving van het Bbgt bij Vodafone te starten, ook wanneer een daaraan voorafgaand feit of signaal niet aanwezig was.

Subsidiair merk ik op dat naar aanleiding van signalen bij een andere aanbieder van openbare telecommunicatienetwerken en –diensten de toezichthouder ervoor heeft gekozen om bij alle grote aanbieders een onderzoek naar de naleving van het bepaalde in het Bbgt te starten.

De toezichthouder heeft zijn onderzoeken naar de naleving van het Bbgt door de aanbieders van openbare telecommunicatienetwerken en –diensten op vergelijkbare wijze uitgevoerd en heeft daarbij in essentie dezelfde systemen onderzocht.

De uitkomsten van het onderzoek bij Vodafone en de uitkomsten van het onderzoek in het door Vodafone aangehaalde sanctiebesluit verschillen op een aantal punten wezenlijk van elkaar. Dat licht ik hieronder toe.

Zoals volgt uit het hiervoor overwogene in dit besluit, had Vodafone over de gehele linie de beveiliging van LI-gegevens niet op orde. Daarmee heb ik geconstateerd dat Vodafone artikel 2, 3, 4 en 8 van het Bbgt in samenhang gelezen met de artikelen I, II, III en V van de bijlage bij het Bbgt heeft overtreden.

Deze overtredingen acht ik niet alleen afzonderlijk, maar zeker ook in onderlinge samenhang bezien ernstig. Een adequate beveiliging bestaat namelijk uit een combinatie van maatregelen op het gebied van preventie en detectie alsook administratieve en personele maatregelen. Hierbij heeft de toezichthouder vastgesteld dat de beveiliging van de LI-keten van Vodafone conceptueel, zoals dient te worden vastgelegd in het beveiligingsplan, als in de daadwerkelijke uitvoering ernstig tekortschoot.

Een groot deel van deze overtredingen zijn bij de andere aanbieder niet geconstateerd. De overtredingen die wel zijn geconstateerd zijn bovendien qua

[184] CBb 15 oktober 2019, ECLI:NL:CBB:2019:496, r.o. 4.1.

omvang en scope veel beperkter dan de geconstateerde overtredingen bij Vodafone. Bovendien betrof de groep die onbevoegde toegang had tot LI-gegevens dezelfde groep als die (onbevoegde) toegang hadden door middel van groepsaccounts. Daarom is bij deze aanbieder niet voor twee separate boetes gekozen, maar achtte ik op basis van deze feiten en omstandigheden een boete passend en geboden.

Dat is bij Vodafone niet het geval. Bij Vodafone schoten de beveiligingsmaatregelen ten aanzien van de LI-gegevens over de gehele linie tekort. Daarbij heb ik meerdere overtredingen geconstateerd dan bij de andere aanbieder het geval was. Bovendien betroffen die geconstateerde overtredingen bij Vodafone verschillende groepen en was de omvang van de overtredingen groter dan bij de andere aanbieder.

In reactie op de door Vodafone gegeven zienswijze ten aanzien van de omvang van het onderzoek van de toezichthouder, overweeg ik het volgende.

De toezichthouder heeft zich bij het onderzoek bij de andere aanbieder ook allereerst gericht op de LI-systemen van deze aanbieder. Wat betreft de LI-systemen van deze aanbieder zijn er geen overtredingen van het Bbgt en de bijlage daarbij geconstateerd. De toezichthouder heeft daarna verder onderzoek gedaan naar de beveiligingsmaatregelen ten aanzien van LI-gegevens binnen de [VERTROUWELIJK] van deze aanbieder. De geconstateerde overtredingen van het Bbgt zien op dat gedeelte van het onderzoek van de toezichthouder.

De toezichthouder heeft zich bij het onderzoek bij Vodafone beperkt tot de LI-systemen. Zoals blijkt uit bovenstaande, heeft de toezichthouder in deze fase van het onderzoek al vijf overtredingen van het Bbgt vastgesteld.

Zoals door mij overwogen, acht ik deze overtredingen zeer ernstig. De LI-systemen bestaan enkel om uitvoering te geven aan taplasten. Het staat daarmee buiten kijf dat deze systemen aan de vereisten van het Bbgt moeten voldoen. Vanwege de geconstateerde overtredingen in de LI-systemen van Vodafone is de toezichthouder niet toegekomen aan een onderzoek naar de beveiligings-maatregelen ten aanzien van LI-gegevens in de [VERTROUWELIJK] van Vodafone.

Ten overvloede merk ik op dat niet door mij is vastgesteld dat zich een beveiligingsincident heeft voorgedaan, bij de aanbieder aan wie het door Vodafone aangehaalde sanctiebesluit is gericht.

Op grond van bovenstaande concludeer ik dat de door mij voorgenomen boetehoogte, ook in vergelijking met een vergelijkbare sanctiezaak, vanwege alle relevante feiten en omstandigheden passend en geboden is. De door Vodafone gegeven zienswijze vormt voor mij geen aanleiding om van mijn voornemen af te wijken.

11. Boetehoogte

11.1 Vaststelling boetehoogte

Op dit moment hanteer ik voor de overtredingen van het Bbgt geen vastgesteld sanctiebeleid. In een casus als de onderhavige kom ik op basis van een afweging van alle relevante omstandigheden en feiten tot een oordeel. Voor het bepalen van de boetehoogte geldt op grond van artikel 15.4 van de Tw een maximumbedrag per overtreding van € 900.000,-.

Hiervoor heb ik reeds toegelicht dat ik de verschillende overtredingen als zeer ernstig heb gekwalificeerd. Bij de kwalificatie heb ik oog gehad voor de belangen die met de naleving van de betrokken bepalingen van het Bbgt zijn gediend en de mate waarin Vodafone deze schendt. Voor dergelijke overtredingen hanteer ik in beginsel een boetebedrag binnen de bandbreedte van € 300.000,- tot € 600.000,- per overtreding.

Zakelijk en verkort weergegeven heb ik, op basis van de onderzoeksbevindingen van mijn toezichthouder, de volgende overtredingen vastgesteld.

Overtreding 1

Artikel 3 van het Bbgt vereist dat de aanbieder zorg draagt voor een beveiligingsplan, waarin hij aangeeft op welke wijze uitvoering is gegeven aan zijn beveiligingsplicht. Dat plan dient ten minste aan te geven op weke wijze uitvoering is gegeven aan de maatregelen genoemd in de bijlage. Bij Vodafone was dit plan niet volledig en bovendien sterk verouderd.

Overtreding 2

Onderdelen van het proces van bevoegd aftappen kan een aanbieder buiten zijn organisatie beleggen. Artikel 8 van het Bbgt vereist in geval van uitbesteding de derde zich verplicht LI-gegevens te beveiligen tegen kennisneming door onbevoegden, dat geheimhouding met betrekking tot die gegevens wordt betracht en dat de ingevolge het Bbgt gestelde maatregelen worden nageleefd. Vodafone heeft onderdelen van haar LI-proces aan derden uitbesteed. Vodafone heeft daarbij de vereiste afspraken niet afdoende volledig en concreet met al haar leveranciers gemaakt.

Overtreding 3

Artikel 4, tweede lid, van het Bbgt vereist – kort en goed – dat de medewerking aan taplasten uitsluitend mag worden verleend door personen aan wie een VOG is verstrekt. In artikel II van de bijlage bij het Bbgt zijn voorts concrete beveiligingseisen ten aanzien van personeel opgenomen. Zo is daarin bepaald dat in de functiebeschrijving van personeel dat belast is met de verwerking van LI-gegevens de verantwoordelijkheid voor de beveiliging daarvan is beschreven (a),

dat personeel dat in aanraking komt met LI-gegevens een geheimhoudingsverklaring tekent (b), en dat uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van LI-gegevens toegang tot die gegevens heeft.

De beveiligingseisen van Vodafone ten aanzien van het personeel waren onvoldoende:

a. Personeel dat niet was belast met verwerking van LI-gegevens had toegang tot de LI-gegevens;
b. Er ontbraken Verklaringen Omtrent Gedrag (VOG's) of daarmee gelijk te stellen documenten van personeel dat belast is met het verwerken van LI-gegevens;
c. Er ontbraken functieomschrijvingen van personeel belast met het verwerken van LI-gegevens;
d. Er ontbraken geheimhoudingsverklaringen van personeel belast met het verwerken van LI-gegevens.

Overtreding 4

In artikel III van de bijlage bij het Bbgt staan concrete vereisten met betrekking tot de fysieke beveiliging en beveiliging van de omgeving waarin LI-gegevens zich bevinden opgenomen.

De fysieke beveiliging van de ruimte waarin LI-gegevens aanwezig waren was onvoldoende:

a. Er kon eenvoudig toegang door onbevoegden tot de fysieke ruimte waarin LI-gegevens aanwezig waren worden verkregen;
b. Toegang tot die fysieke ruimte was niet uitsluitend toegestaan voor geautoriseerde personen voor zover dit voor hun functie noodzakelijk was;
c. Tijdens het onderzoek is gebleken dat er voor onderhoud door niet-geautoriseerde personen geen begeleiding was van een geautoriseerd persoon;
d. Er was geen gecontroleerde en achteraf herleidbare toegang op individueel niveau;
e. Er was geen detectie van toegang tot de fysieke ruimte en ook ontbrak de mogelijkheid tot het tijdig interveniëren.

Overtreding 5

In artikel V van de bijlage bij het Bbgt staan concrete maatregelen met betrekking tot toegangsbeveiliging van geautomatiseerde informatiesystemen opgenomen.

De toegangsbeveiliging tot geautomatiseerde systemen waarin LI-gegevens worden verwerkt was onvoldoende:

a. Op drie systemen was geen sprake van een deugdelijke beveiliging, onder meer doordat persoonsgebonden authenticatie ontbrak;

b. Op drie systemen zat geen blokkering bij overschrijding van drie foutieve inlogpogingen;
c. Op drie systemen was geen externe logging en detectie geactiveerd;
d. Handelingen met betrekking tot de verwerking van de LI-gegevens werden niet persoonsgebonden vastgelegd om onderzoek mogelijk te maken.

De wetgever heeft, gelet op de zwaarwegende aard van de genoemde belangen, ervoor gekozen om op meerdere niveaus minimumbeschermingsmaatregelen voor te schrijven. De minimumbeveiligingsmaatregelen die het Bbgt voorschrijft, vullen elkaar aan. Voor elk van deze overtredingen geldt dat Vodafone het minimumniveau van beveiliging van LI-gegevens dat vereist wordt door het Bbgt niet heeft gehaald, met alle mogelijke risico's van dien. Iedere overtreding in casu is naar mijn oordeel aan te merken als een zeer ernstige overtreding. Voor ieder van de vijf hierboven beschreven 'hoofdovertredingen' leg ik Vodafone, op basis van de door mij vastgestelde aard, ernst, duur en verwijtbaarheid van de overtredingen, daarom een bestuurlijke boete op van € 450.000,-. Ik licht dit hierna toe.

Een aanbieder moet zorg dragen voor het treffen van alle noodzakelijke beveiligingsmaatregelen om kennisneming door onbevoegden te voorkomen. De basis hiervoor wordt gelegd door het hebben van een deugdelijk beveiligingsplan. In het beveiligingsplan moet allereerst aangegeven worden op welke wijze uitvoering wordt gegeven aan de beveiligingsplicht. De functionaris moet vervolgens toezicht houden op de uitvoering en naleving van de beveiligingsmaatregelen. Deze organisatorische maatregelen zijn bedoeld om te borgen dat de minimumbeveiligingsmaatregelen die het Bbgt voorschrijft worden vastgelegd, zodat risico's op ongeoorloofde inbreuk op de LI-systemen worden voorkomen. Het hebben van een deugdelijk beveiligingsplan is het startpunt voor een goede beveiliging van LI-gegevens. Aan deze basisverplichting heeft Vodafone niet voldaan. Dit reken ik Vodafone als professionele partij zwaar aan. Datzelfde geldt voor het feit dat is vastgesteld dat in de overeenkomsten die Vodafone met haar leveranciers heeft gesloten nergens een concrete invulling is gegeven aan de minimumverplichtingen uit het Bbgt.

Verder merk ik op dat niet alleen de organisatorische maatregelen bij Vodafone niet op orde waren. De toezichthouder heeft ook geconstateerd dat de beveiliging daadwerkelijk niet op orde was. De overige hoofdovertredingen - de beveiligingseisen ten aanzien van het personeel, de fysieke ruimte en de geautomatiseerde systemen - bestaan uit meerdere zeer ernstige overtredingen.

Gebleken is dat Vodafone in de gehele LI-keten de beveiligingsmaatregelen niet op orde had. Zowel aan de voorkant, door het nemen van deugdelijke preventieve beveiligingsmaatregelen, als aan de achterkant, door het nemen van detectieve beveiligingsmaatregelen, schoot Vodafone op vele terreinen tekort. De overtredingen vormen niet alleen op zichzelf, maar zeker ook in onderlinge samenhang bezien, een zeer groot risico op ongeautoriseerde kennisname van LI-

gegevens. De veiligheid van de Staat, dan wel het slagen van een strafrechtelijk onderzoek, worden hierdoor ernstig geschaad.

Gelet hierop acht ik het passend en gerechtvaardigd Vodafone per hoofdovertreding een bestuurlijke boete op te leggen van € 450.000,-.

Ik weeg hierin mee dat Vodafone zich meewerkend heeft opgesteld ten tijde van de inspectie. Verder heeft mijn toezichthouder in april 2023 geconstateerd dat Vodafone de meeste overtredingen inmiddels ongedaan heeft gemaakt. Aan de resterende punten is Vodafone hard bezig.

Voor de geconstateerde overtredingen vind ik het daarom passend om aan Vodafone, op basis van de door mij vastgestelde aard, ernst, duur en verwijtbaarheid van de overtreding, een bestuurlijke boete op te leggen van in totaal € 2.250.000,-.

12. Publicatie

12.1 Inleiding

Op grond van artikel 3.1 van de Woo kan ik uit eigen beweging de bij mij berustende informatie voor eenieder openbaar maken, als dit zonder onevenredige inspanning of kosten redelijkerwijs mogelijk is, tenzij de artikelen 5.1, eerste, tweede en vijfde lid, en artikel 5.2 van de Woo aan openbaarmaking in de weg staan of met de openbaarmaking geen redelijk belang wordt gediend. Op grond van deze bepaling kan ik overgaan tot publicatie van het uiteindelijke boetebesluit.

12.2 Belangen die met publicatie zijn gediend

Publicatie van het boetebesluit en het uitbrengen van een persbericht op de website van de RDI acht ik van groot belang. Ik zet dat hieronder uiteen.

In de eerste plaats kan van openbaarmaking in het kader van generale preventie een waarschuwend effect van de openbaarmaking naar andere marktpartijen uitgaan en wordt voor hen inzichtelijk welke gedragingen kunnen leiden tot handhaving en welke invulling ik aan bepaalde normen geef. Openbaarmaking dient daarmee het doel dat de wetgever met artikel 13.5 Tw en het Bbgt voor ogen had, namelijk dat aanbieders ook daadwerkelijk de verplichtingen die aan haar zijn opgelegd - LI-gegevens die aan haar worden verstrekt te beveiligen tegen kennisneming door onbevoegden - opvolgen.

In de tweede plaats hebben burgers en overheid (waaronder de bevoegde autoriteiten als bedoeld in artikel 1, onder c) er belang bij om te weten of de LI-gegevens die berusten bij de aanbieders in voldoende mate tegen ongeoorloofde toegang afgeschermd zijn. Dat weegt te meer nu ongeoorloofde toegang tot LI-gegevens grote risico’s voor de nationale veiligheid en de doelmatigheid van

strafrechtelijke onderzoeken met zich brengt. Zij moeten ook kunnen weten welke onderzoeken de RDI heeft verricht en welke bevindingen, overtredingen en maatregelen naar voren zijn gekomen en of gedurende welke periode de overtredingen voortduurden.

Deze belangen zijn het meest gediend bij een zo ruime mogelijke openbaarmaking. Daarom is het uitgangspunt om in beginsel boetebesluiten wel te publiceren, ook als zij betrekking hebben op onderzoeken naar de beveiliging van LI-gegevens.

Het bovenstaande bezie ik echter ook in de sleutel van de uitzonderingsgronden van de Woo. Daarbij heb ik met name het oog op de gronden in artikel 5.1 van de Woo.

12.3 Zienswijze Vodafone

In haar zienswijze gaat Vodafone in op het publicatievoornemen.[185] Vodafone verzoekt primair enerzijds om af te zien van publicatie van een definitief handhavingsbesluit. Openbaarmaking zou risico voor de veiligheid van de Staat en succesvolle opsporing van strafbare feiten kunnen vormen, vanwege de gedetailleerde wijze waarop het tapproces en de beveiliging daarvan wordt beschreven.

Anderzijds verzoekt Vodafone de publicatie op te schorten totdat een rechterlijk oordeel is geveld over de overtredingen en de (hoogte van de) boete. Publicatie voorafgaand aan een dergelijk rechterlijk oordeel kan tot aanzienlijk onomkeerbaar nadeel leiden voor Vodafone.

Vodafone verzoekt subsidiair te volstaan met het publiceren van een beschrijvend persbericht. Met publicatie van een persbericht kunnen dezelfde doelen worden bereikt zonder de risico's voor de veiligheid van de Staat en succesvolle opsporing van strafbare feiten.

Meer subsidiair betoogt Vodafone dat vertrouwelijke passages uit het handhavingsbesluit moeten worden gelakt. Dit betreft passages die binnen het bereik van artikel 5.1 aanhef sub b, c en lid 2 sub c en f (wellicht sub h) van de Woo vallen. Vodafone verzoekt om dit voorgaande in nauw overleg met haar te doen.

Aangaande het persbericht

Vodafone behoudt zich het recht voor om op het persbericht te reageren nadat het handhavingsbesluit is genomen. Inhoudelijk verzoekt Vodafone in het persbericht

[185] Randnummers 173 – 203.

op te nemen dat niet is vastgesteld dat de overtredingen tot ongeautoriseerde toegang tot LI-gegevens hebben geleid.

12.4 Mijn reactie

Na het voorgaande in overweging te hebben genomen heb ik besloten om het onderhavige besluit ten dele te publiceren, voorzien van een begeleidend persbericht. Deze beslissing is gebaseerd op de bij mij bekende feiten en omstandigheden.

Aan het belang van transparantie en het verstrekken van informatie ken ik de grote waarde toe die ik daaraan rechtens dien toe te kennen.[186] Dit belang draagt bij aan het informeren van de samenleving. De maatschappij krijgt uit de publicatie inzicht in het toezicht op de beveiliging van LI-gegevens en op welke wijze Vodafone in overtreding is (geweest). Ik hecht daarbij ook belang aan de generaal preventieve werking die van publicatie van handhavend optreden uitgaat. Vanuit de preventieratio is het van groot belang dat niet alleen een persbericht, maar ook het boetebesluit ten dele openbaar wordt gemaakt.

De door Vodafone aangehaalde belangen heb ik eveneens in mijn afweging betrokken. Ik heb daarbij ook acht geslagen op de relevante uitzonderingsgronden van artikel 5.1 van de Woo. De door Vodafone benoemde belangen zijn naar mijn oordeel niet van zodanige orde dat van publicatie volledig dient te worden afgezien of te volstaan met publicatie van enkel het persbericht. Ook andere belangen benoemd in artikel 5.1 van de Woo zijn voor mij geen aanleiding om niet tot de voorgenomen wijze van publicatie over te gaan.

Ik onderschrijf de stelling van Vodafone dat zij mogelijk onterecht als overtreder zou worden bestempeld niet. Zoals ik in hoofdstuk 6 uiteen heb gezet, acht ik de overtredingen van het Bbgt bewezen. Ik ben verder van oordeel dat de hoogte van de boete past bij de aard, ernst en duur van de overtredingen en de mate waarin ze aan Vodafone kunnen worden verweten.

Voor zover Vodafone deze stelling in de sleutel van artikel 5.1, vijfde lid, van de Woo plaatst, merk ik op dat zich slechts in uitzonderlijke gevallen onevenredige benadeling voordoet. Naar mijn oordeel is daarvan in de onderhavige zaak geen sprake. Vodafone heeft verder ook niet met feiten en omstandigheden onderbouwd dat zich in dit geval een dergelijke uitzonderlijke situatie voordoet. De enkele stelling dat mogelijk onomkeerbaar nadeel aan de zijde van Vodafone ontstaat acht ik geen dusdanig belang dat het algemeen belang dat met publicatie is gediend daarvoor moet wijken. Ik zie dan ook geen reden om een rechterlijk oordeel af te wachten voordat ik tot publicatie overga.

[186] Zie bijvoorbeeld: ABRvS 13 oktober 2021, ECLI:NL:RVS:2021:2295, ro. 22.1.

Vodafone voert een aantal uitzonderingsgronden aan dat zich tegen publicatie verzet, te weten de staatsveiligheid, de opsporing en vervolging van strafbare feiten, vertrouwelijke bedrijfs- en fabricagegegevens, de beveiliging van personen en bedrijven en het voorkomen van sabotage. Ik neem daarover het volgende in overweging.

Ik heb besloten het boetebesluit gedeeltelijk te publiceren en daarbij beoordeeld welke delen niet openbaar gemaakt kunnen worden op grond van de betrokken uitzonderingsgronden. Het boetebesluit bevat beschrijvingen die apart en gecombineerd inzicht geven in de LI-infrastructuur van Vodafone. Kennis van deze infrastructuur bij kwaadwillenden kan onder meer de staatsveiligheid schaden. Dit geldt evenzeer voor beschrijvingen van LI-processen bij Vodafone en de namen van medewerkers. Die onderdelen zijn weggelakt in de (**als bijlage 4**) bijgevoegde publieksversie van het boetebesluit en zullen niet openbaar worden gemaakt.

Ik merk tot slot het volgende op. Tussen toezending van dit besluit en publicatie daarvan met het begeleidend persbericht hanteer ik een termijn van 5 werkdagen. Dat betekent dat ik op **28 mei 2024** zal publiceren. Indien Vodafone de bestuursrechter verzoekt een voorlopige voorziening te treffen, zal ik de openbaarmaking aanhouden totdat op dat verzoek is beslist.

Vodafone heeft mij tot slot verzocht mijn persbericht aan te vullen, kort gezegd, met de opmerking dat niet is bewezen dat ongeautoriseerd is kennisgenomen van LI-gegevens. In dit verzoek volg ik Vodafone. Uit het onderzoek is inderdaad niet gebleken dat zich ongeautoriseerde kennisname van LI-gegevens heeft voorgedaan. Ik neem deze conclusie op in het (**als bijlage 3 aangehechte**) persbericht.

13. Besluit tot oplegging bestuurlijke boete en publicatie

13.1 Bestuurlijke boete

Gezien het voorgaande leg ik aan Vodafone een bestuurlijke boete van € 2.250.000,- op.

13.1.1 Betalingswijze

Voor de betaling van de bestuurlijke boete dient Vodafone gebruik te maken van de factuur die door het Centraal Justitieel Incassobureau (CJIB) wordt toegezonden.

13.2 Publicatie

13.2.1 Publicatie publieksversie sanctiebesluit op de website van de RDI

Ik zal op grond van artikel 3.1 van de Woo het onderhavige besluit openbaar maken, waarbij rekening wordt gehouden met de uitzonderingsgronden van artikel 5.1 van de Woo door bepaalde passages niet openbaar te maken. Concreet gaat dat om artikel 5.1 lid 1 onder b, c, f, h, lid 2 onder c en lid 5 van de Woo. Publicatie van deze publieksversie vindt plaats op **28 mei 2024** op de website van de RDI.

13.2.2 Persbericht en social media

Ik zal over het onderhavige besluit samen met een persbericht publiceren. In dit persbericht zijn de hoofdlijnen van het onderhavige besluit weergegeven. In de bijlage treft u een afschrift aan van het persbericht. Het persbericht wordt eveneens op **28 mei 2024** op de website van de RDI geplaatst. Daarnaast zal dit op hetzelfde moment door de RDI via LinkedIn worden gedeeld. Het bericht op LinkedIn zal bestaan uit de kop van het persbericht en een link naar het persbericht op de website van de RDI.

14. Bezwaarclausule

Bent u het niet eens met dit besluit?

Als u het niet eens bent met dit besluit dan kunt u, binnen zes weken na de verzenddatum van dit besluit, een bezwaarschrift indienen bij de RDI, ter attentie van het team Juridische Zaken, Postbus 450, 9700 AL Groningen. In uw bezwaarschrift moet het volgende staan:

1. Uw naam en adres;
2. De datum van uw bezwaarschrift;
3. Een omschrijving (of kopie) van het besluit waartegen u bezwaar maakt;
4. De reden waarom u het niet eens bent met dit besluit;
5. Uw handtekening.

Hoogachtend,
De Minister van Economische Zaken en Klimaat,
namens deze,
[VERTROUWELIJK]

mr. F. de Jong-van Kammen
plv. Coördinerend jurist
Rijksinspectie Digitale Infrastructuur

Bijlage 1. Juridisch kader

Van toepassing zijn de Telecommunicatiewet (hierna: Tw), het Bbgt, de bijlage bij het Bbgt en de Wet open overheid (hierna: Woo). De feiten en omstandigheden in deze zaak zijn beoordeeld op grond van deze wettelijke kaders.

In de Telecommunicatiewet, het Bbgt en de bijlage bij het Bbgt staan de kaders voor de beveiliging van gegevens die betrekking hebben op Lawful Interception, dat wil zeggen het bevoegd aftappen of opnemen van telecommunicatie (hierna: LI-gegevens).[187] De te nemen maatregelen in verband met de beveiliging waarborging van LI-gegevens zijn gesteld in het Bbgt en de bijlage daarvan.

De wetgever onderstreept het zwaarwegend belang van geheimhouding en bescherming van LI-gegevens door aanbieders. In de memorie van toelichting bij de Tw is daarover onder meer het volgende opgenomen:

> *'Gegevens betreffende aftappen en informatieverstrekkingen die in het belang van de staat geheim moeten worden gehouden, zijn formele staatsgeheimen en worden bij de overheid aan een beveiligingsregime onderworpen. Deze gegevens dienen ook bij aanbieders van openbare telecommunicatienetwerken en openbare diensten op gelijkwaardige wijze en op basis van een wettelijke bepaling te worden beveiligd. De gegevens waar het hier om gaat zijn bijvoorbeeld abonneegegevens en het feit dat er een tap geplaatst is.*'[188]

Bbgt

In het Bbgt en de bijlage daarvan zijn nadere regels gesteld met betrekking tot de beveiliging van LI-gegevens. Hierin wordt onder meer bepaald welke beveiligingsmaatregelen een aanbieder moet nemen om kennisneming van LI-gegevens door onbevoegden te voorkomen.

In artikel 2, eerste lid, van het Bbgt is - onder meer – bepaald dat de aanbieder zorg draagt voor het treffen van alle noodzakelijke beveiligingsmaatregelen om kennisneming door onbevoegden te voorkomen van de navolgende gegevens en informatie:

> *a. de gegevens welke in het kader van het verlenen van medewerking aan de uitvoering van een bevoegd gegeven bijzondere last dan wel een opdracht op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 tot het aftappen of opnemen van telecommunicatie door een bevoegde autoriteit aan de aanbieder zijn verstrekt;*
> *(…)*

Het tweede lid van artikel 2 van het Bbgt bepaalt dat de maatregelen, bedoeld in het eerste lid, ten minste dienen te bestaan uit:

---

[187] Zie artikel 13.5, eerste lid van de Tw.
[188] Kamerstukken II 1996/97, 25 533, nr. 3, p. 125 (MvT).

a. maatregelen gericht op de personen die werkzaam zijn voor de aanbieder;
b. maatregelen gericht op de toegang tot de gebouwen en ruimten waarin de gegevens en informatie aanwezig zijn;
c. maatregelen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarin de gegevens en informatie worden verwerkt;
d. maatregelen gericht op het voorkomen, vaststellen en onderzoeken van een ongeoorloofde inbreuk op de vertrouwelijkheid van de gegevens en informatie;
e. maatregelen in het geval van calamiteiten.

In artikel 2, derde lid, van het Bbgt is bepaald dat tot de maatregelen, bedoeld in het eerste en tweede lid in ieder geval worden gerekend de maatregelen, bedoeld in de bijlage bij dit besluit.

Artikel 3, eerste lid, van het Bbgt bepaalt dat de aanbieder zorgdraagt voor een beveiligingsplan, waarin hij aangeeft op welke wijze door hem uitvoering is gegeven aan zijn beveiligingsplicht. In het beveiligingsplan wordt ten minste aangegeven op welke wijze uitvoering is gegeven aan de maatregelen, bedoeld in de bijlage.

Artikel 4, tweede lid van het Bbgt bepaalt dat de aanbieder er zorg voor draagt dat aan de uitvoering van de in artikel 13.2, eerste en tweede lid van de wet bedoelde bevoegd gegeven bijzondere last en de in de artikelen 13.2b en 13.4 van de wet neergelegde verplichting tot het verstrekken van informatie, de medewerking uitsluitend wordt verleend door personen, die aan hem een verklaring omtrent het gedrag als bedoeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag hebben overlegd.

Artikel 7 van het Bbgt bepaalt dat de aanbieder er zorg voor draagt dat de personeelsleden die belast zijn met a) de werkzaamheden ter uitvoering van een bevoegd gegeven bijzondere last dan wel een opdracht op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 als bedoeld in artikel 13.2, eerste en tweede lid, van de wet en b) de werkzaamheden verbonden aan de informatieverstrekking als bedoeld in de artikelen 13.2b en 13.4 van de wet, met betrekking tot deze werkzaamheden en de gegevens en informatie waarvan zij in dat kader kennis nemen, geheimhouding betrachten.

Artikel 8, eerste lid, van het Bbgt bepaalt dat indien de aanbieder de uitvoering van werkzaamheden uitbesteedt aan een derde en in dat kader de derde kennis neemt of kan nemen van gegevens en informatie als bedoeld in artikel 2, eerste lid, de aanbieder er zorg voor draagt dat de derde zich verplicht:

a. de desbetreffende gegevens en informatie te beveiligen tegen kennisneming door onbevoegden;
b. met betrekking tot de desbetreffende gegevens en informatie geheimhouding te betrachten;
c. de ingevolge dit besluit gestelde maatregelen na te leven;

d. alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

Ingevolge artikel 8, tweede lid, van het Bbgt worden de verplichtingen van de derde als bedoeld in het eerste lid geregeld in een schriftelijke overeenkomst tussen aanbieder en derde. Op een daartoe strekkend verzoek van de bevoegde autoriteit wordt inzage verleend in de overeenkomst.

In artikel 8, derde lid, van het Bbgt is bepaald dat de aanbieder verantwoordelijk is voor de naleving door de derde van de verplichtingen, bedoeld in het eerste lid.

De toelichting bij het Bbgt benadrukt het uiterst gevoelige karakter van de LI-gegevens en de noodzakelijkheid dat een aanbieder ten aanzien van LI-gegevens adequate beveiligingsmaatregelen neemt teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen en, voor zover een dergelijke inbreuk wel heeft plaatsgevonden, maatregelen te treffen waarmee daarop op een snelle en adequate wijze kan worden gereageerd, zie:

> *"(…) bij artikel 13.4 gaat het om de verplichting tot verstrekking van informatie aan de desbetreffende autoriteiten die zij nodig hebben om een dergelijke taplast op te kunnen stellen dan wel een vordering tot het verstrekken van verkeersgegevens te kunnen doen. Het is evident dat in beide gevallen de desbetreffende gegevens en informatie een uiterst gevoelig karakter hebben. Indien de gegevens bekend zouden worden met betrekking tot wie een taplast is afgegeven, komt – al naar gelang het doel waarvoor de taplast is afgegeven – het welslagen van een strafrechtelijk onderzoek of de veiligheid van de staat in ernstige mate in het geding.*
> *Dit geldt evenzeer voor de informatie die benodigd is om een taplast op te kunnen stellen; ook dan wordt immers kenbaar wie in het belang van het strafrechtelijk onderzoek of de veiligheid van de staat de aandacht van de met opsporing en vervolging van strafbare feiten belaste autoriteiten onderscheidenlijk de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft. Het is dan ook noodzakelijk dat ter zake van de hier bedoelde gegevens en informatie wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen en, voor zover een dergelijke inbreuk wel plaats heeft gevonden, in maatregelen waarmee op een snelle en adequate wijze daarop kan worden gereageerd."*[189]

Daarnaast onderstreept de toelichting bij het Bbgt het belang van tijdige detectie van ongeautoriseerde toegang:

> *"Het is evident dat voorkomen dient te worden dat niet daartoe gerechtigde personen kennis kunnen nemen van de gegevens of de informatie, bedoeld in artikel 2. Geschiedt dat wel, dan is er sprake van een ongeoorloofde inbreuk op de vertrouwelijkheid van die gegevens en informatie. Als gevolg daarvan kan onder meer schade ontstaan voor het desbetreffende strafrechtelijk onderzoek of voor de veiligheid van de staat. Het is dan ook van groot belang dat wordt voorzien in maatregelen die erop gericht zijn te voorkomen dat een dergelijke ongeoorloofde inbreuk kan plaatsvinden en waar deze wel*

[189] NvT bij het Bbgt, *Stb.* 2003, 472, p. 7.

plaatsvindt, deze zo spoedig mogelijk wordt ontdekt. Ingevolge artikel 2, tweede lid, onder d, van het besluit dient de aanbieder daartoe beveiligingsmaatregelen te treffen; in de bijlage bij het besluit is een aantal van deze maatregelen reeds geëxpliciteerd (vergelijk onderdeel V, onder b en e). De door de aanbieder getroffen maatregelen dienen in het in artikel 3 bedoelde beveiligingsplan te worden vastgelegd."[190]

[190] NvT bij het Bbgt, *Stb*. 2003, 472, p. 13.