

> Retouradres Postbus 450 9700 AL Groningen

PER KOERIER

Odido Netherlands B.V.
[VERTROUWELIJK]

Tevens per infoportal verzonden:
[VERTROUWELIJK]

Datum

Betreft Beschikking tot oplegging bestuurlijke boete en publicatie publieksversie
bestuurlijke boete

Geachte heren [VERTROUWELIJK],

1 Inleiding

Hierbij informeer ik Odido Netherlands B.V. (hierna: Odido) dat ik aan Odido een bestuurlijke boete als bedoeld in artikel 15.4, eerste lid, van de Telecommunicatiewet (hierna: Tw) van in totaal € 1.518.750,- opleg. De reden voor de oplegging van de bestuurlijke boete is dat Odido als aanbieder van openbare telecommunicatienetwerken en -diensten onvoldoende zorg heeft gedragen voor het treffen van noodzakelijke beveiligingsmaatregelen om kennisneming van LI-gegevens¹ door onbevoegden te voorkomen. Daarmee heeft Odido een overtreding begaan van de artikelen 2, 3 en 4, van het Besluit beveiliging gegevens telecommunicatie (hierna: Bbgt) in samenhang gelezen met de artikelen II en V van de bijlage bij het Bbgt.

Daarnaast besluit ik een publieksversie van dit besluit alsmede een nieuwsbericht op de website van de Rijksinspectie Digitale Infrastructuur (hierna: RDI) te publiceren op grond van artikel 3.1 van de Wet open overheid (hierna: Woo).

Mijn overwegingen treft u hieronder aan.

2 Samenvatting: kern van het besluit

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. Een essentieel onderdeel is het werk dat onder andere de

¹ Gegevens die betrekking hebben op Lawful Interception, dat wil zeggen het bevoegd aftappen of opnemen van telecommunicatie.

**Rijksinspectie Digitale
Infrastructuur**

Bezoekadres
Emmasingel 1
9726 AH Groningen

Postadres
Postbus 450
9700 AL Groningen

T +31 (0)88 04 16 000
E info@rdi.nl
www.rdi.nl

Contactpersoon
[VERTROUWELIJK]

Ons kenmerk
[VERTROUWELIJK]

Uw kenmerk

Bijlage(n)

1. Juridisch kader
2. Verslag zienswijzezitting
3. Nieuwsbericht
4. Publieksversie besluit

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

**Rijksinspectie Digitale
Infrastructuur**

Ons kenmerk
[VERTROUWEL
1121

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 dan 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 (hierna ook: de aanbieder(s)) 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 van de RDI heeft geconstateerd dat de beveiliging door Odido van LI-gegevens op meerdere punten tekortschoot. Deze tekortkomingen waren zowel op organisatorisch als technisch vlak aanwezig. Het gaat om de volgende hoofdovertredingen.

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 welke wijze uitvoering is gegeven aan de maatregelen genoemd in de bijlage bij het Bbgt. Bij Odido was dit plan niet aanwezig.

Overtreding 2

Artikel 4, tweede lid, van het Bbgt bepaalt – kort en goed – dat de medewerking aan taplasten uitsluitend mag worden verleend door personen aan wie een Verklaring Omtrent het Gedrag (hierna: 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 (c).

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

- a. Er ontbraken VOG's van personeel dat medewerking verleent aan de uitvoering van taplasten;
- b. Er ontbraken functieomschrijvingen van personeel belast met het verwerken van LI-gegevens;
- c. Er ontbraken geheimhoudingsverklaringen van personeel dat in aanraking komt met LI-gegevens.
- d. Personeel dat niet was belast met verwerking van LI-gegevens had toegang tot de LI-gegevens.

**Rijksinspectie Digitale
Infrastructuur**

Ons kenmerk
[VERTROUWEL
11171

Overtreding 3

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 twee systemen was geen sprake van een deugdelijke beveiliging, onder meer doordat persoonsgebonden authenticatie ontbrak en gebruik werd gemaakt van (oude) standaardwachtwoorden;
- b. Op twee systemen was geen blokkering van kracht bij overschrijding van drie foutieve inlogpogingen;
- c. Op twee systemen was geen centrale 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 gezien zeer ernstig. Een adequate beveiliging van LI-gegevens bestaat namelijk uit een combinatie van maatregelen op het gebied van preventie en detectie alsook administratieve en personele maatregelen. De toezichthouder heeft vastgesteld dat de beveiliging van de LI-keten van Odido conceptueel, zoals dient te worden vastgelegd in het beveiligingsplan, als in de daadwerkelijke uitvoering zeer ernstig tekort schoot. In hoofdstuk 8 en 9 licht ik de aard en ernst van deze overtredingen verder toe en motiveer ik waarom deze overtredingen Odido te verwijten zijn. In hoofdstuk 10 en 11 ga ik in op de zienswijze van Odido.

In dit besluit leg ik Odido een bestuurlijke boete op voor elk van de drie hoofdovertredingen. Ook heb ik besloten een publieksversie van het besluit met een begeleidend nieuwsbericht openbaar te maken.

3 Inhoudsopgave

Rijksinspectie Digitale
Infrastructuur

1	INLEIDING.....	1
2	SAMENVATTING: KERN VAN HET BESLUIT	1
3	INHOUDSOPGAVE.....	4
4	JURIDISCH KADER	6
5	ONDERZOEK VAN DE TOEZICHTHOUDER	6
5.1	VERLOOP PROCEDURE	6
5.2	RESULTATEN ONDERZOEK.....	7
5.3	ONDERZOEKSBEVINDINGEN	7
5.4	INRICHTING LI-PROCES ODIDO	8
6	OVERTREDINGEN.....	9
6.1	ONTBREKEN BEVEILIGINGSPLAN	9
6.2	BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL.....	13
6.3	TOEGANG GEAUTOMATISEERDE SYSTEMEN	23
7	HANDHAVINGSBEVOEGDHEID VAN DE RDI	35
8	AARD, ERNST EN DUUR VAN DE OVERTREDINGEN	36
8.1	ALGEMEEN.....	36
8.2	OVERTREDING 1. BEVEILIGINGSPLAN.....	38
8.3	OVERTREDING 2. BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL	38
8.4	OVERTREDING 3. BEVEILIGINGSEISEN TEN AANZIEN VAN DE GEAUTOMATISEERDE SYSTEMEN	39
9	VERWIJTBAAARHEID.....	41
9.1	ALGEMEEN.....	41
9.2	OVERTREDING 1. BEVEILIGINGSPLAN.....	41
9.3	OVERTREDING 2. BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL	41
9.4	OVERTREDING 3. TOEGANG GEAUTOMATISEERDE SYSTEMEN	42
10	ZIENSWIJZE ODIDO.....	42
10.1	ALGEMEEN	43
10.2	OVERTREDING 1. ONTBREKEN BEVEILIGINGSPLAN	46
10.3	OVERTREDING 2. BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL	50
10.4	OVERTREDING 3. TOEGANGSBEVEILIGING	64
11	BOETEHOOGTE.....	69
11.1	VASTSTELLING BOETEHOOGTE.....	69
11.2	MATIGING BOETE VANWEGE DUUR ONDERZOEK.....	70
11.3	TOTALE CUMULATIEVE BOETE	71
12	PUBLICATIE	71
12.1	INLEIDING.....	71
12.2	BELANGEN DIE MET PUBLICATIE ZIJN GEDIEND.....	71
12.3	ZIENSWIJZE ODIDO.....	72
12.4	MIJN REACTIE	73
12.5	PUBLICATIE PUBLIEKSVERSIE BOETEBESLUIT OP DE WEBSITE VAN RDI.....	74
12.6	NIEUWSBERICHT EN SOCIAL MEDIA	74

Ons kenmerk
[VERTROUWEL V
11/21

13	BESLUIT TOT OPLEGGING BESTUURLIJKE BOETE EN PUBLICATIE	74
13.1	BESTUURLIJKE BOETE	74
13.2	PUBLICATIE	75
14	BEZWAARCLAUSULE	75
	BIJLAGE 1. JURIDISCH KADER	77

**Rijksinspectie Digitale
Infrastructuur**

Ons kenmerk
[VERTROUWEL
11/21]

4 Juridisch kader

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

**Rijksinspectie Digitale
Infrastructuur**

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.

Ons kenmerk
[VERTROUWEL
1121

5.1 Verloop procedure

Op 5 oktober 2021 is de toezichthouder een onderzoek gestart naar de naleving van het Bbgt door Odido. Dit onderzoek is afgerond op 14 september 2022. Voor een volledige weergave van het procesverloop gedurende de inspectiefase verwijst ik naar hoofdstuk 2 van het Rapport van bevindingen van 4 februari 2025 (hierna: Rvb).

Per brief van 20 mei 2025, met kenmerk ^[VERTROUWELIJK], heb ik mijn voornemen om een bestuurlijke boete aan Odido en mijn voornemen een publieksversie van dit boetebesluit te publiceren kenbaar gemaakt aan Odido. Als bijlage aan dit voornemen was het Rvb gehecht. Ik heb Odido in de gelegenheid gesteld een zienswijze te geven op mijn voornemen. De termijn hiervoor liep tot 10 juni 2025.

Op 26 mei 2025 heb ik het verzoek van Odido ontvangen om de zienswijzetermijn uit te stellen tot 8 juli 2025.

Op 27 mei 2025 heb ik per e-mailbericht het verzoek van Odido gedeeltelijk gehonoreerd en de zienswijzetermijn verlengd tot 1 juli 2025.

Op 3 juni 2025 heb ik het verzoek van Odido ontvangen om de zienswijzetermijn uit te stellen tot 8 juli 2025.

Op 4 juni 2025 heb ik per e-mailbericht het verzoek van Odido gedeeltelijk gehonoreerd en de zienswijzetermijn verlengd tot 3 juli 2025.

Op 3 juli 2025 heb ik de zienswijze van Odido ontvangen.

Op 8 juli 2025 heeft Odido, bijgestaan door haar gemachtigden, een mondelinge toelichting gegeven op haar zienswijze. Het verslag van de zienswijzezitting is als bijlage 2 aan dit besluit gehecht.

5.2 Resultaten onderzoek

5.2.1 Hoedanigheid Odido

Odido is naast Vodafone Libertel B.V. en KPN B.V. een van de drie bedrijven in Nederland die beschikt over een eigen mobiel netwerk. In 2024 had Odido 7,3 miljoen klanten en een omzet van 2,3 miljard euro.²

De toezichthouder heeft zijn onderzoek gericht op Odido als aanbieder van een openbaar telecommunicatienetwerk of van een openbare telecommunicatiedienst in de zin van artikel 1.1 van de Tw.³

Odido is in het handelsregister van de Kamer van Koophandel ingeschreven onder het nummer 007053022 en is gevestigd op de Waldorpstraat 60 te 's-Gravenhage. Odido is per 12 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 14 september 2022 onderzoek naar de naleving van het Bbgt door Odido verricht. Voor het verloop van het onderzoek verwijs ik naar hoofdstuk 2 van het door mijn toezichthouder opgestelde Rvb van 4 februari 2025 en de daarbij behorende bijlagen.

De toezichthouder heeft zijn onderzoek gericht op drie LI-systemen van Odido waarin de gegevens van alle mobiele aftapverzoeken die in het kader van een taplast aan Odido worden verstrekt om een taplast uit te kunnen voeren, worden verwerkt.⁴ Ik verwijs naar paragraaf 5.4 van dit besluit voor een uitgebreidere omschrijving van deze systemen en een visuele weergave hiervan.

5.3 Onderzoeksbevindingen

De minimumnormen die in de bijlage bij het Bbgt zijn gesteld, beogen een inbreuk op de vertrouwelijkheid van gegevens die gebruikt worden voor strafvorderlijke onderzoeken en van staatsgeheime informatie te voorkomen, en voor zover een dergelijke inbreuk wel heeft plaatsgevonden, in maatregelen waarmee op een snelle en adequate wijze daarop kan worden gereageerd. Voorgeschreven zijn maatregelen die beogen te voorkomen dat ongeautoriseerde toegang plaatsvindt, maatregelen die toegang registreren en maatregelen die een tijdige detectie van ongeautoriseerde toegang mogelijk maken.

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.

² Odido Netherlands B.V. Annual Report 2024, zoals gedeponereerd bij de Kamer van Koophandel op 30 april 2025.

³ Bij de start van het onderzoek heette Odido nog T-Mobile Netherlands B.V. T-Mobile is van naam veranderd naar Odido in september 2023.

⁴ Rvb, p. 5.

5.4 Inrichting LI-proces Odido

Rijksinspectie Digitale
Infrastructuur

De toezichthouder heeft vastgesteld dat bij de uitvoering van taplasten één leverancier van Odido is betrokken, te weten [VERTROUWELIJK] (hierna: [VERTROUWELIJK]). [VERTROUWELIJK] is een leverancier van een LI-systeem die een technische rol vervult in de LI-keten.

Ons kenmerk
[VERTROUWELIJK]
1121

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

[VERTROUWELIJK]

Figuur 1. Schematische weergave inrichting LI-proces Odido⁵

De toezichthouder heeft op basis van het onderzoek, diverse gesprekken, documenten en onderzochte systemen (en diens functionaliteiten) het LI-proces ten aanzien van mobiele aftapverzoeken bij Odido uitgewerkt in bovenstaand schema en onderstaande stappen. Het proces voor bevoegd aftappen bestaat, verkort weergegeven, uit de volgende stappen⁶:

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.⁷

[VERTROUWELIJK]

⁵ Rvb, p. 17.

⁶ Rvb, p. 17 en 18.

⁷ De Officier van Justitie kan dit slechts bevelen na schriftelijke machtiging van de rechter-commissaris. Voor de AIVD en MIVD geldt dat deze bevoegdheden slechts uitgeoefend mogen worden na toestemming door de Minister van Binnenlandse zaken en Koninkrijksrelaties respectievelijk de Minister van Defensie aan het hoofd van de betreffende dienst.

5. De afgetapte informatie wordt door de [VERTROUWELIJK] en het [VERTROUWELIJK] 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 en op te treffen beveiligingsmaatregelen ten aanzien van personeel dat in aanraking komt met LI-gegevens.

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 de getroffen beveiligingsmaatregelen ten aanzien van de LI-keten van Odido onderzocht, namelijk de logische beveiliging van de drie systemen die LI-gegevens bevatten, te weten de [VERTROUWELIJK] van de [VERTROUWELIJK] (hierna: [VERTROUWELIJK])⁸, [VERTROUWELIJK] en de LI-Firewall. Deze LI-systemen worden door Odido gebruikt bij het bevoegd aftappen in de zin van artikel 13.2 van de Tw. Daarnaast heeft de toezichthouder de getroffen beveiligingsmaatregelen ten aanzien van personeel dat (kort gezegd) belast is met de verwerking van LI-gegevens onderzocht. Ook heeft de toezichthouder onderzoek gedaan naar het beveiligingsplan. Op basis van het onderzoek heeft de toezichthouder vastgesteld dat Odido in totaal negen normen uit het Bbgt en de bijlage heeft overtreden. Deze overtredingen zijn door mij zijn gegroepeerd in drie hoofdovertredingen. In de hiernavolgende paragrafen worden de constatering van de toezichthouder besproken per onderdeel waar de norm van het Bbgt op ziet.

6.1 Ontbreken 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.

⁸ [VERTROUWELIJK]

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.

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
1121

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 RDI/JZ)

Uit de nota van toelichting van het Bbgt volgt ook dat het beveiligingsplan niet aan bijzondere vormvereisten is gebonden en jaarlijks moet worden geüpdatet:

"(...) Het beveiligingsplan is niet aan bijzondere vormvereisten gebonden; de aanbieder is dan ook vrij om te bepalen in welke vorm en omvang hij het beveiligingsplan giet. (...)

Naast de eenmalige kosten die aan het opstellen van een beveiligingsplan zijn verbonden, dienen ook kosten te worden gemaakt om de plannen actueel te houden, waarbij wordt uitgegaan van een jaarlijkse up-date; (...)"¹²

Odido moet als aanbieder aan artikel 3, eerste lid, van het Bbgt voldoen en over een beveiligingsplan beschikken. Uit de wettekst, in samenhang gelezen met de nota van toelichting daarbij, zoals hierboven is opgenomen, blijkt duidelijk dat het aan Odido is om de omvang en de vorm van het beveiligingsplan te bepalen. In het beveiligingsplan moet echter minimaal zijn opgenomen op welke wijze de aanbieder uitvoering geeft aan zijn beveiligingsplicht. Daarbij moet de aanbieder ten minste aangeven op welke wijze door hem uitvoering is gegeven aan de

⁹ Stb. 2003, 472, p. 10.

¹⁰ Stb. 2003, 472, p. 13.

¹¹ Stb. 2009, 350, p. 6 en 7.

¹² Stb. 2003, 472, p. 16.

maatregelen genoemd in de bijlage bij het Bbgt. Daarnaast moet het beveiligingsplan jaarlijks worden ge-updatet.

**Rijksinspectie Digitale
Infrastructuur**

De bijlage bij het Bbgt bevat zes categorieën van de te treffen beveiligingsmaatregelen, 1) te weten 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.

Ons kenmerk
[VERTROUWEL
11/21]

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.¹³ Bovendien volgt uit de nota van toelichting dat hierbij specifieke aandacht besteed moet worden aan het onderscheid in de verschillende beveiligingsregimes.¹⁴

De toezichthouder heeft het beveiligingsplan, als bedoeld in artikel 3, eerste lid, van het Bbgt, bij Odido opgevraagd op 5 oktober 2021:

"Aanleveren binnen 1 week na verzoek

*- De BBGT beveiligingsplannen zoals benoemd in het BBGT onder artikel 3.
(...)"*

De toezichthouder heeft het beveiligingsplan op 13 oktober 2021 van Odido ontvangen. Odido geeft daarbij de volgende toelichting::

"Ik heb zojuist de gevraagde documenten die vandaag moesten worden opgeleverd via de AT portal naar je ge-upload.

Het gaat om de volgende documenten:

- De BBGT beveiligingsplannen (...)"

De toezichthouder heeft vervolgens bij Odido vier aanvullende documenten opgevraagd:

"Wel hebben we als AT de vraag of een 4-tal in het beveiligingsplan genoemde documenten ook gedeeld kunnen worden, dit kan tegelijkertijd met de resterende documenten uiterlijk dinsdag 19 oktober 2021.

1. Group Security Policy Versie 1.1 Laatste wijziging Maart 2021

2. Physical Security Policy Versie 1.0 Laatste wijziging December 2020

3. TMNL Policy Core Locations Versie 1.6 Laatste wijziging September 2021

4. Screening Beleid Versie 1.0 Laatste wijziging Oktober 2021

(...)"

De toezichthouder heeft de aanvullende documenten op 19 oktober 2021 van Odido ontvangen.

¹³ Stb. 2009, 350, p. 10.

¹⁴ Stb. 2009, 350, p. 7.

In paragraaf 4.3.2 van het Rvb heeft de toezichthouder een verslag opgenomen van het onderzoek naar het beveiligingsplan. Samengevat blijkt daaruit het volgende.

De toezichthouder heeft vastgesteld dat Odido één PDF-bestand heeft aangeleverd dat volgens Odido zou zijn aan te merken als een beveiligingsplan in de zin van artikel 3, eerste lid, van het Bbgt. Dit betreft het document 'TMNL Beveiligingsplan Lawfull Intercept'. De toezichthouder heeft vastgesteld dat het aangeleverde beveiligingsplan versie 1.0 betreft en dat er ten aanzien van alle datums alleen de maand en het jaartal zijn opgenomen. Daaruit is gebleken dat het document dateert van oktober 2021. Vervolgens heeft de toezichthouder op basis van de metadata van het PDF-bestand vastgesteld dat het aangeleverde beveiligingsplan is aangemaakt op 13 oktober 2021. Op basis hiervan heeft de toezichthouder vastgesteld dat het beveiligingsplan nieuw is aangemaakt en eerder niet bestond. Oudere plannen dan het plan dat in oktober 2021 is opgesteld, heeft de toezichthouder niet ontvangen van Odido. Op basis daarvan heeft de toezichthouder vastgesteld dat Odido tot 13 oktober 2021 niet beschikte over een beveiligingsplan.

Het voorgaande is bevestigd door Odido. Uit het verslag van een gesprek tussen de toezichthouder en Odido, dat heeft plaatsgevonden op 29 oktober 2021, blijkt dat een medewerker van Odido heeft aangegeven dat het aangeleverde beveiligingsplan de eerste versie van het beveiligingsplan is en er geen voorgaande versies waren. Uit het verslag van een gesprek tussen de toezichthouder en Odido, dat heeft plaatsgevonden op 29 oktober 2021, volgt eveneens dat voorafgaand aan het opstellen van het beveiligingsplan er alleen 'losse snippets' waren. [VERTROUWELIJK]

15

Op verzoek van de toezichthouder heeft Odido op 19 oktober 2021 vier aanvullende documenten aangeleverd. Ook met deze documenten wordt niet aan artikel 3, eerste lid, van het Bbgt voldaan, omdat niet voor alle maatregelen uit de bijlage bij het Bbgt gestructureerd is aangegeven hoe daaraan uitvoering is gegeven. Deze documenten zijn, nog los van de vraag wanneer deze documenten zijn opgesteld, ook mede daarom niet aan te merken als een beveiligingsplan in de zin van artikel 3, eerste lid, van het Bbgt.

Wat betreft de duur van de overtreding overweeg ik als volgt. Uit het onderzoek van de toezichthouder volgt dat Odido pas vanaf 13 oktober 2021 over een beveiligingsplan beschikte. Odido beschikte daarvoor in het geheel niet over een beveiligingsplan en heeft pas een beveiligingsplan opgesteld toen de toezichthouder dit plan opvroeg.

Het voorgaande levert een overtreding op van artikel 3, eerste lid, van het Bbgt voor in ieder geval de periode van 5 oktober 2021¹⁶ tot en met 12 oktober 2021.

¹⁵ [VERTROUWELIJK]

¹⁶ Dit is de datum waarop het onderzoek van de toezichthouder is gestart.

6.2 Beveiligingseisen ten aanzien van personeel

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 4, tweede lid, van het Bbgt in samenhang gelezen met artikel 2, tweede en derde lid, van het Bbgt en artikel II, onder a, b en c, van de bijlage bij het Bbgt, gericht op het treffen van noodzakelijke beveiligingsmaatregelen ten aanzien van personeel.¹⁷

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 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.*

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 in de zin van het Bbgt, een VOG (of een VGB)¹⁸ en dat een geheimhoudingsverklaring in de zin van het Bbgt heeft getekend, toegang mag hebben tot LI-gegevens, LI-gegevens mag verwerken of daarmee in aanraking mag komen. Ongeautoriseerde toegang tot LI-gegevens, dat wil zeggen toegang door personen die aan voormelde eisen niet voldoen, is verboden.

Onderdelen van het proces van bevoegd aftappen kan een aanbieder uitbesteden. Op deze situatie ziet artikel 8 van het Bbgt. Dit artikel 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;*

¹⁷ Ook wel aangeduid als Bbgt HR.

¹⁸ Voor een verklaring van geen bezwaar (VGB) vindt een zwaardere screening plaats dan voor VOG en geschiet voor personen met een vertrouwensfunctie (zoals bedoeld in het nog niet in werking getreden artikel 4, eerste lid, van het Bbgt).

- 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.

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. De eisen die het Bbgt stelt aan personeel dat in aanraking komt en belast is met de verwerking van LI-gegevens zijn onderdeel van die maatregelen. Odido draagt met andere woorden de verantwoordelijkheid voor het feit dat de normen uit het Bbgt door een leverancier worden nageleefd, indien zij tot uitbesteding besluit.

6.2.1 Geautoriseerde toegang

Op grond van het Bbgt mag alleen toegang worden verkregen tot LI-gegevens door geautoriseerd personeel. Daarvoor geldt een aantal vereisten,¹⁹ die volgen uit artikel 4, tweede lid, van het Bbgt en uit artikel II, onder a en b, van de bijlage bij het Bbgt.

De toezichthouder heeft bij de aanvang van het onderzoek op 5 oktober 2021 een uitvraag gedaan naar de VOG's (of VGB's), de functieomschrijving in de zin van het Bbgt en de geheimhoudingsverklaring in de zin van het Bbgt van medewerkers die onder het Bbgt HR-regime vallen:

"Lijst met medewerkers per datum 6 oktober 2021 onder BBGT HR Regime zoals bedoeld onder Bijlage BBGT II onder a, b en BBGT artikel 4 lid 2;

- o Volledige naam van medewerker
- o Functie van medewerker
- o Datum ondertekening geheimhoudingsverklaring
- o Datum (ondertekening) functiebeschrijving
- o Datum afgifte VOG of VGB (aangeven welke van toepassing is)

(...)"

Odido heeft op 13 oktober 2021 een overzicht aangeleverd, te weten TMNL – Overzicht medewerkers LI, waarop vier medewerkers staan die volgens Odido onder het Bbgt HR Regime vallen.

Vervolgens heeft er op 29 oktober 2021 een gesprek plaatsgevonden tussen de toezichthouder en Odido. Tijdens dit gesprek heeft de toezichthouder inzage gehad in de VGB's en de arbeidsovereenkomsten van de vier medewerkers. Odido heeft vervolgens op 5 november 2021 de betreffende arbeidsovereenkomsten aangeleverd bij de toezichthouder.

¹⁹ Ook wel aangeduid als Bbgt HR.

Op 16 december 2021 heeft de toezichthouder het kantoor van Odido en het kantoor van ^[VERTROUWELIJK] bezocht. Op 7 februari 2022 heeft Odido aanvullende stukken opgestuurd ten aanzien van de Bbgt HR-administratie.

Rijksinspectie Digitale
Infrastructuur

Vervolgens heeft de toezichthouder op 19 juli 2022 informatie gevorderd:

Ons kenmerk
[VERTROUWELIJK]

*"Op basis van artikel 5.16 en 5.17 van de Awb vorder ik in verband met voornoemde inspectie de navolgende informatie/bescheiden:
De volledige Bbgt HR administratie, van personen die toegang hebben tot LI-informatie, waaruit blijkt dat de beveiligingseisen ten aanzien van deze personen zijn genomen. (...)*

Per persoon acht ik drie documenten relevant:

- 1. De LI-specifieke functieomschrijving⁴*
- 2. De LI-specifieke getekende geheimhoudingsverklaring⁵*
- 3. De verklaring omtrent het gedrag (VOG)⁶*

(...)"

In reactie op deze vordering heeft Odido op 26 augustus 2022 aangegeven dat de (rechtsvoorganger) van de RDI al beschikte over alle relevante informatie.

" (...) Ten gevolge daarvan is T-Mobile van mening dat AT al beschikt over de relevante gevorderde informatie."

Vervolgens is het onderzoek naar de Bbgt HR administratie afgesloten met een laatste brief van 14 september 2022. Daarin is onder andere aangegeven:

" (...) Uit uw reactie trek ik daarom de conclusie dat u niet aan mijn vordering kunt voldoen omdat er – los van de vraag of dit al dan niet verplicht is – naast de vier T-Mobile medewerkers geen andere personen zijn waarop T-Mobile voormelde eisen uit het Bbgt heeft toegepast. Bij het vervolg van het onderzoek zal ik dit daarom tot uitgangspunt nemen."

Hierop is geen reactie van Odido gekomen. Door de toezichthouder is vastgesteld dat aan de vereisten ten aanzien van geautoriseerd personeel om meerdere redenen niet is voldaan. Dit zet ik hieronder nader uiteen.

a. Geen VOG

Uit artikel 4, tweede lid, van het Bbgt volgt dat personeel dat belast is met de verwerking van LI-gegevens moet beschikken over een VOG (of VGB). De toezichthouder heeft op 5 oktober 2021 een uitvraag gedaan naar de VOG (of VGB's), van medewerkers die belast zijn met de verwerking van LI-gegevens. Ook heeft de toezichthouder de VOG's (of VGB) van de betreffende medewerkers gevorderd op 19 juli 2022. Door Odido is inzage geboden in de VGB's van vier medewerkers van Odido.

De toezichthouder heeft op 16 december 2021 vastgesteld dat vijf medewerkers van ^[VERTROUWELIJK] toegang hadden tot LI-gegevens. Deze medewerkers zijn belast met het eerste- en tweedelijns beheer van het ^[VERTROUWELIJK]. Onder de werkzaamheden van eerstelijns beheer worden de simpele handelingen en het

oplossen van simpele verstoringen verstaan. Dit zijn gangbare zaken die met simpele (vaak generieke) handelingen kunnen worden afgedaan (bijvoorbeeld opnieuw opstarten, instellingen wijzigen, accounts aanmaken). Onder de werkzaamheden van tweedelijnsbeheer worden alle andere zaken ten aanzien van het systeem verstaan zoals grote/complexere wijzigingen, vernieuwingen en het verhelpen van verstoringen. Onder zowel eerste- als tweedelijns beheer valt het verhelpen van storingen. Deze medewerkers van [VERTROUWELIJK] zijn dus onmisbaar in het proces van het geven van uitvoering aan een taplast. Zonder de werkzaamheden van de [VERTROUWELIJK] kan immers door Odido niet goed uitvoering aan taplasten worden gegeven. Uit het voorgaande volgt dat de vijf medewerkers van [VERTROUWELIJK] uit hoofde van hun functie geautoriseerde toegang hadden tot en zijn belast met het verlenen van medewerking aan taplasten (en daarmee ook met de verwerking van LI-gegevens).²⁰

Uit artikel 8, derde lid, van het Bbgt volgt dat Odido verantwoordelijk is voor de naleving van de eisen die het Bbgt stelt aan de medewerkers van [VERTROUWELIJK]. Artikel 4, tweede lid, van het Bbgt bepaalt in dat verband dat uitsluitend de medewerking wordt verleend aan de uitvoering van taplasten door personen die aan de aanbieder, Odido dus, een VOG hebben overgelegd. Met betrekking tot de vijf medewerkers van [VERTROUWELIJK] heeft Odido na een uitvraag en een vordering van de toezichthouder geen kopieën verstrekt of inzage geboden in de relevante documenten, waaronder de VOG's. De toezichthouder heeft daarop vastgesteld dat Odido niet beschikt over de benodigde en opgevraagde VOG's.²¹

Bij haar zienswijze van 3 juli 2025 heeft Odido alsnog VOG's overgelegd van de vijf medewerkers van [VERTROUWELIJK]. Ondanks dat deze VOG's dateren van voor 5 oktober 2021, is niet vast komen te staan dat Odido ten tijde van het onderzoek beschikte over deze VOG's. Integendeel. Zoals hiervoor is toegelicht, heeft de toezichthouder vastgesteld dat Odido ten tijde van het onderzoek niet beschikte over de desbetreffende VOG's. Tijdens de zienswijzezitting van 7 juli 2025 is door Odido ook bevestigd dat zij ten tijde van het onderzoek niet over deze VOG's beschikte.

De toezichthouder heeft verder vastgesteld dat de beheerder van het [VERTROUWELIJK], die in dienst is van Odido, in de periode van in ieder geval 5 oktober 2021 tot en met 14 september 2022 toegang had tot LI-gegevens op het USN-systeem. Voor deze beheerder geldt dat zijn werkzaamheden bestaat uit het eerste- en tweedelijns beheer²² van het [VERTROUWELIJK]. Kortgezegd bestaan zijn werkzaamheden uit het zorgen voor de blijvende goede werking van de digitale infrastructuur van Odido in de vorm van regulier onderhoud en het verhelpen van technische problemen en het installeren van updates ten behoeve van verbeteringen. Zonder de werkzaamheden van de beheerder kan daarom niet goed uitvoering aan taplasten worden gegeven. De toezichthouder heeft vastgesteld dat de [VERTROUWELIJK] als root-gebruiker kon inloggen op het [VERTROUWELIJK] en toegang had tot LI-gegevens.²³ Uit het voorgaande volgt dat de [VERTROUWELIJK] uit hoofde van zijn functie toegang nodig had tot en belast is met het

²⁰ Rvb, p. 39 en 40.

²¹ Rvb, p. 40 en 47.

²² Zie ook de hiervoor gegeven uitgebreide uitleg over de begrippen eerste- en tweedelijnsbeheer op pagina 15 van dit besluit.

²³ Rvb, p. 36 en 47.

verlenen van medewerking aan taplasten (en daarmee ook met de verwerking van LI-gegevens).

Na de uitvraag van de toezichthouder van 5 oktober 2021 heeft Odido geen inzage geboden in de VOG (of VGB) van de [VERTROUWELIJK]. Gedurende de inspectie van de RDI heeft Odido een extern screeningsonderzoek laten uitvoeren. Uit een rapportage van dit externe screeningsonderzoek, gedateerd op 3 december 2021 en dat is overgelegd aan de toezichthouder op 7 februari 2022, volgt dat de [VERTROUWELIJK] beschikt over een VOG.²⁴ De toezichthouder heeft evenwel geconstateerd dat de het screeningsonderzoek dateert van na de aanvang van zijn onderzoek op 5 oktober 2021. Hiervoor geldt dat er niet voldaan is aan de gestelde eisen van het Bbgt, nu de VOG voor de [VERTROUWELIJK] bij aanvang van het onderzoek ontbrak.

Het voorgaande levert een overtreding op van artikel 4, tweede lid, van het Bbgt voor in ieder geval de periode van 5 oktober 2021²⁵ tot en met 14 september 2022.²⁶

b. Geen functieomschrijving

Uit artikel II, onder a, van het Bbgt volgt dat in de functieomschrijving van personeel dat dat belast is met de verwerking van LI-gegevens de verantwoordelijkheid voor de beveiliging van LI-gegevens moet zijn beschreven. De toezichthouder heeft op 5 oktober 2021 een uitvraag gedaan naar functies van de medewerkers die belast zijn met de verwerking van LI-gegevens. Odido heeft in reactie op deze uitvraag een lijst met vier medewerkers aangeleverd. Vervolgens heeft de toezichthouder inzage gehad in en zijn door Odido kopieën verstrekt van de arbeidsovereenkomsten van deze vier medewerkers. De toezichthouder heeft de LI-functieomschrijvingen van alle overige personen, die belast zijn met de verwerking van LI-gegevens, nogmaals opgevraagd door middel van de vordering van 19 juli 2022. Naar aanleiding van de vordering heeft Odido geen informatie dan wel bescheiden overgelegd die zien op de LI-functieomschrijvingen van de overige personen.

De toezichthouder heeft vastgesteld dat drie van de vier door Odido opgegeven medewerkers²⁷ toegang hadden tot LI-gegevens, doordat zij beschikten over een account in de [VERTROUWELIJK].²⁸ Uit het verslag van een gesprek tussen de toezichthouder en Odido, dat heeft plaatsgevonden op 29 oktober 2021, volgt dat deze medewerkers binnengekomen tapverzoeken behandelen, tapverzoeken doorzetten en het aanspreekpunt zijn voor vragen van de bevoegde autoriteiten. Gelet hierop zijn deze medewerkers belast met de verwerking van LI-gegevens.

Op het overzicht dat Odido heeft aangeleverd op 13 oktober 2021 staan bij deze drie medewerkers de functietitels [VERTROUWELIJK]

. Uit dit overzicht

²⁴ Rvb. p. 25 en 47.

²⁵ Dit is de datum waarop het onderzoek van de toezichthouder is gestart.

²⁶ Op 14 september 2022 is het traject met betrekking tot de Bbgt HR-vordering van 19 juli 2022 afgesloten met een laatste brief vanuit de RDI.

²⁷ Dit betreffen drie van de vier personen die zijn opgenomen in het TMNL Overzicht medewerkers LI.

²⁸ [VERTROUWELIJK]

volgen geen functieomschrijvingen waarin de verantwoordelijkheden zijn beschreven voor de beveiliging van LI-gegevens. Bij de zienswijze heeft Odido een functieomschrijving van 12 april 2019 aangeleverd voor [VERTROUWELIJK]

waarin verantwoordelijkheden zijn beschreven ten aanzien van LI-gegevens. Deze functieomschrijving komt overeen met de functietitel van één persoon uit het overzicht van 13 oktober 2021. Uit de overlegde functieomschrijving volgt echter niet dat deze medewerker ten tijde van het onderzoek ook bekend was met deze functieomschrijving.

Op verzoek van de toezichthouder heeft Odido van deze drie LI-medewerkers op 5 november 2021 een arbeidsovereenkomst overgelegd. De toezichthouder heeft vastgesteld dat deze drie arbeidsovereenkomsten geen functiebeschrijving bevatten waarin de verantwoordelijkheid is beschreven voor de beveiliging van LI-gegevens zoals bedoeld in het Bbgt. Uit de functieomschrijvingen volgt niet dat aan deze medewerkers een LI-taak is toebedeeld en dat die taak ook tot hun functie behoort. Zoals hiervoor is beschreven, zijn er ook geen andere documenten overgelegd waaruit een functiebeschrijving blijkt waarin de verantwoordelijkheid is beschreven voor de beveiliging van LI-gegevens.

De toezichthouder heeft vastgesteld dat voor de vijf medewerkers van [VERTROUWELIJK], zoals hierboven genoemd onder a, en voor de beheerder van het [VERTROUWELIJK], zoals hierboven genoemd onder a, die uit hoofde van hun functie belast zijn met de verwerking van LI-gegevens, na een uitvraag en een vordering, door Odido geen kopieën zijn verstrekt of inzage is geboden in relevante documenten, waaronder arbeidsovereenkomsten dan wel functieomschrijvingen. Daarop heeft de toezichthouder geconcludeerd dat de functieomschrijvingen waarin de verantwoordelijkheid is beschreven voor de beveiliging van LI-gegevens, zoals bedoeld in het Bbgt, voor deze zes medewerkers niet aanwezig waren.²⁹

Bij de zienswijze heeft Odido van de [VERTROUWELIJK] een arbeidsovereenkomst overgelegd met als ingangsdatum [VERTROUWELIJK]. Uit deze arbeidsovereenkomst is op te maken dat de beheerder ten tijde van het onderzoek de functie van [VERTROUWELIJK] vervulde. Deze arbeidsovereenkomst bevat ook geen functieomschrijving waarin de verantwoordelijkheid is beschreven voor de beveiliging van LI-gegevens.

Het voorgaande levert een overtreding op van artikel II, onder a, van de bijlage bij het Bbgt voor in ieder geval de periode van 5 oktober 2021³⁰ tot en met 14 september 2022.³¹

c. Geen geheimhoudingsverklaring

Uit artikel II, onder b, van het Bbgt volgt dat personeel dat in aanraking komt met LI-gegevens over geheimhoudingsverklaringen beschikt waarin de verantwoordelijkheid is beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens. De toezichthouder heeft op 5 oktober 2021 een uitvraag gedaan naar de datum van de geheimhoudingsverklaringen van het personeel dat

²⁹ Rvb, p. 26, 36 en 47.

³⁰ Dit is de datum waarop het onderzoek van de toezichthouder is gestart.

³¹ Op 14 september 2022 is het traject met betrekking tot de Bbgt HR-vordering van 19 juli 2022 afgesloten met een laatste brief vanuit de RDI.

in aanraking komt met LI-gegevens. Odido heeft in reactie op deze uitvraag op 13 oktober een overzicht met vier medewerkers aangeleverd waarin data uit [VERTROUWELIJK] staan. Deze data komen overeen met de data van de arbeidsovereenkomst uit het overzicht van Odido. Vervolgens heeft de toezichthouder inzage gehad in en zijn door Odido kopieën verstrekt van de arbeidsovereenkomsten van deze vier medewerkers. De toezichthouder heeft de geheimhoudingsverklaringen van alle overige personen, die ook in aanraking komen LI-gegevens, nogmaals opgevraagd door middel van de vordering van 19 juli 2022. Naar aanleiding van de vordering heeft Odido geen informatie dan wel bescheiden overgelegd die zien op de geheimhoudingsverklaringen inzake LI-gegevens van de overige personen.

Rijksinspectie Digitale Infrastructuur

Ons kenmerk
[VERTROUWELIJK]

De toezichthouder heeft vastgesteld dat voor de drie medewerkers van Odido, zoals hierboven genoemd onder b, die belast zijn met de verwerking van LI-gegevens geen geheimhoudingsverklaring aanwezig is in de zin van het Bbgt. De arbeidsovereenkomsten die Odido heeft overgelegd bevatten bovendien enkel een algemene geheimhoudingsverklaring. Dit betreft echter geen geheimhoudingsverklaring zoals bedoeld in het Bbgt, omdat hierin geen verantwoordelijkheid is beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens.³²

De toezichthouder heeft vastgesteld dat Odido voor de beheerder van het [VERTROUWELIJK], zoals hierboven genoemd onder a en b, en voor de vijf medewerkers van [VERTROUWELIJK], zoals hierboven genoemd onder a en b, die belast zijn met de verwerking van LI-gegevens, na een uitvraag en een vordering, geen kopieën heeft verstrekt of inzage heeft geboden in relevante documenten, waaronder arbeidsovereenkomsten dan wel geheimhoudingsverklaringen. Daarop heeft de toezichthouder geconcludeerd dat de geheimhoudingsverklaringen waarin de verantwoordelijkheid is beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens voor de [VERTROUWELIJK] en de vijf medewerkers van [VERTROUWELIJK] niet aanwezig waren.³³

Bij de zienswijze heeft Odido een arbeidsovereenkomst overgelegd van de [VERTROUWELIJK] met ingangsdatum [VERTROUWELIJK]. Deze arbeidsovereenkomst bevat een algemene geheimhoudingsverklaring, maar er is geen verantwoordelijkheid beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens. Bij de zienswijze heeft Odido geheimhoudingsverklaringen overgelegd van de [VERTROUWELIJK] medewerkers uit [VERTROUWELIJK]. Dit betreffen eveneens algemene geheimhoudingsverklaringen waarin geen verantwoordelijkheid is beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens. Ook is niet vast komen te staan dat Odido ten tijde van het onderzoek beschikte over deze geheimhoudingsverklaringen.

In dat verband merk ik op dat Odido het personeel dat belast is met LI-gegevens dient voor te lichten over het belang van geheimhouding en te wijzen op de gevolgen van schending van deze verplichting. De verplichting geldt op grond van artikel 8 van het Bbgt dus ook ten aanzien van medewerkers van [VERTROUWELIJK] waarvoor Odido verantwoordelijk is. De culminatie van dit bewustwordings- en voorlichtingstraject is het ondertekenen van de geheimhoudingsverklaring met

³² Rvb, p. 36 en 47.

³³ Rvb, p. 36, 40 en 47.

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. Een algemene verplichting in een arbeidsovereenkomst dat medewerkers gehouden zijn zich aan wet- en regelgeving te houden en dat een geheimhoudingsplicht van toepassing is, is – mede gezien het belang van de bescherming van LI-gegevens uit hoofde van de aard van die gegevens – dan ook onvoldoende.

Het voorgaande levert een overtreding op van artikel II, onder b, van de bijlage bij het Bbgt voor in ieder geval de periode van 5 oktober 2021³⁴ tot en met 14 september 2022.³⁵

Tussenconclusie

Schematisch zijn de hierboven beschreven feiten uit paragraaf 6.2.1 als volgt weergegeven.

	VOG of VGB ³⁶	Functiebeschrijving met relatie tot LI-gegevens	Geheimhoudings-verklaring met relatie tot LI-gegevens
[VERTROUWELIJK]			
3 LI-medewerkers van Odido	VGB's gecontroleerd op 29 oktober 2021 en akkoord bevonden	Geen	Geen
5 medewerkers van [VERTROUWELIJK]	VOG's overgelegd bij zienswijze, maar daarover beschikte Odido niet tijdens de inspectie.	Geen	Geen
[VERTROUWELIJK]			
1 beheerder van Odido	Geen VOG aanwezig bij aanvang onderzoek. VOG blijkt uit screeningsonderzoek dat door de toezichthouder is ontvangen op 7 februari 2022 en akkoord is bevonden.	Geen	Geen

Tabel. 1 Geautoriseerde toegang³⁷

Ik kom tot de conclusie dat Odido artikel 4, tweede lid, in samenhang met artikel 2, tweede en derde lid, van het Bbgt en artikel II, onder a en b, van de bijlage bij het Bbgt heeft overtreden voor in ieder geval de periode van 5 oktober 2021 tot en met 14 september 2022.

³⁴ Dit is de datum waarop het onderzoek van de toezichthouder is gestart.

³⁵ Op 14 september 2022 is het traject met betrekking tot de Bbgt HR-vordering van 19 juli 2022 afgesloten met een laatste brief vanuit de RDI.

³⁶ Voor een VGB vindt een zwaardere screening plaats dan voor een VOG. Met een VGB wordt daarom ook voldaan aan het vereiste uit artikel 4, eerste lid, van het Bbgt.

³⁷ Rvb, p. 47.

6.2.2 Ongeautoriseerde toegang

Op grond van het Bbgt is ongeautoriseerde toegang tot LI-gegevens, dat wil zeggen toegang door personen die niet aan de onder paragraaf 6.2.1 genoemde eisen voldoen, verboden. Dit volgt uit artikel II, onder c, van de bijlage bij het Bbgt. Odido moet voorkomen dat personen dat niet zijn belast met de verwerking van LI-gegevens wel toegang zouden kunnen hebben tot deze gegevens. Door de toezichthouder is vastgesteld dat ten aanzien van het [VERTROUWELIJK] en de LI-Firewall ongeautoriseerde toegang kon worden verkregen tot LI-gegevens. Voor de bevindingen ten aanzien van het [VERTROUWELIJK] verwijs ik naar paragraaf 6.3.1.6. Op welke wijze ongeautoriseerde toegang ten aanzien van de LI-Firewall kon plaatsvinden, zet ik hieronder verder uiteen.

De LI-Firewall

De toezichthouder heeft onderzoek gedaan naar de LI-Firewall. De LI-Firewall van Odido bevindt zich tussen het [VERTROUWELIJK] en het [VERTROUWELIJK] en versleutelt een gedeelte van deze verbinding. In paragraaf 4.3.6 van het Rvb heeft de toezichthouder een verslag opgenomen van het onderzoek naar de [VERTROUWELIJK].

Samengevat blijkt daaruit het volgende. Uit het verslag van een gesprek tussen de toezichthouder en Odido, dat heeft plaatsgevonden op 19 januari 2022, blijkt dat Odido de LI-Firewall op 14 december 2021, twee dagen voorafgaand aan het bezoek van de toezichthouder, heeft geïnstalleerd als noodmaatregel om de verbinding alsnog te versleutelen. Het installeren van de LI-Firewall en de overwegingen van Odido daarvoor zijn eveneens te zien in de uitdraai van de change tickets uit de change management registratie die de toezichthouder op 2 maart 2022 van Odido heeft ontvangen.³⁸ De toezichthouder is door Odido niet geïnformeerd over het installeren van de LI-Firewall. Uit het verslag van een gesprek tussen de toezichthouder en Odido, dat heeft plaatsgevonden op 19 januari 2022, blijkt ook dat de LI-Firewall op 17 december 2021, dus na het bezoek van de toezichthouder weer is uitgezet, omdat deze niet naar behoren functioneerde.

Uit het onderzoek van de toezichthouder blijkt verder dat door het overhaast installeren van de LI-Firewall 81 personen in de periode van 14 december 2021 tot en met 17 december 2021 ongeautoriseerde toegang hadden [VERTROUWELIJK] en de mogelijkheid hadden om een PCAP-file aan te maken. Een PCAP-file bevat een 'packet capture' (kopie van netwerkverkeer) van een bepaalde geselecteerde verbinding voor een nader te specificeren lengte (aan pakketten of tijd). De functionaliteit voor het aanmaken van een dergelijke file wordt normaliter ingezet voor het onderzoeken van storingen in het netwerkverkeer. Als een persoon een PCAP-file kan aanmaken, dan kan hij ook de inhoud van het netwerkverkeer inzien. Zoals volgt uit paragraaf 6.3.1, heeft de toezichthouder vastgesteld dat het [VERTROUWELIJK] en [VERTROUWELIJK] van Odido onversleutelde (leesbare) LI-gegevens bevatten.³⁹ Personen die een PCAP-file kunnen aanmaken, hebben dus ook toegang tot LI-gegevens, nu deze gegevens onversleuteld zijn.

De toezichthouder heeft vastgesteld dat de 81 personen met toegang tot de LI-Firewall, en daardoor de mogelijkheid hadden om een PCAP-file te maken, toegang hadden tot LI-gegevens.⁴⁰ Deze personen hadden vanuit hun functie

³⁸ Rvb p. 44 en 62.

³⁹ Zie paragraaf 6.3.1 voor een nadere onderbouwing hiervan.

⁴⁰ Rvb p. 43 en 48.

geen toegang nodig tot deze gegevens en waren niet belast met de verwerking van LI-gegevens, waardoor er sprake is van ongeautoriseerde toegang. Uit een e-mailbericht van Odido van 17 januari 2022 blijkt dat dit een misconfiguratie van het systeem betrof en de PCAP-file onversleutelde LI-gegevens bevatte. Hierdoor is sprake is van een overtreding van artikel II, onder c, van de bijlage bij het Bbgt.

Tussenconclusie

Ik kom tot de conclusie dat Odido artikel II, onder c, van de bijlage bij het Bbgt in de periode van 14 december 2021 tot en met 17 december 2021 heeft overtreden, omdat een groot aantal personen ongeautoriseerde toegang had tot de LI-gegevens van Odido.

6.2.3 Conclusie

De hierboven beschreven feiten uit paragrafen 6.2.1 en 6.2.2 leiden tot de volgende conclusies:

- a. Ik stel vast voor in totaal zes personen, te weten vijf medewerkers van [VERTROUWELIJK] en de beheerder van het [VERTROUWELIJK] van Odido, die medewerking verleenden aan de uitvoering van taplasten geen VOG bij Odido aanwezig was tijdens het onderzoek. Ten aanzien van één medewerker, te weten de [VERTROUWELIJK] van Odido, is gedurende het onderzoek een VOG aangeleverd met als datum 3 december 2021, dit is na datum van de start van het onderzoek door mijn toezichthouder.
- b. Daarnaast stel ik vast dat van negen personen, te weten drie LI-medewerkers van Odido, vijf medewerkers van [VERTROUWELIJK] en de beheerder van het [VERTROUWELIJK] van Odido, met toegang tot de LI-gegevens geen functiebeschrijving aanwezig was of geen functiebeschrijving is overgelegd waaruit bleek dat zij verantwoordelijkheden hebben voor de verwerking en beveiliging van LI-gegevens.
- c. Daarnaast stel ik vast dat er met betrekking tot negen personen, te weten drie LI-medewerkers van Odido, vijf medewerkers van [VERTROUWELIJK] en de beheerder van het [VERTROUWELIJK] van Odido geen (toereikende) geheimhoudingsverklaring aanwezig was.
- d. Daarnaast stel ik vast dat 81 ongeautoriseerde personen toegang hadden tot de LI-gegevens via de LI-Firewall.

Ik stel vast dat Odido voor in ieder geval de periode van 5 oktober 2021 tot en met 14 september 2022 niet voldeed aan de verplichtingen die gelden voor geautoriseerd personeel dat (kort gezegd) in aanraking komt met LI-gegevens. Ik kom tot de conclusie dat Odido artikel 4, tweede lid, in samenhang met artikel 2, tweede en derde lid, van het Bbgt en artikel II, onder a en b, van de bijlage bij het Bbgt heeft overtreden voor de periode van in ieder geval van 5 oktober 2021 tot en met 14 september 2022.

Daarnaast kom ik tot de conclusie dat Odido artikel II, onder c, van de bijlage bij het Bbgt heeft overtreden voor in ieder geval de periode van 1 november 2021 tot en met 14 februari 2022 omdat een groot aantal personen ongeautoriseerde toegang had tot de LI-gegevens van Odido.

6.3 Toegang geautomatiseerde systemen

De toezichthouder heeft onderzoek gedaan naar de naleving van artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V van de bijlage bij het Bbgt, gericht op het treffen van maatregelen met betrekking tot de toegangsbeveiliging van geautomatiseerde informatiesystemen.

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.

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 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, dienen bij 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."⁴¹

⁴¹ Stb. 2003, 472, p. 9.

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:

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
11/21

"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." (onderstreping RDI/JZ)⁴²

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. Daaruit vloeit logischerwijs voort dat de te treffen beveiligingsmaatregelen moeten aansluiten bij de huidige stand van de techniek, zoals ook in de rechtspraak is bevestigd.⁴³

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 bij het Bbgt.

De toezichthouder heeft bij Odido drie LI-systemen aangetroffen, te weten het [VERTROUWELIJK], het [VERTROUWELIJK] en de LI-Firewall. De toezichthouder heeft de logische deugdelijke beveiliging van deze systemen onderzocht.

Voor de volledige beschrijving van de inrichting van het LI-proces bij Odido verwijs ik naar paragraaf 5.4 van dit besluit en naar paragraaf 4.3 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.

⁴² Stb. 2003, 472, p. 7.

⁴³ Zie de uitspraak van het College van Beroep voor het bedrijfsleven van 16 november 2016, ECLI:NL:CBB:2016:346 en de uitspraak van de Rechtbank Rotterdam van 21 oktober 2024, ECLI:NL:RBROT:2024:1037, r.o. 23.9.

6.3.1 Deugdelijke beveiliging, onder meer door persoonsgebonden authenticatie

Artikel V, onder a, van de bijlage bij het Bbgt vereist dat Odido een deugdelijke toegangsbeveiliging van geautomatiseerde informatiesystemen die LI-gegevens bevatten heeft, onder meer door middel van persoonsgebonden authenticatie.

De nota van toelichting bij het Bbgt zegt over persoonsgebonden authenticatie 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 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."⁴⁴

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 identificeerbaar persoon.

6.3.1.1 Niet-persoonsgebonden authenticatie

De toezichthouder heeft vastgesteld dat op het [VERTROUWELIJK] en het [VERTROUWELIJK] [VERTROUWELIJK] kon worden ingelogd door middel van niet-persoonsgebonden accounts.

a. *Het* [VERTROUWELIJK]

Het [VERTROUWELIJK] van Odido bestaat uit meerdere lagen. Om toegang te verkrijgen tot LI-gegevens [VERTROUWELIJK]

De toezichthouder heeft de toegangsbeveiliging van de [VERTROUWELIJK], de [VERTROUWELIJK] en de relevante [VERTROUWELIJK], te weten [VERTROUWELIJK] en [VERTROUWELIJK] separaat onderzocht. Voor de volledige beschrijving van het [VERTROUWELIJK] van Odido verwijs ik naar paragraaf 4.3.4 van het Rvb.

De toezichthouder heeft vastgesteld dat een beheerder van Odido vanaf het [VERTROUWELIJK] de mogelijkheid heeft tot het doen van inlogpogingen op het [VERTROUWELIJK] [VERTROUWELIJK] via de Secure Shell (SSH)⁴⁷. Op de [VERTROUWELIJK] kon uitsluitend ingelogd worden met de niet-persoonsgebonden accounts [VERTROUWELIJK] en [VERTROUWELIJK]. De

⁴⁴ Stb. 2003, 472, p. 10.

⁴⁵ [VERTROUWELIJK]

⁴⁶ [VERTROUWELIJK]

⁴⁷ De Secure Shell is de zogeheten command line interface (CLI) van Linux. Dit is een omgeving waar bediening geschiedt via commandoregels in een terminal.

toezichthouder heeft vastgesteld dat beide accounts vanaf in ieder geval 7 december 2012 in gebruik zijn. Op de [VERTROUWELIJK] kon uitsluitend worden ingelogd met de niet-persoonsgebonden accounts [VERTROUWELIJK] en [VERTROUWELIJK]. Op [VERTROUWELIJK] kon uitsluitend worden ingelogd met het niet-persoonsgebonden account [VERTROUWELIJK]. De toezichthouder heeft tevens vastgesteld dat er geen persoonsgebonden accounts aanwezig waren.⁴⁸ Hiermee heeft de toezichthouder vastgesteld dat via niet-persoonsgebonden accounts toegang verkregen kon worden tot LI-gegevens die via het [VERTROUWELIJK] worden verwerkt. Dat is in strijd met artikel V, onder a, van de bijlage bij het Bbgt.

De toezichthouder heeft op basis van de shadowfile⁴⁹ vastgesteld, zoals verder beschreven wordt in paragraaf 6.3.1.2, dat beide accounts een wachtwoord hebben dat voor het laatst is gewijzigd op 7 december 2012, tien dagen voor de oplevering van het [VERTROUWELIJK] door [VERTROUWELIJK] aan Odido.⁵⁰

Deze niet-persoonsgebonden accounts zijn dus in gebruik sinds voornoemde datum, zijnde 7 december 2012. Verder heeft de toezichthouder vastgesteld, op basis van onderzoek naar de shadowfile, dat er tijdens het onderzoek geen persoonsgebonden accounts aanwezig waren.⁵¹ Sinds de implementatie van het [VERTROUWELIJK] zijn er dus niet-persoonsgebonden accounts gebruikt om in te loggen op het [VERTROUWELIJK]. Deze overtreding heeft in ieder geval in de periode van 17 december 2012⁵² tot 7 februari 2022⁵³ plaatsgevonden.⁵⁴

b. Het [VERTROUWELIJK]

Het [VERTROUWELIJK] van Odido is een ingekocht IT-systeem van de firma [VERTROUWELIJK] gevestigd in [VERTROUWELIJK] voert het onderhoud en beheer uit op het [VERTROUWELIJK] van Odido. De toezichthouder heeft op basis van de configuratie van het [VERTROUWELIJK] bij Odido en door middel van het uitgevoerde script vastgesteld dat er vanaf 24 december 2015, de datum van installatie van het [VERTROUWELIJK], tot en met 16 december 2021⁵⁵ gebruik werd gemaakt van het niet-persoonsgebonden account [VERTROUWELIJK].⁵⁶ Dit betekent dat Odido in ieder geval zes jaar lang gebruik heeft gemaakt van een niet-persoonsgebonden account.

Hiermee heeft de toezichthouder vastgesteld dat via een niet-persoonsgebonden account toegang kon worden verkregen tot LI-gegevens die via het [VERTROUWELIJK] - systeem worden verwerkt. Dit is in strijd met artikel V, onder a, van de bijlage bij het Bbgt.

⁴⁸ Rvb, p. 31, p. 33 en p. 35.

⁴⁹ Een shadowfile is een bestand waarin de gebruikersnamen en de versleutelde wachtwoorden zijn opgeslagen van de gebruikers van het systeem.

⁵⁰ Dit blijkt uit de shadowfile, zie Rvb, p. 31.

⁵¹ Rvb, p. 31.

⁵² Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

⁵³ Dit betreft de datum waarop Odido de uitkomsten van het AT-script, zoals door Odido uitgevoerd op de [VERTROUWELIJK] en de [VERTROUWELIJK] bij de toezichthouder heeft aangeleverd. Na deze datum heeft Odido de eerste verbeteringen wat betreft de logische deugdelijke beveiliging van het [VERTROUWELIJK] doorgevoerd, zoals is vastgelegd in [VERTROUWELIJK].

⁵⁴ Rvb, p. 33.

⁵⁵ Dit betreft de datum waarop er voor het laatst is ingelogd met dit account. Na dit tijdstip heeft dit account op deze datum de status 'disabled' gekregen, waardoor er niet meer mee kon worden ingelogd.

⁵⁶ Rvb, p. 39-40.

De toezichthouder heeft tevens vastgesteld dat er vanaf 8 december 2021 vijf persoonsgebonden accounts aanwezig waren. Eén van deze accounts is op 8 december 2021 voor het eerst gebruikt om in te loggen op het [VERTROUWELIJK], de overige vier accounts waren op het moment van onderzoek op 16 december 2021 niet gebruikt om in te loggen op het [VERTROUWELIJK].⁵⁷ Op grond hiervan stel ik vast dat er geen gebruik werd gemaakt van persoonsgebonden accounts, maar dat dit pas ten tijde van het onderzoek door de toezichthouder is ingeregeld.

Tussenconclusie

Op grond van bovenstaande stel ik vast dat op zowel het [VERTROUWELIJK] als het [VERTROUWELIJK] van Odido ingelogd kon worden door middel van niet-persoonsgebonden accounts. Dit maakt reeds dat de toegang tot geautomatiseerde systemen waarin LI-gegevens worden verwerkt niet op deugdelijke wijze is beveiligd. Ik kom tot de conclusie dat Odido 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 bij het Bbgt heeft overtreden voor in ieder geval de periode van 17 december 2012⁵⁸ tot 7 februari 2022⁵⁹.

6.3.1.2 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 Odido, ontbraken ook overige maatregelen in het kader van de toegangsbeveiliging van de LI-systemen, zoals artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder a, van de bijlage bij het Bbgt vereist. Artikel V, onder a, van de bijlage bij het Bbgt vereist immers dat Odido de toegang tot geautomatiseerde informatiesystemen waarin LI-gegevens worden verwerkt op deugdelijke wijze beveiligd.

Om te beoordelen of deze systemen deugdelijke beveiligd zijn, ga ik uit van internationaal breed erkende en geaccepteerde standaarden voor logische toegangsbeveiliging van informatiesystemen- en netwerken. 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.⁶⁰

Uit de internationale standaarden volgt dat een adequate toegangsbeveiliging bestaat uit een aantal essentiële onderdelen, zoals versleuteling van gegevens (encryptie), zonering (netwerksegmentatie) en deugdelijke wachtwoordbeveiliging van accounts waarmee toegang verkregen kan worden tot LI-gegevens. Deze

⁵⁷ Rvb, p. 39-40.

⁵⁸ Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

⁵⁹ Dit betreft de datum waarop Odido de uitkomsten van het AT-script, zoals door Odido uitgevoerd op de [VERTROUWELIJK] en de [VERTROUWELIJK] bij de toezichthouder heeft aangeleverd. Na deze datum heeft Odido de eerste verbeteringen wat betreft de logische deugdelijke beveiliging van het [VERTROUWELIJK] doorgevoerd, zoals is vastgelegd in [VERTROUWELIJK].

⁶⁰ Rechtbank Rotterdam 21 oktober 2024, ECLI:NL:RBROT:2024:1037, r.o. 23.9.

deugdelijke wachtwoordbeveiliging houdt onder meer in dat 'default' geheime authenticatie-informatie – zoals 'default' wachtwoorden, zijnde standaardwachtwoorden – van een leverancier gewijzigd behoort te worden na de installatie van systemen of software.⁶¹

In de paragrafen hieronder volgt op welke punten de toegangsbeveiliging van Odido tekort schoot.

6.3.1.3 Deugdelijke wachtwoordbeveiliging schoot tekort

De toezichthouder heeft de deugdelijke wachtwoordbeveiliging van het [VERTROUWELIJK] onderzocht. Uit dit onderzoek blijkt, samengevat, het volgende.

De toezichthouder heeft vastgesteld dat in de shadowfile bij de accounts [VERTROUWELIJK] en [VERTROUWELIJK] het getal 15681 staat:

[VERTROUWELIJK]:\$6:15681:....." & [VERTROUWELIJK]:\$6:15681:0::7::"

Dit getal is de optelsom van het aantal dagen na de datum 1 januari 1970 tot het moment dat het wachtwoord voor het laatst is gewijzigd.⁶² Deze wachtwoorden zijn dus voor het laatst gewijzigd 15.681 dagen na 1 januari 1970. De toezichthouder heeft daarop vastgesteld dat beide accounts een wachtwoord hebben dat voor het laatst is gewijzigd op 7 december 2012, tien dagen voor de oplevering van het [VERTROUWELIJK] door [VERTROUWELIJK] aan Odido.⁶³ Voorts heeft de toezichthouder vastgesteld dat dit wachtwoord het standaardwachtwoord betrof,⁶⁴ zoals dit was opgenomen in de handleiding van de leverancier [VERTROUWELIJK].⁶⁵

Daarnaast heeft de toezichthouder vastgesteld dat op de [VERTROUWELIJK] en de [VERTROUWELIJK] eveneens kon worden ingelogd met het standaard wachtwoord van de leverancier [VERTROUWELIJK], die in de handleiding voor het [VERTROUWELIJK] te vinden waren.⁶⁶ De wachtwoorden van het [VERTROUWELIJK] account voor [VERTROUWELIJK] en [VERTROUWELIJK] waren bovendien identiek aan elkaar.⁶⁷ Voor beide accounts heeft de toezichthouder op 7 februari 2022 vastgesteld dat deze wachtwoorden voor het laatst gewijzigd zijn op 7 januari 2001.

Dit betekent dus dat Odido al ruim tien jaar de standaardwachtwoorden van de leverancier gebruikte, die in de handleiding van het [VERTROUWELIJK] van deze leverancier te vinden was, en deze tien jaar lang, na implementatie van het [VERTROUWELIJK], niet heeft gewijzigd. Het voorgaande levert een overtreding op van artikel V, onder a, van de bijlage bij het Bbgt voor in ieder geval de periode van 17 december 2012⁶⁸ tot en met 7 februari 2022, omdat er geen sprake was van deugdelijke logische toegangsbeveiliging.

⁶¹ Zie de NEN-EN-ISO/IEC 27002:2017 nl, paragraaf 9.2.4, onder g, welke inhoudt dat 'default' geheime authenticatie-informatie van een leverancier gewijzigd behoort te worden na de installatie van systemen of software.

⁶² Zie bijvoorbeeld: <https://www.cyberciti.biz/faq/understanding-etcshadow-file/> onder punt 3 en het Rvb pagina 31.

⁶³ Dit blijkt uit de shadowfile, zie Rvb, p. 31.

⁶⁴ Rvb, p. 34.

⁶⁵ Rvb, p. 36.

⁶⁶ Rvb, p. 36.

⁶⁷ Rvb, p. 33.

⁶⁸ Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

6.3.1.4 Geen versleuteling en onversleutelde overdracht van LI-gegevens

Zoals uiteengezet in paragraaf 6.3.1.2 houdt een deugdelijke beveiliging ook in dat gegevens versleuteld worden. De toezichthouder heeft daarom onderzoek gedaan naar de beveiliging van verbindingen waarover LI-gegevens verzonden worden. Samengevat blijkt hieruit het volgende.

De toezichthouder heeft vastgesteld dat de X1-, X2- en X3-verbindingen⁶⁹ van en naar het [VERTROUWELIJK], zoals geïnstalleerd door [VERTROUWELIJK], tijdens de ingebruikname van het [VERTROUWELIJK] door Odido op 17 december 2012, onversleuteld zijn geïnstalleerd.

De toezichthouder heeft de "[VERTROUWELIJK] lawful interception Statement of Compliance (SoC)" van Odido ontvangen.⁷⁰ Dit document is in 2012 opgesteld als onderdeel van de leverancierselectie door Deutsche Telecom Group. De betreffende bijlage is een 1.0 versie en heeft als datum 17/12/2012. Dat is dezelfde datum als de datum waarop Odido het [VERTROUWELIJK] in gebruik heeft genomen. Dit document geeft weer welke mogelijkheden de leverancier [VERTROUWELIJK] biedt ten aanzien van bevoegd aftappen. Daaruit blijkt het volgende.

"De 115 in dit document genoemde verplichtingen kennen drie verschillende varianten van implementatie:

- "Fully Compliant"
- "Partly Compliant"
- "NA" kort voor: *Not Applicable (niet van toepassing)*"⁷¹

Van deze verplichtingen ziet verplichting nummer 8 uit het [VERTROUWELIJK] lawful interception Statement of Compliance (SoC) op de installatie en mogelijke beveiliging van de X1-, X2- en X3-verbindingen.

*"It SHALL be possible for data to be transferred over the X1_1, X_2 and X1_3 interfaces in a secure manner using appropriate encryption mechanisms defines by the buyer, e.g. IPsec or SSH."*⁷²

De toezichthouder heeft vastgesteld dat achter deze verplichting de implementatievariant "NA" is ingevuld door Odido. Deze verbindingen zijn dus op 17 december 2012, op verzoek van Odido, bewust onversleuteld geïmplementeerd door [VERTROUWELIJK].

De toezichthouder heeft zijn onderzoek ook gericht op de verbindingen tussen het [VERTROUWELIJK] van Odido en diverse LI-apparatuur, waaronder het [VERTROUWELIJK] systeem, van Odido. De toezichthouder heeft vastgesteld dat de X1-, X2- en X3-verbindingen van het [VERTROUWELIJK] verbonden zijn aan het [VERTROUWELIJK] van Odido.⁷³ De toezichthouder heeft tevens vastgesteld dat deze verbinding op 16

⁶⁹ X1-verbindingen worden gebruikt om de taplijst op het betreffende systeem aan te brengen en te muteren, zie voor een uitgebreide beschrijving paragraaf 4.3.1 van het Rvb. De X2-verbinding bevat de meta-informatie die afkomstig is van een tap, bijvoorbeeld informatie welke telefoonnummers met elkaar bellen en de gespreksduur. X3-verbindingen bevatten het dataverkeer of het audiobestand van de tap waarin het getapte gesprek te horen is.

⁷⁰ Rvb, p. 27.

⁷¹ Rvb, p. 27.

⁷² Rvb, p. 28.

⁷³ Rvb, p. 28.

december 2021 onversleuteld was.⁷⁴ Odido heeft daarnaast tijdens een bezoek van de toezichthouder aan het kantoor van Odido op 19 januari 2022 verklaard dat deze verbinding sinds de aansluiting van het [VERTROUWELIJK]-systeem op het [VERTROUWELIJK] op 24 december 2015 onversleuteld was.⁷⁵ Deze verklaring luidt als volgt.

"(...) AT's sessie heeft er namelijk toe geleid dat TM eens goed ging kijken naar de systemen omtrent het Bbgt en kwam hierbij tot de conclusie dat de verbindingen tussen [VERTROUWELIJK] en de [VERTROUWELIJK] (X1, X2 en X3) niet versleuteld waren. TM geeft aan dat de onversleutelde verbinding altijd zo is geweest sinds de implementatie van de [VERTROUWELIJK] aansluiting op de mobile core. Het is niet zo dat dit eerst wel versleuteld was, toen niet en daarna door de pre-audit firewall implementatie actie voorafgaand aan 16 december 2021 weer wel. (...)"⁷⁶

Op basis van voorgaande stel ik vast dat de X1-, X2- en X3-verbindingen tussen het [VERTROUWELIJK] en het [VERTROUWELIJK] onversleuteld zijn sinds de ingebruikname van het [VERTROUWELIJK] op 17 december 2012 tot en met 12 januari 2022, een periode van ruim negen jaar. De X1-, X2- en X3-verbindingen zijn door Odido bewust onversleuteld geïmplementeerd op 17 december 2012 en sindsdien niet versleuteld.

Voorgaande brengt met zich dat een ieder met fysieke toegang tot de bekabeling van deze onversleutelde LI-verbinding, die liep tussen de datacenters van Odido te [VERTROUWELIJK], deze gegevens kon afvangen en vanwege het ontbreken van versleuteling kon inzien.⁷⁸

Het voorgaande levert een overtreding op van artikel V, onder a, van de bijlage bij het Bbgt voor in ieder geval de periode van 17 december 2012⁷⁹ tot en met 16 december 2021⁸⁰.

6.3.1.5 Medewerkers [VERTROUWELIJK] hadden ongelimiteerd toegang tot LI-gegevens

De toezichthouder heeft vastgesteld dat medewerkers van [VERTROUWELIJK] onbeperkte en zelfstandige toegang hadden tot het [VERTROUWELIJK] van Odido.⁸¹ Deze toegang ging zover, dat het voor medewerkers van [VERTROUWELIJK] mogelijk was om zelfstandig taps te zetten. Ook konden medewerkers van [VERTROUWELIJK] bevestigingen doen op de taplijst van Odido om erachter te komen of een bepaald nummer onder de tap staat. Ook hiervoor stel ik vast dat van een deugdelijke logische toegangsbeveiliging geen sprake was en dat sprake is van een overtreding van artikel V, onder a, van de bijlage bij het Bbgt. Deze situatie heeft bestaan in de periode van 24 december 2015 tot 16 december 2021.

⁷⁴ Rvb, p. 28.

⁷⁵ 20220119 Verslag [T-Mobile] Mobile Core [VERTROUWELIJK] v1.0.pdf.

⁷⁶ 20220119 Verslag [T-Mobile] Mobile Core [VERTROUWELIJK] v1.0.pdf, p. 5.

⁷⁷ Rvb, p. 18.

⁷⁸ Rvb, p. 44.

⁷⁹ Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

⁸⁰ Dit is de datum waarop het onderzoek naar de X1-, X2- en X3-verbindingen van Odido heeft plaatsgevonden.

⁸¹ Rvb, p. 38-39.

6.3.1.6 Geen deugdelijke logische beveiliging toegangspad LI-gegevens

Op grond van artikel 2, eerste lid, van het Bbgt dient een aanbieder zorg te dragen voor het treffen van alle noodzakelijke beveiligingsmaatregelen om kennisneming van LI-gegevens door onbevoegden te voorkomen. Op grond van het tweede lid, onder c, van dit artikel dienen deze maatregelen ten minste te bestaan uit maatregelen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarin LI-informatie wordt verwerkt.

De toezichthouder heeft daarom onderzoek gedaan naar de logische beveiliging van het toegangspad naar de LI-gegevens op het [VERTROUWELIJK]. In paragraaf 4.3.4 van het Rvb heeft de toezichthouder een verslag opgenomen van het onderzoek naar het [VERTROUWELIJK]. Samengevat blijkt daaruit het volgende.

De toegang tot LI-gegevens op het [VERTROUWELIJK] wordt verkregen vanaf het [VERTROUWELIJK]. Het [VERTROUWELIJK] is het managementnetwerk van Odido dat voor verschillende systemen wordt gebruikt.⁸² Dit is ook te zien in de logbestanden van het [VERTROUWELIJK] die de toezichthouder heeft ontvangen van Odido, waarin naast medewerkers van Odido, ook personen staan die werkzaam zijn voor verschillende leveranciers zoals [VERTROUWELIJK]. In het [VERTROUWELIJK] is door Odido geen zonerings toegepast. Zonerings, ook wel aangeduid als netwerksegmentatie, is het opsplitsen van een netwerk in verschillende afgescheiden zones. Doordat Odido in het [VERTROUWELIJK] geen zonerings heeft toegepast, hebben beheerders van één systeem ook de mogelijkheid tot het doen van inlogpogingen op andere systemen.

De toezichthouder heeft op basis van drie ontvangen bestanden⁸³ vastgesteld dat tussen 1 november 2021 en 14 februari 2022 een groot aantal personen, te weten circa 588, toegang had tot het [VERTROUWELIJK].⁸⁴ Deze toegang betrof zowel personen die permante toegang hadden vanaf het [VERTROUWELIJK], circa 393⁸⁵ personen, als personen die diverse keren tijdelijke toegang hebben gehad, circa 195 personen.⁸⁶ Van deze 195 personen waren er 25 werkzaam voor [VERTROUWELIJK]. Deze 25 personen hebben tussen 1 november 2021 en 14 februari 2022 in totaal 79 keer tijdelijke toegang gehad tot het [VERTROUWELIJK].⁸⁷

Zodra een persoon is ingelogd op het [VERTROUWELIJK], kunnen vanaf het [VERTROUWELIJK] inlogpogingen gedaan worden op het [VERTROUWELIJK], dat LI-gegevens bevat. Dit, gezien in combinatie met het feit dat er vanaf het [VERTROUWELIJK] inlogpogingen gedaan konden worden op het [VERTROUWELIJK], en dat er op het [VERTROUWELIJK] ingelogd kon worden met standaard niet-persoonsgebonden accounts en de standaard wachtwoorden van [VERTROUWELIJK], welke al in gebruik waren sinds de implementatie van het [VERTROUWELIJK] door [VERTROUWELIJK] en er

⁸² Het [VERTROUWELIJK] wordt voor verschillende systemen gebruikt, waaronder het [VERTROUWELIJK]. Wanneer een beheerder is ingelogd op het [VERTROUWELIJK] kan worden doorgestapt naar de beheerdersinterface van het betreffende systeem.

⁸³ De bestanden bestaan uit autorisatielijsten met daarop personen die permanent toegang hadden of tijdelijke toegang hebben gehad tot het [VERTROUWELIJK].

⁸⁴ Zoals op pagina 28 het Rvb is opgemerkt wordt, het [VERTROUWELIJK] ook met andere termen aangeduid, zoals het management netwerk.

⁸⁵ In het voornemen stond er abusievelijk circa 391 personen. Uit het Rvb volgt echter dat er circa 393 personen toegang hadden waarvan de één geautoriseerd ([VERTROUWELIJK]).

⁸⁶ De drie bestanden die van Odido zijn ontvangen op 28 februari 2022, 16 maart 2022 en 8 april 2022 zijn door de toezichthouder zoveel mogelijk ontdekt. Gelet op de verschillende schrijfwijzen van (buitenlandse) namen die op de lijsten voorkomen, is precieze vaststelling van het aantal personen niet mogelijk.

⁸⁷ Rvb p. 30.

op dit systeem bewust onversleutelde taplijsten aanwezig waren, zoals vastgesteld in de paragrafen 6.3.1.1 tot en met 6.3.1.4, maakt de kans op ongeautoriseerde leverancierstoegang zeer groot.

Gelet op het voorgaande is er daarom sprake is van een overtreding van artikel V, onder a, van de bijlage bij het Bbgt van 1 november 2021 tot en met 14 februari 2022, nu de toegang tot geautomatiseerde informatiesystemen waarin LI-gegevens worden verwerkt niet op deugdelijke wijze is beveiligd.

Daarbij merk ik op dat in het voornemen bovenstaande feiten ten aanzien van het [VERTROUWELIJK] Odido verweten werden onder artikel II, onder c, van de bijlage bij het Bbgt. In reactie op de door Odido gegeven zienswijze besluit ik om deze feiten onder artikel V, onder a, van de bijlage bij het Bbgt te scharen. Bovenstaande feiten zijn onderdeel van het feitencomplex dat ziet op het logische toegangspad om toegang tot LI-gegevens te verkrijgen. Dit wordt Odido daarom verweten als overtreding ten aanzien van de logische deugdelijke toegangsbeveiliging, zoals wordt vereist door artikel V, onder a, van de bijlage bij het Bbgt. Desalniettemin heeft bovenstaande ook tot gevolg dat er ongeautoriseerde toegang plaats kan vinden, wanneer de logische beveiliging niet deugdelijk is. Zonering van het [VERTROUWELIJK] blijft dan ook onverminderd belangrijk om ongeautoriseerde toegang tot LI-gegevens te voorkomen.

6.3.1.7 Conclusie

Op grond van bovenstaande stel ik vast dat op het [VERTROUWELIJK] en het [VERTROUWELIJK] van Odido ingelogd kon worden door middel van niet-persoonsgebonden accounts. Ook stel ik op grond van bovenstaande vast dat de beveiligingsmaatregelen ten aanzien van de logische (toegangs)beveiliging van het [VERTROUWELIJK] en het [VERTROUWELIJK], van Odido tekortschoten. Zo ontbrak een deugdelijke wachtwoordbeveiliging voor een periode van ruim negen jaar, waren LI-gegevens bewust niet versleuteld en kon onversleutelde overdracht van LI-gegevens plaatsvinden. Daarnaast hadden medewerkers van [VERTROUWELIJK] zelfstandig en ongelimiteerd toegang tot de LI-gegevens en is er geen zonering toegepast op het [VERTROUWELIJK] waardoor een groot aantal personen inlogpogingen konden doen op het [VERTROUWELIJK].

Ik kom tot de conclusie dat Odido 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 bij het Bbgt heeft overtreden voor een langdurige periode van ruim negen jaar, namelijk in ieder geval van 17 december 2012⁸⁸ tot in ieder geval 14 februari 2022⁸⁹.

6.3.2 Blokkering bij drie foutieve inlogpogingen

Artikel V, onder c, van de bijlage bij het 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 artikel I van de bijlage bij het Bbgt, kan worden opgeheven.

⁸⁸ Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

⁸⁹ Dit betreft de laatste datum uit de ontvangen logbestanden.

De toezichthouder heeft vastgesteld dat het [VERTROUWELIJK] een onbeperkt aantal foutieve inlogpogingen toestaat vanaf de datum van ingebruikname van het [VERTROUWELIJK] door Odido op 17 december 2012⁹⁰ tot de datum van vaststelling op [VERTROUWELIJK] februari 2022.⁹¹ Er vond geen blokkering plaats.

De toezichthouder heeft vastgesteld dat het [VERTROUWELIJK] het aantal foutieve inlogpogingen niet beperkt tot drie.⁹² Er vond in het geheel geen blokkering plaats, ook niet bij meer dan drie foutieve inlogpogingen. Deze vaststelling geldt voor eveneens een lange periode, namelijk vanaf de ingebruikname van het [VERTROUWELIJK] op 24 december 2015 tot in ieder geval de datum van vaststelling op 16 december 2021.

Het voorgaande levert een langdurige overtreding op van artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder c, van de bijlage bij het Bbgt voor in ieder geval de periode van 17 december 2012 tot 7 februari 2022.

6.3.3 Detectie van ongeautoriseerde toegang en pogingen daartoe

Artikel V, onder b, van de bijlage bij het 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 van artikel V, onder b, van de bijlage bij het Bbgt kan voldaan worden door allereerst adequate detectie in te richten. Zonder adequate detectie kan er immers ook geen tijdige interventie plaatsvinden. Uit internationaal breed erkende en geaccepteerde standaarden voor logische toegangsbeveiliging van informatiesystemen en netwerken volgt dat detectie van ongeautoriseerde toegang en pogingen daartoe inhoudt dat geslaagde en geweigerde pogingen om toegang te verkrijgen tot een systeem worden vastgelegd.⁹³ Uit deze norm volgt tevens dat gebruikers, ook die met speciale toegangsrechten⁹⁴, geen toestemming behoren te hebben om logbestanden van hun eigen activiteiten te verwijderen of te deactiveren. Zij kunnen mogelijk de logbestanden over informatieverwerkende faciliteiten waarover zij het directe bestuur hebben, manipuleren. De detectie op ongeautoriseerde toegang en pogingen daartoe dient dusdanig ingericht te zijn dat dergelijke manipulatie van logbestanden door gebruikers of beheerders met speciale rechten op het systeem niet mogelijk is.

Uit de internationaal breed erkende en geaccepteerde standaarden volgt dat de maatregelen die genomen worden om informatie in logbestanden te beschermen tegen onbevoegde veranderingen onder meer gericht dienen te zijn op het beperken van veranderingen aan de soorten berichten die worden vastgelegd en het bewerken of verwijderen van logbestanden.⁹⁵ Uit internationaal erkende en

⁹⁰ Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

⁹¹ Rvb, p. 34.

⁹² Rvb, p. 41.

⁹³ NEN-EN-ISO/IEC 27001:2023 en NEN-EN-ISO/IEC 27002:2022, punt 8.15.

⁹⁴ Speciale toegangsrechten houdt onder meer in administrator- en rootrechten.

⁹⁵ NEN-EN-ISO/IEC 27001:2023 en NEN-EN-ISO/IEC 27002:2022, punt 8.15.

geaccepteerde standaarden volgt ook dat deze logging centraal vastgelegd moet worden.⁹⁶

Aan de norm van artikel V, onder b, van de bijlage bij het Bbgt kan bijvoorbeeld voldaan worden door (ongeautoriseerde) inlogpogingen centraal te registreren, door bijvoorbeeld een (geautomatiseerde) lijst aan te leggen met het voor de inlogpoging gebruikte IP-adres, de gebruikersnaam en de 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 centraal, extern systeem of door middel van een andere organisatorische maatregel, waardoor bovengenoemde bescherming van de logbestanden tegen onbevoegde manipulatie gerealiseerd wordt. Het doel hiervan is om te voorkomen dat bij ongeautoriseerde toegang de registratie van de ongeautoriseerde toegang direct verwijderd kan worden door degene die ongeautoriseerde toegang heeft verkregen.

De toezichthouder heeft vastgesteld dat er op het [VERTROUWELIJK]⁹⁷ en het [VERTROUWELIJK]⁹⁸ systeem van Odido geen centrale logging aanwezig is. Op beide systemen is enkel lokale logging aanwezig. Zoals volgt uit de hiervoor aangehaalde standaarden, is lokale logging niet effectief voor detectie van inlogpogingen, omdat lokale logging geen centraal systeem alarmeert wanneer er foutieve inlogpogingen worden gedaan. Hierdoor is tijdige interventie bij ongeautoriseerde toegang en pogingen daartoe niet mogelijk, terwijl artikel V, onder b, van de bijlage bij het Bbgt dit wel vereist. Bovendien kan een gebruiker met root- of administratorrechten lokale logging zelfstandig en ongezien aanpassen en verwijderen. Daarnaast heeft de toezichthouder vastgesteld dat er op [VERTROUWELIJK]⁹⁹ geen enkele vorm van logging is ingericht, zelfs geen lokale logging.

Het voorgaande levert een langdurige overtreding op van artikel 2, eerste lid, juncto artikel 2, tweede en derde lid van het Bbgt in samenhang gelezen met artikel V, onder b, van de bijlage bij het Bbgt voor in ieder geval voor de periode van 17 december 2012 tot 7 februari 2022.

6.3.4 Handelingen met betrekking tot de verwerking van LI-gegevens worden niet-persoonsgebonden vastgelegd

Artikel V, onder e, van de bijlage bij het 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 [VERTROUWELIJK] en het [VERTROUWELIJK] konden worden

⁹⁶ <https://cas7.1.docs.cisecurity.org/en/latest/controls/control-6/control-6.5.html>.

⁹⁷ Rvb, p. 33-34.

⁹⁸ Rvb, p. 41.

⁹⁹ Rvb, p. 33-34.

¹⁰⁰ Rvb, p. 41.

uitgevoerd met niet-persoonsgebonden accounts. Deze handelingen werden dus niet persoonsgebonden vastgelegd.

Rijksinspectie Digitale
Infrastructuur

De toezichthouder heeft vastgesteld dat op het [VERTROUWELIJK] en het [VERTROUWELIJK] systeem alleen lokale registratie in de vorm van logging aanwezig is, met uitzondering van handelingen op [VERTROUWELIJK]. Ten aanzien van deze [VERTROUWELIJK] ontbreekt elke vorm van logging.

Ons kenmerk
[VERTROUWELIJK]
1111

Voor handelingen met betrekking tot de verwerking van LI-gegevens is geen enkele vorm van centrale logging geactiveerd. 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 de niet-persoonsgebonden accounts [VERTROUWELIJK] en [VERTROUWELIJK] van het [VERTROUWELIJK] rootrechten hebben en gebruikers van niet-persoonsgebonden accounts van het [VERTROUWELIJK] administratorrechten¹⁰¹ en medewerkers van [VERTROUWELIJK] zelfstandig met gebruik van een niet-persoonsgebonden account taps konden zetten¹⁰².

Ik stel op grond van bovenstaande vast dat het [VERTROUWELIJK] en het [VERTROUWELIJK] van Odido niet voldoen aan de vereisten van artikel V, onder e, van de bijlage bij het Bbgt. Ik stel dan ook vast dat Odido artikel 2, eerste lid, juncto artikel 2, tweede en derde lid, van het Bbgt in samenhang gelezen met artikel V, onder e, van de bijlage bij het Bbgt langdurig heeft overtreden in ieder geval voor de periode van 17 december 2012¹⁰³ tot 7 februari 2022.¹⁰⁴

6.3.5 Conclusie

Op grond van bovenstaande kom ik tot de conclusie dat Odido artikel 2, eerste lid, van het Bbgt in samenhang met artikel 2, tweede en derde lid en artikel V, onder a, b, c en e, van de bijlage bij het Bbgt langdurig heeft overtreden voor in ieder geval de periode van 17 december 2012 tot 14 februari 2022.

7 Handhavingsbevoegdheid van de RDI

In hoofdstuk 6 zijn de geconstateerde overtredingen gegroepeerd in drie hoofdovertredingen. Dit zijn 1) het ontbreken van het beveiligingsplan, 2) de beveiligingseisen ten aanzien van het personeel waren niet op orde en 3) de toegangsbeveiliging tot geautomatiseerde systemen waarin LI-gegevens worden verwerkt was onvoldoende. Ingevolge artikel 15.4 van de Tw in samenhang met artikel 15.1, eerste lid, onder j, 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.

¹⁰¹ Rvb, p. 40.

¹⁰² Rvb, p. 38-39.

¹⁰³ Dit is de datum waarop het [VERTROUWELIJK] is geïmplementeerd bij Odido.

¹⁰⁴ Dit betreft de datum waarop Odido de uitkomsten van het AT-script, zoals door Odido uitgevoerd op de [VERTROUWELIJK] bij de toezichthouder heeft aangeleverd. Na deze datum heeft Odido de eerste verbeteringen wat betreft de logische deugdelijke beveiliging van het [VERTROUWELIJK] doorgevoerd, zoals is vastgelegd in [VERTROUWELIJK].

In hoofdstuk 8 en 9 overweeg ik of het opleggen van een bestuurlijke boete vanwege de geconstateerde overtredingen passend en geboden is. Ik maak hierbij een belangenafweging en beoordeel daarbij alle relevante omstandigheden van het geval, waaronder de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten. Ook neem ik hierbij de door Odido naar voren gebrachte zienswijze in aanmerking.

8 Aard, ernst en duur van de overtredingen

8.1 Algemeen

Volgens hoofdstuk 13 van de Tw zijn aanbieders van openbare telecommunicatienetwerken 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:

"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."¹⁰⁵

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.¹⁰⁶ De artikelen 2, 3, 4 en 8 van het Bbgt en de bijbehorende bijlage expliciteren de minimumbeveiligingsmaatregelen.

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

¹⁰⁵ Kamerstukken II 1996/97, 25 533, nr. 3, p. 125 (MvT).

¹⁰⁶ NvT bij het Bbgt, *Stb. 2003*, 472, p. 9.

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 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."*¹⁰⁷

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
11171

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 Odido diverse van deze beveiligingsmaatregelen niet heeft getroffen. Over vrijwel de gehele linie van de beveiliging van LI-gegevens, heeft Odido nagelaten adequate beveiligingsmaatregelen te treffen.

In zijn algemeenheid overweeg ik hierbij dat het van zwaarwegend belang is dat Odido geen weet had van de overtredingen, terwijl Odido 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, en die bovendien langere tijd hebben voortgeduurd.

¹⁰⁷ NvT bij het Bbgt, Stb. 2003, 472, p. 7.

Door het aantal geconstateerde overtredingen en de aard van deze overtredingen in de LI-keten van Odido acht ik het risico dat er ongeautoriseerde toegang plaats heeft kunnen vinden zeer 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.

Een adequate beveiliging van LI-gegevens 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 Odido conceptueel, zoals dient te worden vastgelegd in het beveiligingsplan, als in de daadwerkelijke uitvoering zeer ernstig tekort schoot.

De overtredingen zijn gegroepeerd in drie hoofdovertredingen. In de hiernavolgende paragrafen ga ik nader in op de aard en de ernst per vastgestelde hoofdovertreding.

8.2 Overtreding 1. Beveiligingsplan

Odido had geen beveiligingsplan. Dit beveiligingsplan had het startpunt moeten vormen van een deugdelijke beveiliging van LI-gegevens door Odido. Zonder deugdelijk plan is het onmogelijk om 'in control' te zijn ten aanzien van de beveiliging. Dat Odido in de praktijk ook daadwerkelijk niet 'in control' was, blijkt uit de overige overtredingen. Een beveiligingsplan vormt het startpunt en het fundament van een deugdelijke beveiliging en is daarmee ook een essentieel onderdeel van de beveiliging van LI-gegevens. Daarbij wil ik er ook nog op wijzen dat uit het Bbgt de verplichting volgt om het beveiligingsplan jaarlijks te updaten. Ik ben daarom van oordeel dat het in het geheel ontbreken van een beveiligingsplan een verhoogde ernst oplevert. Het feit dat Odido naar aanleiding van het onderzoek van de toezichthouder een beveiligingsplan heeft opgesteld, maakt dat niet anders. Het bleef immers de zelfstandige verplichting voor Odido om het Bbgt na te leven en dit heeft zij niet gedaan.

Ten aanzien van de duur van de overtreding merk ik op dat Odido een lange(re) periode in het geheel niet over beveiligingsplan beschikte. Doordat Odido eerst op 13 oktober 2021 een beveiligingsplan heeft opgesteld, beschikte zij vanaf die datum in ieder geval over een beveiligingsplan.¹⁰⁸ Voor de duur van de overtreding ga ik uit van de start van het onderzoek tot het moment dat Odido een beveiligingsplan heeft opgesteld, te weten van 5 oktober 2021 tot 13 oktober 2021, de dag waarop Odido een beveiligingsplan heeft opgesteld.

8.3 Overtreding 2. Beveiligingseisen ten aanzien van personeel

De toezichthouder heeft meerdere overtredingen vastgesteld ten aanzien van de vereisten die gelden voor personeel. Dit betreffen stuk voor stuk zeer ernstige tekortkomingen. De medewerkers die belast zijn met, dan wel in aanraking kunnen komen met LI-gegevens dienen namelijk zeer zorgvuldig met deze

¹⁰⁸ De toezichthouder heeft niet onderzocht of het beveiligingsplan van 13 oktober 2021 ook daadwerkelijk voldoet aan artikel 3, eerste lid, van het Bbgt.

informatie om te gaan. Odido dient ervoor te zorgen dat deze personen geheimhouding met betrekking tot de LI-gegevens betrachtingen. Het is daarom van belang dat uitsluitend daartoe bevoegd en aangewezen personeel kennis kan nemen van LI-gegevens en daartoe toegang heeft. Odido dient ook zicht te hebben op de personen die daartoe bevoegd zijn. Enkel op die manier kan Odido maatregelen treffen ter waarborging van de geheimhouding, waaronder door middel van geheimhoudingsverklaringen en VOG's en door medewerkers ook (bij wijze van functiebeschrijvingen) te wijzen op de belangrijke verantwoordelijkheid die zij hebben. Odido had hier gezien voormelde tekortkomingen geen zicht op. Als gevolg van de vastgestelde tekortkomingen heeft Odido gedurende een lange periode een ernstig risico gelopen op onbevoegde toegang of een schending van de strikt vereiste geheimhouding.

Odido heeft daarnaast een resultaatsverplichting om te voorkomen dat personen die niet zijn belast met de verwerking van LI-gegevens toegang zou kunnen hebben tot deze gegevens. Hierin is zij niet geslaagd, nu de toezichthouder heeft vastgesteld dat 81 ongeautoriseerde personen toegang hadden tot de LI-gegevens via de LI-Firewall door een slordige uitgevoerde configuratie. Ook dit betreft een zeer ernstige tekortkoming.

Ten aanzien van de duur van de overtreding ga ik uit van de onderzoeksperiode van de toezichthouder zoals is vastgelegd in het Rvb, te weten voor in ieder geval de periode van 5 oktober 2021 (het begin van het onderzoek door de toezichthouder) tot en met 14 september 2022 (de datum waarop het traject met betrekking tot de Bbgt HR-vordering van 19 juli 2022 is afgesloten met een laatste brief vanuit de RDI).

8.4 Overtreding 3. Beveiligingseisen ten aanzien van de geautomatiseerde systemen

Odido heeft de toegang tot haar geautomatiseerde systemen waarin LI-gegevens worden verwerkt onvoldoende beveiligd. Op meerdere vlakken schoot de toegangsbeveiliging door Odido tekort.

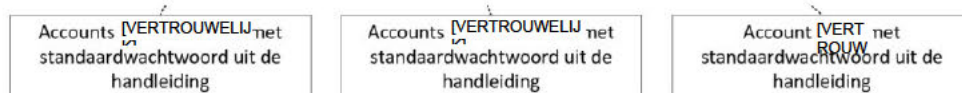
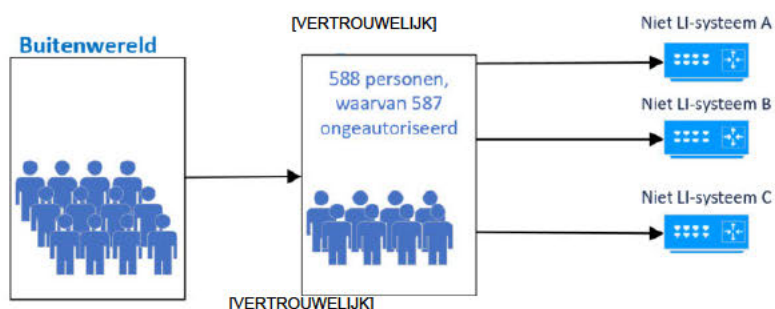
- I. Op twee systemen was geen sprake van deugdelijke beveiliging, onder meer doordat persoonsgebonden authenticatie ontbrak en gebruik werd gemaakt van (oude) standaardwachtwoorden (artikel V, onder a, bijlage Bbgt);
- II. Op twee systemen was geen blokkering van kracht bij overschrijding van drie foutieve inlogpogingen (artikel V, onder c, bijlage Bbgt);
- III. Op twee systemen was geen centrale logging en detectie geactiveerd (artikel V, onder b, bijlage Bbgt);
- IV. Handelingen met betrekking tot de verwerking van LI-gegevens werden niet persoonsgebonden vastgelegd om onderzoek mogelijk te maken (artikel V, onder e, bijlage Bbgt).

Dit zijn zeer ernstige overtredingen van het Bbgt. Deze overtredingen hebben bovendien zeer lange tijd, ruim negen jaar, geduurd. Daarmee hebben zich gedurende lange tijd zeer grote risico's op ongeoorloofde toegang voorgedaan. Daarbij zijn bovendien, gezien de aard van de vastgestelde tekortkomingen – waaronder de afwezigheid van persoonsgebonden authenticatie en van centrale

logging en detectie – de precieze gevolgen van de vastgestelde tekortkomingen niet in te schatten of vast te stellen.

Wat vaststaat, is dat een groot aantal beheerders van leveranciers van Odido, waaronder [VERTROUWELIJK], toegang had tot het [VERTROUWELIJK] van Odido en dat van deze toegangsmogelijkheid ook daadwerkelijk gebruik is gemaakt door medewerkers van [VERTROUWELIJK]. Dit, gezien in combinatie met het feit dat er vanaf het [VERTROUWELIJK] inlogpogingen gedaan konden worden op het [VERTROUWELIJK], en dat er op het [VERTROUWELIJK] ingelogd kon worden met standaard niet-persoonsgebonden accounts en de standaardwachtwoorden van [VERTROUWELIJK], welke al in gebruik waren sinds de implementatie van het [VERTROUWELIJK] door [VERTROUWELIJK] en er op dit systeem bewust onversleutelde taplijsten aanwezig waren, maakt de kans op ongeautoriseerde leverancierstoegang zeer groot.

Hieronder is bovenstaande schematisch weergegeven.



Figuur 2. Schematisch overzicht toegang tot LI-gegevens op het [VERTROUWELIJK]

Ik ben van oordeel dat de aard en de omvang van deze overtreding een verhoogde ernst oplevert. Zoals gezegd gaat het om de meest gevoelige, veelal staatsgeheime informatie. Van een partij die onderdeel is van de vitale infrastructuur in Nederland mag worden verwacht dat zij op de hoogte is van de regels ter bescherming van zwaarwegende maatschappelijke belangen, zoals de beveiliging van staatsgeheime informatie.

Ten aanzien van de duur van de overtreding ga ik uit van het moment van ingebruikname van het [VERTROUWELIJK] tot het moment van vaststelling van vaststelling van de overtreding, te weten voor de periode van in ieder geval 17 december 2012 tot en met 7 februari 2022. De lange duur van deze overtreding

maakt de omvang van de overtreding zeer groot. Ook dit levert daarom een verhoogde ernst op.

9 Verwijtbaarheid

9.1 Algemeen

Als gevolg van de geconstateerde overtredingen heeft Odido onvoldoende dan wel ontoereikende maatregelen getroffen ter beveiliging tegen onbevoegde kennisneming en geheimhouding van LI-gegevens.

Van Odido mag verwacht worden dat zij op zijn minst de basis op orde heeft en zorgdraagt voor een toereikende beveiliging van LI-gegevens. Odido is immers een van de drie grote mobiele operators in Nederland met 7,3 miljoen klanten in 2024¹⁰⁹ en het werken met telecomgegevens raakt haar kernactiviteiten.

In de hiernavolgende paragrafen ga ik nader in op de verwijtbaarheid per vastgestelde hoofdovertreding.

9.2 Overtreding 1. Beveiligingsplan

Het hebben van een deugdelijk beveiligingsplan is het startpunt voor een goede beveiliging van LI-gegevens. Aan deze basisverplichting heeft Odido niet voldaan. Dit is ook zichtbaar geworden in de onderzochte LI-systemen. De verplichting om over beveiligingsplan te beschikken staat al sinds 2003 in artikel 3, eerste lid, van het Bbgt.¹¹⁰ Een professionele marktpartij als Odido wist, of in ieder geval behoorde te weten, dat zij diende te beschikken over een beveiligingsplan. Dat Odido in zijn geheel niet beschikte een beveiligingsplan en zich hier niet bewust van was reken ik Odido als professionele partij zwaar aan. Ik ben daarom van oordeel dat de overtreding aan haar te verwijten is.

9.3 Overtreding 2. Beveiligingseisen ten aanzien van personeel

Uit het Bbgt en de bijlage bij het Bbgt blijkt duidelijk welke maatregelen Odido diende te treffen ten aanzien van personeel dat (kort gezegd) in aanraking komt met LI-gegevens en dat ongeautoriseerde toegang voorkomen moet worden.

Ook deze basisverplichtingen staan al sinds 2003 in het Bbgt¹¹¹, welke in 2005 in werking is getreden.¹¹² De bevindingen van mijn toezichthouder laten zien dat bij Odido de minimum beveiligingseisen ten aanzien van het personeel niet werden nageleefd. Ook hierbij geldt dat een professionele marktpartij als Odido wist of in ieder geval behoorde te weten, dat voorgenoemde eisen gelden. Dat Odido de beveiligingseisen ten aanzien van personeel niet naleefde en zich daar niet van bewust van was reken ik Odido als professionele marktpartij zwaar aan. Ik ben daarom van oordeel dat de overtreding aan haar te verwijten is.

¹⁰⁹ Zie paragraaf 5.2.1 van dit besluit.

¹¹⁰ *Stb.* 2003, 472, p.2.

¹¹¹ *Stb.* 2003, 472, p.2, en p.5.

¹¹² *Stb.* 2005, 141.

9.4 Overtreding 3. Toegang geautomatiseerde systemen

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
11171

Uit het Bbgt en de bijlage volgt duidelijk dat (de toegang tot) de geautomatiseerde systemen waarin LI-gegevens worden verwerkt deugdelijk logisch beveiligd dienen te worden. Ook volgt hieruit duidelijk welke maatregelen daartoe *minimaal* getroffen dienen te worden. De bevindingen van de toezichthouder laten zien dat bij Odido de minimum beveiligingsmaatregelen niet zijn getroffen ten aanzien van de logische beveiliging van LI-gegevens. Ook hiervoor geldt dat van een professionele marktpartij als Odido verwacht mag worden dat zij op de hoogte is van de precieze inhoud van de normen en zich de nodige inspanningen getroost om daar ook daadwerkelijk aan te voldoen. Het is daarmee primair de eigen verantwoordelijkheid van de marktdeelnemer om deze wettelijke verplichtingen na te komen en om in dit verband veiligheidsrisico's te ondervangen.

Ik reken het Odido als professionele marktpartij daarom zwaar aan dat zij de vereiste beveiligingsmaatregelen ter bescherming van de toegang tot geautomatiseerde systemen waarin LI-gegevens verwerkt worden niet heeft getroffen. Ik ben daarom van oordeel dat deze overtreding aan haar te verwijten is.

Gelet op voorgaande reken ik het Odido zeer zwaar aan dat zij bewust een risico heeft genomen ten aanzien van de beveiliging van LI-gegevens. In dit verband reken ik Odido zeer zwaar aan dat Odido weloverwogen de X1-, X2- en X3-verbindingen onversleuteld heeft laten implementeren. Dit levert een verhoogde mate van verwijtbaarheid op.

10 Zienswijze Odido

Bij brief van 20 mei 2025 heb ik Odido in kennis gesteld van mijn voornemen tot het opleggen van een bestuurlijke boete wegens de overtredingen van de artikelen 2, 3 en 4 van het Bbgt en de bijbehorende bijlage en op mijn voornemen een publieksversie van dit besluit te publiceren (hierna: voornemen). Odido is in de gelegenheid gesteld naar aanleiding hiervan mondeling dan wel schriftelijk een zienswijze naar voren te brengen.

Odido heeft op 3 juli 2025 een schriftelijke zienswijze gegeven op mijn voornemen. Daarnaast heeft Odido tijdens de zienswijzezitting van 8 juli 2025 een aanvullende zienswijze gegeven. Odido heeft daarbij pleitaantekeningen verstrekt van de door haar voorgedragen zienswijze. Deze pleitaantekeningen zijn bij het verslag van de zienswijzezitting gevoegd, zie bijlage 3.

Overkoepelend betwist Odido de geconstateerde overtredingen ten aanzien van het beveiligingsplan en de geconstateerde overtredingen die zien op de vereiste beveiligingsmaatregelen ten aanzien van personeel. Odido erkent dat de toegangsbeveiliging van de geautomatiseerde systemen waarin LI-gegevens worden verwerkt, beter had gekund. Odido stelt zich op het standpunt dat de voorgenomen boetehoogte voor de overtreding ten aanzien van de beveiliging van de toegang tot de geautomatiseerde systemen waarin LI-gegevens worden verwerkt onevenredig hoog is.

Odido voert aan dat ik in het voorgenomen besluit de normen uit het Bbgt uitleg volgens de maatstaven in het huidige tijdsgewricht, en niet op de wijze zoals die destijds door de regelgever is beoogd. Odido acht dit problematisch, omdat de

RDI deze – in de ogen van Odido – striktere normuitlegging niet kenbaar heeft gemaakt via beleidsregels, richtsnoeren of op andere wijze. Odido had hierdoor niet op de hoogte kunnen zijn van de wijze waarop zij aan de normen uit het Bbgt kon voldoen. Odido stelt dat ik op basis van deze normuitlegging niet over had mogen gaan tot boeteoplegging.

Odido voert daarnaast aan dat zij een ontoereikende termijn heeft gekregen om haar zienswijze op het voorgenomen besluit te geven.¹¹³ Ik bespreek de zienswijze van Odido in de hiernavolgende paragrafen.

10.1 Algemeen

10.1.1 Zienswijze Odido duidelijkheid normen

Odido voert, kort en zakelijk weergegeven, aan dat ik niet tot handhavend optreden had mogen besluiten, vanwege de striktere uitleg van de normen uit het Bbgt door de RDI en het gebrek aan voorzienbaarheid van deze uitleg. Odido onderkent daarbij dat het cyberlandschap de afgelopen 15 jaar aanzienlijk is veranderd, mede door geopolitieke verschuivingen en dat dit ook invloed heeft op opvattingen over informatiebeveiliging. Dit betekent volgens Odido niet dat de RDI de normen uit het Bbgt, dat stamt uit 2003, in mag vullen naar de maatstaven van 2025.¹¹⁴ Odido benoemt hierbij een aantal specifieke normen uit het Bbgt, waar ik volgens Odido een strengere normuitlegging toepas dan door de wetgever is beoogd.¹¹⁵

Odido merkt daarbij ook op dat de inrichting van mobiele netwerken als gevolg van technologische ontwikkelingen sinds 2003 sterk is veranderd, en dat deze ontwikkelingen invloed hebben op het feitelijke werkproces rondom aftappen. Het tapproces vormt anno nu een geïntegreerd onderdeel van de functionaliteit van de netwerken die 5G-aanbieders, zoals Odido, exploiteren.¹¹⁶

Op grond van bovenstaande betwist Odido dat zij de wettelijke normen uit het Bbgt heeft overtreden.

10.1.2 Mijn reactie

In reactie op de stellingen van Odido stel ik voorop dat ik bevoegd ben om handhavend op te treden tegen overtredingen van de Tw en de normen uit het Bbgt. Artikel 2, eerste lid, van het Bbgt bepaalt in dat verband dat aanbieders zorg moeten dragen 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. Ik meen dan ook dat een

¹¹³ Randnummer 6-9.

¹¹⁴ Randnummer 12-14.

¹¹⁵ Randnummer 17.

¹¹⁶ Randnummer 15.

professionele marktdeelnemer als Odido 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. Ik heb hiervoor vastgesteld dat Odido hier niet aan heeft voldaan, nu Odido negen normen uit het Bbgt en de bijlage heeft overtreden, over meerdere lagen van de interne organisatie. Deze bevindingen laten zien dat Odido de minimumbeveiligingseisen, zoals die door het Bbgt vereist worden, volstrekt niet op orde had.

Het standpunt van Odido dat ik hierbij een striktere normuitleg hanteer dan de wetgever bij het opstellen van de regelgeving heeft beoogd, kan ik niet volgen. Zoals beschreven in het juridisch kader volgt uit het Bbgt duidelijk dat de maatregelen bij dienen te dragen aan het doel van het Bbgt, te weten het bewerkstelligen van een minimumniveau van beveiliging.¹¹⁷ De wetgever benadrukt in aanvulling daarop tevens dat het Bbgt als doel heeft de beveiliging van LI-gegevens en het voorkomen van een inbreuk op de vertrouwelijkheid daarvan. Daaruit vloeit logischerwijs voort dat de te treffen beveiligingsmaatregelen aan moeten sluiten bij de huidige stand van de techniek. Dit is ook bevestigd in de rechtspraak.¹¹⁸

Technologische ontwikkelingen die zich voor hebben gedaan afgelopen 20 jaar en die zich nog voor zullen gaan doen in de toekomst, zullen daarom blijvend in ogenschouw genomen moeten worden om aan het Bbgt te (blijven) voldoen. Immers bepaalt het Bbgt aan welk doel een aanbieder, zoals Odido, moet voldoen, namelijk het behalen van een minimumniveau van beveiliging, om kennisneming van LI-gegevens door onbevoegden te voorkomen. Uit vaste rechtspraak volgt dat van een professionele marktpartij, zoals Odido, mag worden verwacht dat deze de nodige inspanningen verricht om zich op de hoogte te stellen van de geldende wet- en regelgeving, zich daarnaar te gedragen en zich terdege te informeren over de daaruit voortvloeiende beperkingen en verplichtingen¹¹⁹ en om veiligheidsrisico's te ondervangen.¹²⁰ Odido kan dus niet volstaan met verouderde maatregelen.¹²¹ Gelet op het voorgaande kan Odido zich dus niet verschuilen achter het uitblijven van een normconcretiserende aanwijzing door de RDI.

Daarbij merk ik ook op dat de aanbieders die later zijn opgegaan in de rechtsvoorganger van Odido¹²² onderdeel uitmaakten van het deelorgaan aftappen in het Overlegorgaan Post en Telecommunicatie (het zogenaamde 'OPT/DAF').¹²³ Zoals uit de toelichting van het Bbgt blijkt is het OPT/DAF betrokken geweest bij de totstandkoming van het Bbgt en hebben de leden ingestemd met het ontwerpbesluit:

"Een ontwerp van het onderhavige besluit is bij brief van 26 april 2002 voorgelegd aan het deelorgaan aftappen van het Permanent overlegorgaan post en telecommunicatie (OPT/DAF). Het ontwerp is in het overlegorgaan op 15 mei en 26

¹¹⁷ Stb. 2003, 472, p. 9.

¹¹⁸ CBb 16 november 2016, ECLI:NL:CBB:2016:346 en Rechtbank Rotterdam 21 oktober 2024, ECLI:NL:RBROT:2024:10347, r.o. 23.5.

¹¹⁹ EHRM 11 november 1996, ECLI:CE:ECHR:1996:1115JUD001786291 (Cantoni/Frankrijk), r.o. 35; EHRM, 20 januari 2009, ECLI:CE:ECHR:2009:0120JUD007590901 (Sud Fondi SRL e.a./Italië), r.o. 109; CBb, 22 februari 2012, ECLI:NL:CBB:2012:BV6713, r.o. 4.3; CBb, 21 mei 2019, ECLI:NL:CBB:2019:207, r.o. 4.10 en 4.11; CBb, 30 juni 2020, ECLI:NL:CBB:2020:419, r.o. 6.2.

¹²⁰ CBb, 20 juli 2017, ECLI:NL:CBB:2017:274, r.o. 6.2; CBb, 26 maart 2024, ECLI:NL:CBB:2024:223, r.o. 4.7.3.

¹²¹ Rechtbank Rotterdam 21 oktober 2024, ECLI:NL:RBROT:2024:10347, r.o. 23.5.

¹²² Ben Nederland B.V., Dutchtone N.V. en Versatel Telecom B.V. zijn opgegaan in T-Mobile.

¹²³ Zie artikel 2 van het (vervallen) Instellingsbesluit deelorgaan aftappen.

juni 2002 aan de orde gesteld. Voorts is – naar aanleiding van de uitvoerige bespreking in het OPT/DAF – een aangepast ontwerp in augustus 2002 nog voor een schriftelijke commentaarronde aan de leden van OPT/DAF voorgelegd. Bij brief van 23 september 2002 heeft het OPT/DAF uiteindelijk zijn rapport van bevindingen uitgebracht. Daarin wordt aangegeven dat de leden van het OPT/DAF kunnen instemmen met het ontwerpbesluit.”¹²⁴

Rijksinspectie Digitale Infrastructuur

Ons kenmerk
[VERTROUWEL
1111]

Gezien het voorgaande wist (en wisten de rechtsvoorgangers van) Odido al vanaf het moment dat het Bbgt van kracht werd wat van haar werd verwacht. Dat de digitale infrastructuur van Odido er hedendaags anders uitziet dan in 2003 doet hier niets aan af.

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

10.1.3 Zienswijze Odido reactietermijn

Odido voert in haar zienswijze aan dat ze de aan haar gegeven reactietermijn voor het geven van een zienswijze onvoldoende acht om adequaat te kunnen reageren op mijn voornemen en het bijbehorende Rvb.¹²⁵

10.1.4 Mijn reactie

In reactie op de zienswijze van Odido dat de termijn die zij heeft gekregen voor het geven van een zienswijze tekort zou zijn, overweeg ik het volgende. Ik volg Odido niet in dit standpunt. Het concept Rvb is op 27 november 2024 door mijn toezichthouder met Odido gedeeld. Dat mijn toezichthouder aan Odido het concept Rvb zou toesturen was al aangekondigd op 24 oktober 2024. Het concept Rvb betrof een verregaand gereed concept, welke als laatste processtap in het toezichttraject met Odido is gedeeld, voor een feitenverificatie.¹²⁶ Odido heeft , inclusief een verlenging die verzoek van Odido is verleend, een termijn van zes weken gekregen om feitelijke onjuistheden te adresseren. Odido heeft hierop op 14 januari 2025 tijdig een reactie gegeven met daarin een aantal punten die volgens Odido tot wijziging, verbetering of aanvulling van de feiten moesten leiden en Odido heeft enkele tekstuele wijzigingsvoorstellen aangedragen.¹²⁷ Dit betrof met name kleine (tekstuele) wijzigingen en verduidelijkingsvragen, geen fundamentele wijzigingen of aanvullingen ten aanzien van de feiten. Na ontvangst hiervan heeft de toezichthouder de finale versie van het Rvb vastgesteld.

Odido heeft dus vanaf 27 november 2024 kennis kunnen nemen van de feitelijke bevindingen zoals geconstateerd door mijn toezichthouder, welke aan haar voor wederhoor zijn voorgelegd.

De mogelijkheid een zienswijze op mijn voornemen te geven, bood Odido nogmaals de gelegenheid om een reactie te geven. Odido was hiervan tijdig op de hoogte, nu ik haar tijdig op de hoogte heb gesteld wanneer dit voornemen aan

¹²⁴ Stb. 2003, 472, p. 17.

¹²⁵ Randnummer 5-9.

¹²⁶ [VERTROUWELIJK]

¹²⁷ [VERTROUWELIJK]

haar verzonden zou worden.¹²⁸ Odido heeft hiervoor een standaardtermijn van drie weken gekregen, welke op haar verzoek is verlengd met ruim drie weken. Ik merk op dat dat slechts drie werkdagen korter is dan waar zij om had gevraagd. Bovendien vond de zienswijzezitting plaats vijf dagen nadat de zienswijzetermijn was verlopen. Tijdens de zienswijzezitting is Odido de gelegenheid geboden een mondeling pleidooi te houden, waarin zij de ruimte kreeg om nieuwe punten aan te dragen en van deze ruimte is ook gebruik gemaakt door Odido. Odido is daarmee ruim voldoende in de gelegenheid gesteld om zich voor te bereiden, de feiten tot zich te nemen en haar reactie voor te bereiden. Bovenstaande in acht genomen, acht ik de zienswijzetermijn die aan Odido is gegeven voldoende om adequaat te kunnen reageren. Immers heeft Odido vanaf het moment dat het concept Rvb aan haar is toegezonden in totaal ruim zeven maanden de tijd gekregen zich voor te bereiden.

10.2 Overtreding 1. Ontbreken beveiligingsplan

10.2.1 Zienswijze Odido

Odido voert, kort en zakelijk weergegeven, aan dat ik artikel 3, eerste lid, van het Bbgt zo strikt uitlegt dat een beveiligingsplan moet bestaan uit één document. Odido stelt dat dit niet overeenkomt met het Bbgt en de toelichting daarop waaruit zou volgen dat er geen bijzondere vormvereisten gelden ten aanzien van het beveiligingsplan en dat bij complexe organisaties – zoals Odido - rekening gehouden moet worden met de uitvoerbaarheid.¹²⁹ Volgens Odido wijkt deze strikte uitleg ook af van de uitleg die de RDI heeft gehanteerd bij eerdere inspecties in 2005 en 2016 en de uitleg die in het boetebesluit van KPN in 2022 is gehanteerd.¹³⁰

Daarnaast voert Odido aan dat er door de RDI geen verder onderzoek is gedaan naar de oorsprong en inhoud van het beveiligingsplan dat door Odido is opgeleverd op 13 oktober 2021 waardoor de overtreding niet is te bewijzen en de grondslag voor overtreding en de verhoging ontbreekt.¹³¹ Tijdens de zienswijzezitting is door Odido aangegeven dat de toezichthouder had moeten doorvragen toen door Odido is aangegeven dat het beveiligingsplan voor 13 oktober 2021 bestond uit 'losse snippets'.

Odido geeft aan dat zij gecertificeerd is volgens internationale standaarden en normen, waaronder ISO 27001, waaruit bijzondere verplichtingen volgen. Aangezien Odido aan veel verplichtingen gelijktijdig en uniform uitvoering moet geven, beschikt Odido over een policy house dat gebaseerd is op dat de NIST standaard.¹³² Het policy house is één plan dat bestaat uit meerdere documenten, waarmee volgens Odido wordt voldaan aan artikel 3, eerste lid, van het Bbgt.¹³³

Subsidiair betoogt Odido met een verwijzing naar artikel 5:46 van de Awb dat als ik vasthoud aan de strikte uitleg van artikel 3, eerste lid, van het Bbgt het onevenredig is om zonder waarschuwing een zware boete op te leggen. Volgens Odido had moeten worden volstaan met een reparatoire maatregel al dan niet in

¹²⁸ [VERTROUWELIJK]

¹²⁹ Randnummer 29-33.

¹³⁰ Randnummer 34-37 en 55.

¹³¹ Randnummer 39-42.

¹³² Het National Institute of Standards and Technology (NIST) is een Amerikaanse wetenschappelijke instelling.

¹³³ Randnummer 45-49 en bijlage 1.

combinatie met een lichte sanctie zoals een waarschuwing of berisping. De reden hiervoor is dat bij eerdere inspecties geen overtreding is vastgesteld en door de RDI geen uitleg is gepubliceerd over de (gewijzigde) normuitleg waardoor Odido hiervan niet op de hoogte was.¹³⁴

10.2.2 *Mijn reactie*

Zoals ik heb overwogen in paragraaf 6.1 volgt uit de wettekst en de toelichting van het Bbgt dat er geen bijzondere vormvereisten gelden ten aanzien van het beveiligingsplan, maar dat in het beveiligingsplan minimaal alle maatregelen die in de zes genoemde categorieën beveiligingsmaatregelen in de bijlage bij het Bbgt in het beveiligingsplan aan bod moeten komen. Met het oog hierop heeft de toezichthouder Odido op 5 oktober 2021 verzocht de beveiligingsplannen, zoals bedoeld in artikel 3, eerste lid, van het Bbgt, aan te leveren. In tegendeel tot wat Odido stelt, is hierbij niet de suggestie gewekt dat het beveiligingsplan niet mag bestaan uit meerdere documenten. Uit de uitvraag van mijn toezichthouder van 5 oktober 2021 blijkt juist dat expliciet gevraagd is naar beveiligingsplannen (meervoud) en uit de reactie van Odido van 13 oktober 2021 blijkt dat Odido dit ook zo heeft opgevat. Odido geeft namelijk zelf aan dat zij 'De BBGT beveiligingsplannen' heeft aangeleverd. De stelling van Odido, dat ik artikel 3, eerste lid, van het Bbgt zo zou uitleggen dat het beveiligingsplan niet mag bestaan uit meerdere documenten, is dan ook ongefundeerd en onjuist. Dit is in ieder geval niet gesuggereerd door mijn toezichthouder.

Doordat Odido vervolgens slechts één document aanlevert dat ook nog eens is opgesteld op 13 oktober 2021, is mijn toezichthouder tot het oordeel gekomen dat het beveiligingsplan van Odido alleen dit document omvat. Dat in het Rvb en in dit besluit wordt gesproken over beveiligingsplan (enkelvoud) maakt dat niet anders. Artikel 3, eerste lid, van het Bbgt heeft het over een beveiligingsplan en in het Rvb en in dit besluit is ervoor gekozen om hierbij aan te sluiten. Dit laat echter onverlet dat een beveiligingsplan mag bestaan uit meerdere documenten en de toezichthouder ook met die insteek de uitvraag heeft gedaan bij Odido.

De redenering uit de zienswijze van Odido dat het policy house, dat Odido overigens niet heeft overgelegd gedurende de inspectie en bij haar zienswijze, zou kwalificeren als een beveiligingsplan in de zin van artikel 3, eerste lid, van het Bbgt, kan ik niet volgen. Wat vaststaat is dat Odido het policy house niet heeft overgelegd toen mijn toezichthouder om een beveiligingsplan vroeg. Het standpunt dat de toezichthouder had moeten doorvragen toen een medewerker van Odido aangaf dat er 'losse snippets' waren kan ik evenmin volgen. Het had de weg van Odido gelegen om het policy house aan te leveren als zij van mening is dat dit zou kwalificeren als een beveiligingsplan in de zin van artikel 3, eerste lid, van het Bbgt. Daarbij vraag ik mij af of het policy house door een medewerker van Odido zou worden gekwalificeerd als 'losse snippets'. Een 'snippet' betekent immers fragment of snipper, terwijl 'policy house' suggereert dat het gaat om een gestructureerd bouwwerk aan beleidsdocumenten.¹³⁵

Odido betoogt verder dat er door de toezichthouder geen nader onderzoek is gedaan naar de oorsprong en inhoud van het beveiligingsplan van 13 oktober 2021. Dit beeld herken ik niet. Zoals hiervoor is overwogen, ligt het op de weg

¹³⁴ Randnummer 54 en 56.

¹³⁵ Snippet is van oorsprong een Engelstalig woord dat wat in het Nederlands wordt vertaald met fragment, knipsel of snipper.

van Odido om de documenten die zij kwalificeert als beveiligingsplan in de zin van het Bbgt te overleggen als een toezichthouder hierom vraagt. Ik wil er daarbij ook op wijzen dat de toezichthouder, zoals is beschreven in paragraaf 6.1, nog vier aanvullende documenten heeft opgevraagd waar in het beveiligingsplan naar wordt verwezen. Verder heeft de toezichthouder in het gesprek van 29 oktober 2021 ook gevraagd om inzage in eerdere versies van het beveiligingsplan. Dit alles bij elkaar maakt dat de toezichthouder naar mijn oordeel zeer grondig onderzoek heeft gedaan naar de oorsprong van het beveiligingsplan van Odido.

Odido verwijst in haar zienswijze naar vaststellingen of uitlatingen die zouden zijn gedaan tijdens eerdere inspecties in 2005 en 2016. Uit vaste jurisprudentie volgt dat degene wie zich beroept op het vertrouwensbeginsel aannemelijk moet maken dat van de kant van de overheid toezeggingen of andere uitlatingen zijn gedaan of gedragingen zijn verricht waaruit hij in de gegeven omstandigheden redelijkerwijs kon en mocht afleiden of het bestuursorgaan een bepaalde bevoegdheid zou uitoefenen en zo ja hoe.¹³⁶ Ook volgt uit jurisprudentie dat in de situatie dat er in het verleden geen overtredingen zijn vastgesteld niet zonder meer leidt tot een geslaagd beroep op het vertrouwensbeginsel.¹³⁷ Odido heeft noch in haar schriftelijke zienswijze noch in haar mondelinge zienswijze aannemelijk gemaakt dat er tijdens deze eerdere inspecties uitlatingen zouden zijn gedaan over het beveiligingsplan die haaks zouden staan op onderhavig besluit. Het had op de weg van Odido gelegen om dit aannemelijk te maken, bijvoorbeeld door documenten te overleggen waaruit dergelijke uitlatingen zouden volgen. Gelet hierop kan ik het standpunt van Odido al niet volgen.

Subsidiair kan ik ook inhoudelijk gezien het standpunt van Odido dat tijdens eerdere inspecties in 2005 en 2016 en in het boetebesluit van KPN uit 2022¹³⁸ een andere uitleg zou zijn gegeven aan artikel 3, eerste lid, van het Bbgt niet volgen. Dit zal ik hierna uiteenzetten.

Ten tijde van de inwerkingtreding van het Bbgt per 1 juni 2005¹³⁹ is door (de rechtsvoorganger van) de RDI gebruikt gemaakt van de Checklist inspecties beveiliging gegevens bevoegd aftappen telecommunicatie (hierna: de checklist). In deze checklist wordt over het beveiligingsplan het volgende aangegeven:

*"Hoe een aanbieder aan deze beveiligingsverplichting voldoet mag de aanbieder zelf weten. Er moet wel een, op de aard van de gegevens toegesneden, minimum niveau van beveiligingsmaatregelen zijn getroffen. De regels voor dit minimum niveau zijn opgenomen in het Besluit beveiliging gegevens aftappen telecommunicatie. De aanbieder kan aan de hand van een beveiligingsplan dit minimum niveau aantonen. De vorm van het beveiligingsplan staat niet vast. Iedere aanbieder mag zijn eigen vorm kiezen en het op de eigen specifieke situatie toespitsen."*¹⁴⁰

En ook:

¹³⁶ Zie bijvoorbeeld ABRvS 10 juli 2024, ECLI:NL:RVS:2024:2822, r.o. 10.2

¹³⁷ Zie ABRvS 25 mei 2022, ECLI:NL:RVS:20221495, r.o. 9.2.

¹³⁸ De overtreding ten aanzien van het beveiligingsplan is vastgesteld voor de periode van in ieder geval 5 oktober 2021 tot en met 12 oktober 2021. Het boetebesluit van KPN dateert van 11 augustus 2022 en dit is dus na de overtredingsperiode van Odido.

¹³⁹ Stb. 2005, 141.

¹⁴⁰ Checklist inspecties beveiliging gegevens bevoegd aftappen telecommunicatie 24 mei 2005, p.3.

"Maatregelen die een aanbieder treft om de gegevens te beveiligen moeten worden vastgelegd in een beveiligingsplan. In het beveiligingsplan moet de koppeling zijn gemaakt met het relevante deel van het bedrijfsproces waarvoor de maatregel is getroffen. De beoordeling van de beveiligingmaatregelen kan niet zonder inzicht in het tapproces zoals dat bij de aanbieder verloopt. Daarom moet dit proces ook in het beveiligingsplan zijn beschreven. Aandachtspunten bij de beschrijving zijn:

- bij wie en hoe komen taplasten binnen;
- hoe lopen papierstromen;
- systemen waarop taplasten worden ingevoerd;
- procedure opvragen NAW gegevens en verkeersgegevens;
- procedure ongeoorloofde inbreuk vertrouwelijkheid gegevens."¹⁴¹

Vervolgens staat in deze checklist over het beveiligingsplan de volgende vragen:

Bestaat er binnen de organisatie een (zelfstandig) beveiligingsplan m.b.t. bevoegd aftappen?	o ja o nee (niet zelfstandig/aanwezig, onvolledig,)	Kopie verstrekt? o ja o nee
Maakt beveiliging aftappen onderdeel uit van een algeheel beveiligingsplan binnen de organisatie?	o ja o nee	Kopie verstrekt? o ja o nee
Is dit beveiligingsplan geaccordeerd door het management?	o ja o nee	management/directie/.....

De checklist die in 2005 is gehanteerd, is naar mijn oordeel in lijn met de uitleg die ik nu hanteer ten aanzien van artikel 3, eerste lid, van het Bbgt. In de checklist wordt uitgelegd dat een aanbieder de vrijheid heeft om het beveiligingsplan toe te spitsen op de specifieke situatie. Een beveiligingsplan hoeft niet te bestaan uit één zelfstandig document, maar mag ook bestaan uit meerdere documenten of mag onderdeel uitmaken van een algeheel beveiligingsplan binnen de organisatie, zolang minimaal alle vereisen uit de bijlage van het Bbgt aan bod komen.

Verder staan in het rapport van de inspectie uit 2016¹⁴² geen passages over het beveiligingsplan van de (rechtsvoorganger van) Odido. Ook in het boetebesluit van KPN uit 2022¹⁴³ staan geen passages waarin een andere uitleg wordt gehanteerd dan in dit besluit. Het enige verschil dat in het boetebesluit van KPN wordt gesproken over beveiligingsplannen (meervoud) en in dit besluit over beveiligingsplan (enkelvoud). Zoals ik hiervoor heb toegelicht, heb ik er in dit besluit voor gekomen om aan te sluiten bij de terminologie uit artikel 3, eerste lid, van het Bbgt, mede omdat Odido zelf op verzoek van de toezichthouder één document heeft overgelegd.

¹⁴¹ Checklist inspecties beveiliging gegevens bevoegd aftappen telecommunicatie 24 mei 2005, p.4.
¹⁴² [VERTROUWELIJK]

¹⁴³ Beschikking tot oplegging bestuurlijke boete en publicatie van 11 augustus 2022, met kenmerk [VE
[VERTROUWEL
RT
11171

Tenslotte doet Odido subsidiair een beroep op het evenredigheidsbeginsel. In aanvulling op hetgeen ik al heb aangegeven in paragraaf 10.1 en in paragraaf 11.1.1 van dit besluit zal toelichten, merk ik specifiek ten aanzien van verhoging op dat ik deze toepas, omdat Odido in zijn geheel niet beschikte over een beveiligingsplan en dit een verhoogde mate van ernst oplevert. Hetgeen Odido in haar zienswijze heeft aangevoerd heeft niet tot een ander oordeel daarover geleid. Ik ben daarom van oordeel dat de boete en de toegepaste verhoging evenredig zijn.

Conclusie

De zienswijze van Odido heeft ten aanzien van overtreding ten aanzien van het beveiligingsplan dan ook niet tot een ander oordeel geleid.

10.3 Overtreding 2. Beveiligingseisen ten aanzien van personeel

10.3.1 Zienswijze Odido geautoriseerde toegang

Odido voert, kort en zakelijk weergegeven, aan dat ik in zijn algemeenheid onvoldoende rekening heb gehouden met het bredere beveiligingsbeeld. Hierbij geeft Odido aan dat de drie LI-medewerkers van Odido gescreend zijn door de AIVD, waarmee het risico op inbreuk van de vertrouwelijkheid van de LI-gegevens wordt beperkt. Volgens Odido is de reden voor de screening dat deze medewerkers zijn belast met het verwerken van LI-gegevens en moet ook aan deze medewerkers worden uitgelegd waarom ze gescreend worden. Binnen de organisatie zou het voor deze medewerkers daarom voldoende duidelijk dat zij een LI-taak vervullen.¹⁴⁴ Tijdens de zienswijzezitting heeft Odido in aanvulling op het voorgaande aangegeven dat het doel van de Bbgt is om ervoor te zorgen dat personeel dat belast is met een LI-taak is doordrongen is van de taak en de vertrouwelijkheid die daarbij hoort. Hieraan wordt volgens Odido voldaan.

Vervolgens geeft Odido aan dat ten aanzien van alle personen uit paragraaf 6.2.1 van dit besluit er geen sprake is van een overtreding en dat er onvoldoende bewijs wordt aangeleverd.

a. Geen VOG

Volgens Odido beschikten de medewerkers van [VERTROUWELIJK] gedurende de inspectie wel over een VOG. Deze VOG's zijn ten onrechte niet zijn overgelegd tijdens de inspectie vanwege een miscommunicatie.¹⁴⁵ Tijdens de zienswijzezitting heeft Odido aangegeven dat er een bezoek heeft plaatsgevonden van de toezichthouder bij [VERTROUWELIJK] in Rotterdam. De toezichthouder had volgens Odido de VOG's daar kunnen opvragen. Tijdens de zienswijzezitting heeft Odido verder aangegeven dat zij tijdens de inspectie niet beschikte over de VOG's van de [VERTROUWELIJK] medewerkers en dat het aan [VERTROUWELIJK] is om ervoor te zorgen dat deze medewerkers voldoen aan het Bbgt. Odido verwijst hierbij naar een overeenkomst tussen Odido en [VERTROUWELIJK].

Odido betwist niet dat de [VERTROUWELIJK] toegang had het [VERTROUWELIJK], maar is van mening dat de [VERTROUWELIJK] geen medewerking verleent aan de uitvoering van taplasten. Odido geeft hierbij aan dat het [VERTROUWELIJK] slechts voor een klein deel gebruikt wordt voor de verwerking van LI-gegevens. Het [VERTROUWELIJK] als

¹⁴⁴ Randnummer 58.

¹⁴⁵ Randnummer 61 en 62.

geheel is volgens Odido daarom geen LI-systeem, waardoor het uitvoeren van reguliere onderhoudswerkzaamheden aan het [VERTROUWELIJK] niet betekent dat er medewerking wordt verleend aan de uitvoering van taplasten. Odido verwijst daarbij ook nog naar het feit dat deze beheerder geen account had in de [VERTROUWELIJK] en dat de [VERTROUWELIJK] inmiddels is vervangen.¹⁴⁶

b. Geen functieomschrijving

Ten aanzien van de drie LI-medewerkers stelt Odido zich op het standpunt dat zij wel over een toereikende functieomschrijving beschikken, namelijk [VERTROUWELIJK] en deze personen ook bekend waren met deze functieomschrijving. Odido stelt verder dat dit een algemene functieomschrijving is waarin de verantwoordelijkheid is beschreven ten aanzien LI-gegevens. Hiermee wordt volgens Odido voldaan aan het Bbgt. Odido beschikt dus niet over 'LI-specifieke functieomschrijvingen' en heeft deze dus ook niet kunnen overleggen toen deze zijn gevorderd.¹⁴⁷ Tijdens de zienswijzezitting heeft Odido aangegeven dat deze functieomschrijving ten tijde van de inspectie gold, maar dat de HR-systemen inmiddels zijn vervangen en ze dit daarom niet kan aantonen. Odido geeft daarbij aan dat het document dat bij de zienswijze is overgelegd is geprint in 2019. Volgens Odido is deze functieomschrijving, of in ieder geval een algemene omschrijving daarvan, tijdens de inspectie overgelegd.

Ten aanzien van de [VERTROUWELIJK] medewerkers stelt Odido dat zij geen inzage hoeft te hebben in de functieomschrijvingen van het [VERTROUWELIJK] personeel, omdat functieomschrijvingen alleen dienen om binnen de organisatie duidelijkheid te verschaffen over de vertrouwelijkheid van LI-gegevens. Deze personen worden ingehuurd bij een specialistisch bedrijf in LI-ondersteuning waardoor het vanzelfsprekend is dat deze personen LI-gegevens verwerken. Het is daarbij aannemelijk dat zij in hun interne functieomschrijving of arbeidsovereenkomsten hierop worden gewezen. Volgens Odido was het voor haarzelf en deze personen volstrekt duidelijk dat zij verantwoordelijk waren voor de verwerking van LI-gegevens waarmee wordt voldaan aan de doelstelling van artikel 2, onder a en de bijlage van het Bbgt. Tenslotte geeft Odido aan dat het gelet op de AVG niet passend zou zijn om deze gegevens structureel op te slaan of te verwerken.¹⁴⁸ Tijdens de zienswijzezitting heeft Odido aangegeven dat er afspraken zijn gemaakt met [VERTROUWELIJK] in een serviceovereenkomst en dat er accountgesprekken plaatsvinden.

Voor wat betreft de [VERTROUWELIJK] verwijst Odido naar hetgeen zij hiervoor heeft aangegeven over dat deze persoon niet belast is met het verwerken van LI-gegevens.

c. Geen geheimhoudingsverklaring

Odido geeft aan dat in het voornemen is erkend dat voor de drie LI-medewerkers een algemene geheimhoudingsverklaring is overgelegd. Over de geheimhoudingsverklaringen geeft Odido aan dat uit het Bbgt niet volgt dat er sprake moet zijn van een afzonderlijke geheimhoudingsverklaring. Volgens Odido volgt uit de toelichting uit het Bbgt juist het tegenovergestelde. Odido geeft aan dat dit een zorgplicht betreft waarbij de aanbieder zelf ruimte heeft om dit in te vullen. Odido

¹⁴⁶ Randnummer 65-67

¹⁴⁷ Randnummer 72-76

¹⁴⁸ Randnummer 79 – 84.

heeft deze zorgplicht ingevuld door algemene geheimhoudingsverklaringen in combinatie met organisatorische en educatieve maatregelen. Over de verwijzing naar de uitspraak van de voorzieningenrechter van de rechtbank Rotterdam geeft Odido aan hiervan niet de relevantie in te zien en daarnaast stelt Odido dat de uitspraak slechts een voorlopig karakter heeft. Volgens Odido is er ten aanzien van de drie LI-medewerkers geen toereikend bewijs geleverd voor deze overtreding.¹⁴⁹ Tijdens de zienswijzezitting heeft Odido aangegeven dat de organisatorische en educatieve maatregelen onder andere bestaan uit het volgen van een verplichte security awareness training, het volgen van aanvullende sessies geheimhouding, maar bijvoorbeeld ook interne screening, het gebruik van afgesloten ruimtes en aparte laptops.

Ten aanzien van de [VERTROUWELIJK] en de [VERTROUWELIJK] stelt Odido zich op het standpunt dat deze personen eveneens onderworpen waren aan een algemene geheimhoudingsverklaring in combinatie met organisatorische en educatieve maatregelen, waarmee aan de zorgplicht wordt voldaan. Verder geeft Odido aan dat van deze personen nooit de arbeidsovereenkomsten zijn gevorderd op 19 juli 2022, omdat alleen de LI-specifieke getekende geheimhoudingsverklaringen zijn gevorderd waarover Odido niet beschikte.¹⁵⁰

10.3.2 Mijn reactie

Het standpunt van Odido dat ik onvoldoende rekening heb gehouden met het bredere beveiligingsbeeld, waardoor de risico's op inbreuk van de vertrouwelijkheid van de LI-gegevens worden beperkt, kan ik niet volgen. Het Bbgt gaat niet om het beperken van risico's, maar dat kennisname van LI-gegevens door onbevoegden te allen tijde worden moet voorkomen. Dit vanwege het uiterst gevoelige karakter van de LI-gegevens.

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 wetslagen van een strafrechtelijk onderzoek of de veiligheid van de staat in ernstige mate in het geding. Het is dan ook noodzakelijk dat wordt voorzien in adequate beveiligingsmaatregelen van LI-gegevens.

In artikel 13.5, eerste lid, van de Tw is voor de aanbieders de basisverplichting neergelegd om de gegevens, die aan de aanbieders worden verstrekt om uitvoering te kunnen geven aan taplasten, te beveiligen tegen kennisneming door onbevoegden en om geheimhouding te betrachten met betrekking tot deze gegevens. Deze basisverplichting is nader uitgewerkt in het Bbgt. Op grond van het Bbgt dienen aanbieders zorg te dragen voor het treffen van in ieder geval de daarin voorgeschreven minimum beveiligingsmaatregelen om kennisneming van LI-gegevens door onbevoegden te voorkomen. De maatregelen die aanbieders minimaal dienen te treffen, zijn uitgewerkt in het Bbgt en de bijlage daarbij.

Dat Odido stelt dat op haar alleen een zorgplicht rust waardoor Odido ruimte heeft om aan de eisen uit het Bbgt invulling te geven, rijmt niet het voorgaande. De zorgplicht bestaat uit een resultaatsverplichting om te voorkomen dat personen die niet belast zijn met de verwerking van LI-gegevens wel toegang zouden kunnen hebben tot deze gegevens. Zoals aangegeven volgen uit het Bbgt

¹⁴⁹ Randnummer 87-93.

¹⁵⁰ Randnummer 95-97.

minimumverplichtingen waaraan Odido in ieder geval moet voldoen. Voor personeel dat is belast met de verwerking van LI-gegevens gelden derhalve drie minimumverplichtingen, namelijk dat zij beschikken over een VOG (of VGB), beschikken over een functieomschrijving waarin de verantwoordelijkheid is beschreven voor de beveiliging van LI-gegevens en beschikken over een geheimhoudingsverklaringen waarin de verantwoordelijkheid is beschreven ten aanzien van de geheimhoudingsplicht inzake LI-gegevens. Een screeningsonderzoek dat leidt tot een VGB zorgt er daarom, al dan niet in combinatie met organisatorische en educatieve maatregelen, niet voor dat ook aan het vereiste van een functieomschrijving en geheimhoudingsverklaring uit het Bbgt wordt voldaan. Dit betreffen zelfstandige verplichtingen waar Odido in ieder geval ook aan moet voldoen. Dat Odido ook eigen interne processen, zoals organisatorische en educatieve maatregelen, heeft om risico's te beperken juich ik toe, maar doet niet af aan het feit dat Odido aan de minimumeisen van het Bbgt moet voldoen. Aan deze minimumeisen heeft Odido niet voldaan.

a. *Geen VOG*

Over de stelling van Odido dat zij geen inzage hoeft te hebben in de functieomschrijvingen van het ^[VERTROUWELIJK] personeel, merk ik op dat ik daar in paragraaf 6.2 en 6.2.1 reeds uitgebreid op in ben gegaan. Ik heb in dat verband uiteengezet dat 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 bij uitbesteding verantwoordelijk is voor, onder meer, de naleving door de derde van ingevolge het Bbgt gestelde maatregelen. De eisen die het Bbgt stelt aan personeel dat in aanraking komt en belast is met de verwerking van LI-gegevens zijn onderdeel van die maatregelen. Odido 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. Dat artikel 8, eerste lid, onder c, van het Bbgt ziet op de naleving van alle voorschriften en maatregelen die zijn gesteld in het Bbgt, volgt ook uit de toelichting bij het Bbgt:

"In artikel 7 wordt deze zorgplicht nader geëxpliciteerd en wel in die zin, dat de aanbieder wordt verplicht om in een schriftelijke overeenkomst met de derde vast te leggen dat deze zich onder meer ertoe verplicht om de in het besluit gestelde maatregelen na te leven(..)

Voor de goede orde wordt opgemerkt dat ook bij de hier bedoelde derden vertrouwensfuncties kunnen worden aangewezen."¹⁵¹

De opmerking van Odido dat de toezichthouder de VOG's had moeten opvragen bij ^[VERTROUWELIJK] kan ik in het licht van het bovenstaande ook niet volgen. Uit artikel 8, derde lid, van het Bbgt in samenhang met artikel 4, tweede lid, van het Bbgt volgt immers dat Odido hiervoor verantwoordelijk is en deze verantwoordelijkheid niet kan 'doorschuiven' naar ^[VERTROUWELIJK]. Ik wil hierbij ook wijzen op de toelichting op het Bbgt waarin ook expliciet is opgenomen dat dit behoort tot de zorgplicht van Odido:

"Artikel 13.5 Tw biedt niet de grondslag om aan dergelijke derden, niet zijnde aanbieders van openbare telecommunicatienetwerken of -diensten, rechtstreeks

¹⁵¹ Stb. 2003, 472, p.14.

verplichtingen ter zake van de noodzakelijk geachte beveiligingsmaatregelen op te leggen. Niettemin moet het tot de zorgplicht van de aanbieder worden gerekend, dat in het geval dat hij werkzaamheden als hier bedoeld uitbesteedt, hij er op toeziet dat de noodzakelijke beveiligingsmaatregelen worden getroffen.”¹⁵²

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
1121

Dat Odido bij haar zienswijze alsnog de VOG's van deze medewerkers heeft overgelegd maakt dit niet anders. De toezichthouder heeft vastgesteld dat Odido in ieder geval ten tijde van de overtredingsperiode niet beschikte over de VOG's van deze medewerkers. Zoals ook in paragraaf 6.2.1 is aangegeven, is door Odido noch gesteld noch gebleken dat gedurende de periode van overtreding (5 oktober 2021 tot en met 14 september 2022) Odido beschikte over de VOG's van de betrokken vijf medewerkers. Sterker nog, door Odido is tijdens de zienswijzezitting expliciet onderkend dat zij ten tijde van het onderzoek niet beschikte over de VOG's van deze medewerkers. Met andere woorden: dat Odido inmiddels heeft laten zien dat zij nu over de VOG's beschikt, laat onverlet dat Odido die informatie tijdens de overtredingsperiode niet had.

Ten aanzien van de [VERTROUWELIJK] waarvan Odido betwist dat hij medewerking verleent aan de uitvoering van taplasten merk ik op dat, zoals ik in de inleiding van hoofdstuk 6 heb opgemerkt, in het [VERTROUWELIJK] gegevens worden verwerkt die vallen onder artikel 2, eerste lid, van het Bbgt waardoor voldaan moet worden aan het Bbgt. Dat het [VERTROUWELIJK] ook voor andere doeleinden wordt gebruikt en er (in meerderheid) andere gegevens worden verwerkt op dit systeem maakt dat niet anders.

Tijdens de kliksessies van 19 januari 2022 is gebleken dat de [VERTROUWELIJK] daadwerkelijk toegang had tot onversleutelde LI-gegevens, omdat hij kon inloggen [VERTROUWELIJK] en op alle benodigde componenten van het [VERTROUWELIJK] had¹⁵³ [VERTROUWELIJK] had deze toegang, omdat hij eerste- en tweedelijns beheerwerkzaamheden uitvoerde ten aanzien van het [VERTROUWELIJK]. In tegenstelling tot hetgeen Odido in haar zienswijze stelt, ben ik van oordeel dat het eerste- en tweedelijns beheer van LI-systemen, in combinatie met het hebben van toegang tot LI-gegevens, kwalificeert als het verlenen van medewerking aan de uitvoering van een bevoegd gegeven last en een verplichting tot het verstrekken van informatie. Zoals ook uiteen is gezet in paragraaf 6.2.1, kan zonder de werkzaamheden van de [VERTROUWELIJK] immers niet goed uitvoering aan taplasten worden gegeven.

b. Geen functieomschrijving

Het standpunt van Odido dat de drie LI-medewerkers van Odido wel over een toereikende functieomschrijving beschikten kan ik niet volgen. Zoals in paragraaf 6.2.1 uiteen is gezet, heeft de toezichthouder bij aanvang van het onderzoek een uitvraag gedaan waarin onder andere is gevraagd naar de functie van de medewerkers die onder het Bbgt HR Regime vallen en de datum van de (ondertekende) functiebeschrijving. Vervolgens heeft Odido een overzicht aangeleverd waarin, voor zover hier relevant, bij de betreffende drie medewerkers de volgende informatie staat:

¹⁵² Stb. 2003, 472, p.13.

¹⁵³ RvB, p.31 en p. 32.

Functie	Datum (ondertekening) functie omschrijving
[VERTROUWELIJK]	[VERTROUW ELIJK]
[VERTROUWELIJK]	[VERTROUWE LIJK]
[VERTROUWELIJK]	[VERTROUWE LIJK]

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWELIJK]

De toezichthouder heeft vervolgens de arbeidsovereenkomsten van deze drie personen, die voor wat betreft de datum overeenkomen met de datum uit het overzicht, ingezien en opgevraagd. Hierin zijn echter geen functiebeschrijvingen opgenomen waarin is vermeld dat zij verantwoordelijkheden hebben voor de verwerking en beveiliging van LI-gegevens. Daarmee wordt niet voldaan wordt aan de eis van artikel II, onder a, van de bijlage bij het Bbgt.

De functieomschrijving van [VERTROUWELIJK], die Odido bij haar zienswijze heeft overgelegd, is niet tijdens de inspectie is overgelegd. De functietitel [VERTROUWELIJK] is zonder verder duiding opgenomen bij één persoon in het overzicht dat is aangeleverd door Odido. Als aan alle drie deze medewerkers een LI-taak was toebedeeld en die taak tot hun functie behoorde dan had op de weg van Odido gelegen om naar aanleiding van het verzoek van de toezichthouder hiertoe hierover documentatie aan te leveren. Dat deze medewerkers waarschijnlijk verschillende functies hebben vervuld, maakt dit niet anders. Bij functiewijzingen is het aan Odido om een nieuwe functiebeschrijving op te stellen of ervoor te zorgen dat de bestaande functiebeschrijvingen worden aangevuld met een vermelding van verantwoordelijkheid voor een LI-taak. Uit de documentatie die is overgelegd is niet op te maken dat deze medewerkers gedurende de periode van in ieder geval 5 oktober 2021 tot en met 14 september 2022 een LI-taak vervulden, terwijl dit in de praktijk wel het geval was.

Odido verwijst ook nog naar de vordering van 19 juli 2022 waarin zou zijn gevraagd om de LI-specifieke functieomschrijvingen. De relevantie van deze opmerking zie ik niet. In deze vordering is expliciet aangegeven dat deze vordering niet zag op de personen die eerder al door Odido waren opgenomen in het overzicht TMNL – Overzicht medewerkers LI:

"Aan het begin van de inspectie, in de aankondigingse-mail, is door AT gevraagd naar het opleveren van de "Lijst met medewerkers per datum 6 oktober 2021 onder BBGT HR Regime...". Hierop is een door T-Mobile aangeleverde lijst retour gekomen in bestand "TMNL - Overzicht medewerkers LI.pdf" met daarin vier personen. Vervolgens zijn een aantal achterliggende documenten van deze lijst door inspecteurs op 29 oktober 2021 bij u op kantoor ingezien. Gedurende de inspectie hebben inspecteurs van AT vastgesteld dat een groter aantal personen dan deze vier personen, in aanraking kunnen komen met de LI-gegevens. Ik wil u middels deze vordering de gelegenheid geven om voor deze overige, door ons vastgestelde personen, de benodigde BBGT HR administratie aan ons op te leveren."
(onderstreping RDI/JZ)

Over de functieomschrijvingen van medewerkers van [VERTROUWELIJK] geeft Odido aan dat zij hierin geen inzage hoeft te hebben, omdat deze personen worden ingehuurd bij een specialistisch bedrijf. Zoals ik hiervoor ook onder a al uiteen heb gezet, ben ik van oordeel dat Odido op grond van artikel 8, eerste lid sub c en derde lid, Bbgt in samenhang met artikel II, onder a, van de bijlage van het Bbgt hiertoe wel is gehouden. Dat [VERTROUWELIJK] een gespecialiseerd bedrijf in LI-ondersteuning en

het voor Odido aannemelijk zou zijn dat de betreffende medewerkers over toereikende functieomschrijvingen beschikken doet hier niets aan af. Deze opmerking bevestigt naar mijn oordeel alleen maar dat Odido geen zicht had of de vijf ^[VERTROUWELIJK] medewerkers die, kortgezegd, een LI-taak vervulden ook daadwerkelijk voldeden aan de eisen uit het Bbgt. Anders dan Odido ben ik ook van oordeel dat de AVG er niet aan in de weg staat om te voldoen aan deze verplichting. Uit artikel 6, eerste lid onder c, van de AVG volgt immers dat persoonsgegevens morgen worden verwerkt om te voldoen aan een wettelijke verplichting.

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWELIJK]
1121

Ten aanzien van de ^[VERTROUWELIJK] zijn de argumenten van Odido gelijk als die bij onderdeel a. Ik verwijs daarom naar de motivering onder onderdeel a. Daarnaast verwijs ik naar hetgeen in paragraaf 6.2.1 staat over de arbeidsovereenkomst van de ^[VERTROUWELIJK] die is overgelegd bij de zienswijze. Kort gezegd is de conclusie dat deze arbeidsovereenkomst geen functieomschrijving bevat waarin de verantwoordelijkheid is beschreven voor de beveiliging van LI-gegevens.

c. Geen geheimhoudingsverklaring

Odido verwijst in haar zienswijze naar het bestaan van algemene contractuele geheimhoudingsverklaringen voor de drie LI-medewerkers, de ^[VERTROUWELIJK] en de ^[VERTROUWELIJK]. Anders dan Odido ben ik van oordeel dat een algemene contractuele geheimhoudingsverklaring onvoldoende is om te voldoen aan artikel II, onder b, van de bijlage bij het Bbgt.

Zoals ook in paragraaf 6.2.1 uiteen is gezet, vormt een geheimhoudingsverklaring voor personeel dat in aanraking komt met LI-gegevens, het sluitstuk van het bewustwordingsproces van voornoemd personeel van de vertrouwelijkheid van de LI-gegevens. Ik ben van oordeel dat uit de norm van artikel II, onderdeel b, van de bijlage bij het Bbgt volgt dat deze geheimhoudingsverklaring specifiek ziet op de verklaring van betrokken medewerkers dat zij geheimhouding betrachten ten aanzien van LI-gegevens. Een algemene en/of contractuele geheimhoudingsverklaring waarin (het belang van) de geheimhouding van LI-gegevens niet wordt genoemd, is dus niet voldoende en past ook overigens niet bij de strekking van de norm. Educatieve en/of organisatorische maatregelen maken dat niet anders.

Voor wat betreft de verwijzing naar de uitspraak van de voorzieningsrechter van de rechtbank Rotterdam van 21 oktober 2024¹⁵⁴ merk ik op dat, hoewel het tijdens de behandeling ter zitting van die zaak ook is stilgestaan bij algemene geheimhoudingsverklaringen voor personeel dat in aanraking komt met LI-gegevens, rechtsoverweging 23.7 alleen ziet op de geheimhoudingsverklaring uit artikel 8 van het Bbgt. Ik ben van oordeel dat deze rechtsoverweging naar analogie ook toepasbaar is voor de geheimhoudingsverklaring voor personeel dat in aanraking komt met LI-gegevens. Immers, artikel 8 van het Bbgt maakt uitsluitend duidelijk dat ook in geval van uitbesteding moet worden voldaan aan de normen die elders in het Bbgt zijn opgenomen. In de desbetreffende rechtsoverweging wordt ten aanzien van artikel 8 van het Bbgt overwogen dat algemene geheimhoudingsverplichtingen onvoldoende zijn. Daarmee is deze overweging onverminderd relevant.

¹⁵⁴ Rb. Rotterdam, 21 oktober 2024, ECLI:NL:RBROT:2024:10347.

Tenslotte kan ik de stelling van Odido dat ten aanzien van de ^[VERTROUWELIJK] medewerkers en de ^[VERTROUWELIJK] nooit de arbeidsovereenkomsten zijn gevorderd, maar slechts 'LI-specifieke geheimhoudingsverklaring' waarover Odido niet beschikt niet volgen. In de vordering van 19 juli 2022 is de gehele Bbgt HR-administratie gevorderd:

Rijksinspectie Digitale Infrastructuur

Ons kenmerk
[VERTROUWELIJK]
1121

Op basis van artikel 5.16 en 5.17 van de Awb vorder ik in verband met voornoemde inspectie de navolgende informatie/bescheiden:

De volledige Bbgt HR administratie, van personen die toegang hebben tot LI-informatie, waaruit blijkt dat de beveiligingseisen ten aanzien van deze personen zijn genomen. (...)

Per persoon acht ik drie documenten relevant:

1. (...)
2. De LI-specifieke getekende geheimhoudingsverklaring⁵
3. (...)

Als Odido van mening was dat in de arbeidsovereenkomsten van de betreffende medewerkers een geheimhoudingsverklaring was opgenomen waarmee wordt voldaan aan artikel II, onder b, van de bijlage van het Bbgt, dan had het op de weg van Odido gelegen om deze te overleggen in haar reactie op de vordering. Helemaal nu in voetnoot 5 van deze vordering ook nog expliciet is verwezen naar artikel II, onder b, van de bijlage bij het Bbgt. Tenslotte wil ik hierbij nog verwijzen naar paragraaf 6.2.1 waarin ik al heb geconcludeerd dat ook overlegde documentatie bij de zienswijze geen toereikende geheimhoudingsverklaringen in de zin van artikel II, onder b, van de bijlage van het Bbgt bevatten.

10.3.3 Zienswijze Odido ongeautoriseerde toegang

Odido voert, kort en zakelijk weergegeven, aan dat uit het Bbgt en de toelichting daarop geen definitie volgt van 'LI-systeem'. De definitie van LI-systeem die wordt gehanteerd is volgens Odido dusdanig ruim dat toegang tot het ^[VERTROUWELIJK] in feite gelijk staat aan toegang tot LI-gegevens waardoor de ^[VERTROUWELIJK] uit het Bbgt van toepassing zouden zijn op een zeer brede groep medewerkers en een groot deel van de (digitale) infrastructuur van Odido. Volgens Odido is dit praktisch onuitvoerbaar en in strijd met hetgeen de wetgever voor ogen heeft gehad bij de totstandkoming van het Bbgt. Volgens Odido moet gekeken worden of personen daadwerkelijk toegang hadden tot LI-gegevens.¹⁵⁵ Tijdens de zienswijzezitting heeft Odido aangegeven dat alleen de ^[VERTROUWELIJK] en de specifieke ^[VERTROUWELIJK] onder het Bbgt zouden vallen.

Odido heeft tijdens de zienswijzezitting aangegeven dat het Bbgt stamt uit 2003 en dat de uitleg dat iedere netwerkcomponent die toegang faciliteert tot LI-gegevens ook onder het Bbgt zou vallen hiermee niet strookt. Volgens Odido is de bedoeling van het Bbgt geweest dat de kern van het netwerk, in haar woorden: 'de aftapkamer' goed beveiligd zou worden en is het niet relevant wat daarbuiten gebeurt. Odido heeft hierbij het voorbeeld geschetst dat de logging van administratieve informatieverzoeken ten aanzien van een bepaald telefoonnummers geen tapinformatie is.

¹⁵⁵ Randnummer 102-105.

Voor wat betreft het [VERTROUWELIJK] en het [VERTROUWELIJK] geeft Odido aan dat dit algemene technische systemen zijn die voor verschillende toepassingen gebruikt worden. Daarbij bevinden de LI-gegevens zich alleen op de [VERTROUWELIJK] stelt Odido en komen de betreffende medewerkers in de praktijk altijd binnen via een graphical user interface (GUI) en niet via de SSH-ingang. Volgens Odido is het daarom ten aanzien van ongeautoriseerde toegang alleen relevant wie toegang had tot de betreffende [VERTROUWELIJK]. Dat 586 personen toegang hadden tot het [VERTROUWELIJK] is onvoldoende om aan te nemen dat er sprake is van een overtreding.¹⁵⁶

Volgens Odido is het onvoldoende om uit te gaan van een theoretische ongeautoriseerde toegang, maar moet er daadwerkelijk sprake zijn van ongeautoriseerde toegang. Odido is geeft aan dat het niet vanzelfsprekend is dat een persoon die kan inloggen op het [VERTROUWELIJK] ook weet hoe toegang verkregen wordt verkregen tot LI-gegevens. Volgens Odido is een beveiliging nooit 100 procent waterdicht, maar gaat het om het reduceren van risico's tot een aanvaardbaar niveau.¹⁵⁷

Voor wat betreft de LI-Firewall merkt Odido op dat het een tijdelijke misconfiguratie was en dat Odido die betreurt, maar dat dat bij dergelijke complexe systemen niet volledig is te voorkomen. Door Odido wordt vervolgens aangegeven dat het van belang is dat eventuele risico's effectief worden verholpen zodra deze geconstateerd zijn en dat ze dit heeft gedaan. Odido is van mening dat de 81 personen die ongeautoriseerde toegang zouden hebben gehad, vermoedelijk niet op de hoogte waren hiervan en dat er geen aanwijzingen zijn dat zij daarvan gebruik hebben gemaakt. Volgens Odido is hierbij slechts hooguit sprake van een theoretische kans op toegang, waardoor het daadwerkelijke beveiligingsrisico wordt beperkt.¹⁵⁸

10.3.4 Mijn reactie

Over het standpunt van Odido over dat de gehanteerde definitie van LI-systeem niet in lijn zou zijn het Bbgt merk ik op dat ik dit niet kan volgen. Zoals in de inleiding van hoofdstuk 6 en paragraaf 10.3.3 uiteen is gezet hanteer ik als maatstaf dat als in een digitaal systeem gegevens worden verwerkt die vallen onder artikel 2, eerste lid, van het Bbgt dit systeem moet voldoen aan het Bbgt. Dat een systeem ook voor andere doeleinden wordt gebruikt en er (al dan niet in meerderheid) daarom ook andere gegevens worden verwerkt op dit systeem maakt dat niet anders. Anders dan Odido ben ik van oordeel dat daarom niet alleen de [VERTROUWELIJK] van het [VERTROUWELIJK] en de [VERTROUWELIJK] van het [VERTROUWELIJK] systeem onder het Bbgt vallen, maar het [VERTROUWELIJK] als geheel en het [VERTROUWELIJK] als geheel.

Dat Odido hierbij verwijst naar het doel dat de wetgever voor ogen heeft gehad en dat daarbij rekening is gehouden met de uitvoerbaarheid kan ik in zoverre ook niet volgen. Het klopt dat bij de totstandkoming van het Bbgt aandacht is geweest voor de uitvoerbaarheid. Dit heeft onder andere toe geleid dat er sprake is van minimumvereisten waaraan *ten minste* moet worden voldaan:

¹⁵⁶ Randnummer 106-109

¹⁵⁷ Randnummer 110-112.

¹⁵⁸ Randnummer 116-118.

In de bijlage bij het besluit is een aantal maatregelen voorgeschreven, die door iedere aanbieder ten minste dienen te worden getroffen. De maatregelen zijn onderverdeeld in een zestal categorieën. De aanduiding van de verschillende categorieën sluit weliswaar niet geheel aan op de in artikel 2, tweede lid, geformuleerde aspecten, maar laten zich daar wel degelijk inpassen. Bij de formulering van de verschillende maatregelen is nadrukkelijk gelet op de aspecten relevantie en uitvoerbaarheid. Relevantie spreekt voor zich; de maatregelen dienen bij te dragen aan het doel van het besluit, te weten het bewerkstelligen van een minimum-niveau aan beveiliging. Uitvoerbaarheid is nadrukkelijk aandachtspunt geweest vanwege het feit dat de maatregelen door verschillende soorten aanbieders met uiteenlopende omvang en organisatievorm dienen te worden geïmplementeerd.

Dat de eisen uit het Bbgt voor Odido praktisch niet uitvoerbaar zouden zijn, kan ik dan ook niet volgen.

Odido betwist in de kern verder dat het alleen maar van belang is dat de betreffende personen daadwerkelijk toegang hebben gehad. In reactie hierop merk ik op tussen Odido en mij geen verschil van inzicht bestaat over de vraag of de personen genoemd in paragraaf 6.3.1.6 te weten circa 588 personen voor wat betreft het [VERTROUWELIJK] en de 81 personen uit paragraaf 6.2.2. ten aanzien van de LI-Firewall, belast waren met verwerking van LI-gegevens en al dan niet bevoegd waren om hiervan kennis te nemen¹⁵⁹

Odido miskent in haar zienswijze dat de norm uit artikel II, onder c, van de bijlage bij het Bbgt vereist dat personen die niet is belast met de verwerking van LI-gegevens *in geen geval* toegang heeft tot LI-gegevens. Dat ik niet zou hebben onderzocht of de betreffende personen daadwerkelijk toegang hebben gehad tot LI-gegevens althans dat niet zou hebben aangetoond, doet dan ook niet ter zake: het gaat om een resultaatsverplichting van Odido om te voorkomen dat personen dat niet zijn belast met de verwerking van LI-gegevens wel toegang zouden kunnen hebben tot deze gegevens. Reeds daarom meen ik dat al hetgeen Odido heeft opgemerkt over of de betreffende personen al dan niet weten dat zij de mogelijkheid daartoe zouden hebben, nog los van de vraag of deze stelling daadwerkelijk klopt, niet ter zake doet.

De stelling van Odido dat de tekortkoming van de LI-Firewall geen tekortkoming is van de eisen die gelden voor personeel, maar een tekortkoming in de toegangsbeveiliging van een technisch systeem kan ik niet volgen. Zoals de inleiding van paragraaf 6 is aangegeven, heb ik de vastgestelde overtredingen gegroepeerd in drie hoofdovertredingen. Door deze groepering is deze overtreding geschaard onder de hoofdovertreding beveiligingseisen van personeel, waaronder ook de overtredingen van artikel 4, eerste lid, van het Bbgt (VOG), artikel II, onder a, van de bijlage bij het Bbgt (functieomschrijving) en artikel II, onder b, van de bijlage bij het Bbgt (geheimhoudingsverklaring) zijn gegroepeerd.

Hoewel er enigszins een parallel te trekken is, omdat er (mede) door de misconfiguratie van de LI-Firewall er ongeautoriseerde toegang kon plaatsvinden, gaat het voor mij in de eerste plaats om de ongeautoriseerde toegang. Zoals in paragraaf 6.2.2 is uitgelegd hadden door deze 'tekortkoming' 81 personen de

¹⁵⁹ Alleen de [VERTROUWELIJK] was belast met de verwerking van LI-gegevens en was daarom bevoegd om hiervan kennis te nemen. Ten aanzien van het [VERTROUWELIJK] waren dus 587 van de 588 personen hiertoe niet bevoegd

mogelijkheid om toegang te verkrijgen tot LI-gegevens terwijl zij niet belast waren met de verwerking van LI-gegevens. Dit is een overtreding van artikel II, onder c, van de bijlage van het Bbgt, omdat uit dit artikel een volgt dat ongeautoriseerde personen geen toegang mogen hebben tot LI-gegevens. Ik zie daarom niet in waarom ik deze overtreding onder hoofdovertreding 3 had moeten groeperen.

10.3.5 Zienswijze Odido ne bis in idem overtreding 2 en 3

Odido voert, kort en zakelijk weergegeven, aan dat er ten aanzien overtreding 2 en 3 sprake is van schending van het ne bis in idem beginsel en dan specifiek eendaadse samenloop. Volgens Odido vloeit het risico op ongeautoriseerde toegang voort uit de mate van beveiliging. Odido stelt dat de LI-Firewall en het [VERTROUWELIJK] beide onder de reikwijdte van overtreding 2 en 3 vallen.¹⁶⁰

10.3.6 Mijn reactie

Ik herhaal in reactie op de zienswijze van Odido nogmaals dat artikel 2, eerste lid, van het Bbgt bepaalt 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 waaruit de maatregelen als bedoeld in het eerste lid *ten minste* dienen te bestaan. In het derde lid is vervolgens bepaald dat tot de maatregelen, bedoeld in het eerste en tweede lid, in ieder geval de maatregelen worden gerekend die zijn opgenomen in de bijlage bij het Bbgt. Hiermee heeft de wetgever beoogd om zelfstandige normen in het leven te roepen, die elk individueel en afzonderlijk nageleefd moeten worden. De Bbgt-verplichtingen zien elk op een eigen beveiligingsdoelstelling, in dit geval beveiligingseisen ten aanzien van personeel enerzijds en beveiliging van geautomatiseerde informatiesystemen anderzijds.¹⁶¹

De normen uit het Bbgt vormen een minimumniveau aan beveiligingsmaatregelen die de aanbieders in ieder geval en stuk voor stuk dienen te treffen. Zoals in de inleiding van hoofdstuk 6 en paragraaf 10.3.4 is opgemerkt heb ik meerdere overtredingen vastgesteld op alle vlakken van de minimale te treffen maatregelen. Odido heeft negen normen uit het Bbgt en de bijlage bij het Bbgt overtreden. Gezien het voorgaande ben ik bevoegd om per overtreding van de normen uit het Bbgt een bestuurlijke boete van maximaal € 900.000,- op te leggen. Ik heb de door mij vastgestelde overtredingen evenwel gegroepeerd in drie hoofdovertredingen. Dit heeft geleid tot de volgende drie hoofdovertredingen:

- I. Tekortkoming met betrekking tot het vereiste van een beveiligingsplan(artikel 3 Bbgt);
- II. Tekortkomingen ten aanzien van het personeel dat al dan niet toegang tot LI-gegevens mag hebben (artikel 4 Bbgt en art. II bijlage Bbgt);
- III. Tekortkomingen in de beveiliging van geautomatiseerde informatiesystemen (artikel V bijlage Bbgt).

¹⁶⁰ Randnummer 120–124.

¹⁶¹ Vgl. Cbb 25 augustus 2015, ECLI:NL:CBB:2015:285, r.o.11.5.

Dat sprake is van enige samenhang tussen de beveiligingseisen die in het Bbgt zijn opgenomen, maakt het voorgaande niet anders. Vanwege die samenhang heb ik immers besloten om de vastgestelde overtredingen te groeperen en onder te brengen in drie hoofdovertredingen. Die hoofdovertredingen dienen weliswaar hetzelfde doel – namelijk het zorgen voor een minimumniveau van beveiliging zodat zoveel mogelijk wordt voorkomen dat sprake is van ongeoorloofde toegang en zodat geheimhouding van LI-gegevens wordt betracht - maar dat laat onverlet dat deze groepen van overtredingen stuk voor stuk van elkaar verschillen en andere kenmerken en vereisten hebben.

Uit het ne bis in idem-beginsel volgt dat een overtreder niet tweemaal mag worden gestraft voor dezelfde gedraging.¹⁶² Eendaadse samenloop houdt in dat als door één gedraging twee of meer voorschriften worden overtreden die naar hun strekking zodanig nauw samenhangen dat slechts één overtreding plaatsvindt.¹⁶³ Hierbij wil ik ook wijzen op de volgende jurisprudentie waaruit volgt dat een verband tussen gedragingen niet zonder meer betekent dat er sprake is van hetzelfde feit:

“Naar het oordeel van het College verschillen de bovenbeschreven feitelijke gedragingen naar hun aard en strekking zodanig van elkaar dat niet van "hetzelfde feit" kan worden gesproken. De omstandigheid dat beide gedragingen gedeeltelijk gelijktijdig hebben plaatsgevonden en de omstandigheid dat AFM de vakbekwaamheid nader heeft onderzocht naar aanleiding van haar bevindingen met betrekking tot de adviespraktijk, doen aan het vorenstaande niet af. Voorts overweegt het College dat er weliswaar een verband kan bestaan tussen onvoldoende vakbekwaamheid en het onvoldoende inwinnen van cliëntspecifieke informatie, maar dit verband is niet zodanig dat geoordeeld dient te worden dat sprake is van dezelfde gedraging.”¹⁶⁴

En zie ook de uitspraak van het College van Beroep voor het bedrijfsleven (hierna: CBB) van 13 november 2017 waarin wordt aangegeven dat wanneer twee gedragingen door het veranderen van een omstandigheid beide niet langer als overtreding zouden worden aangemerkt, dit nog niet leidt tot een zodanig verband dat er sprake is van hetzelfde feit:

“In de tweede plaats dient gekeken te worden naar de gedragingen van appellante. Ook hier is naar het oordeel van het College sprake van een zodanig verschil in aard en kennelijke strekking dat niet van "hetzelfde feit" kan worden gesproken. De gedraging die tot de overtreding van artikel 7 van de Msw heeft geleid, komt kort gezegd erop neer dat appellante te veel mest heeft uitgereden. De gedraging die tot de overtreding van artikel 53 van het Uitvoeringsbesluit heeft geleid, is dat appellante heeft nagelaten vrachten mest te registreren. Dat beide gedragingen geen overtreding zouden zijn geweest als de percelen tot het bedrijf behorende oppervlakte landbouwgrond waren geweest, geeft nog niet een zodanig verband dat sprake is van hetzelfde feit.”¹⁶⁵

De zienswijze van Odido heeft betrekking op de LI-Firewall en het ^[VERTROUWELIJK] . Ten aanzien van de LI-Firewall merk ik op dat overtreding 3 daar niet op ziet en ik

¹⁶² Zie artikel 5:43 van de Awb.

¹⁶³ Vgl. artikel 55, eerste lid, van het Wetboek van Strafrecht

¹⁶⁴ CBB 29 juni 2012, ECLI:NL:CBB:2012:BW9888, r.o. 5.8

¹⁶⁵ CBB 13 november 2017, ECLI:NL:CBB:2017:434, r.o. 4.4

de zienswijze alleen om die reden al niet kan volgen. Deze overtreding verwijt ik Odido enkel onder hoofdovertreding 2.

Ten aanzien van het [VERTROUWELIJK] waren er in het voornemen zowel onder hoofdovertreding 2 als hoofdovertreding 3 feiten vastgesteld die zien op ongeautoriseerde toegang tot LI-gegevens op het [VERTROUWELIJK]. Daarbij geldt dat de zienswijze van Odido slechts ziet op enkele feiten die ten grondslag liggen aan hoofdovertreding 2.

Ten aanzien van het [VERTROUWELIJK] overweeg ik inhoudelijk dat voor het plegen van de overtredingen andere feiten en gedragingen aan ten grondslag liggen. Dit zal ik hierna uiteenzetten.

Zoals in paragraaf 6.3.1.6 is opgemerkt wordt het [VERTROUWELIJK] gebruikt als managementnetwerk voor verschillende systemen waaronder het [VERTROUWELIJK]. Deze inrichting heeft tot gevolg dat alle beheerders van de diverse leveranciers van Odido en eigen personeel van Odido die toegang hadden tot het [VERTROUWELIJK] inlogpogingen konden doen op het [VERTROUWELIJK]. Dit in combinatie met het feit dat op het [VERTROUWELIJK] sprake is van niet-persoonsgebonden accounts met standaardwachtwoorden die volgden uit de handleiding van de leverancier [VERTROUWELIJK], zie daarvoor paragraaf 6.3.1.1 en 6.3.1.3, leidt tot de conclusie dat er sprake is van ongeautoriseerde toegang tot LI-gegevens door een zeer grote groep personen. Het voorgaande is ook visueel weergegeven in figuur 2 op pagina 40.

In paragraaf 6.3.1.1 is beschreven via welk logisch toegangspad beheerders toegang konden krijgen tot het [VERTROUWELIJK]. Dit is door vanuit het [VERTROUWELIJK] achtereenvolgens in te loggen op de [VERTROUWELIJK], zie ook figuur 2 op pagina 40. Nu het via deze route mogelijk was om toegang te verkrijgen tot LI-gegevens, zie ik de relevantie van de stelling van Odido dat deze route in de praktijk niet gebruik wordt en dat er altijd gebruikt zou worden gemaakt van de graphical user interface (GUI) om in te loggen op het [VERTROUWELIJK] niet in. Zoals uit het Bbgt volgt moet ongeautoriseerde toegang te allen tijde worden voorkomen. Odido moet ervoor zorgen dat wordt te allen tijde wordt voorkomen dat via deze route ongeautoriseerde personen toegang zouden kunnen krijgen tot LI-gegevens. Dit heeft Odido niet gedaan. Het ligt daarbij op de weg van Odido om deze route definitief te blokkoren als deze nooit werd gebruikt.

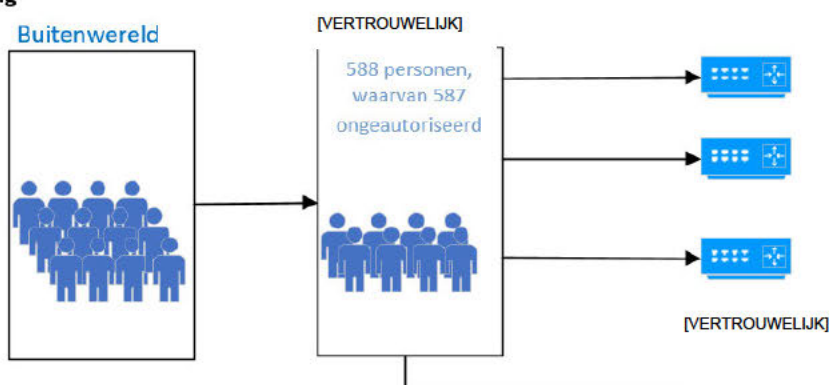
De ongeautoriseerde toegang tot LI-gegevens van circa 587 personen op het [VERTROUWELIJK] was er niet geweest als Odido op het [VERTROUWELIJK] zoneringsmaatregel had toegepast. Zoneringsmaatregel, ook wel aangeduid als netwerksegmentatie, is een beheersmaatregel die ook volgt uit internationale standaarden, waaronder ISO 27001 en ISO 27002.¹⁶⁶ Over ISO 27001 heeft Odido in haar zienswijze aangegeven dat zij hiervoor gecertificeerd is.

Als Odido het [VERTROUWELIJK] door middel van zoneringsmaatregel zodanig had ingericht dat alleen de personen die daadwerkelijk toegang zouden moeten verkrijgen tot het [VERTROUWELIJK], zoals de [VERTROUWELIJK], inlogpogingen konden doen op het [VERTROUWELIJK], dan was het risico op ongeautoriseerde toegang tot LI-gegevens op het [VERTROUWELIJK] vele malen kleiner geweest. Echter zou er in dat geval nog steeds

¹⁶⁶ Zie NEN-EN-ISO/IEC 27001:2017 nl en NEN-EN-ISO/IEC 27001:2017 nl beheersmaatregel 9.4.1.

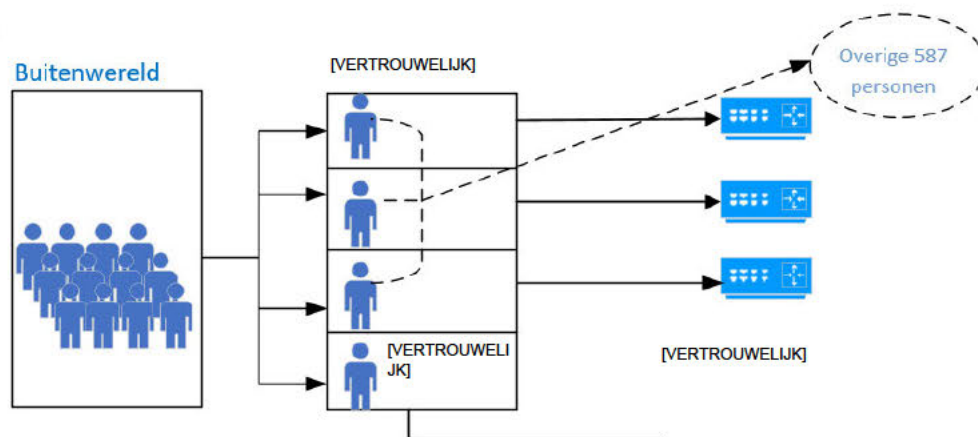
sprake zijn van een overtreding van artikel V, onder a, van de bijlage bij het Bbgt, omdat er geen sprake is van een deugdelijke beveiliging van het [VERTROUWELIJK] vanwege het gebruik van niet-persoonsgebonden accounts met standaard-wachtwoorden. Het voorgaande is ook visueel weergegeven in de schematische overzichten hieronder.

Zonder zonering



Figuur 3. Schematisch overzicht [VERTROUWELIJK] zonder zonering

Met zonering



Figuur 4. Schematisch overzicht [VERTROUWELIJK] met zonering

Omgekeerd zou gelden dat als Odido op het [VERTROUWELIJK] gebruik zou maken van persoonsgebonden accounts met deugdelijke wachtwoordbeveiliging, er ten aanzien van deze twee aspecten geen sprake meer zou zijn van overtreding van artikel V, onder a, van de bijlage bij het Bbgt, maar ook niet van artikel II, onder c, van de bijlage bij het Bbgt.

Gelet op het voorgaande zijn beide gedragingen gelegen in hetzelfde feitencomplex, namelijk de ondeugdelijke beveiliging van het logische toegangspad tot LI-gegevens op het [VERTROUWELIJK] van Odido. Vanwege deze samenloop heb ik in hoofdstuk 6 van dit besluit, in tegenstelling tot het voornemen, het feit dat circa 587 ongeautoriseerde personen toegang hadden tot het [VERTROUWELIJK] en vanuit daaruit inlogpogingen konden doen op het [VERTROUWELIJK] onder hoofdovertreding 3, van de logische toegangscontrole, geschaard.

Voor iedere hoofdovertreding heb ik ervoor heb gekozen om een basisbedrag van € 450.000,- te hanteren, zie paragraaf 11.1. Het feitencomplex blijft, ongeacht de zienswijze van Odido hetzelfde, zij het dat de feiten ten aanzien van de ongeautoriseerde toegang tot LI-gegevens op het [VERTROUWELIJK] via het [VERTROUWELIJK] niet onder hoofdovertreding 2 aan Odido worden tegengeworpen, maar onder hoofdovertreding 3 meegewogen worden in de aard en de ernst van de overtreding. Gezien het feit dat uit het voorgaande blijkt dat Odido door middel van zonering (zoals dat voortvloeit uit internationale standaarden) had kunnen voorkomen dat deze overtreding zou bestaan naast de overtredingen met betrekking tot de persoonsgebonden accounts met standaardwachtwoorden, meen ik dat dit geen gevolgen moet hebben voor de boetehoogte. Dat laat onverlet dat het aantal overtredingen gelijk blijft en de overtreding ten aanzien van de beveiligingseisen van personeel niet in zijn geheel wegvalt. Immers heb ik ervoor gekozen om meerdere overtredingen, zoals vastgesteld in paragraaf 6.2.1 over de geautoriseerde toegang en de ongeautoriseerde toegang tot de LI-Firewall uit paragraaf 6.2.2, te scharen onder een hoofdovertreding van artikel II van de bijlage bij het Bbgt. Daarbij geldt bovendien dat de verwijten niet worden ingetrokken, maar worden verplaatst. Het basisboetebedrag van € 450.000,- voor de hoofdovertreding 2 verandert daarom niet.

10.4 Overtreding 3. Toegangsbeveiliging

10.4.1 Zienswijze Odido boetehoogte

Odido voert, kort en zakelijk weergegeven, in haar zienswijze aan dat zij ervan bewust is dat haar toegangsbeveiliging tot LI-gegevens in 2021 aan verbetering en vernieuwing toe was. Inmiddels is deze vernieuwing, en daarmee ook verbetering, doorgevoerd. Hiermee is de beveiliging naar een hoger niveau gebracht. Odido betwist daarom de opportuniteit van de boete en de evenredigheid van de voorgenomen boetehoogte. Odido is van oordeel dat het geven van een aanwijzing of waarschuwing passender en meer proportioneel zou zijn geweest.¹⁶⁷

Ook voert Odido aan dat ik niet stel dat de gesignaleerde risico's tot gevolgen of geëffectueerde risico's hebben geleid. In lijn met eerdere boetebesluiten van de RDI is dit volgens Odido grond om de boete te verlagen, in plaats van te verhogen.¹⁶⁸ Odido verwijst daarbij naar de beslissing op bezwaar dat is ingesteld tegen een aan Odido opgelegde boete in het kader van een overtreding van artikel 11.5 van de Tw.

Voorts richt Odido haar zienswijze op de twee door mij toegepaste verhogingen van het boetebasisbedrag. Hiertoe voert Odido allereerst aan, kort en zakelijk weergegeven, dat ik uitsluitend een theoretische mogelijkheid tot ongeautoriseerde toegang tot LI-gegevens constateer. Ik heb niet vastgesteld dat daadwerkelijk sprake is geweest van ongeautoriseerde toegang. Dit zou volgens Odido normaliter aanleiding zijn voor een matiging van de basisboete. Dat ik naar aanleiding hiervan, nu een verhoging toepas op het basisboetebedrag, is volgens Odido onterecht en disproportioneel.¹⁶⁹

¹⁶⁷ Randnummer 131-132.

¹⁶⁸ Randnummer 133.

¹⁶⁹ Randnummer 134.

Ten tweede richt Odido haar zienswijze op de door mij toegepaste verhoging naar aanleiding van het door Odido bewust onversleuteld implementeren van de X1-, X2- en X3-verbindingen. Odido betwist, kort en zakelijk weergegeven, dat de omstandigheden geen verhoging van de boete rechtvaardigen. Zij voert daartoe aan dat in werkelijkheid niemand zonder autorisatie toegang had tot de betreffende kabels. Deze infrastructuur is niet publiek toegankelijk en toegang tot de bekabeling werd beperkt door beveiligingsmaatregelen op de betreffende locaties, waaronder (maar niet beperkt tot) fysieke toegangscontrole en cameratoezicht. Ook zou volgens Odido een indringer in de praktijk geen aanknopingspunten hebben om te bepalen welke kabel getapt zou moeten worden. Het door mij geschetste scenario zou volgens Odido daarom puur hypothetisch zijn. Daarbij zou ik hebben nagelaten om het geheel van getroffen maatregelen in samenhang te beschouwen en een verhoging te hebben toegepast zonder het totale beveiligingsbeeld in ogenschouw te nemen.¹⁷⁰ Odido is van mening dat de boetehoogte van € 675.000,- voor overtreding 3 onevenredig is.¹⁷¹

Tijdens de zienswijzezitting heeft Odido in aanvulling op het voorgaande, aangegeven dat het niet duidelijk is wat de status van het document uit 2012 is waarin 'Not Applicable' staat en welke opvolging daaraan is gegeven door Deutsche Telecom. Daarnaast stelt Odido dat ^[VERTROUWELIJK]

Tenslotte

geeft Odido aan dat de tekortkomingen van beveiligingsmaatregelen niet in zijn geheel zijn bekeken, waardoor er onvoldoende aandacht is voor contractuele geheimhoudingsverklaringen met ^[VERTROUWELIJK] en het niet eenvoudig was om fysieke toegang te verkrijgen tot onversleutelde X1-, X2- en X3 verbindingen. Volgens Odido zou hieruit volgen dat als een maatregel tekortschiet er niet gelijk een hoog risico is op een beveiligingsinbreuk.

10.4.2 Mijn reactie

Ik volg Odido niet in het standpunt dat boeteoplegging niet opportuun is. Daartoe overweeg ik het volgende. Op basis van artikel 15.4, eerste lid, van de Tw ben ik bevoegd om voor iedere overtreding van de Tw en het Bbgt handhavend op te treden door middel van een bestuurlijke boete van maximaal € 900.000,-.

a. Verandering van de feitelijke situatie

Ik heb geconstateerd dat Odido, als professionele marktpartij en als een van de grootste mobile operators van Nederland, de eisen die het Bbgt aan haar stelt heeft geschonden. Dit blijkt uit het feit dat zij geen beveiligingsplan in de zin van het Bbgt had, de op grond van het Bbgt vereiste maatregelen jegens haar personeel niet heeft getroffen en de toegangsbeveiliging van haar geautomatiseerde systemen waarin LI-gegevens worden verwerkt volstrekt niet op orde had. Dit zijn structurele en zeer ernstige overtredingen, die bovendien langere tijd hebben geduurd. Ik ben daarom van oordeel dat ik in redelijkheid gebruik kan maken van mijn bevoegdheid om een boete op te leggen aan Odido.¹⁷² Ook als Odido de geconstateerde overtredingen heeft beëindigd – nog

¹⁷⁰ Randnummer 135-137.

¹⁷¹ Randnummer 138-139.

¹⁷² Rb. Rotterdam, 12 juli 2024, ECLI:NL:RBROT:2024:6458, r.o. 39.

los van de vraag of dit voor alle overtredingen daadwerkelijk het geval is- ben ik bevoegd om over te gaan tot bestraffende bestuursrechtelijke handhaving. Dat Odido eerst na afloop van de periode van overtredingen maatregelen heeft genomen om de overtreding te beëindigen, doet niet af aan mijn bevoegdheid om – mede in het licht van de ernst en de verwijtbaarheid – voor de geconstateerde overtredingen een boete op te leggen.

Gelet op voorgaande staat een veranderde feitelijke situatie ten aanzien van het [VERTROUWELIJK] van Odido dus niet in de weg aan bestuursrechtelijke bestraffende handhaving voor eerder geconstateerde overtredingen. Dat Odido stelt dat de overtredingen inmiddels zijn beëindigd, is dus, nog los van de vraag of deze stelling juist is, niet bepalend voor het oordeel dat boeteoplegging opportuun is. De zienswijze van Odido op dit punt treft dus geen doel.

b. Effecturen van risico's

In reactie op de zienswijze van Odido dat niet is vastgesteld dat de gesignaleerde risico's geëffectueerd zijn en dat dit een grond zou zijn voor boetematiging, overweeg ik als volgt. Ik heb vastgesteld dat Odido op meerdere punten het Bbgt heeft overtreden. De combinatie van deze overtredingen maakt dat het niet controleerbaar is of risico's geëffectueerd zijn, vanwege de afwezigheid van logging en detectiemaat-regelen.¹⁷³ Of er sprake is geweest van ongeautoriseerde toegang, kan ik dus niet vaststellen (en Odido zelf ook niet). Dit is echter geen grond voor boetematiging, zoals Odido betoogt.

Odido had op grond van het Bbgt toereikende maatregelen moeten nemen om te voorkomen dat ongeautoriseerde toegang kon plaatsvinden. Ik heb vastgesteld dat deze maatregelen ontbraken. Zo beschikte Odido niet over een beveiligingsplan, zijn er tekortkomingen vastgesteld ten aanzien van het personeel dat al dan niet toegang tot LI-gegevens mag hebben en ernstige tekortkomingen in de logische beveiliging van de systemen waarin LI-gegevens worden verwerkt. Bovendien heb ik vastgesteld dat deze overtredingen lange tijd hebben geduurd en structureel van aard waren.

Dat niet meer kan worden vastgesteld of de risico's op ongeautoriseerde toegang hebben plaats gevonden vanwege de afwezigheid van logging en detectiemaat-regelen, acht ik dan ook geen grond voor boetematiging.

Integendeel, dit is een zeer ernstig gevolg van het niet voldoen aan het Bbgt. Immers is een van de doelen van het Bbgt om LI-gegevens tegen ongeautoriseerde toegang te beschermen en tijdig in te kunnen grijpen wanneer er onverhoopt toch ongeautoriseerde toegang plaats heeft gevonden. Dat maatregelen om ongeautoriseerde toegang tijdig op te kunnen merken en tijdig in te kunnen grijpen ontbraken, vormt daarmee een zeer ernstige inbreuk op de vertrouwelijkheid van de LI-gegevens waar Odido verantwoordelijk voor is. Van Odido mag verwacht worden dat zij op zijn minst de basis op orde heeft en zorgdraagt voor een toereikende beveiliging van LI-gegevens. Odido is immers een van de drie grote mobiele operators in Nederland en het werken met telecomgegevens raakt haar kernactiviteiten. De mogelijke impact van de vastgestelde overtredingen is daarmee van enorme omvang. Ik volg Odido dus

¹⁷³ Zoals beschreven in paragraaf 6.3.

niet in het standpunt dat de door haar aangedragen omstandigheden aanleiding geven tot een matiging van het basisboetebedrag.

Rijksinspectie Digitale
Infrastructuur

Daarbij merk ik subsidiair op dat de zaak waarnaar Odido verwijst een andere overtreding betrof, namelijk een overtreding van artikel 11.5 van de Tw. Deze norm beschermt andere belangen dan de belangen die het Bbgt beoogt te beschermen. De risico's die zich voordoen bij een overtreding van deze norm zijn dan ook niet vergelijkbaar met de risico's die zich voordoen bij een overtreding van het Bbgt. Een ander belangrijk verschil, waardoor de vergelijking die Odido maakt ten aanzien van verzachtende omstandigheden niet opgaat, is dat in de zaak waarnaar Odido verwijst in de zienswijze, ik heb kunnen *vaststellen* dat de risico's zich niet geëffectueerd hebben. Dit, in tegenstelling tot de onderhavige zaak, waar ik juist vanwege de aard van de overtredingen *niet* heb kunnen vaststellen of de risico's zich geëffectueerd hebben, zoals ik hierboven uiteen heb gezet. De zienswijze van Odido op dit punt treft dus geen doel.

Ons kenmerk
[VERTROUWEL
11/17]

Het doel van het Bbgt is om een minimumniveau van beveiliging te behalen, ter bescherming van ongeautoriseerde toegang van LI-gegevens en daarmee ook de bescherming van zwaarwegende publieke belangen. Aanbieders als Odido moeten daarom maatregelen treffen om ongeautoriseerde toegang te voorkomen. Met andere woorden, Odido moet 'in control' zijn over toegangsmogelijkheden tot LI-gegevens en dient de LI-gegevens op adequate wijze te beveiligen. Het standpunt van Odido dat de beveiliging op orde is, als er een ongeautoriseerde toegangsmogelijkheid is, maar van deze mogelijkheid geen gebruik van is gemaakt, is daarom uiterst zorgwekkend. Bovendien merk ik nogmaals op, zoals eerder ook uiteengezet, dat het vanwege gebrek aan detectiemaatregelen niet vast te stellen is of er gebruik is gemaakt van ongeautoriseerde toegangsmogelijkheden. De zienswijze van Odido op dit punt treft daarom geen doel.

c. Verhoging vanwege onversleutelde verbindingen

Odido betwist dat de door mij geschetste omstandigheden een verhoging van de basisboete voor overtreding 3 rechtvaardigen. Daartoe voert Odido aan dat in werkelijkheid niemand toegang had tot deze infrastructuur, omdat dit geen publiek toegankelijke infrastructuur betreft en dat toegang werd beperkt door beveiligingsmaatregelen op de betreffende locaties. Het door mij geschetste scenario zou daarom puur hypothetisch zijn. Volgens Odido zou een eventuele indringer geen aanknopingspunten hebben om te bepalen welke kabel getapt zou moeten worden.

Ik volg Odido niet in haar zienswijze. Uit het onderzoek van de toezichthouder is gebleken dat Odido bij de implementatie van het ^[VERTROUWELIJK] de X1-, X2- en X3-verbindingen bewust onversleuteld heeft laten implementeren, zoals beschreven is in paragraaf 6.3. Het is algemeen bekend dat informatiestromen versleuteld dienen te zijn.¹⁷⁴ Dat geldt voor iedere informatiestroom, en zeker voor informatiestromen die staatsgeheime informatie bevatten. Dat Odido er bewust voor heeft gekozen deze dataverbindingen onversleuteld te implementeren, levert reeds daarom een verhoogde verwijtbaarheid op. Hierdoor acht ik een verhoging van het basisboetebedrag passend en geboden.

¹⁷⁴ Zie bijvoorbeeld de ICT-Beveiligingsrichtlijnen Webapplicaties van het Nationaal Cybersecurity Center uit 2012 en 2015, beveiligingsmaatregel U/WA.05.

Subsidiar merk ik het volgende op in reactie op de zienswijze van Odido. Het klopt inderdaad dat de datacenters van Odido niet publiek toegankelijk zijn. Echter vermindert dat de door mij geconstateerde risico's ten aanzien van onversleutelde X1-, X2- en X3-verbindingen niet. De datacenters van Odido staan op verschillende plekken in Nederland. Tussen deze datacenters lopen de X1-, X2- en X3-verbindingen, waarover onversleutelde LI-gegevens verzonden worden. Anders dan Odido suggereert in haar zienswijze, kan er op iedere plaats data getapt worden uit deze kabels, ook buiten de datacenters. Ik acht de zienswijze van Odido dat de toegang tot deze kabels beschermd wordt door middel van cameratoezicht en fysieke toegangscontrole niet overtuigend. [VERTROUWELIJK]

Aangaande de stelling van Odido dat een eventuele indringer in de praktijk geen aanknopingspunten zou hebben om te bepalen welke kabel getapt zou moeten worden, overweeg ik het volgende. Ik volg Odido niet in deze zienswijze. De hiervoor benodigde informatie is deels openbaar toegankelijke informatie, die via het Kadaster te raadplegen is. Daarbij wordt ook aangegeven wie de netbeheerder van de betreffende kabel is. Dat vormt dus een concreet eerste aanknopingspunt, waarna met enige zoektocht de betreffende kabels te achterhalen zijn. Hierbij merk ik op dat het Bbgt niet bedoeld is om bescherming te bieden aan een willekeurige gelegenheidsovertreder, maar is opgesteld met het oog op statelijke actoren en kwaadwillenden, met bijbehorende kennis en middelen. Meer subsidiar overweeg ik dat er naast fysieke aanvallen op de netwerkkabels ook andere mogelijkheden zijn om tot de onversleutelde LI-gegevens te komen.

In reactie op de zienswijze van Odido dat het onduidelijk is welke opvolging er is gegeven aan de status 'Not Applicable', overweeg ik het volgende. Deze zienswijze ziet op bijlage 14 van het document [VERTROUWELIJK] SoC, genaamd Platform Specific Lawful Interception Requirements.¹⁷⁵ Zoals ik uiteen heb gezet in paragraaf 6.1.3.4, betreft dit document een 1.0 versie en heeft dit document als datum 17/12/2012. Dat is dezelfde datum als de datum waarop Odido het [VERTROUWELIJK] in gebruik heeft genomen. Daarnaast is door mijn toezichthouder vastgesteld dat ten tijde van het onderzoek de X1-, X2- en X3-verbindingen tussen het [VERTROUWELIJK] en het [VERTROUWELIJK] onversleuteld waren. Odido lijkt met haar zienswijze te suggereren dat deze verbindingen eerder wel versleuteld zouden kunnen zijn geweest. Odido heeft hiervoor geen enkele nadere onderbouwing of documentatie aangeleverd. Ik volg daarom de vaststelling van de toezichthouder dat dit de voorwaarden zijn waaronder het [VERTROUWELIJK] bij Odido is geïmplementeerd.

Odido noemt daarbij ook dat niet bekend is door welke andere beveiligingsmaatregelen dit punt geadresseerd is. Het versleutelen van data is de meest voor de hand liggende wijze om de gesignaleerde risico's te mitigeren. Odido heeft dit nagelaten en er bewust voor gekozen om deze dataverbindingen onversleuteld te installeren. De door Odido aangedragen zienswijze leidt daarom niet tot een ander oordeel dan dat een verhoging van 25% van het basisboetebedrag ten aanzien van overtreding 3 passend en geboden is.

¹⁷⁵ [VERTROUWELIJK]

11 Boetehoogte

11.1 Vaststelling boetehoogte

Voor het bepalen van de boetehoogte geldt op grond van artikel 15.4 van de Tw een maximumbedrag per overtreding van € 900.000,-. De door mijn toezichthouder geconstateerde overtredingen hebben plaatsgevonden voordat mijn huidige boetebeleid in werking is getreden. Uit het overgangsregime uit mijn boetebeleid blijkt dat dat beleid niet van toepassing is op overtredingen die zijn begaan voor de inwerkingtreding daarvan. Daarvan is hier sprake. In een casus als de onderhavige kom ik daarom op basis van een afweging van alle relevante omstandigheden, feiten en vergelijkbare sanctiezaken tot een oordeel.

Hiervoor heb ik reeds toegelicht dat ik de verschillende overtredingen als zeer ernstig en verwijtbaar 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 Odido deze heeft geschonden. Voor dergelijke overtredingen hanteer ik als uitgangspunt een basisbedrag van € 450.000,- per overtreding.¹⁷⁶ In dit bedrag ligt een gemiddelde ernst, duur en mate van verwijtbaarheid van een overtreding van het Bbgt de besloten. Dit uitgangspunt sluit overigens ook aan bij het basisbedrag dat op grond van mijn boetebeleid wordt gehanteerd bij overtredingen zoals hier aan de orde.

Mijn toezichthouder heeft vastgesteld dat Odido negen normen uit het Bbgt en de bijlage heeft overtreden. Dit betreffen overtredingen van de minimumvereisten uit het Bbgt, die uiteindelijk door mij zijn gegroepeerd in drie hoofdovertredingen. Ik besluit daarom om aan Odido voor ieder van de drie hoofdovertredingen een bestuurlijke boete op te leggen. Per hoofdovertreding zal ik hierna toelichten welke boetehoogte ik passend vind.

11.1.1 Overtreding 1. Beveiligingsplan

Vastgesteld is dat Odido in het geheel niet beschikte over een beveiligingsplan. Dit acht ik zeer ernstig, zoals ik heb overwogen in paragraaf 8.2. Het beveiligingsplan vormt immers het startpunt van een deugdelijke beveiliging van LI-gegevens. Gelet op het feit dat een beveiligingsplan bij Odido in het geheel ontbrak, besluit ik om het basisboetebedrag van € 450.000,- met 25% te verhogen en aan Odido voor deze overtreding een bestuurlijke boete op te leggen van € 562.500,-.

¹⁷⁶ Zie ook <https://www.rdi.nl/actueel/nieuws/2022/08/30/tekortkomingen-in-beveiliging-van-aftapvoorziening-kpn> en <https://www.rdi.nl/documenten/bsluiten/2024/10/22/boetebesluit-vodafone-onvoldoende-beveiligd-aftapsysteem>

11.1.2 Overtreding 2. Beveiligingseisen ten aanzien van personeel

Vastgesteld is dat de beveiligingseisen van Odido ten aanzien van het personeel onvoldoende waren gedurende in ieder geval de periode van 5 oktober 2021 tot en met 14 september 2022. Odido heeft er onvoldoende voor gezorgd dat personen die belast zijn met de verwerking van, medewerking verlenen aan, dan wel in aanraking kunnen komen met LI-gegevens zeer zorgvuldig met deze informatie omgaan en geheimhouding betrachten met betrekking tot de LI-gegevens. Als gevolg van de vastgestelde tekortkomingen heeft Odido gedurende een lange periode een ernstig risico gelopen op onbevoegde toegang of een schending van de strikt vereiste geheimhouding. Ik besluit daarom om aan Odido voor deze overtreding een bestuurlijke boete op te leggen van € 450.000,-. Daarbij zijn er geen redenen om een verhoogde of verlaagde ernst dan wel verwijtbaarheid aan te nemen.

11.1.3 Overtreding 3. Toegang geautomatiseerde systemen

Vastgesteld is dat de toegangsbeveiliging van geautomatiseerde informatie-systemen waarin LI-gegevens worden verwerkt onvoldoende was gedurende de periode van in ieder geval 17 december 2012 tot 7 februari 2022. Ook hiervoor hanteert ik een basisboetebedrag van € 450.000,-.

Ik besluit om het basisboetebedrag van € 450.000,- met 25% te verhogen vanwege de ernst van de overtredingen. Voor een lange periode van ruim negen jaar bestond een zeer groot risico op ongeautoriseerde (leveranciers)toegang tot LI-gegevens, nu een groot aantal ongeautoriseerde personen, waaronder medewerkers van [VERTROUWELIJK], toegang hadden tot het [VERTROUWELIJK] van Odido en dat door medewerkers van [VERTROUWELIJK] van deze toegangsmogelijkheid ook daadwerkelijk gebruik is gemaakt. Dit, gezien in combinatie met het feit dat er vanaf het [VERTROUWELIJK] inlogpogingen gedaan konden worden op het [VERTROUWELIJK], en dat er op het [VERTROUWELIJK] ingelogd kon worden met de standaardwachtwoorden van [VERTROUWELIJK], welke al in gebruik waren sinds de implementatie van het [VERTROUWELIJK] door [VERTROUWELIJK] en er op dit systeem bewust onversleutelde taplijsten aanwezig waren, maakt de kans op ongeautoriseerde (leveranciers)toegang zeer groot en de overtreding daarmee zeer ernstig.

Verder besluit ik dit basisboetebedrag van € 450.000,- nogmaals met 25% te verhogen vanwege de verhoogde verwijtbaarheid. Ik reken het Odido zwaar aan dat zij weloverwogen de X1-, X2- en X3-verbindingen onversleuteld heeft laten implementeren ten tijde van de implementatie van het [VERTROUWELIJK] op 17 december 2012 en daarna gedurende een periode van ruim negen jaar heeft verzuimd deze verbindingen adequaat te beveiligen door middel van versleuteling.

Ik besluit daarom om aan Odido voor deze overtreding een bestuurlijke boete op te leggen van € 675.000,-.

11.2 Matiging boete vanwege duur onderzoek

Uit het bovenstaande volgt dat ik besluit aan Odido een bestuurlijke boete op te leggen voor een bedrag van in totaal € 1.687.500,-. Gelet op de lange duur van

het onderzoek van mijn toezichthouder, van 5 oktober 2021, de start van onderzoek, tot 4 februari 2025, het moment waarop het Rvb is vastgesteld, besluit ik om de bestuurlijke boete te matigen. Ik besluit om dit bedrag met 10% te matigen en Odido een bestuurlijk boete op te leggen voor een bedrag van in totaal van € 1.518.750,-.

11.3 Totale cumulatieve boete

Gelet op het voorgaande besluit ik om aan Odido daarom in totaal een bestuurlijke boete voor een bedrag van in totaal van € 1.518.750,- voor de vastgestelde overtredingen op te leggen.

12 Publicatie

12.1 Inleiding

Op grond van artikel 3.1 van de Woo ben ik bevoegd om 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 dit boetebesluit.

Daarbij geldt dat ik een standaardpraktijk hanteer waarbij bestuurlijke boetes op grond van het Bbgt na het nemen daarvan gepubliceerd worden.¹⁷⁷ Ik zal daarom in beginsel uitsluitend in bijzondere, individuele omstandigheden aanleiding zien om geheel van publicatie van de bestuurlijke boete af te zien.¹⁷⁸ In de hiernavolgende paragraaf zal ik beoordelen of voornoemde omstandigheden aanwezig zijn, en indien deze omstandigheden aanwezig zijn, of deze omstandigheden zwaarder wegen dan de belangen die met publicatie zijn gediend.

12.2 Belangen die met publicatie zijn gediend

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

In de eerste plaats is het belang van beveiliging van gegevens een actueel thema dat de maatschappij bezighoudt. Dat geldt temeer als het gaat om de beveiliging van gegevens door een aanbieder die deel uitmaakt van de vitale infrastructuur en die zeer veel gevoelige gegevens verwerkt. Als een dergelijke aanbieder niet de minimale, voorgeschreven maatregelen treft, is er een groot maatschappelijk belang dat die constatering op zo kort mogelijke termijn publiekelijk kenbaar wordt gemaakt.

In de tweede plaats hebben burgers en overheidsdiensten (waaronder de bevoegde autoriteiten als bedoeld in artikel 1, onder c, van het Bbgt) er belang bij

¹⁷⁷ Vgl. <https://www.rdi.nl/documenten/besluiten/2022/08/30/boetebesluit-bdh-832070> en <https://www.rdi.nl/documenten/besluiten/2024/09/27/beschikking-boete-vodafone>.

¹⁷⁸ Zie o.a. Vزر. Rb. Rotterdam 15 juni 2023, ECLI:NL:RBROT:2023:5209; CbB 12 oktober 2017, ECLI:NL:CBB:2017:327.

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 die betrekking hebben op onderzoeken naar de beveiliging van LI-gegevens te publiceren.

In de derde plaats gaat van openbaarmaking in het kader van generale preventie een waarschuwend effect van de openbaarmaking naar andere marktpartijen uit 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 van de 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.

Ten vierde dient publicatie ook het belang van generale preventie naar marktpartijen die onderdeel zijn van de vitale infrastructuur en te maken hebben met soortgelijke normen, zoals essentiële dienstverleners die vallen onder de Wet beveiliging netwerk- en informatiesystemen. Publicatie van het boetebesluit bewerkstelligt dat andere marktpartijen hun naleving van het Bbgt of naleving van vergelijkbare normen kritisch tegen het licht houden en blijven houden.

In dat verband merk ik op dat cyberveiligheid een doel is dat continu aandacht vraagt van een vitale dienstverlener. Immers is het van groot belang dat de aanbieder continue op de hoogte is van dreigingen en daarop passend anticipeert. Cyberveiligheid is een zeer belangrijk en relevant maatschappelijk thema. Verstoringen en incidenten leiden tot maatschappelijke onrust. Daarom acht ik het van groot belang dat het voor de maatschappij kenbaar is dat ik de normen die bijdragen aan cyberveiligheid handhaaf en dat de overheid optreedt tegen aanbieders die zich onvoldoende inspannen om Nederland cyberveilig te houden. Ook hierom acht ik het van groot belang om het boetebesluit openbaar te maken. Deze belangen zijn het meest gediend bij een zo ruim mogelijk openbaarmaking. Daarom is het uitgangspunt om in beginsel boetebesluiten te publiceren, ook als zij betrekking hebben op onderzoeken naar de beveiliging van LI-gegevens.

Daarbij houd ik rekening met de belangen van zowel de Staat als van Odido om staatsgeheime en bedrijfsvertrouwelijke informatie over de LI-systemen van Odido niet openbaar te maken, waarvoor de uitzonderingsgronden in artikel 5.1 van de Woo als kader gelden.

12.3 Zienswijze Odido

In de zienswijze gaat Odido in op het publicatievoornemen. Odido betoogt dat indien een besluit tot oplegging van een bestuurlijke boete niet op goede gronden is opgelegd, volgens vaste jurisprudentie reeds om die reden een aanleiding tot schorsing van de beslissing tot openbaarmaking daarvan bestaat. Odido draagt aan dat de boetes voor overtreding 1 en overtreding 2 geen stand kunnen houden

en dat de boete voor overtreding 3 onevenredig hoog is.¹⁷⁹ Odido betoogt daarom dat, nu het voorgenomen besluit in belangrijke mate geen stand kan houden, het nieuwsbericht niet, of in ieder geval niet in de vorm zoals dit aan Odido medegedeeld is, kan worden gepubliceerd.¹⁸⁰

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
11171

Odido verzoekt, mocht ik toch besluiten tot publicatie van het nieuwsbericht, in elk geval rekening te houden met het volgende. Volgens Odido blijkt uit het concept nieuwsbericht onvoldoende dat de boete is opgelegd naar aanleiding van onderzoek dat bijna vier jaar geleden is gestart en is afgerond in september 2022. Odido verwacht dat een toezichthouder transparant communiceert over de tijdslijn van een handhavingstraject. Het nalaten van een duidelijke tijdsaanduiding zou Odido onevenredig schaden, aangezien daardoor ten onrechte de indruk kan ontstaan dat de geconstateerde situatie actueler is dan in werkelijkheid het geval is.¹⁸¹

12.4 Mijn reactie

In reactie op de zienswijze van Odido op mijn voornemen een publieksversie van het boetebesluit te publiceren, overweeg ik als volgt. In hoofdstuk 10 van dit besluit ben ik ingegaan op de zienswijze van Odido ten aanzien van de door haar gegeven zienswijze op de opportuniteit van boeteoplegging, de inhoudelijke zienswijze op overtreding 1, 2 en 3 en de hoogte van de boete. Waar nodig heb ik de motivering van de overtredingen uitgebreid of aangevuld. Concluderend geeft de zienswijze van Odido geen aanleiding om af te wijken van mijn voornemen. Ik ben daarom van oordeel dat de bestuurlijke boete op goede gronden opgelegd wordt en dat de hoogte van de bestuurlijke boete passend en geboden is. Ik volg daarom Odido niet in haar zienswijze dat er aanleiding bestaat om van publicatie af te zien.

Voor het overige zie ik naar aanleiding van de door Odido gegeven zienswijze geen reden om van mijn standaardpraktijk af te wijken ten aanzien van de publicatie van het boetebesluit.

Anders dan Odido ben ik van oordeel dat niet duidelijk is of alle overtredingen inmiddels zijn beëindigd. Hierbij gaat dan specifiek om een aantal overtredingen die zijn vastgesteld onder hoofdovertreding 2. Het is voor mij niet duidelijk dat de drie LI-medewerkers van Odido en de vijf medewerkers van ^[VERTROUWELIJK] inmiddels wel over een functieomschrijving in de zin van het Bbgt en een geheimhoudingsverklaring in de zin van het Bbgt beschikken. Ook bij haar zienswijze heeft Odido geen stukken overgelegd waaruit blijkt dat deze overtredingen inmiddels zijn beëindigd, zie daarvoor ook paragraaf 6.2.1. Gelet op het voorgaande is in het nieuwsbericht niet aangegeven dat de overtredingen zijn beëindigd. In het nieuwsbericht is wel aangegeven dat de feitelijke situatie is veranderd waardoor de risico's op ongeoorloofde toegang zijn weggenomen. ^[VERTROUWELIJK]

Daarmee meen ik dat ik in het nieuwsbericht voldoende recht heb gedaan aan de feitelijke situatie en de belangen van Odido.

¹⁷⁹ Randnummer 141 en 142.

¹⁸⁰ Randnummer 143 en 147.

¹⁸¹ Randnummer 144.

In reactie op de zienswijze dat het concept nieuwsbericht onvoldoende transparant is over de tijdlijn van het handhavingstraject en de duur van de overtredingen en dat dit Odido onevenredig zou schaden, overweeg ik het volgende.

Tijdens de zienswijzezitting is aangegeven dat ik ervoor opensta om de opbouw van de boete uiteen te zetten in het nieuwsbericht. Ik volg Odido daarom in zoverre in haar zienswijze dat ik het nieuwsbericht zal aanpassen en daarin zal communiceren over de opbouw van de boete waarbij ik ook zal aangeven dat de boete is gematigd vanwege de lange duur van het onderzoek.

Met inachtneming van het bovenstaande besluit ik daarom om een publieksversie van dit besluit conform de door mij gehanteerde standaardpraktijk openbaar te maken en een nieuwsbericht op mijn website te plaatsen.¹⁸² Hieronder licht ik toe op welke wijze ik het boetebesluit openbaar maak.

12.5 Publicatie publieksversie boetebesluit op de website van RDI

Ik besluit om op grond van artikel 3.1 van de Woo een publieksversie van het boetebesluit openbaar te maken op de website van de RDI (www.rdi.nl).

Hierbij zal rekening worden gehouden met de uitzonderingsgronden van artikel 5.1 van de Woo door bepaalde passages niet openbaar te maken. Het betreft passages uit het boetebesluit die inzicht kunnen geven in de LI-infrastructuur van Odido. Kennis van deze infrastructuur bij derden kan de staatsveiligheid schaden.

Dit geldt ook voor beschrijvingen van LI-processen bij Odido en namen van medewerkers. Deze gegevens dienen op grond van artikel 5.1, eerste lid, onder b, c, tweede lid, onder c, e, f, h en het vijfde lid van de Woo te worden weggelakt. Deze passages zullen daarom door mij uit het boetebesluit worden weggelakt en zullen niet openbaar worden gemaakt. De publieksversie van het boetebesluit is als bijlage 4 aan dit besluit gehecht.

12.6 Nieuwsbericht en social media

Ik zal het boetebesluit samen met een nieuwsbericht publiceren. In dit nieuwsbericht zijn de hoofdlijnen van het onderhavige besluit weergegeven. In bijlage 3 treft u een afschrift aan van nieuwsbericht aan. Het nieuwsbericht zal eveneens op de website van de RDI worden geplaatst. Daarnaast zal ik op hetzelfde moment een bericht via LinkedIn te delen. Het bericht op LinkedIn zal bestaan uit de kop van het nieuwsbericht en een link naar het nieuwsbericht op de website van de RDI.

13 Besluit tot oplegging bestuurlijke boete en publicatie

13.1 Bestuurlijke boete

Gezien het voorgaande leg ik aan Odido een bestuurlijke boete van € 1.518.750,- op.

¹⁸² Vgl. Rb. Rotterdam 21 oktober 2024, ECLI:NL:RBROT:2024:10347, r.o. 10. en 29.

13.1.1 *Betalingswijze*

Voor de betaling van de bestuurlijke boete dient Odido gebruik te maken van de factuur die door het Centraal Justitieel Incassobureau (CJIB) wordt toegezonden. Deze factuur wordt aan Odido toegezonden zodra onderhavig besluit formele rechtskracht heeft gekregen.¹⁸³

Rijksinspectie Digitale
Infrastructuur

Ons kenmerk
[VERTROUWEL
11171

13.2 *Publicatie*

13.2.1 *Publicatie publieksversie boetebesluit 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, eerste lid, onder b, c, tweede lid, onder c, e, f, h en het vijfde lid van de Woo. Publicatie van deze publieksversie vindt plaats op **17 oktober 2025** op de website van de RDI.

13.2.2 *Nieuwsbericht en social media*

Ik zal over het onderhavige besluit samen met een nieuwsbericht publiceren. In dit nieuwsbericht zijn de hoofdlijnen van het onderhavige besluit weergegeven. In bijlage 3 treft u een afschrift aan van het nieuwsbericht. Het nieuwsbericht wordt eveneens op **17 oktober 2025** 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 nieuwsbericht en een link naar het nieuwsbericht op de website van de RDI.

14 **Bezwaarclausule**

Tegen dit besluit kan iedere belanghebbende binnen zes weken na de dag van bekendmaking (pro forma) bezwaar maken. U kunt een ondertekend bezwaarschrift per post 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.

¹⁸³ Op grond van artikel 15.12 van de Tw in samenhang met het incassobeleid van de Rijksinspectie Digitale Infrastructuur.

Om u de mogelijkheid te geven de publicatie van de publieksversie van het boetebesluit en het nieuwsbericht tegen te houden, krijgt u twee weken de tijd, tot uiterlijk **16 oktober 2025**. Als u de publicatie tegen wil houden, dient u een bezwaarschrift in te dienen en daarnaast de voorzieningenrechter van de sector bestuursrecht van de rechtbank Rotterdam te vragen dit besluit te schorsen. Dit laatste kan zowel per brief als online via <http://loket.rechtspraak.nl/bestuursrecht>. Als u gebruik maakt van deze mogelijkheid, stel ik de publicatie in ieder geval uit tot het moment dat de rechter heeft bepaald dat de publicatie plaats kan vinden.

Hoogachtend,
De minister van Economische Zaken
namens deze,

[VERTROUWELIJK]

mr. F. de Jong – van Kammen
Plv. Coördinerend jurist
Rijksinspectie Digitale Infrastructuur

**Rijksinspectie Digitale
Infrastructuur**

Ons kenmerk
[VERTROUWEL
1121

Bijlage 1. Juridisch kader

Rijksinspectie Digitale
Infrastructuur

Bij de beoordeling van de feiten en omstandigheden van deze zaak zijn de Tw, het Bbgt en de Wet open overheid (hierna: Woo) van toepassing.

Ons kenmerk
[VERTROUWEL
1121

Met name de volgende bepalingen zijn van belang.

Tw

Op grond van artikel 15.1, eerste lid, aanhef en onder h, van de Tw, zijn met het toezicht op de naleving op het bepaalde bij of krachtens deze wet de bij besluit van Onze Minister aangewezen ambtenaren, voor zover het betreft de bepalingen die betrekking hebben op bevoegd aftappen en het bewaren van gegevens als geregeld in hoofdstuk 13.

Artikel 15.4, eerste lid, van de Tw bepaalt dat ik in geval van een overtreding van de bij of krachtens de in artikel 15.1, eerste lid, van de Tw, bedoelde voorschriften, alsmede van artikel 5:20 van de Awb, de overtreder een bestuurlijke boete van ten hoogste € 900.000 per overtreding kan opleggen.

De op grond van artikel 13.5, vierde lid, van de Tw bedoelde regels, met betrekking tot de te nemen maatregelen in verband met de beveiliging en waarborging van de tapgegevens, zijn gesteld in het Bbgt.

Voor de betekenis van het bovengenoemde juridisch kader heb ik acht geslagen op de toelichting die de wetgever bij dit kader heeft gegeven. De wetgever onderstreept het zwaarwegend belang van geheimhouding en bescherming van gegevens en informatie door aanbieders. In de memorie van toelichting bij de Tw is daarover onder meer het volgende opgenomen:

"Gegevens betreffende aftappen en informatieverstrekkings 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."¹⁸⁴

Bbgt

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

¹⁸⁴ Kamerstukken II 1996/97, 25 533, nr. 3, p. 125 (MvT).

2017 tot het aftappen of opnemen van telecommunicatie door een bevoegde autoriteit aan de aanbieder zijn verstrekt;
(...)

**Rijksinspectie Digitale
Infrastructuur**

Ons kenmerk
[VERTROUWEL
1121

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

- 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 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 bijlage bij het Bbgt bevat, onder meer, de volgende maatregelen:

I. Beveiligingseis algemeen

Er is een functionaris, belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen. De functionaris voert daartoe regelmatig controles uit en legt de resultaten daarvan vast.

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.

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.

(...)

Ook de toelichting bij het Bbgt is richtinggevend voor mijn weging van de feiten in deze zaak. Relevant zijn de volgende passages met betrekking tot het belang van vertrouwelijkheid en beveiliging van tapgegevens en -informatie:

"(...) 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 wetslagen 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.”¹⁸⁵

De toelichting bij het Bbgt onderstreept verder 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 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.

Indien door een aanbieder wordt vastgesteld dat een ongeoorloofde inbreuk heeft plaatsgevonden, dan is deze verplicht de desbetreffende bevoegde autoriteit terstond daaromtrent te informeren. Immers, opsporingsonderzoeken of onderzoeken in het kader van de veiligheid van de staat kunnen door het bekend raken van de vertrouwelijke gegevens buiten de kring van personen die tot kennisneming gerechtigd zijn worden gefrustreerd met alle gevolgen van dien. Daarbij dient hij aan te geven welke gegevens of informatie het betreft. Verder dient de aanbieder te vermelden op welke wijze de inbreuk heeft plaatsgevonden en welke maatregelen hij heeft genomen om verdere verspreiding van de bedoelde gegevens of informatie tegen te gaan en herhaling van het gebeurde te voorkomen. Op basis van de aldus verstrekte informatie kan de bevoegde autoriteit de maatregelen nemen die deze aangewezen acht om de gevolgen voor bedoelde onderzoeken tot een minimum te beperken.”¹⁸⁶

Woo

Artikel 3.1, eerste lid, van de Woo bepaalt dat het bestuursorgaan dat het rechtstreeks aangaat, bij de uitvoering van zijn taak uit eigen beweging de bij het bestuursorgaan berustende informatie neergelegd in documenten voor eenieder

¹⁸⁵ NvT bij het Bbgt, Stb. 2003, 472, p. 7.

¹⁸⁶ NvT bij het Bbgt, Stb. 2003, 472, p. 13.

openbaar maakt, indien dit zonder onevenredige inspanning of kosten redelijkerwijs mogelijk is, behoudens voor zover de artikelen 5.1, eerste, tweede en vijfde lid, en 5.2 van de Woo aan openbaarmaking in de weg staan of met de openbaarmaking geen redelijk belang wordt gediend. Deze informatie betreft in ieder geval informatie over het beleid, inclusief de voorbereiding, uitvoering, naleving, handhaving en evaluatie.

Artikel 3.1, tweede lid, van de Woo bepaalt dat het bestuursorgaan bij een gedeeltelijke niet-openbaarmaking hiervan mededeling doet, gelijktijdig met de openbaarmaking.

Artikel 3.1, derde lid, van de Woo bepaalt dat documenten als bedoeld in het eerste lid niet openbaar worden gemaakt dan nadat belanghebbenden die naar verwachting bedenkingen zullen hebben tegen openbaarmaking, in de gelegenheid zijn gesteld binnen een door het bestuursorgaan gestelde termijn hun zienswijze naar voren te brengen.

Artikel 3.1, vierde lid, van de Woo bepaalt dat het bestuursorgaan een belanghebbende mededeling doet dat toepassing wordt gegeven aan het eerste lid, onder vermelding van het tijdstip van openbaarmaking en de openbaar te maken documenten. De mededeling wordt gelijkgesteld met een besluit.

Artikel 5.1, eerste lid, van de Woo bepaalt dat het openbaar maken van informatie ingevolge de Woo achterwege blijft achterwege voor zover dit:

- a. de eenheid van de Kroon in gevaar zou kunnen brengen;
- b. de veiligheid van de Staat zou kunnen schaden;
- c. bedrijfs- en fabricagegegevens betreft die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
- d. persoonsgegevens betreft als bedoeld in paragraaf 3.1 onderscheidenlijk paragraaf 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de openbaarmaking van deze persoonsgegevens of deze persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt;
- e. nummers betreft die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven als bedoeld in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de levenssfeer maakt.

Artikel 5.1, tweede lid, van de Woo bepaalt dat het openbaar maken van informatie eveneens achterwege blijft voor zover het belang daarvan niet opweegt tegen de volgende belangen:

- a. de betrekkingen van Nederland met andere landen en staten en met internationale organisaties;
- b. de economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, in geval van milieu-informatie slechts voor zover de informatie betrekking heeft op handelingen met een vertrouwelijk karakter;
- c. de opsporing en vervolging van strafbare feiten;
- d. de inspectie, controle en toezicht door bestuursorganen;

- e. de eerbiediging van de persoonlijke levenssfeer;
- f. de bescherming van andere dan in het eerste lid, onderdeel c, genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens;
- g. de bescherming van het milieu waarop deze informatie betrekking heeft;
- h. de beveiliging van personen en bedrijven en het voorkomen van sabotage;
- i. het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.

**Rijksinspectie Digitale
Infrastructuur**

Ons kenmerk
[VERTROUWEL
11/21]

Artikel 5.1, vijfde lid, van de Woo bepaalt dat in uitzonderlijke gevallen openbaarmaking van andere informatie dan milieu-informatie voorts achterwege kan blijven indien openbaarmaking onevenredige benadeling toebrengt aan een ander belang dan genoemd in het eerste of tweede lid en het algemeen belang van openbaarheid niet tegen deze benadeling opweegt. Voorts bepaalt dit artikel dat het bestuursorgaan een beslissing tot het achterwege laten van de openbaarmaking van enige informatie baseert op deze grond ten aanzien van dezelfde informatie niet tevens op een van de in het eerste of tweede lid genoemde gronden.