

> Retouradres Postbus 450 9700 AL Groningen

VERTROUWELIJK

Odido Netherlands B.V.
[Vertrouwelijk]

**Rijksinspectie Digitale
Infrastructuur**

Bezoekadres
Emmasingel 1
9726 AH Groningen

Postadres
Postbus 450
9700 AL Groningen

T 0088 04 16 000
E info@rdi.nl
RDI.NL

Contactpersonen
[Vertrouwelijk]

Tevens elektronisch verzonden aan: [Vertrouwelijk]

Datum 3 juli 2026
Betreft Beslissing op het bezwaar van Odido Netherlands B.V.

Ons kenmerk
[Vertrouwelijk]

Uw kenmerk
[Vertrouwelijk]

Bijlage(n)
-

Geachte [Vertrouwelijk]

1. Inleiding

Op respectievelijk 13 november en 17 november 2025 heb ik uw e-mailbericht en brief ontvangen waarmee u namens Odido Netherlands B.V. (hierna: Odido) bezwaar maakt tegen mijn besluit van 3 oktober 2025, met kenmerk [Vertrouwelijk], waarbij aan Odido een bestuurlijke boete is opgelegd (hierna: het bestreden Besluit) en tevens is besloten tot publicatie van de sanctie (inclusief persbericht).

Ik heb een beslissing op uw bezwaar genomen. Ik verklaar uw bezwaar gedeeltelijk gegrond. Mijn overwegingen treft u hieronder aan.

2. Samenvatting: kern van het besluit

Het gaat in deze zaak om zeer zwaarwegende maatschappelijk belangen, namelijk de veiligheid van onze digitale infrastructuur en de bescherming van extreem gevoelige, veelal staatsgeheime¹, gegevens. Meer specifiek gaat het erom op welke wijze aanbieders van openbare telecommunicatienetwerken en -diensten, waaronder Odido, om dienen te gaan met gegevens die aan hen ter beschikking zijn gesteld voor de uitvoering van zogeheten taplasten. Op grond van artikel 13.2 van de Tw zijn voornoemde aanbieders verplicht om medewerking te verlenen aan de uitvoering van taplasten. Dat betreffen lasten van bijvoorbeeld de inlichtingen- en veiligheidsdiensten en het Openbaar Ministerie om bepaalde personen te kunnen aftappen. Dergelijke taplasten kunnen door de daartoe bevoegd verklaarde instanties worden afgegeven in het belang van de nationale veiligheid of in het belang van de opsporing van strafbare feiten. Deze instanties verstrekken, als zij verzoeken om uitvoering te geven aan een taplast, uiterst gevoelige, veelal staatsgeheime, LI-gegevens², die de af te tappen persoon of organisatie

¹Voor zover het gaat om een taplast ten behoeve van de veiligheid van de staat, gaat het formeel om 'staatsgeheimen' (vgl. Nota van Toelichting van het Besluit beveiliging gegevens telecommunicatie).

² Lawful Intercept-gegevens.

identificeren, aan de desbetreffende aanbieder. Deze gegevens kunnen dus interessant zijn voor de (zware) georganiseerde criminaliteit, voor terroristen of voor kwaadwillende statelijke actoren. Als gevolg hiervan zijn regels gesteld voor de beveiliging van deze LI-gegevens. In de memorie van toelichting bij de Tw staat hierover:

"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 wettelijk bepaling te worden beveiligd. De gegevens waar het hier om gaat zijn bijvoorbeeld abonneegegevens en het feit dat er een tap geplaatst is."³

De kennisname van deze LI-gegevens door onbevoegden moet gezien het voorgaande steeds worden voorkomen. Immers, wanneer bekend zou worden met betrekking tot wie een dergelijke taplast is afgegeven komt, al naar gelang het doel waarvoor de taplast is afgegeven, de veiligheid van de staat of het slagen van een strafrechtelijk onderzoek in ernstige mate in het geding. Vanwege deze belangen geldt een hoog beveiligingsniveau ten aanzien van LI-gegevens.

In artikel 13.5, eerste lid, van de Tw is voor de aanbieders van openbare telecommunicatienetwerken en -diensten de basisverplichting neergelegd om de LI-gegevens, die aan hen 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 Besluit beveiliging gegevens telecommunicatie (hierna: Bbgt). Op grond van het Bbgt dienen voornoemde aanbieders zorg te dragen voor het treffen van in ieder geval de daarin voorgeschreven minimum beveiligingsmaatregelen om zodoende kennisneming van LI-gegevens door onbevoegden te voorkomen. De maatregelen die minimaal getroffen dienen te worden, zijn uitgewerkt in het Bbgt en de bijlage bij het Bbgt.

De basismaatregelen die aanbieders in ieder geval dienen te treffen gelden al zeer geruime tijd. Het Bbgt is immers in 2003 tot stand gekomen, na bovendien een zeer uitvoerig overleg met de sector. Onder andere Vodafone, KPN en aanbieders die later opgingen in T-Mobile (tegenwoordig Odido) waren nauw betrokken bij die overleggen en hebben als deelnemer in het deelorgaan aftappen in het Overlegorgaan Post en Telecommunicatie (het zogenaamde 'OPT-Daf') input kunnen leveren op de teksten van het Bbgt. Na deze afstemming en na verwerking van de input van de sector is het Bbgt op 28 oktober 2003 tot stand gebracht. Odido wist gezien het voorgaande al vanaf het moment dat het Bbgt van kracht werd wat van haar werd verwacht.⁴

³ Kamerstukken II 1996/97, 25 533, nr. 3, p. 125.

⁴ (De rechtsvoorganger van) Odido was via overlegorgaan OPT/DAF betrokken bij de totstandkoming van het Bbgt en Odido heeft ook na de totstandkoming geen vragen gesteld aan de RDI over de uitleg van het Bbgt.

Een toezichthouder van de Rijksinspectie Digitale Infrastructuur (hierna: RDI) heeft onderzoek gedaan naar de naleving door Odido van de vereisten die het Bbgt stelt aan de beveiliging van LI-gegevens. De toezichthouder heeft vastgesteld dat Odido op meerdere onderdelen tekort is geschoten in haar verplichting om te zorgen voor adequate beveiligingsmaatregelen. In het bestreden Besluit heb ik overwogen dat Odido negen minimumnormen van het Bbgt heeft overtreden. Ik heb deze overtredingen gegroepeerd en in de volgende drie groepen van overtredingen ingedeeld:

- I. Tekortkomingen ten aanzien van de verplichting een beveiligingsplan te hebben (artikel 3 van het Bbgt);
- II. Tekortkomingen ten aanzien van het personeel (artikel 4 van het Bbgt en artikel II van de bijlage bij het Bbgt);
- III. Tekortkomingen met betrekking tot de toegangsbeveiliging van geautomatiseerde informatiesystemen (artikel V van de bijlage bij het Bbgt).

Illustratief voor de wijze waarop Odido is omgesprongen met de LI-gegevens, is dat Odido, tegen het advies van de leverancier in, bewust heeft gekozen voor onversleutelde installatie van verbindingen waarover de gevoelige informatie werd verzonden. Dit betekent dat potentiële toegang tot de verbindingen gelijkstond aan toegang tot de informatie, waarmee een onacceptabel risico werd genomen. Voor twee LI-systemen werd het standaardwachtwoord gebruikt dat in de handleiding stond, zonder dit nadien te wijzigen. Minimumvereisten zoals persoonsgebonden authenticatie, blokkering bij meer dan drie foute inlogpogingen, centrale logging en detectie en het persoonsgebonden vastleggen van handelingen waren (deels) afwezig. Een gemiddeld burger die zich op internet begeeft wordt gehouden aan hogere standaarden dan de standaarden die Odido hier heeft toegepast ten aanzien van de aan haar toevertrouwde zeer vertrouwelijke en bovendien staatsgeheime LI-gegevens.

Ik heb in het bestreden Besluit besloten om voor deze drie groepen van overtredingen boetes op te leggen. Op grond van artikel 15.4 van de Tw ben ik bevoegd om per overtreding van de beveiligingseisen uit het Bbgt een boete op te leggen van maximaal € 900.000,-. Ik heb evenwel besloten om voor de geconstateerde overtredingen per groep overtredingen een basisboete van € 450.000,- te hanteren. Voor overtredingsgroep I heb ik die basisboete verhoogd tot € 562.500,-, omdat het beveiligingsplan geheel afwezig was. Vanwege de verhoogde ernst, duur en verwijtbaarheid van de overtredingen in groep III heb ik die basisboete verhoogd tot € 675.000,-. Gelet op de 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, heb ik besloten om de bestuurlijke boete met 10 % te matigen. Het totaalbedrag van de boetes is daarmee € 1.518.750,-.

INHOUDSOPGAVE

1. INLEIDING	1
2. SAMENVATTING: KERN VAN HET BESLUIT	1
3. ACHTERGROND EN PROCESVERLOOP	6
3.1 Onderzoek	6
3.2 Procedure bestreden Besluit	7
3.3 Bezwaarprocedure	8
4. UW BEZWAREN	9
4.1 Algemene bezwaargronden	9
4.1.1 Normuitleg Tw en Bbgt	9
4.1.2 Definitie LI-systeem	9
4.1.3 Bredere beveiligingsbeeld	10
4.2 Bezwaargronden per afzonderlijke overtreding	10
4.2.1 Overtreding 1: beveiligingsplan	10
4.2.2 Overtreding 2: beveiligingseisen ten aanzien van personeel	11
4.2.3 VOG-verplichting	11
4.2.4 Functieomschrijving	12
4.2.5 Geheimhoudingsverklaring	12
4.2.6 Ongeautoriseerde toegang	12
4.2.7 Boetehoogte overtreding 2 onevenredig	13
4.2.8 Overtreding 3: logische toegangsbeveiliging	13
5. ONTVANKELIJKHEID	14
6. JURIDISCH KADER	14
7. HEROVERWEGING	19
7.1 Bespreking van uw algemene bezwaren	20
7.1.1 Normuitleg Tw en Bbgt	21
7.1.2 Definitie LI-systeem	23
7.1.3 Bredere beveiligingsbeeld	23
7.2 Bespreking van uw specifieke bezwaren	23

7.2.1 Overtreding 1: beveiligingsplan	23	Ons kenmerk [Vertrouwelijk]
7.2.2 Overtreding 2: beveiligingseisen ten aanzien van personeel	30	
7.2.3 Betwisting evenredigheid en opslagen boete overtreding 3	42	
7.3 Conclusie	48	
7.3.1 Totale cumulatieve boete	49	
8. BESLISSING OP BEZWAAR	49	
9. BEROEP	49	

3. Achtergrond en procesverloop

Hieronder volgt een weergave van het verloop van het proces, voor zover dit relevant is voor deze beslissing op bezwaar. Daarbij zal ik ook ingaan op de omvang van het uitgevoerde onderzoek en de vastgestelde overtredingen in het bestreden Besluit.

3.1 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.

Het proces voor bevoegd aftappen bestaat, verkort weergegeven, uit de volgende stappen:

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.
2. Het tapverzoek wordt als aanvraag ingelezen in de [Vertrouwelijk], die onderdeel is van het [Vertrouwelijk]⁵. De [Vertrouwelijk] wordt door drie medewerkers van Odido gebruikt voor dagelijkse functionele LI-taken, waaronder het beantwoorden van vragen die worden gesteld door de bevoegde autoriteiten over nieuwe en lopende tapverzoeken.
3. Na goedkeuring van het tapverzoek wordt vanuit de [Vertrouwelijk] door het [Vertrouwelijk] de tap technisch geplaatst in een aantal systemen die de tap technisch verzorgen, waaronder de [Vertrouwelijk]
4. De afgetapte informatie (zoals gesprekken en internetverkeer) wordt aan de hand van de LI-gegevens verzameld binnen de [Vertrouwelijk]⁶
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.

Schematisch ziet dit proces waarin Odido tapverzoeken verwerkt er als volgt uit:

⁵ [Vertrouwelijk]

⁶ [Vertrouwelijk]

[Vertrouwelijk]

Voor een volledige weergave van het procesverloop gedurende de inspectiefase en de vastgestelde feiten verwijs ik naar het Rvb.

3.2 Procedure bestreden Besluit

Per brief van 20 mei 2025, met kenmerk [Vertrouwelijk] , heb ik mijn voornemen om een bestuurlijke boete aan Odido op te leggen en mijn voornemen een publieksversie van dit boetebesluit te publiceren kenbaar gemaakt aan Odido.

Op 3 juli 2025 heb ik de zienswijze van Odido ontvangen. Op 8 juli 2025 heeft Odido deze zienswijze mondeling toegelicht.

Op 3 oktober 2025 heb ik het bestreden Besluit, met kenmerk [Vertrouwelijk] genomen.

In het bestreden Besluit heb ik op basis van het onderzoek van de toezichthouder geconcludeerd dat de beveiliging van LI-gegevens door Odido op meerdere punten tekortschoot. Ik heb de tekortkomingen onderscheiden in de volgende drie groepen overtredingen van het Bbgt:

- I. Tekortkomingen ten aanzien van de verplichting een beveiligingsplan te hebben (artikel 3 van het Bbgt).

- Odido beschikte niet over een beveiligingsplan als bedoeld in artikel 3 Bbgt.
- II. Tekortkomingen ten aanzien van het personeel (artikel 4 van het Bbgt en artikel II van de bijlage bij het Bbgt).
- Er ontbraken VOG's van personeel dat medewerking verleent aan de uitvoering van taplasten.
 - Er ontbraken functiebeschrijvingen van personeel belast met het verwerken van LI-gegevens.
 - Er ontbraken geheimhoudingsverklaringen van personeel dat in aanraking komt met LI-gegevens.
 - Personeel dat niet was belast met verwerking van LI-gegevens had toegang tot de LI-gegevens.
- III. Tekortkomingen met betrekking tot de toegangsbeveiliging van geautomatiseerde informatiesystemen (artikel V van de bijlage bij het Bbgt).
- Op twee systemen was geen sprake van een deugdelijke beveiliging, onder meer doordat persoonsgebonden authenticatie ontbrak en gebruik werd gemaakt van (oude) standaardwachtwoorden.
 - Op twee systemen was geen blokkering van kracht bij overschrijding van drie foutieve inlogpogingen.
 - Op twee systemen was geen centrale logging en detectie geactiveerd.
 - Handelingen met betrekking tot de verwerking van de LI-gegevens werden niet persoonsgebonden vastgelegd om onderzoek mogelijk te maken.

Ik heb in het bestreden Besluit besloten om voor deze drie groepen van overtredingen boetes op te leggen. Ik heb besloten om per groep overtredingen een basisboete van € 450.000,- te hanteren. Voor overtredingsgroep I heb ik die basisboete verhoogd tot € 562.500,-, omdat het beveiligingsplan geheel afwezig was. Vanwege de verhoogde ernst, duur en verwijtbaarheid van de overtredingen in groep III heb ik die basisboete verhoogd tot € 675.000,-. Vanwege de lange duur van het onderzoek van mijn toezichthouder heb ik de totale bestuurlijke boete met 10% gematigd. Het totaalbedrag van de boetes is daarmee € 1.518.750,-.

Voorts heb ik op grond van artikel 3.1 van de Wet open overheid – en conform mijn publicatiepraktijk van boetebesluiten op grond van het Bbgt – besloten tot publicatie van het bestreden Besluit (inclusief persbericht) over te gaan.

3.3 Bezwaarprocedure

Op respectievelijk 13 november en 17 november 2025 heb ik uw e-mailbericht en brief ontvangen waarmee u namens Odido pro forma bezwaar heeft gemaakt tegen het bestreden Besluit.

Bij brief van 21 november 2025 heb ik de ontvangst van dit bezwaarschrift bevestigd en de gevraagde termijn tot en met 9 januari 2026 geboden om de gronden van het bezwaar aan te vullen. In deze brief heb ik tevens de beslistermijn met zes weken uitgesteld.

Op 9 januari 2026 heb ik de gronden van het bezwaar ontvangen. Bij e-mailbericht van 29 januari 2026 heeft u desgevraagd aangegeven dat Odido afziet van een hoorzitting om het bezwaarschrift mondeling toe te lichten.

4. Uw bezwaren

Met betrekking tot de beschikking tot oplegging van de bestuurlijke boete gaat u namens Odido in op een aantal algemene bezwaargronden en daarnaast op bezwaargronden per afzonderlijke overtreding. Uw bezwaargronden worden hieronder uiteengezet. In paragraaf 7 ga ik in op de bezwaargronden.

4.1 Algemene bezwaargronden

4.1.1 Normuitleg Tw en Bbgt

Odido acht mijn interpretatie van het Bbgt in het bestreden Besluit niet conform de strekking bij de totstandkoming daarvan. Onder verwijzing naar haar zienswijze benoemt Odido de uitleg van een aantal specifieke beveiligingsnormen voor het personeel. Uw betwisting van mijn interpretatie licht u verder toe in uw bezwaargronden bij overtreding 2. Ten algemene voert Odido nog het volgende aan.

U voert aan dat Odido zich niet op deze normuitlegging kon voorbereiden, omdat ik deze niet in beleidsregels of andere communicatie richting Odido heb uitgelegd. Verder benoemt u dat mijn interpretatie van het Bbgt aan verandering onderhevig is naarmate de stand der techniek vordert.⁷ U betwist dit uitgangspunt en voert aan dat mijn interpretatie afwijkt van hetgeen de regelgever heeft vastgesteld.

Om voornoemde redenen betwist u dat Odido de relevante normen uit het Bbgt heeft overtreden. U geeft aan dat ik in het bestreden Besluit Odido zeer hoge boetes opleg op basis van een strengere normuitlegging achteraf, hetgeen niet zou zijn toegestaan.

4.1.2 Definitie LI-systeem

Odido voert aan dat het begrip 'LI-systeem' niet op het Bbgt terug te voeren is en betwist dat het [Vertrouwelijk] als zodanig kwalificeert. Hierdoor zou de reikwijdte van het Bbgt volgens Odido worden opgerekt. De vereisten van het Bbgt zijn als gevolg van mijn interpretatie volgens Odido van toepassing op een zeer groot aantal personen en systemen. Voor de uitvoering van de taplasten gebruikt Odido echter slechts een zeer beperkt aantal systemen en slechts drie gescreende medewerkers. De door mij gehanteerde uitleg is ook in strijd met de randvoorwaarde van uitvoerbaarheid die de wetgever volgens Odido voor ogen had.

⁷ Zie ook het bestreden Besluit, p. 44.

Volgens Odido baseer ik de overtreding met betrekking tot de tekortkomingen aanzien van het personeel in wezen op het relevante criterium dat ongeautoriseerde toegang tot LI-gegevens in strijd is met het Bbgt. Het [Vertrouwelijk]

en [Vertrouwelijk]⁸ zijn echter systemen die maar op een zeer beperkt onderdeel LI-gegevens bevatten, namelijk op de relevante [Vertrouwelijk] Odido acht daarom ook alleen die [Vertrouwelijk] waar LI-gegevens op voorkomen relevante systemen en niet het hele [Vertrouwelijk]. Toegang tot het [Vertrouwelijk] is niet gelijk aan toegang tot LI-gegevens. Odido stelt verder dat toegang tot de [Vertrouwelijk] in de praktijk via de graphical user interface verloopt en niet mogelijk is via de door mij geschetste route door de SSH-ingang.

4.1.3 Bredere beveiligingsbeeld

Op verschillende plekken in uw aanvullend bezwaarschrift betoogt u dat het bredere beveiligingsbeeld van Odido moet worden betrokken bij het oordeel van de RDI. Dit punt wordt aangevoerd ten aanzien van overtreding 2 en de evenredigheid van de opgelegde boetes ten aanzien van overtredingen 2 en 3. Hetgeen u aandraagt is hieronder per subonderdeel weergegeven.

Om onnodige herhalingen te voorkomen vat ik dit punt op als een algemene bezwaargrond, waarbij ik hier onder 7.1.3 op reageer en er op de diverse subonderdelen naar verwijs.

4.2 Bezwaargronden per afzonderlijke overtreding

Naast de hierboven aangehaalde algemene bezwaargronden heeft Odido bezwaargronden per afzonderlijke overtreding.

4.2.1 Overtreding 1: beveiligingsplan

Odido is het niet eens met de conclusie dat zij geen beveiligingsplan had. Odido licht toe dat het plan niet uit een afzonderlijk document bestond, maar onderdeel was van een *policy house* waarvan delen kwalificeerden als een in het Bbgt bedoeld beveiligingsplan. Om aan de vordering tot het overleggen van het beveiligingsplan te voldoen, heeft zij verschillende bestaande delen van het *policy house* samengevoegd tot één document. Dit document is op 13 oktober 2021 verstrekt aan de toezichthouder. In de kern meent Odido dat aan een beveiligingsplan geen bijzondere eisen zijn gesteld. Daardoor is voldoende dat alle ingrediënten daarvoor aanwezig waren in de organisatie. Daarnaast stelt Odido zich op het standpunt dat haar ten onrechte in het bestreden Besluit is tegengeworpen dat zij het *policy house* niet alsnog heeft verstrekt. Hierbij stelt Odido dat het voor haar niet meer mogelijk is het destijds geldende *policy house* te verstrekken, omdat dit vanwege fundamentele wijzigingen niet meer te reproduceren is, terwijl de toezichthouder bovendien bekend zou zijn met het gegeven dat het beveiligingsplan uit meerdere onderdelen bestond. De toezichthouder had dit met andere woorden direct kunnen inzien indien hij daarom destijds zou hebben gevraagd.

⁸ [Vertrouwelijk]

Odido concludeert daarom dat er niet voldoende bewijs is voor overtreding 1.

4.2.2 Overtreding 2: beveiligingseisen ten aanzien van personeel

U stelt dat de overtreding inzake de beveiligingseisen ten aanzien van personeel ten onrechte is vastgesteld. Deze overtreding bestaat uit vier afzonderlijke onderdelen, waartegen separate gronden zijn gericht. Die bespreek ik hierna afzonderlijk.

Ten algemene is het bredere beveiligingsbeeld van Odido volgens u ten onrechte niet betrokken bij de beoordeling. In het bijzonder merkt u op dat het personeel dat belast is met LI-werkzaamheden een AIVD-screening hebben ondergaan en een VGB hebben. Deze screening en de voorlichting die daarbij is gegeven is volgens Odido ten onrechte niet benoemd in het bestreden Besluit.

4.2.3 VOG-verplichting

4.2.3.1 [Vertrouwelijk]-medewerkers

Bij haar zienswijze heeft Odido de geldige VOG's van medewerkers van [Vertrouwelijk] verstrekt. Odido betwist dat artikel 8 van het Bbgt zo moet worden uitgelegd dat een aanbieder de VOG's van medewerkers waaraan zij LI-werkzaamheden uitbesteedt zelf aanwezig moet hebben. Het is volgens de toelichting bij het Bbgt slechts vereist voor een aanbieder om de derde contractueel te verplichten de informatie aan te leveren als de toezichthouder daarom vraagt. Daarbij komt dat de bevoegdheid voor de toezichthouder om zich rechtstreeks tot de derde te wenden zinledig zou zijn als de aanbieder permanent over alle documentatie moet beschikken. Deze wijze van verwerking van persoonsgegevens is bovendien strijdig met de AVG wegens het ontbreken van een wettelijke verplichting. Het trage aanleveren van de VOG's betekent niet dat de VOG's niet bestonden. Volgens u was het doelmatiger en minder bezwarend geweest om de VOG's rechtstreeks bij [Vertrouwelijk] op te vragen.

4.2.3.2 [Vertrouwelijk]

De [Vertrouwelijk] verleent volgens u geen medewerking aan de uitvoering van taplasten, maar is slechts betrokken bij onderhoud aan dat systeem. Het [Vertrouwelijk] is geen LI-systeem, maar een algemeen systeem dat voor een zeer klein gedeelte taplasten uitvoert. Odido ziet geen onderbouwing van het begrip LI-systeem of voor de relevantie van eerste- en tweedelijns beheer in het Bbgt. U ziet verder samenloop tussen dit verwijt en overtreding 3, waarvoor een aparte boete is opgelegd. In wezen bestaan beide overtredingen uit de kans dat de [Vertrouwelijk] tegen de regels toegang zou kunnen hebben tot LI-gegevens.

4.2.4 Functieomschrijving

Odido stelt primair dat de overtreding met betrekking tot de functieomschrijvingen niet is bewezen. De bedoelde drie medewerkers voerden in deeltijd LI-werkzaamheden uit en hadden daarom ook andere functietitels. Uit het Bbgt volgt volgens u niet dat de omschrijvingen in de arbeidsovereenkomst moeten worden opgenomen. Daarnaast volgt niet uit het Bbgt dat Odido moet aantonen dat de omschrijvingen geldig waren in de periode van 5 oktober 2021 tot 14 september 2022 doordat deze bijvoorbeeld opnieuw is ondertekend. Een normale arbeidspraktijk brengt mee dat een functieomschrijving geldig blijft totdat deze wijzigt. Het verwijt dat Odido geen aanvullende stukken heeft aangeleverd over de functieomschrijving kunt u niet plaatsen. Het werd Odido pas na lezing van het voornemen duidelijk hoe ik deze norm uitleg en de toezichthouder heeft de informatie niet gevorderd.

Hoewel Odido volgens u hiermee haar onschuld moet bewijzen hecht zij er (subsidiar) waarde aan om toch aan te tonen dat de functieomschrijvingen wel beschikbaar waren. De Odido-medewerkers^[Vertrouwelijk] en [Vertrouwelijk] voerden de titel [Vertrouwelijk] en later [Vertrouwelijk] in hun formele aanstelling. Deze aanstelling is voor medewerker^[Vertrouwelijk] niet meer beschikbaar. Uit^[Vertrouwelijk] VGB blijkt dat ook^[Vertrouwelijk] deze functieomschrijving gebruikte.

Voor de [Vertrouwelijk] geldt dat^[Vertrouwelijk] niet belast was met de verwerking van LI-gegevens.^[Vertrouwelijk] hoefde daarom geen LI-functieomschrijving te voeren.

In de overeenkomst met^[Vertrouwelijk] heeft Odido beschreven welke functieomschrijving de vijf^[Vertrouwelijk]-medewerkers uitoefenen. Odido haalt hierbij de toelichting bij het Bbgt aan waarin wordt overwogen dat duidelijk moet zijn dat de LI-taak tot de werkzaamheden van een medewerker behoort. Deze omschrijvingen had Odido in haar eigen administratie beschikbaar. Het zou niet in lijn zijn met de AVG om ook de arbeidsovereenkomsten van de^[Vertrouwelijk]-medewerkers te bewaren.

4.2.5 Geheimhoudingsverklaring

U bent van mening dat de drie Odido-medewerkers wel een geldige geheimhoudingsverklaring hebben ondertekend. Nergens in het Bbgt is bepaald dat een aparte LI-geheimhoudingsverklaring moet worden opgesteld. Ook de uitspraak van de voorzieningenrechter⁹ is niet relevant, omdat die gaat om een geheimhoudingsverklaring van een leverancier en de uitspraak een voorlopig en dus geen richtinggevend karakter heeft.

Voor de [Vertrouwelijk] en^[Vertrouwelijk]-medewerkers geldt volgens u ook dat deze een algemene geheimhoudingsverklaring hebben ondertekend. Geheimhouding werd verder benadrukt in voorlichting en organisatorische maatregelen. Ook betwist Odido dat het Bbgt de verplichting bevat dat Odido de geheimhoudingsverklaringen altijd onder zich moet hebben.

Odido acht deze overtreding daarom niet bewezen.

4.2.6 Ongeautoriseerde toegang

U stelt dat noch het rapport van bevindingen noch het bestreden Besluit bewijs bevat voor de (daadwerkelijke) onbevoegde toegang van onbevoegden tot LI-gegevens. Door een tijdelijk foutieve configuratie van de LI-Firewall konden 81 personen in theorie toegang forceren tot LI-gegevens. Alleen door een PCAP-bestand te genereren konden 81 personen, die hiervan vermoedelijk niet op de hoogte waren, toegang krijgen tot LI-gegevens. Dit soort veiligheidsrisico's zijn nooit volledig uit te sluiten. Odido heeft meteen actie ondernomen toen zij van de misconfiguratie afwist.

U acht daarmee niet bewezen dat 81 ongeautoriseerde personen toegang hadden tot LI-gegevens.

4.2.7 Boetehoogte overtreding 2 onevenredig

Odido voert subsidiair, voor zover ik haar bewijsverweren tegen overtreding 2 niet honoreer, het volgende aan.

Voor de VOG's van ^[Vertrouwelijk]-medewerkers zou ik er bij het boetevoornemen vanuit zijn gegaan dat deze in het geheel niet bestonden. U stelt dat ik naar aanleiding van de zienswijze het verwijt heb aangepast tot het niet in de administratie aanwezig hebben van de betreffende VOG's. Dit had volgens u consequenties moeten hebben voor de boetehoogte. Dit geldt eveneens voor de functieomschrijvingen.

Met betrekking tot de Odido-medewerkers zou volgens u moeten meewegen dat deze allen in bezit zijn van een VGB. De boetehoogte zou het algemene veiligheidsbeeld moeten weerspiegelen waarbij de zware maatregel van een VGB zeer duidelijk maakt dat een medewerker met een LI-taak belast is en maakt het risico op ongeautoriseerde toegang aldus kleiner. De VGB's laten zien dat Odido goed zicht had op de personen die aan taplasten medewerking boden. Odido stelt dat dit ten onrechte niet in de boetehoogte is verdisconteerd.

Odido voert tot slot aan dat ik in mijn boetevoornemen uitging van ongeautoriseerde toegang door circa 667 personen en dat in mijn besluit heb teruggebracht tot 81 personen. Deze verlaging weegt volgens u ten onrechte niet mee in de ernst van de overtreding. Daarnaast betwist u dat ik het risico op ongeoorloofde toegang daadwerkelijk als groot inschat. Ware dat zo geweest dan had ik niet tot de toezending van het Rvb in februari 2025 gewacht om dit Odido duidelijk te maken.

Om bovengenoemde redenen acht Odido de betreffende boetehoogte onevenredig en vraagt zij om verlaging van de boete.

4.2.8 Overtreding 3: logische toegangsbeveiliging

Odido voert ten algemene aan dat de beveiliging sinds 2021 met voorrang verbeterd is. Een zware boete is daarom niet passend of geboden, een waarschuwing is volgens Odido passender. Drie verzachtende omstandigheden maken dat

⁹ Rb. Rotterdam, 22 oktober 2024, ECLI:NL:RBROT:2024:10347.

uitgangspunt nog passender: er is geen daadwerkelijke beveiligingsinbreuk vastgesteld, Odido heeft de overtreding zelf beëindigd en ik heb het oog alleen op de tekortkomingen en niet op het algehele beveiligingsbeeld gehad. Wat de eerste omstandigheid betreft geeft u aan dat uit forensisch onderzoek had kunnen blijken of er daadwerkelijk ongeautoriseerde toegang is geweest.

Wat de eerste boeteverhoging betreft voert u aan dat dit alleen om een theoretische mogelijkheid van toegang tot LI-gegevens gaat. Normaliter geeft een zuiver theoretisch risico dat zich niet (aantoonbaar) heeft verwezenlijkt juist aanleiding tot boetematiging. U stelt verder dat ik uitga van een inlogmethode op de [Vertrouwelijk] die feitelijk niet werd gebruikt. Dit zou volgens u het theoretische karakter van de overtreding onderstrepen.

Verhoging 2 betreft het bewust niet versleutelen van de X1-, X2-, en X3-verbindingen op 17 december 2012. U voert aan dat er niemand zonder autorisatie toegang had tot de betrokken kabels. Deze kabels werden bewaakt door fysieke maatregelen op de locaties in kwestie. Een indringer zou bovendien zonder verdere kennis niet weten welke kabel hij moet aftappen. Het totale beveiligingsniveau is wederom niet benoemd. De in het bestreden Besluit benoemde scenario's, (1) op locatie graven naar de kabels (2) binnen een kabelbundel naar de kabels in kwestie zoeken en (3) deze heimelijk aftappen, acht u niet realistisch.

Odido voert voorts aan dat zij grote delen van haar infrastructuur op last van de overheid heeft moeten vervangen. Dit ging gepaard met aanzienlijke kosten die niet zijn vergoed. In samenloop met de volgens u hoge boete leidt dit tot een onevenredige benadeling van Odido.

5. Ontvankelijkheid

Allereerst dien ik de ontvankelijkheid van uw bezwaarschrift te beoordelen.

Hierbij stel ik vast dat uw bezwaarschrift binnen de bezwaartermijn is ingediend en dat tevens aan de overige eisen voor ontvankelijkheid is voldaan. Dat betekent dat ik toekom aan de inhoudelijke beoordeling van uw bezwaren.

6. Juridisch kader

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

In de Telecommunicatiewet, het Bbgt en de bijlage bij het Bbgt staan de kaders voor de beveiliging van gegevens die betrekking hebben op *Lawful Interception*, dat wil zeggen het bevoegd aftappen of opnemen van telecommunicatie, de zogenaamde LI-gegevens.

Op grond van artikel 13.2 van de Tw zijn aanbieders verplicht hun medewerking te verlenen aan een, kort gezegd, bevoegd gegeven aftapverzoek. Deze aftapverzoeken worden door de daartoe bevoegde autoriteiten – zijnde de Officier van Justitie, de AIVD en de MIVD – gedaan in het belang van de strafvordering of

in het belang van de veiligheid van de staat.¹⁰ De bevoegde autoriteiten verstrekken de aanbieder bij een dergelijk verzoek LI-gegevens die de af te tappen persoon of organisatie identificeren. Deze gegevens hebben een uiterst gevoelig karakter. Ik verwijs hiervoor naar de Nota van Toelichting (hierna: NvT) bij het Bbgt waarin dit uiterst gevoelige karakter wordt benadrukt:

*"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. (...) 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."*¹¹

En:

*"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."*¹²

Hieruit volgt de noodzakelijkheid dat een aanbieder ten aanzien van LI-gegevens adequate beveiligingsmaatregelen neemt teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen en, voor zover een dergelijke inbreuk wel heeft plaatsgevonden, maatregelen te treffen waarmee daarop op een snelle en adequate wijze kan worden gereageerd. Daarom zijn in, onder meer, artikel 13.5 van de Tw en het Bbgt regels gesteld omtrent de beveiliging van de verstrekte gegevens en informatie. Hiervoor verwijs ik ook naar de memorie van toelichting (hierna: MvT) bij artikel 13.5 van de Tw, waarin de wetgever het zwaarwegend belang van geheimhouding en bescherming van LI-gegevens door aanbieders onderstreept door aan te geven dat het bij deze gegevens gaat om staatsgeheimen:

¹⁰ NvT bij het Bbgt, Stb. 2003, 472 p. 7.

¹¹ NvT bij het Bbgt, Stb. 2003, 472 p. 7.

¹² NvT bij het Bbgt, Stb. 2003, 472, p. 13.

Ons kenmerk
[Vertrouwelijk]

*"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."*¹³

In dit kader wijs ik ook op de NvT bij het Bbgt:

*"Bij de invulling van de beveiligingsmaatregelen dient onderscheid gemaakt te worden tussen de gevallen waarin de te beveiligen gegevens en informatie betrekking hebben op de veiligheid van de staat enerzijds en strafvordering anderzijds. Voor zover de veiligheid van de staat in het geding is, gaat het om (formeel) als staatsgeheim gerubriceerde gegevens en informatie waarop binnen de rijksdienst een verzwaaard regime van toepassing is. Dergelijke gegevens en informatie dienen bij de rijksdienst immers beveiligd te worden overeenkomstig de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst ((AAR 9) (Stcrt. 1989, 26)). (...)"*¹⁴

In artikel 13.5, eerste lid, van de Tw is voor aanbieders de basisverplichting neergelegd om de gegevens die aan de aanbieders worden verstrekt om uitvoering te kunnen geven aan taplasten adequaat te beveiligen tegen kennisneming door onbevoegden en om geheimhouding te betrachten met betrekking tot deze gegevens. 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 (zoals voorgeschreven in het Bbgt, zie hierna), vormt een potentieel grote bedreiging van de genoemde belangen. Het is dan ook noodzakelijk dat wordt voorzien in adequate beveiligingsmaatregelen om een inbreuk te voorkomen op de vertrouwelijkheid van de LI-gegevens. In artikel 13.5, eerste lid, van de Tw is opgenomen:

Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht gegevens met betrekking tot een bijzondere last dan wel toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 als bedoeld in artikel 13.2 dan wel een vordering of een verzoek als bedoeld in artikel 13.2b of artikel 13.4, eerste, tweede of derde lid, te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.

Deze basisverplichting is nader uitgewerkt in het Bbgt en de bijlage daarbij. Hierin wordt onder meer bepaald welke minimum beveiligingsmaatregelen een aanbieder moet nemen om kennisneming van LI-gegevens door onbevoegden te voorkomen. Zie ook de NvT bij het Bbgt:

¹³ Kamerstukken II 1996/97, 25 533, nr. 3, p. 125.

¹⁴ NvT bij het Bbgt, Stb. 2003, 472 p. 8.

*"In artikel 13.5, eerste lid, Tw is voor de aanbieders de basisverplichting neergelegd om de gegevens welke aan de aanbieders worden verstrekt om uitvoering te kunnen geven aan een bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, Tw, alsmede de informatie welke de aanbieders binnen het kader van artikel 13.4 Tw verstrekken aan de tot aftappen bevoegde instanties, te beveiligen tegen kennisneming door onbevoegden; voorts wordt hen verplicht geheimhouding te betrachten met betrekking tot deze gegevens. De wijze waarop de aanbieders invulling geven aan deze beveiligingsverplichting is in beginsel een eigen aangelegenheid. De wetgever heeft echter gemeend dat het noodzakelijk kan zijn dat ter zake van de door de aanbieder te nemen beveiligingsmaatregelen regels worden gesteld. In artikel 13.5, tweede lid, Tw, is daarvoor de grondslag gelegd. Door het stellen van dergelijke regels kan worden bewerkstelligd dat bij elke aanbieder in ieder geval een op de aard van de gegevens toegesneden minimumniveau van beveiligingsmaatregelen wordt getroffen."*¹⁵

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

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

(...)

Artikel 2, tweede lid, van het Bbgt bepaalt dat de minimaal te treffen beveiligingsmaatregelen, bedoeld in het eerste lid, ten minste dienen 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 het Bbgt. In de bijlage bij het Bbgt zijn de beveiligingsmaatregelen die dienen te worden getroffen zeer concreet en per categorie uitgewerkt. Het gaat om de volgende categorieën:

I. Beveiligingseis algemeen;

¹⁵ NvT bij het Bbgt, *Stb.* 2003, 472 p. 7 en 8.

- II. Beveiligingseisen ten aanzien van personeel;
- III. Fysieke beveiliging en beveiliging van de omgeving;
- IV. Beheer van communicatie- en bedieningsprocessen;
- V. Toegangsbeveiliging van geautomatiseerde informatiesystemen;
- VI. Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen.

Uit de NvT alsook het verslag van de consultatie blijkt dat het enkel een minimum set aan maatregelen betreft, die afhankelijk van de soort organisatie en inrichting moet worden uitgebreid.

In de NvT staat hierover:

*"De specifiek in het besluit en de bijlage voorgeschreven maatregelen zijn van dien aard dat verwacht wordt dat de daarmee gepaard gaande kosten, mede doordat de aanbieder zelf de nodige ruimte is gelaten om daaraan op een specifiek op zijn organisatie toegesneden wijze invulling te geven, binnen redelijke grenzen kunnen worden gehouden. Een kwantificering van deze kosten is echter moeilijk te geven, gelet op het feit dat de beveiligingsplicht diverse soorten aanbieders raakt met verschillen in omvang en organisatievorm."*¹⁶

Daarnaast wordt verwezen naar het verslag van het overleg (DAF 2022/22) van het Overlegorgaan Post en Telecommunicatie, Deelorgaan Aftappen van 26 juni 2002, waarin staat:

"Zoals ook in de toelichting is vermeld, gaat het om minimum eisen die worden gesteld. Afhankelijk van de soort organisatie en inrichting, zullen er meer maatregelen nodig zijn. En als er een lek wordt geconstateerd waar deze AmvB niet in voorziet, dan zal daar, los van de procedure tot wijziging, snel in moeten worden voorzien."

Daarnaast volgen uit het Bbgt nog andere verplichtingen ten aanzien van de beveiliging van LI-gegevens. Artikel 3, eerste lid, van het Bbgt vereist 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.

In de NvT staat hierover:

*"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. Het beveiligingsplan kan door elke aanbieder – zij het met inachtneming van de in het besluit reeds geëxpliciteerde eisen – op de specifieke situatie van de eigen organisatie worden toegesneden."*¹⁷

¹⁶ NvT bij het Bbgt, Stb. 2003, 472 p. 15.

¹⁷ NvT bij het Bbgt, Stb. 2003, 472, p. 10.

Hiermee vormt het beveiligingsplan een belangrijke basis voor de door de aanbieder te treffen en getroffen maatregelen.

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 Tw bedoelde bevoegd gegeven bijzondere last en de in de artikelen 13.2b en 13.4 van de Tw 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.

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 van artikel 8 van het Bbgt.

Samengevat betekent dit dat een aanbieder de minimumbeveiligingsmaatregelen uit het Bbgt dient te treffen om een inbreuk op de vertrouwelijkheid van LI-gegevens te voorkomen. Dit is van belang voor het welslagen van een strafrechtelijk onderzoek en de veiligheid van de staat. Wanneer het gaat om de veiligheid van de staat, zijn dergelijke LI-gegevens staatsgeheime informatie. Aan de beveiliging van LI-gegevens worden daarom hoge eisen gesteld.

7. Heroverweging

Naar aanleiding van uw bezwaar heb ik de beslissing waartegen u bezwaar maakt opnieuw overwogen. Mijn overwegingen treft u hieronder aan. Ik begin met de twee door Odido aangevoerde algemene bezwaren en zal daarna reageren op de specifieke bezwaren van Odido, waarbij er enige overlap bestaat tussen de algemene punten en de specifieke punten.

Voordat ik inga op de bezwaargronden is het belangrijk eerst de context van de regelgeving te duiden. Deze context is namelijk relevant voor mijn reactie op uw bezwaargronden. Het is van groot maatschappelijk belang dat LI-gegevens deugdelijk worden beveiligd.

Als de veiligheid van de staat of de opsporing van strafbare feiten dat vordert, kunnen de AIVD, MIVD of de Officier van Justitie, na een schriftelijke machtiging van de rechter-commissaris, een taplast afgeven aan Odido. Op grond van artikel 13.2 van de Tw is Odido gehouden haar medewerking daaraan te verlenen. De genoemde autoriteiten overleggen bij het geven van een taplast LI-gegevens, zoals een naam en het telefoonnummer van degene op wie de taplast betrekking heeft. Dit zijn buitengewoon gevoelige gegevens die, in het geval de taplast is afgegeven wegens de nationale veiligheid, formele staatsgeheimen zijn.¹⁸ Indien degene op wie de taplast betrekking heeft verneemt dat communicatie wordt afgetapt, dan verliest het middel zijn effect. Daarmee zou de bestrijding van (zware) criminaliteit of bescherming van de nationale veiligheid worden bemoeilijkt. Zo kunnen

¹⁸ NvT bij het Bbgt, *Stb.* 2003, 472, p. 8.

betrokken personen hun gedrag aanpassen of bewijsmateriaal wegmaken. Daarnaast kan een beveiligingsincident ervoor zorgen dat inlichtingendiensten van bevriende staten hun inlichtingen minder snel delen met de AIVD of MIVD. Verder is het mogelijk dat een hacker de buitgemaakte LI-gegevens gebruikt als chantagemiddel tegen een aanbieder. Bovendien is van belang dat de kwaadwillenden met interesse in LI-gegevens veelal statelijke actoren en de georganiseerde misdaad zullen zijn. Deze partijen zijn bij uitstek in staat om gerichte aanvallen van geavanceerd niveau uit te voeren. Het beveiligingsniveau zal op deze dreiging moeten worden afgestemd.

Om de genoemde zwaarwegende belangen te dienen is met het Bbgt een aantal minimumeisen aan de beveiliging van LI-gegevens gesteld. De belangen van de veiligheid van de staat en het welslagen van strafrechtelijke onderzoeken vergen aan de kant van de aanbieders een goed begrip van de beveiligingseisen en een nauwgezette naleving. Daarom is vooraf intensief met de betrokken sector, onder andere met (de rechtsvoorgangers van) Odido, in overleg getreden over de inhoud van de beveiligingsplichten. Het is van bijzonder maatschappelijk belang om voldoende veiligheidsmaatregelen te treffen om een inbreuk te voorkomen en snel opvolging te kunnen geven als er signalen zijn dat een inbreuk gaande is.

Gegeven dit grote maatschappelijke belang kan ik de bezwaargronden van Odido niet volgen. Odido wekt een beeld alsof er zou zijn gezocht naar 'spijkers op laag water', waarbij het volgens Odido zou gaan om onduidelijke normen zonder zwaarwegend maatschappelijk belang. Dit beeld is niet correct. Odido kent als geen ander het belang van het Bbgt. Zij is intensief betrokken geweest bij de totstandkoming ervan. Mede gegeven de rol van Odido als vitale dienstverlener en de verwachte professionaliteit van een telecomprovider, mag van Odido worden verwacht dat zij het belang van de regels begrijpt en daar in de praktijk naar handelt. Dit betekent dan ook dat Odido niet lichtvaardig de conclusie kan trekken dat de regels in enge zin zouden moeten worden geïnterpreteerd. Dat staat immers haaks op de publieke belangen waarvoor de regels bescherming moeten bieden.

Gezien deze grote belangen valt bijvoorbeeld niet in te zien (zoals Odido stelt) dat het Bbgt alleen betrekking heeft op systemen die enkel voor het verwerken van LI-gegevens worden gebruikt. Deze zeer enge (en bovendien evident onjuiste) lezing van het Bbgt zou betekenen dat er geen beveiligingseisen gesteld zouden worden aan systemen die weliswaar de verwerking van LI-gegevens niet als kerntaak hebben, maar waarin zich wel LI-gegevens bevinden. Een dergelijk standpunt verdraagt zich in de eerste plaats niet met de letterlijke tekst van het Bbgt. Daarnaast staat dat standpunt ook haaks op de strekking van het Bbgt en de belangen die de regels uit het Bbgt beogen te beschermen. Zoals ook door de rechtbank Rotterdam is bevestigd, maken de belangen die achter het Bbgt schuilgaan en de tekst en toelichting van het Bbgt duidelijk dat het Bbgt ruim moet worden uitgelegd.

7.1 Bespreking van uw algemene bezwaren

Hieronder volgt mijn reactie op de algemene bezwaren van Odido.

7.1.1 Normuitleg Tw en Bbgt

Odido betwist met haar eerste bezwaargrond de uitleg die ik in het bestreden Besluit aan diverse normen heb gegeven. Odido doelt specifiek op de bepalingen die met de personeelsbeveiliging van doen hebben. Op deze specifieke normuitleggingen, die zij op pagina 4 en 5 van het aanvullend bezwaarschrift aanhaalt, ga ik in bij de bespreking van de bezwaargronden tegen overtreding 2. Uit die bespreking blijkt dat de betrokken normen volstrekt duidelijk zijn. Op de stelling dat ik beleidsregels of andere richtsnoeren had moeten vaststellen reageer ik hieronder.

Uit paragraaf 6 (juridisch kader) volgt dat in het Bbgt minimaal te treffen beveiligingsmaatregelen zijn opgenomen die een aanbieder in ieder geval moet nemen om te komen tot een adequate beveiliging van LI-gegevens. Ten aanzien van deze maatregelen die Odido ten minste dient te nemen, zijn in het bestreden Besluit overtredingen vastgesteld. Op basis van de tekst van het Bbgt, mede bezien in het licht van de uitleg die daaraan is gegeven en de belangen die de normen uit het Bbgt beogen te beschermen, is volstrekt helder wat van Odido wordt verwacht. Dit geldt zeker voor de normen die Odido aanhaalt en die, kort gezegd, op beveiligingseisen voor het personeel zien. Ik zie reeds daarom niet in waarom Odido niet uit de tekst en toelichting van het Bbgt kon afleiden wat van haar wordt verwacht.

Ten aanzien van de stelling van Odido dat de normen uit het Bbgt een open karakter hebben, geldt dan ook het volgende. In de eerste plaats kan ik de gevolgtrekking in algemene zin niet volgen. In het concrete geval geldt dat het Bbgt zelf en in de bijlage bij het Bbgt zeer uitvoerig en per onderdeel uiteen is gezet welke maatregelen aanbieders in ieder geval dienen te treffen. Ik meen dan ook dat een professionele marktdeelnemer als Odido wist, of in ieder geval behoorde te weten, wat van haar (vanaf 2003) werd verwacht ten aanzien van de te treffen beveiligingsmaatregelen met betrekking tot LI-gegevens. Zeker omdat Odido betrokken was bij de totstandkoming van het Bbgt via het Permanent overlegorgaan post en telecommunicatie (OPT/DAF).¹⁹ In dat gremium heeft Odido ingestemd met het ontwerp van het Bbgt en wist zij dus welke verplichtingen op haar rusten. Met betrekking tot deze normen zijn in het bestreden Besluit desondanks overtredingen vastgesteld.

Voor zover (nog) sprake is van enige open normen, geldt bovendien dat nergens uit blijkt dat het mij niet is toegestaan om tegen schendingen van de desbetreffende normen handhavend op te treden. 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 precieze inhoud van een norm en zich de nodige inspanningen getroost om daar ook daadwerkelijk aan te voldoen, desnoods door advies in te winnen. Ook volgt hieruit dat een professionele marktpartij als Odido zich niet kan verschuilen achter het uitblijven van nadere guidance of beleidsregels door de toezichthouder, omdat het primair de

¹⁹ Stb. 2003, 472, p. 17.

eigen verantwoordelijkheid van Odido is om zijn wettelijke verplichtingen na te komen en om in dit verband veiligheidsrisico's te ondervangen. **Ons kenmerk**
[Vertrouwelijk]

In gelijke zin oordeelde de rechtbank Rotterdam recentelijk als volgt omtrent de duidelijkheid van de normen uit het Bbgt²⁰:

De Bbgt bevat inderdaad enige open normen, maar stelt daarnaast ook een reeks concrete eisen aan de beveiligingsmaatregelen die telecomaanbieders moeten nemen om kennismaking van LI-gegevens door onbevoegden te voorkomen. Voor zover sprake is van een open norm geldt het volgende. Van de wet- en regelgever wordt verlangd dat hij met het oog op de rechtszekerheid op een zo duidelijk mogelijke wijze de verboden gedraging omschrijft. Daarbij moet echter niet uit het oog worden verloren dat de wet- of regelgever soms met het gebruik van algemene termen verboden of geboden gedragingen omschrijft om te voorkomen dat gedragingen die strafwaardig zijn buiten het bereik van die omschrijving vallen. Dit kan onvermijdelijk zijn, omdat niet altijd is te voorzien op welke wijze de te beschermen belangen in de toekomst zullen worden geschonden en omdat, indien dit wel is te voorzien, de omschrijvingen van verboden of geboden gedragingen anders te verfijnd worden met als gevolg dat de overzichtelijkheid wegvalt en daarmee het belang van de algemene duidelijkheid van wet- of regelgeving schade lijdt (bijv. ECLI:NL:CBB:2012:BV6713, punt 4.3).

(...)

De rechtbank is van oordeel dat deze toelichting voldoende duidelijk maakt wat van [aanbieder 1] wordt verlangd. (...) Naast open normen stellen de artikelen 2, 3, 4 en 8 van het Bbgt in samenhang gelezen met de onderdelen II, III en V van de Bijlage ook een aantal zeer concrete eisen aan de aanbieder.

(...)

Voor zover het open normen betreft, voegt de rechtbank hieraan toe dat uit vaste rechtspraak volgt dat van een professionele marktpartij als [aanbieder 1] mag worden verwacht dat die de nodige inspanningen verricht om zich op de hoogte te stellen van de precieze inhoud van de norm en zich de nodige inspanningen getroost om daar ook daadwerkelijk aan te voldoen, desnoods door advies in te winnen (bijv. ECLI:NL:CBB:2020:419, punt 6.2). Ook volgt hieruit dat een professionele marktpartij als [aanbieder 1] zich niet kan verschuilen achter het uitblijven van guidance door de toezichthouder, omdat het primair de eigen verantwoordelijkheid van de marktdeelnemer betreft om zijn wettelijke verplichtingen na te komen en om in dit verband veiligheidsrisico's te ondervangen (vgl. ECLI:NL:CBB:2017:274, punt 6.2). De toezichthouder is geen adviseur (ECLI:NL:CBB:2021:575, punt 5). Daarbij merkt de rechtbank op dat zorgplichten als hier aan de orde niet met zich brengen dat [aanbieder 1] die volledig naar eigen inzichten mag invullen, maar dat het – zoals uit de toelichting ook naar voren komt – gaat om na te leven minimumeisen.

Gelet op het voorgaande kan ik bezwaargrond 1 niet volgen.

²⁰ Rb. Rotterdam, 8 mei 2026, ECLI:NL:RBROT:2026:5480.

7.1.2 Definitie LI-systeem

Hoewel deze bezwaargrond door Odido niet bij een specifieke overtreding is geplaatst, blijkt uit de tekst van de grond dat Odido deze grond feitelijk tegen overtreding 2 richt. Odido betoogt in wezen dat personeel dat het [Vertrouwelijk] beheert of gebruikt niet binnen de reikwijdte van artikel II en 4, tweede lid, van het Bbgt valt. Om herhaling te voorkomen behandel ik deze grond bij de andere gronden die tegen overtreding 2 zijn gericht. In paragraaf 7.2.2.2 tot en met 7.2.2.5 ga ik nader op deze grond in.

7.1.3 Bredere beveiligingsbeeld

Odido betoogt ten aanzien van de overtreding onder 2 en de evenredigheid van de boetes onder 2 en 3 dat de RDI zich uitsluitend heeft gericht op vermeende tekortkomingen in specifieke beveiligingsmaatregelen, zonder het bredere beveiligingsbeeld in ogenschouw te nemen. Deze grond slaagt niet.

Ik stel voorop dat het bredere beveiligingsbeeld geen onderdeel is van de voorschriften in het Bbgt. De voorschriften uit het Bbgt schrijven daarentegen heel precies voor wat van Odido wordt verwacht. Dat Odido mogelijk andere maatregelen heeft getroffen op andere vlakken kan, wat daarvan verder zij, reeds daarom niet afdoen aan de vaststelling dat Odido de concreet van haar verlangde maatregelen niet heeft getroffen. Dit verweer kan daarom, los van de inhoudelijke beoordeling daarvan, geen afbreuk doen aan de conclusie dat de betrokken overtredingen door Odido zijn gepleegd. Over het 'bredere beveiligingsbeeld' overweeg ik voorts als volgt.

Met het diepgaande en gedetailleerde onderzoek van mijn toezichthouder heb ik een toereikend beeld verkregen van de beveiliging van LI-gegevens door Odido. Op basis daarvan heb ik grote zorgen omtrent de beveiliging door Odido van LI-gegevens. Odido heeft immers op meerdere onderdelen volstrekt onvoldoende beveiligingsmaatregelen genomen. Een treffend voorbeeld hiervan is dat het standaard-wachtwoord dat door [Vertrouwelijk] is verstrekt en was opgenomen in een document, nadien nooit is gewijzigd. Daarmee had Odido zelfs de minimale basis niet op orde. De overtredingen hebben tot gevolg dat de beveiliging van LI-gegevens tegen onbevoegde kennisname beneden het minimumniveau was. Daarmee zijn de overtredingen elk een directe schending van de met het Bbgt te beschermen belangen en vergroot Odido daarmee het risico voor de staatsveiligheid en strafrechtelijke opsporing.

Al met al zie ik daarom in het bredere beveiligingsbeeld geen aanknopingspunten voor een bijstelling van mijn opvatting over de geconstateerde overtredingen door Odido en/of de zwaarte daarvan.

7.2 Bespreking van uw specifieke bezwaren

7.2.1 Overtreding 1: beveiligingsplan

Artikel 3 van het Bbgt vereist dat de aanbieder zorgdraagt voor een beveiligingsplan, waarin de aanbieder 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.

Het belang van een beveiligingsplan mag niet worden onderschat. Het hebben van een adequaat beveiligingsplan vormt een startpunt van een deugdelijke fysieke en logische beveiliging van LI-gegevens door een aanbieder.²¹ Zonder een deugdelijk plan geeft een aanbieder er immers geen blijk van zich bewust te zijn van het nut en de noodzaak van de te treffen maatregelen en is intern ook niet duidelijk aan welke maatregelen men zich moet houden. De vereisten waaraan het beveiligingsplan moet voldoen, vormen dus niet enkel een (papieren) vormvoorschrift. Het vormt de basis van de minimale te treffen beveiligingsmaatregelen.

Ik maak uit het verweer van Odido niet op dat Odido het belang van een beveiligingsplan betwist. Ook bestaat er tussen Odido en mijzelf geen verschil van mening over de vraag of een beveiligingsplan ook uit verschillende documenten mag bestaan. Er gelden immers geen bijzondere vormvereisten en dit is in beginsel toegestaan, mits dit samenstel van documenten een logisch geheel vormt, aan de inhoudelijke vereisten voldoet en geschikt is om het doel te bewerkstelligen dat voor alle betrokken medewerkers duidelijk is aan welke eisen men zich moet houden. Dit doel kan echter niet worden bereikt als er in het geheel geen beveiligingsplan is, dan wel als het onderlinge verband tussen de documenten ontbreekt of onduidelijk is dat een document deel uitmaakt van een groter geheel dat allemaal evengoed in acht moet worden genomen.

De RDI heeft bij Odido uitvraag gedaan naar het beveiligingsplan. Van belang hierbij is dat deze uitvraag is gedaan op 5 oktober 2021 en dat er op 13 oktober 2021 een stuk is ontvangen. Dit stuk ('TMNL Beveiligingsplan Lawfull Intercept version 1.0') is niet voorzien van een specifieke datum, maar er staat wel in dat dit document van "oktober 2021" is. Mijn inspecteur heeft in de metadata echter achterhaald dat het moment van opstellen 13 oktober 2021 om 18:03 uur is geweest.. Op basis van deze omstandigheid, en de andere omstandigheden die ik hieronder bij de bespreking van het verweer nader toelicht, heb ik het ervoor gehouden dat er voorafgaand aan 12 oktober 2021 geen beveiligingsplan bestond.

Het verweer van Odido is onder 4.2.1 weergegeven, maar komt er in de kern op neer dat Odido meent dat er onvoldoende bewijs is om te stellen dat zij voor 12 oktober 2021 geen beveiligingsplan had. Om dit standpunt goed te kunnen toetsen herhaal ik allereerst hetgeen ik al in het primaire besluit heb overwogen rondom de eisen van een beveiligingsplan.

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

²¹ Zie ook NvT bij het Bbgt, *Stb.* 2003, 472, p. 10.

waaraan de gegevens en informatie zijn onderworpen op een gestructureerde wijze te worden behandeld.(...)"²²

"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."²³

"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."²⁴

Uit de nota van toelichting van het Bbgt volgt ook dat het beveiligingsplan niet aan bijzondere vormvereisten is gebonden. Verder blijkt uit de nota van toelichting dat het plan 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; (...)"²⁵

Recentelijk is een en ander ook bevestigd door de rechtbank Rotterdam²⁶:

In artikel 3, eerste lid, van het Bbgt is de verplichting neergelegd zorg te dragen voor een beveiligingsplan waarin ten minste wordt aangegeven op welke wijze uitvoering is gegeven aan de maatregelen, bedoeld in de Bijlage. Dit zorgdragen houdt naar het oordeel van de rechtbank ook de verplichting in om een eerder opgesteld beveiligingsplan te actualiseren. Dit volgt niet alleen uit de aard van deze zorgplicht, maar ook uit de toelichting bij het Bbgt. Daarin is vermeld dat naast de eenmalige kosten die aan het opstellen van een beveiligingsplan zijn verbonden, ook kosten moeten worden gemaakt om de plannen actueel te houden, waarbij wordt uitgegaan van een jaarlijkse update (Stb. 2003, 472, blz. 16).

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

²² Stb. 2003, 472, p. 10.

²³ Stb. 2003, 472, p. 13.

²⁴ Stb. 2009, 350, p. 6 en 7.

²⁵ Stb. 2003, 472, p. 16.

²⁶ Rb. Rotterdam, 8 mei 2026, ECLI:NL:RBROT:2026:5480.

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 maatregelen genoemd in de bijlage bij het Bbgt. Daarnaast moet het beveiligingsplan jaarlijks van een update worden voorzien.

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

Daarnaast vermeldt de nota van toelichting dat alle beveiligingsaspecten welke aan de orde zijn ten aanzien van de bedrijfsprocessen waaraan LI-gegevens zijn onderworpen op een gestructureerde wijze moeten worden behandeld in het beveiligingsplan.²⁷ Bovendien volgt uit de nota van toelichting dat hierbij specifieke aandacht besteed moet worden aan het onderscheid in de verschillende beveiligingsregimes.²⁸

Het verweer van Odido gaat uit van twee tegengestelde uitgangspunten. Odido stelt in haar bezwaar aan de ene kant dat het niet over één document beschikte dat zij eenvoudig met de RDI kon delen en dat zij aan de toezichthouder tegemoet heeft willen komen door meerdere onderdelen uit het policy house die zagen op het Bbgt samen te voegen in één document. Dit is het document dat Odido op 13 oktober 2021 heeft aangeleverd. Odido stelt dat dit de verschillende onderdelen waren uit het policy house die zagen op het Bbgt. Aan de andere kant stelt Odido dat de RDI haar policy house niet heeft getoetst en dat het dat het beveiligingsplan in het policy house stond. Het aanleveren van het policy house was volgens Odido niet verplicht en het is inmiddels niet meer mogelijk om het policy house zoals dat destijds bestond nog aan te leveren, aldus Odido. Dit suggereert dus dat er meer informatie voorhanden zou zijn geweest.

Ik zie niet in hoe beide door Odido ingenomen standpunten tegelijkertijd waar kunnen zijn. Als reactie hierop schets ik de feiten die ten grondslag liggen aan mijn beoordeling.

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

²⁷ Stb. 2009, 350, p. 10.

²⁸ Stb. 2009, 350, p. 7.

"Aanleveren binnen 1 week na verzoek

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

De toezichthouder heeft het document 'TMNL Beveiligingsplan Lawfull Intercept version 1.0' op 13 oktober 2021 van Odido ontvangen. Uit de metadata van dit document bleek dat dit document is gemaakt en gewijzigd op 13 oktober 2021 om 18:03 uur.²⁹ Dit is door een medewerker van Odido bevestigd. 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 die konden worden verstrekt. Uit dit verslag volgt eveneens dat Odido heeft aangegeven dat er voorafgaand aan het opstellen van het beveiligingsplan alleen 'losse snippets' zouden hebben bestaan. Ook is aangegeven dat men bezig was met het vernieuwen van de policies en een nieuw systeem, zodat er meer zicht zou komen op de policies en het control framework. Door het verzoek van de RDI is dit naar voren gehaald, aldus de medewerker van Odido. Hieruit leid ik af dat met de 'losse snippets' zoals deze er zouden hebben gelegen iets anders wordt bedoeld dan het nog te ontwikkelen systeem dat zicht zou moeten bieden op de policies en dat nu lijkt te worden aangeduid met de term policy house.

Op basis hiervan stel ik vast dat er vanaf 13 oktober 2021 een document is dat volgens de stellingen van Odido een samenvoeging bevat van de 'losse snippets' en als document en dus in onderlinge samenhang kon worden ingezien. Ik heb Odido hier het voordeel van de twijfel gegeven en heb het bestaan van dit document welwillend beschouwd als een reden om de pleegperiode van het verwijt daar te laten eindigen. Als ik hier de door mij hierboven genoemde eisen toepas op de situatie voorafgaand aan 13 oktober 2021, waarbij uiteraard als logische startdatum 5 oktober 2021 geldt omdat het onderzoek door de RDI toen is aangevangen, dan was er geen sprake van een plan waarin de beveiligingsaspecten gestructureerd zijn weergegeven, met aandacht voor de wijze waarop uitvoering wordt gegeven aan de bescherming en beveiliging, laat staan waarbij een onderscheid wordt gemaakt in de verschillende beveiligingsregimes. Maar nog veel essentiëler, en dat is de kern van het verwijt dat Odido hier treft, is dat – voor zover deze stelling al juist zou zijn en er inderdaad losse snippets zouden hebben bestaan (Odido heeft dat immers niet kunnen onderbouwen) – een verzameling losse snippets die kennelijk niet kenbaar zijn als onderdeel van een geheel, geen startpunt kan zijn van een deugdelijke fysieke en logische beveiliging van LI-gegevens, simpelweg omdat intern niet afdoende duidelijk is gemaakt aan welke maatregelen Odido en de bij haar werkzame medewerkers zich moet houden, zoals overigens ook uit het verdere onderzoek is gebleken.

²⁹ RvB, p. 23.

Voor zover er is aangevoerd dat voor de RDI kenbaar had moeten zijn, of dit nu was door de omstandigheden rondom de uitvraag of door bevindingen uit eerdere inspecties in 2005 en 2016, dat er een ouder beveiligingsplan in een andere vorm bestond, merk ik opnieuw op dat ten tijde van het onderzoek (i) door de toezichthouder onomwonden is verzocht om de beveiligingsplannen aan te leveren en (ii) door Odido zelf is aangegeven dat er geen eerdere versie was die kon worden ingezien. Dat er nu wordt gesteld dat het beveiligingsplan onderdeel was van een policy house, wordt eveneens weersproken door de bevindingen rondom het onderzoek, waarbij werd gesteld dat er juist nog zou worden gewerkt aan een systeem dat meer zicht zou bieden op de policies en het control framework.

Voorts merk ik nog op dat het argument dat Odido mocht denken dat zij afdoende informatie had verstrekt, afketst op de volstrekke eenduidigheid van het verzoek van mijn toezichthouder om de beveiligingsplannen en de uitvraag die nadien is gedaan over de compleetheid van de informatie. Ik zie niet in hoe mijn toezichthouder nog duidelijker had kunnen zijn. Hierbij mag ook het een en ander van Odido worden verwacht, als deskundig marktdeelnemer, op zijn minst dat zij zelf nadenkt over de compleetheid van de documenten die zij aanlevert als zij hiertoe gevorderd wordt. Op Odido rust een inspanningsverplichting om aan de vordering van de toezichthouder te voldoen³⁰. Zou de vordering al enige onduidelijkheid in zich hebben gehad – let wel, dat blijkt nergens uit – dan lag het op de weg van Odido om daarover contact op te nemen. Zie in dit verband bijvoorbeeld de uitspraak van de voorzieningenrechter van de rechtbank Rotterdam d.d. 25 juli 2003³¹:

De voorzieningenrechter wenst nog het volgende op te merken. Verzoeksters hebben nadrukkelijk gesteld dat het bestreden besluit aan hen onvoldoende duidelijk maakt welke inlichtingen nu exact van hen wordt verlangd. Zo dit al het geval zou zijn dienen verzoeksters zich het volgende te realiseren. Zowel op basis van de Postwet als op basis van de Algemene wet bestuursrecht zijn verzoeksters verplicht aan verweerder dan wel aan diens (als toezichthouder) aangewezen ambtenaren inlichtingen te verstrekken voorzover dat redelijkerwijs voor de vervulling van verweerders taak nodig is. In het licht van die verplichting dienen verzoeksters, indien verweerder inlichtingen wenst te verkrijgen omtrent een specifiek deel van verzoeksters' activiteiten, aan verweerder die inlichtingen te verschaffen die verweerder in staat stellen voldoende nauwkeurig te omschrijven waaraan behoefte ontstaat. Weliswaar heeft in het kader van de voorprocedure leidend tot het bestreden besluit een van de verzoeksters verweerder bij schrijven van 22 april 2003 op het eerste gezicht vrij uitvoerig van inlichtingen voorzien, maar verweerder is daar, om de enkele reden dat verzoeksters niet de bij zijn schrijven van 1 april 2003 gevraagde stukken hadden overgelegd, niet op ingegaan. Hoewel dit laatste te betreuren valt blijft het op de weg van verzoeksters liggen om, indien en voorzover zij constateren dat verweerder bij zijn verzoek om inlichtingen kennelijk geen goed beeld heeft van de werkelijke situatie, verweerder hieromtrent te informeren en kunnen zij niet volstaan met de mededeling dat het verzoek onduidelijk is.

³⁰ De medewerkingsplicht heeft het karakter van een inspanningsverplichting. Zie bijvoorbeeld: ABRvS 17 februari 2016, ECLI:NL:RVS:2016:378.

³¹ ECLI:NL:RBROT:2003:AI0515

Anders dan Odido weet de toezichthouder bij een vordering niet welke informatie precies aanwezig is, laat staan in welke vorm. Als er beveiligingsplannen worden gevorderd, maar niet geleverd, kan Odido dus niet het verwijt maken dat er niet is gevraagd om 'snippets', waarvan ik het bestaan niet ken noch kan vermoeden.

Dat, zoals nu wordt betoogd, er in het document "20220218 svz T-Mobile opgevraagde doc-vragen-status" van de RDI een vinkje stond bij het actiepunt rondom de beveiligingsplannen, met de tekst "documentatie volledig" zie ik niet als een omstandigheid waaruit Odido kon afleiden dat er voldoende informatie was verstrekt. Dit is slechts de bevestiging van de omstandigheid dat er over en weer is begrepen dat de documentatie die is verstrekt alle documentatie betrof die er bestond. Ik beschouw dit als een extra feit dat bewijst dat er destijds – ondanks wat nu wordt gesteld – geen andere documenten beschikbaar waren. Voor Odido bestond een glasheldere verplichting om het beveiligingsplan aan te leveren. Deze verplichting kan niet jaren later worden omgedraaid door enkel te suggereren dat er meer was en dat de RDI maar moet bewijzen dat dit niet het geval was. Dit standpunt verdraagt zich niet met de medewerkingsplicht van artikel 5:20 van de Awb.

Daarnaast stond het Odido volkomen vrij om op welk moment dan ook in de procedure alsnog de stukken aan te leveren waarvan zij zo vurig betoogt dat de inhoud daarvan maakt dat de RDI tot radicaal andere inzichten zou zijn gekomen. Het argument dat dit nu niet meer kan worden aangeleverd omdat de LI-infrastructuur ingrijpend is gewijzigd overtuigt niet. Dit wekt immers de indruk dat een professionele partij als Odido niet aan document- en versiebeheer doet, wijzigingen niet administreert en geen systeemveranderingen bijhoudt. Als dit onaannemelijke scenario aan de orde zou zijn geweest, dan had er toch op zijn minst andere objectieve aanwijzingen voor de stelling moeten zijn in de vorm van bijvoorbeeld e-mails, managementrapportages, in- of externe audit-bevindingen, tickets of wijzigingsregistraties.

Van Odido mag worden verwacht dat zij naleving van wettelijke beveiligingsverplichtingen achteraf kan aantonen en de daarvoor relevante documentatie adequaat beheert en bewaart. Dit geldt te meer nu het gaat om informatie die in haar eigen ogen cruciaal is en waarover reeds met de toezichthouder was gecommuniceerd. Omdat Odido niet in staat is haar stelling te onderbouwen, komt dit voor haar rekening en risico.

Ik hou het er daarom voor dat de aanvullende informatie niet is verstrekt omdat deze simpelweg niet bestond voor 13 oktober 2021.

Ik ben van mening dat er afdoende bewijs is en daarom levert het voorgaande een overtreding op van artikel 3, eerste lid, van het Bbgt voor de periode van 5 oktober 2021 tot en met 12 oktober 2021.

7.2.2 Overtreding 2: beveiligingseisen ten aanzien van personeel

In het bestreden Besluit heb ik een boete opgelegd voor overtredingen van Bbgt-eisen die aan het personeel worden gesteld. Het betreft de volgende tekortkomingen:

- a. personeel dat niet was belast met verwerking van LI-gegevens had toegang tot de LI-gegevens (overtreding van artikel II, onder c, bijlage bij het Bbgt);
- b. er ontbraken VOG's (of VGB's) van personeel dat de medewerking verleent aan de uitvoering van taplasten (overtreding van artikel 4 van het Bbgt);
- c. er ontbraken functiebeschrijvingen van personeel belast met het verwerken van LI-gegevens (overtreding van artikel II, onder a, bijlage bij het Bbgt);
- d. er ontbraken toereikende geheimhoudingsverklaringen van personeel dat in aanraking komt met het verwerken van LI-gegevens (overtreding van artikel II, onder b, bijlage bij het Bbgt).

In de toelichting bij het Bbgt wordt in duidelijke bewoordingen uitgelegd dat het betrokken personeel mede voor de veiligheid van de staat verantwoordelijk is.³² Het is daarom in de eerste plaats van het grootste belang dat alleen bevoegde personen toegang hebben tot LI-gegevens. Odido dient daarom ook het overzicht te hebben van die geautoriseerde personen onder meer door een toereikende functie-beschrijving. Alleen met dit overzicht kan Odido alle betrokken personen het in het Bbgt bedoelde voorlichtingstraject laten volgen dat culmineert in een schriftelijke verklaring LI-gegevens geheim te houden.³³ Door deze personen dient ook een VOG te zijn verstrekt aan Odido (of een VGB te zijn afgegeven). Gedurende een lange periode heeft Odido onvoldoende maatregelen genomen tegen onbevoegde kennisname van LI-gegevens. Elk van deze maatregelen heeft het karakter van minimumnorm op het gebied van personeelsbeveiliging. Op aanbieders rust de resultaatsverplichting om in ieder geval deze minimumnormen in acht te nemen. Met de overtreding zijn daarmee het waarborgen van de veiligheid van de staat en de integriteit van strafrechtelijke onderzoeken, beide kernbelangen van het Bbgt, in het geding gekomen. Zoals ik al in het bestreden Besluit heb toegelicht is daarom elk van deze vier tekortkomingen ernstig.

7.2.2.1 Bredere beveiligingsbeeld

De stelling dat ik alleen tekortkomingen in mijn oordeel betrek en daarmee voorbijga aan het bredere beveiligingsbeeld kan ik, zoals toegelicht onder 7.1.3, niet volgen.

³² NvT bij het Bbgt, Stb. 2003, 472, p. 11 en 12.

³³ NvT bij het Bbgt, Stb. 2003, 472, p. 12.

7.2.2.2 VOG's

Op grond van artikel 4, tweede lid, van het Bbgt is Odido verplicht ervoor te zorgen dat de medewerking aan de uitvoering van taplasten alleen wordt verleend door personen die aan haar een verklaring omtrent het gedrag (VOG) hebben verstrekt. Ik heb vastgesteld dat Odido deze verplichting voor de vijf medewerkers [Vertrouwelijk] en [Vertrouwelijk] in ieder geval in de periode van 5 oktober 2021 tot en met 14 september 2022 heeft overtreden.

Odido bevestigt dat zij geen VOG's van de betrokken [Vertrouwelijk]-medewerkers in haar bezit had. Odido voert echter, in de kern weergegeven, aan dat artikel 8 van het Bbgt geen verplichting inhoudt voor een aanbieder om de VOG's van medewerkers die bij derden werkzaam zijn in zijn bezit te hebben. Ik onderschrijf dit standpunt niet.

De letterlijke tekst van artikel 4, tweede lid, van het Bbgt laat immers geen ruimte voor het standpunt van Odido. Het artikel luidt:

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.

De tekst schrijft voor dat de aanbieder alleen personen aan de LI-taak laat meewerken die aan hem, dat wil zeggen de aanbieder in de zin van de Tw (Odido), een VOG (of VGB) hebben verstrekt. Is de persoon werkzaam bij een derde, zoals [Vertrouwelijk] in dit geval, dan strekt artikel 8, eerste lid en onder c, van het Bbgt ertoe dat de aanbieder die derde verplicht het Bbgt – en dus ook artikel 4, tweede lid – na te leven. In het bestreden Besluit heb ik vastgesteld dat de [Vertrouwelijk]-medewerkers in kwestie ongelimiteerd toegang hadden tot LI-gegevens. Deze medewerkers waren bij Odido echter volledig buiten beeld. De verantwoordelijkheid om de VOG's in bezit te hebben, kan door Odido niet naar [Vertrouwelijk] worden doorgeschoven. Odido dient ervoor te zorgen dat de betreffende medewerkers, ook van haar leveranciers, over VOG's . De werkwijze die Odido kennelijk hanteert waarbij de VOG's van vijf [Vertrouwelijk]-medewerkers niet aan haar overgelegd zijn en dat Odido bovendien ook niet is nagegaan of de VOG's überhaupt bestonden, voldoet niet aan het Bbgt. Odido heeft de verplichting ervoor zorg te dragen dat de medewerking aan de uitvoering van taplasten uitsluitend wordt verleend door personen die over een VOG beschikken. Nu Odido niet over de betreffende VOG's beschikte en Odido zich er ook niet van heeft vergewist dat de desbetreffende medewerkers over een VOG beschikten, heeft Odido niet voldaan aan de verplichting uit artikel 4 van het Bbgt. In een recente uitspraak heeft de rechtbank hierover het volgende geoordeeld:

Ten aanzien van de negen medewerkers van Backoffice heeft [aanbieder 1] in de bezwaarfase verklaringen overgelegd met betrekking tot met een VOG vergelijkbare

Ons kenmerk
[Vertrouwelijk]

screening door de Roemeense autoriteiten. Uit de verklaringen van [aanbieder 1] volgt verder dat zij ten tijde van de periode in geding geen beschikking had over die verklaringen, terwijl dit in artikel 4, tweede lid van het Bbgt expliciet wel een vereiste is. Daaruit volgt immers dat de VOG moet zijn overgelegd aan de aanbieder voorafgaand aan de werkzaamheden. Met betrekking tot de medewerker van [naam bedrijf 3] heeft [aanbieder 1] de constatering van de staatssecretaris dat een VOG ontbrak verder niet betwist. Daarmee staat de overtreding van artikel 4, tweede lid, van het Bbgt ook vast ten aanzien van de tien genoemde medewerkers.³⁴

In het bestreden Besluit heb ik daarom ook terecht vastgesteld dat Odido hiermee artikel 4, tweede lid, van het Bbgt heeft overtreden. Het bestaan van de VOG's voor de medewerkers van [Vertrouwelijk] is voor mij wel een reden om de opgelegde boete te matigen. In paragraaf 7.2.2.6 licht ik dat nader toe.

Ten aanzien van de [Vertrouwelijk] betoogt Odido, zakelijk weergegeven, dat deze geen medewerking aan de uitvoering van taplasten verleent. Volgens Odido hoefde deze [Vertrouwelijk] daarom geen VOG over te leggen. Meer in het algemeen betoogt Odido dat ik toegang tot en beheer van het [Vertrouwelijk] ten onrechte aan de normen van het Bbgt zou hebben onderworpen. Aanduiding van systemen die niet louter LI-gegevens verwerken, zoals het [Vertrouwelijk], als "LI-systeem" zou de reikwijdte van het Bbgt tot een praktisch niet uitvoerbare situatie leiden. Ik volg dit standpunt niet.

Door Odido wordt niet weersproken dat het [Vertrouwelijk] LI-gegevens bevat en verwerkt. De aanwezigheid van LI-gegevens op een computersysteem en de verwerking daarvan is in wezen waarop ik het oog heb in het bestreden Besluit wanneer de term 'LI-systeem' wordt gebruikt. Dat het [Vertrouwelijk] ook andere functies heeft dan het uitvoeren van de LI-taak, doet dan ook niet ter zake. De term LI-systeem is daarmee slechts een manier om een verwijzing naar die functies korter op te schrijven en geenszins een onderdeel van de kwalificatie van de overtredingen. De vaststelling dat de feiten als overtredingen van het Bbgt kwalificeren, is door mij telkens aan de hand van de letterlijke tekst van de betrokken bepalingen gedaan.

Systemen als het [Vertrouwelijk] hebben netwerkbeheerders nodig om blijvend goed te functioneren. De toezichthouder heeft in het Rvb beschreven welke werkzaamheden een netwerkbeheerder uitvoert.³⁵ Beheerwerkzaamheden kunnen bestaan uit het verhelpen van eenvoudige verstoringen en het uitvoeren van kleine wijzigingen (eerstelijns beheer) tot het oplossen van complexe problemen en het aanbrengen van significante vernieuwingen (tweedelijns beheer). Deze beheerders zijn nodig om een systeem draaiende te houden en daarmee ook om duurzaam uitvoering te kunnen geven aan taplasten.

Uit het onderzoek van mijn toezichthouder is gebleken dat de [Vertrouwelijk] bedoelde toegang had tot LI-gegevens in onversleutelde vorm. Hij kon immers op

³⁴ Rb. Rotterdam, 8 mei 2026, ECLI:NL:RBROT:2026:5480, r.o. 16.11.

³⁵ Rvb, p. 21.

ieder relevant onderdeel van het [Vertrouwelijk] inloggen.³⁶ Deze bevoegde toegang hing samen met zijn onderhoud- en beheerwerkzaamheden voor het [Vertrouwelijk]. Uit dien hoofde had deze [Vertrouwelijk] dan ook de beschikking over de documentatie waarin het actuele beheerwachtwoord was opgenomen. Met dit beheerwachtwoord had hij toegang tot het account met de meest verstrekkende bevoegdheden en mogelijkheden binnen het betrokken systeem waaronder de mogelijkheid om LI-gegevens in te zien. Hiermee staat vast dat de [Vertrouwelijk] de medewerking verleende aan de uitvoering van taplasten: zonder deze [Vertrouwelijk] kon die medewerking immers niet steeds worden gegeven en de [Vertrouwelijk] kon bovendien bij LI-gegevens. Dat maakt dat de verplichting uit artikel 4 Bbgt van toepassing is. De [Vertrouwelijk] beschikte echter niet over een VOG. Om die reden kom ik tot de conclusie dat Odido daarmee artikel 4, tweede lid, van het Bbgt heeft overtreden.

Gegeven de grote maatschappelijke belangen, de noodzaak tot adequate beveiligingsmaatregelen en het gegeven dat het een feit van algemene bekendheid is dat een telecomnetwerk bestaat uit meerdere systemen en functionaliteiten, is de enge uitleg die Odido kennelijk voorstaat met betrekking tot het Bbgt onbegrijpelijk. Op grond van het Bbgt dient een digitaal systeem waarin LI-gegevens worden verwerkt te voldoen aan de vereisten die het Bbgt aan dergelijke systemen (en met name: de beveiliging van LI-gegevens) stelt.

Dat Odido in dat kader voorts verwijst naar het doel dat de wetgever voor ogen heeft gehad en dat daarbij rekening is gehouden met de uitvoerbaarheid kan ik 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:

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 minimumniveau 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.

Ik zie niet in hoe de eisen uit het Bbgt voor een professionele marktpartij met een omvang en organisatievorm als Odido praktisch niet uitvoerbaar zouden zijn. In feite zegt Odido dat het voor haar te veel gevraagd is om in kaart te brengen wie voor hun functie bij staatsgeheime informatie moet kunnen en om daar een passend screeningstraject voor te doorlopen. Dat vind ik een weinig overtuigende, maar bovendien zeer zorgwekkende stelling. Deze stelling komt mij bovendien vergezocht

³⁶ Rvb, p. 36.

voor aangezien een dergelijk signaal mij van Odido noch van haar twee grote concurrenten de afgelopen twintig jaar heeft bereikt.

Ons kenmerk
[Vertrouwelijk]

Odido stelt verder dat de rol van de [Vertrouwelijk] te vergelijken is met een beheerder van een gebouw waarvan één ruimte is ingericht als tapkamer. Beheer van het gebouw impliceert volgens Odido niet het meewerken aan uitvoering van taplasten. Deze vergelijking maakt mijn conclusie niet anders. Als de normen uit het Bbgt op deze analogie zouden worden toegepast, dan zou artikel III, sub g, van het Bbgt immers van toepassing zijn. Als de [Vertrouwelijk] onderhoud moet uitvoeren in de tapkamer, dan zal hij – kort gezegd – gescreend moeten zijn of worden begeleid door een gescreende medewerker.

7.2.2.3 Functiebeschrijvingen

Uit artikel II, onder a, van de bijlage bij het Bbgt volgt dat in de functieomschrijving van personeel dat belast is met de verwerking van LI-gegevens de verantwoordelijkheid voor de beveiliging van LI-gegevens moet zijn beschreven. In de toelichting bij het Bbgt is daarover onder meer het volgende opgemerkt:

Duidelijk dient te zijn dat de desbetreffende taak is toebedeeld aan een persoon en dat de taak tot zijn functie behoort.³⁷

Voor de aanbieder moet duidelijk zijn aan wie hij LI-taken heeft toebedeeld en deze personen dienen zich ervan bewust te zijn dat deze taak en bijbehorende verantwoordelijkheid tot hun functie behoort.

In het bestreden Besluit heb ik vastgesteld dat voor drie LI-medewerkers, [Vertrouwelijk] en vijf [Vertrouwelijk]-medewerkers geen functiebeschrijving met verantwoordelijkheid voor beveiliging van LI-gegevens beschikbaar was. Daarmee heeft Odido artikel II, onder a, van de bijlage bij het Bbgt overtreden.

Odido acht niet bewezen dat zij artikel II, sub a, van de bijlage bij het Bbgt voor de drie Odido-medewerkers heeft overtreden. Volgens Odido heeft zij bij haar zienswijze toereikende functieomschrijvingen overgelegd voor deze medewerkers. Anders dan Odido acht ik deze overtreding wel bewezen. Ik licht dat als volgt toe.

Zoals ik in het bestreden Besluit heb overwogen, heeft mijn toezichthouder bij de start van zijn onderzoek gevraagd naar de functiebeschrijving van medewerkers waarvoor Odido de artikelen 4, tweede lid, en II, onder a en b, van het Bbgt in acht moet nemen.³⁸ Dit geldt in ieder geval voor de genoemde drie Odido-medewerkers. Odido heeft daarop de arbeidsovereenkomsten van deze medewerkers overgelegd. Op 19 juli 2022 heeft de toezichthouder nogmaals onder meer de relevante functiebeschrijvingen opgevraagd van onder andere de drie Odido-medewerkers.³⁹ Daarop heeft Odido geen aanvullende informatie verstrekt. Uit de door Odido verstrekte arbeidsovereenkomsten van deze personen bleek geen functiebeschrijving met een verantwoordelijkheid voor een LI-taak. Van andere

³⁷ NvT bij het Bbgt, Stb. 2003, 472, p. 10.

³⁸ 20211005 F[AT] T[T-M] O[Aankondiging Inspectie Bevoegd Aftappen T-Mobile.msg].

³⁹ 20220719-TM-Vordering-BBGT-HR v1.0.

documentatie waaruit volgt dat er voor de betreffende personen een functiebeschrijving bestond, is mij niet gebleken. Uit de functiebeschrijvingen die Odido had overgelegd voordat ik het bestreden Besluit nam⁴⁰, blijkt niet dat de beschrijvingen ook daadwerkelijk voor de functies van de betrokken personen golden of dat zij bekend waren met deze functiebeschrijvingen. Deze functiebeschrijvingen zagen immers op andere functies dan de betrokken medewerkers volgens de verstrekte arbeidsovereenkomsten uitoefenden.

Volgens Odido kan de functiebeschrijving ook elders zijn opgenomen nu het Bbgt niet verplicht dat deze beschrijving in een arbeidsovereenkomst is opgenomen. Op zichzelf is het naar mijn oordeel juist dat de functiebeschrijving op grond van het Bbgt niet per definitie in een arbeidsovereenkomst moet zijn opgenomen. Daarom is de informatievordering van de toezichthouder vormneutraal (conform het Bbgt) geformuleerd. Odido heeft in reactie op dat neutraal geformuleerde verzoek evenwel de arbeidsovereenkomsten verstrekt. Om die reden is een beoordeling verricht van de verstrekte overeenkomsten. In dat licht moet de overweging in het bestreden Besluit dan ook worden gelezen. Uit de overgelegde arbeidsovereenkomsten volgt geen enkele verantwoordelijkheid voor de bescherming van LI-gegevens. In het bestreden Besluit heb ik dan ook terecht vastgesteld dat Odido artikel II, sub a, van de bijlage bij het Bbgt overtreden met betrekking tot de drie Odido-medewerkers.

Subsidiair voert Odido aan dat zij wel degelijk een specifieke LI-functiebeschrijving van de betreffende drie medewerkers had. Als bijlage bij het bezwaarschrift heeft zij voor twee van deze medewerkers een brief over hun functiewijziging bijgevoegd. Ook heeft zij een beschrijving van de functie 'Lawful Interception Specialist' gedeeld. De beoordeling van de nu pas aangevoerde informatie brengt mij tot de volgende constatering.

Odido heeft als bijlage 8 bij het bezwaarschrift twee brieven gevoegd waaruit blijkt dat [Vertrouwelijk] en [Vertrouwelijk] op respectievelijk 19 augustus 2014 en 24 maart 2015 nieuwe functies hebben gekregen. Dit betreft respectievelijk de functie [Vertrouwelijk] en [Vertrouwelijk]. Uit de beschrijvingen van beide functies in bijlage 3 en 7 bij het bezwaarschrift blijkt dat deze (mede) de beveiliging van LI-gegevens inhouden. Ik acht het aannemelijk dat [Vertrouwelijk] ook gedurende de pleegperiode de betreffende functie uitoefende, omdat Odido deze functie heeft genoemd in haar eigen overzicht dat zij aan de toezichthouder heeft verstrekt. Het bevreemdt mij dat Odido voor [Vertrouwelijk] in haar eigen overzicht een andere functietitel heeft opgegeven, namelijk [Vertrouwelijk].⁴¹ De wijze van het verstrekken van de betrokken documenten wekt de indruk dat bij Odido een goed overzicht op het gebied van personeelsbeveiliging ontbreekt. Op basis van de documenten kan ik echter niet buiten redelijke twijfel vaststellen dat voor de betreffende medewerker de functiebeschrijving van [Vertrouwelijk] niet gold. Ik kom daarom tot de conclusie dat de overtreding

⁴⁰ [Vertrouwelijk]

⁴¹ Rvb, p. 23 en TMNL - Overzicht medewerkers LI.pdf.

van artikel II, onder a, van de bijlage bij het Bbgt met betrekking tot de genoemde twee LI-medewerkers niet is bewezen.

Ons kenmerk
[Vertrouwelijk]

Voor [Vertrouwelijk] de derde Odido-medewerker, heeft Odido alleen een VGB aangeleverd. Ten aanzien hiervan stel ik vast dat een VGB geen functiebeschrijving bevat als bedoeld in artikel II, onder a, van de bijlage Bbgt. Ik constateer dat een relevante functiebeschrijving van welke aard dan ook voor [Vertrouwelijk] nog altijd niet is verstrekt door Odido. Het is dan ook voor mij niet duidelijk waarop Odido het oog heeft met de stellingen dat de 'beschikbare LI-functiebeschrijving' en 'formele aanstelling' zouden voldoen aan het Bbgt. Het enkele feit dat een persoon een VGB heeft verkregen, betekent niet dat zijn functie op een bepaalde manier is beschreven. Het verkrijgen van een VOG/VGB en de verplichting om een functiebeschrijving te hanteren, waarin beveiliging voor LI-gegevens tot de functie behoort, zijn niet voor niets van elkaar te onderscheiden normen in het Bbgt. Het argument dat het tijdsverloop tussen oktober 2021 en het indienen van het bezwaarschrift haar bewijspositie schaadt, kan ik in dit verband evenmin plaatsen. Ik heb Odido gedurende deze periode juist alle kansen geboden om de betreffende functiebeschrijving over te leggen. Mijn conclusie blijft dat Odido artikel II, sub a, van het Bbgt heeft overtreden vanwege het ontbreken van een functiebeschrijving voor de heer Beer.

Voor wat betreft de [Vertrouwelijk] voert Odido in wezen aan dat deze [Vertrouwelijk] geen toegang had tot LI-gegevens. Daarmee zou artikel II, sub a, van de bijlage bij het Bbgt toepassing missen. Ik heb in paragraaf 7.2.2.2 uiteengezet dat deze [Vertrouwelijk] wel degelijk bedoelde toegang heeft tot LI-gegevens. [Vertrouwelijk] was onmisbaar voor een bestendige uitvoering van taplasten. Ik verwijs verder naar die paragraaf voor de nadere motivering. Ik kom ook hier tot de conclusie dat de [Vertrouwelijk] wel degelijk met verwerking van LI-gegevens is belast, terwijl voor [Vertrouwelijk] geen toereikende functiebeschrijving bestond. Ik heb daarom in het bestreden Besluit terecht geoordeeld dat Odido artikel II, sub a, van het Bbgt voor wat betreft de [Vertrouwelijk] heeft overtreden.

Ten aanzien van de medewerkers van [Vertrouwelijk] voert Odido aan dat zij met de schematische weergave van bijlage 4 bij haar zienswijze, die zij ook in de pleegperiode in haar bezit had, heeft laten zien dat zij voldeed aan artikel II, sub a, van het Bbgt. Gelijk aan mijn oordeel over de functiebeschrijving van [Vertrouwelijk] acht ik ook de verstrekte documenten over de medewerkers van [Vertrouwelijk] niet afdoende. Ik licht dat als volgt toe.

De schematische weergave zoals Odido die heeft overgelegd tijdens de zienswijze beantwoordt niet aan het tweeledige doel dat artikel II, sub a, van de bijlage bij het Bbgt dient. Uit het schematische overzicht volgt immers niet dat de medewerkers verantwoordelijk waren voor de beveiliging van LI-gegevens. Het is van groot belang dat de medewerkers zelf zich ervan bewust zijn dat zij de verantwoordelijkheid hebben om LI-gegevens te beveiligen. Het schema biedt dat inzicht niet. Dat [Vertrouwelijk] zoals Odido stelt een bedrijf is dat zich toelegt op LI-dienstverlening doet hier niets aan af. Het Bbgt eist van Odido dat zij op persoonsniveau inzicht heeft in diegenen die voor haar LI-taken uitvoeren. zodat

Odido ook ten aanzien van de vijf ^[Vertrouwelijk]-medewerkers artikel II, sub a, van de **Ons kenmerk**
bijlage bij het Bbgt heeft overtreden. ^[Vertrouwelijk]

7.2.2.4 Geheimhoudingsverklaringen

In het bestreden Besluit heb ik vastgesteld dat drie Odido-medewerkers, vijf ^[Vertrouwelijk]-medewerkers en de ^[Vertrouwelijk] geen geheimhoudingsverklaring hebben ondertekend waarin geheimhouding van LI-gegevens wordt benoemd. Daarmee heeft Odido artikel II, onder b, van de bijlage bij het Bbgt overtreden.

Odido voert aan dat haar personeel een algemene geheimhoudingsverklaring heeft ondertekend. Daarmee zou zij voldoen aan artikel II, onder b, van de bijlage bij het Bbgt. De tekst noch de toelichting bij Bbgt ondersteunt het standpunt van Odido naar mijn oordeel. Ik licht dat als volgt toe.

Odido onderbouwt haar standpunt met verwijzingen die zien op de beveiligingsverplichting. In de toelichting op het Bbgt wordt de invulling van de beveiligings- en geheimhoudingsverplichting tot op zekere hoogte aan de aanbieder zelf overgelaten. De grenzen aan die eigen invulling blijken duidelijk uit de toelichting bij het Bbgt:

Deze zorgplicht kan op verschillende wijzen worden ingevuld. Een adequate voorlichting aan de betrokken personeelsleden waarbij zij worden doordrongen van het gevoelige karakter van de door hen te verrichten werkzaamheden alsmede van de gegevens en informatie waarvan zij in dat kader kennisnemen en de noodzaak ter zake geheimhouding te bewaren is daarbij een allereerste vereiste. In dat verband ware zeker te wijzen op de wettelijke geheimhoudingsverplichtingen die er bestaan; denk daarbij aan de artikelen 98 en 272 van het Wetboek van Strafrecht (schending van geheimen) en - waar het gaat om de veiligheid van de staat - artikel 85 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (een taplast strekt ter uitvoering van de in deze wet neergelegde taak voor de AIVD of MIVD en daarmee ter uitvoering van deze wet, waarvoor de aangescherpte geheimhoudingsverplichting ex artikel 85 geldt). Overigens geldt voor de werkgever, in casu de aanbieder, die een persoon wil belasten met een vertrouwensfunctie, op grond van artikel 4, tweede lid, Wvo de verplichting de betrokken persoon te informeren over de betekenis en de rechtsgevolgen van het feit dat deze voor een veiligheidsonderzoek wordt aangemeld; daartoe behoort op zijn minst ook een aanduiding van de redenen waarom in casu sprake is van een vertrouwensfunctie. Als sluitstuk van het voorlichtingstraject is het wenselijk om de betrokken personeelsleden een geheimhoudingsverklaring te laten ondertekenen. In de bijlage bij het besluit, onderdeel II, onder b, is laatstgenoemde maatregel voorgeschreven.⁴²

Zoals de andere in de bijlage bij het Bbgt genoemde normen heeft artikel II, onder b, van de bijlage bij het Bbgt het karakter van een minimumbeveiligingsnorm. De geheimhoudingsverklaring moet de status hebben van sluitstuk van het bewustwordingsproces over de geheimhoudingsverplichting. In dat proces dienen de LI-medewerkers bewust te worden gemaakt van het specifieke belang van het

42 Stb. 2003-472, Nota van Toelichting, p. 12.

beveiligen en geheimhouden van LI-gegevens. De strekking van artikel II, onder b, van de bijlage bij het Bbgt is dat de betrokken medewerkers zich vervolgens jegens de aanbieder schriftelijk verbinden om de LI-gegevens geheim te houden.

Odido heeft mij echter slechts verwezen naar algemene geheimhoudingsbepalingen in arbeidsovereenkomsten. Een geheimhoudingsverklaring als onderdeel van een arbeidsovereenkomst zonder enige verwijzing naar LI-gegevens voldoet niet aan de strekking van deze norm. Het bewijs dat Odido deze norm heeft geschonden is naar mijn oordeel daarom wel degelijk geleverd. Ik acht het voorts niet aannemelijk dat het in de toelichting beschreven bewustwordingsproces voorafgaand aan het ondertekenen van deze arbeidsovereenkomsten is voltooid. Deze arbeidsovereenkomsten zijn immers gesloten voor de functies '[Vertrouwelijk]', '[Vertrouwelijk]' en tweemaal voor een '[Vertrouwelijk]'.⁴³ Zoals ik in paragraaf 7.2.2.3 heb overwogen wordt in geen van deze overeenkomsten een – kort gezegd – LI-functie beschreven. Odido had deze medewerkers dus alsnog een geheimhoudingsovereenkomst waarin de geheimhouding van LI-gegevens moeten laten ondertekenen.

Odido geeft in haar bezwaarschrift wederom aan dat de vijf medewerkers van [Vertrouwelijk] en ook haar [Vertrouwelijk] slechts een algemene geheimhoudingsverklaring hebben getekend. Ten aanzien van deze algemene geheimhoudingsverklaringen trek ik dezelfde conclusie. Ook voor deze medewerkers dient een geheimhoudingsverklaring te worden getekend waarin de geheimhouding van LI-gegevens specifiek wordt verplicht. Naar mijn oordeel heeft Odido artikel II, onder b, van de bijlage bij het Bbgt overtreden (naast de drie Odido-medewerkers) ook met betrekking tot de vijf medewerkers van [Vertrouwelijk] en de [Vertrouwelijk].

7.2.2.5 Ongeautoriseerde toegang

In het bestreden Besluit heb ik vastgesteld dat 81 personen via een onjuiste configuratie van de LI-Firewall voor de verbinding tussen het [Vertrouwelijk]

LI-gegevens konden inzien. De LI-gegevens werden namelijk in onversleutelde vorm over de betrokken verbinding gezonden. Door het aanmaken van een zogenoemd PCAP-bestand konden deze personen LI-gegevens inzien. Deze personen hadden onbedoeld onbevoegd toegang tot LI-gegevens. Daarmee heeft Odido artikel II, onder c, van de bijlage bij het Bbgt overtreden.

Met bezwaargrond 6 voert Odido aan dat niet bewezen is dat onbevoegden toegang hadden tot LI-gegevens. Zij citeert daarbij pagina 66 van het bestreden Besluit over het effectueren van risico's die met beveiligingshiaten gepaard gaan. De strekking van deze zin is dat ik niet heb kunnen vaststellen of daadwerkelijk van de door Odido geboden mogelijkheid gebruik is gemaakt om LI-gegevens in te zien. Enkel het bieden van die toegangsmogelijkheid aan onbevoegden is echter de kern van de overtreding van artikel II, onder c, van de bijlage bij het Bbgt. Voor Odido geldt een resultaatsverplichting om te voorkomen dat personeel dat niet is belast met de

⁴³ [Vertrouwelijk]

verwerking van LI-gegevens toegang zou kunnen hebben tot deze gegevens. Nu is vastgesteld en ook door Odido is verklaard dat de 81 medewerkers een PCAP-bestand konden aanmaken die onversleutelde LI-gegevens zou bevatten, staat vast dat zij onbevoegde toegang hadden.⁴⁴

De stelling van Odido dat een misconfiguratie van haar LI-firewall niet gelijk zou staan aan het verschaffen van toegang aan de 81 onbevoegden onderschrijf ik niet. Het Bbgt verbiedt het *hebben* van toegang tot LI-gegevens door onbevoegden. De implicatie dat alleen het actief toegang verschaffen door Odido een overtreding zou opleveren strookt reeds daarom niet met de strekking van de betrokken norm. In wezen vloeit onbevoegde toegang altijd voort uit een verkeerde inschatting of omissie die teveel personen de mogelijkheid biedt om LI-gegevens te raadplegen, zonder dat daarbij beveiligingsbarrières doorbroken worden. Een andere uitleg zou de bepaling zinledig maken. In een recente uitspraak in een soortgelijke zaak overweegt de rechtbank Rotterdam hierover het volgende:

*De rechtbank is op grond van het volgende van oordeel dat de staatssecretaris toereikend heeft aangetoond dat 72 medewerkers van Backoffice onbevoegd toegang hadden tot LI-gegevens. Zoals ter zitting is bevestigd door [aanbieder 1], was er onbedoeld een mogelijkheid tot toegang tot LI-gegevens op een verbinding tussen het LI-IMS- en het [naam bedrijf 2] -systeem via een monitoring/SPAN-poort van netwerkswitches. Die enkele mogelijkheid is al in strijd met de op [aanbieder 1] rustende verplichting te waarborgen dat personeel dat niet belast is met de verwerking van LI-gegevens in geen geval toegang heeft tot LI-gegevens. Of medewerkers gebruik hebben gemaakt van die mogelijkheid of daartoe technisch in staat waren, is in dat verband niet relevant nu [aanbieder 1] erkent dat de theoretische mogelijkheid bestond dat personeel dat niet belast is met de verwerking van LI-gegevens toegang had tot LI-gegevens.*⁴⁵

De 81 personen hoefden geen beveiligingsmaatregel te doorbreken of omzeilen om een PCAP-bestand met LI-gegevens in te zien. Ten overvloede merk ik op dat het risico dat via het maken van een PCAP-bestand inzicht wordt verkregen in LI-gegevens geenszins (zuiver) theoretisch is. De 81 personen zijn allen gebruikers van een [Vertrouwelijk].⁴⁶ Het aanmaken van een PCAP-bestand is een eenvoudige handeling die normaliter wordt gedaan om netwerkstoringen te diagnosticeren en op te lossen. Het aanmaken van een PCAP-bestand is daarmee onderdeel van het "standaardgereedschap" van een netwerkbeheerder. Ik acht de overtreding van artikel II, onder c, van de bijlage bij het Bbgt ook voor de 81 personen via de LI-firewall wel degelijk bewezen.

Ten slotte bestrijd ik de stelling van Odido dat de toegang het gevolg is van een enkele misconfiguratie. Odido heeft hiermee bij de vormgeving van haar systemen zelf de omstandigheden gecreëerd waaronder fouten snel gemaakt worden. Juist hier had naleving van een beveiligingsplan, met daarin een periodieke herevaluatie,

⁴⁴ [Vertrouwelijk]

⁴⁵ Rb. Rotterdam, 8 mei 2026, ECLI:NL:RBROT:2026:5480, r.o. 16.9.

⁴⁶ [Vertrouwelijk]

veel beveiligingsomissies kunnen voorkomen. Deze planmatige aanpak ontbreekt echter. Ik licht dat als volgt toe.

Ons kenmerk
[Vertrouwelijk]

De verbinding tussen het [Vertrouwelijk]-systeem en de [Vertrouwelijk] van Odido was tien jaar voorafgaand aan het onderzoek, sinds de ingebruikname van de [Vertrouwelijk], onversleuteld in bedrijf. Pas gedurende het onderzoek van de toezichthouders heeft Odido aanleiding gezien om de beveiliging van deze verbinding te herbeoordelen. Uit het onderzoek van de toezichthouder blijkt dat de LI-Firewall twee dagen voorafgaand aan een inspectie in is geplaatst als voorbereiding voor die inspectie. Odido heeft hierover namelijk het volgende verklaard:

Twee dagen voor de meeting tussen TM en AT op 16 december heeft TM een wijziging in het LI netwerk aangebracht door een firewall te plaatsen waarop versleuteling tussen de [Vertrouwelijk] systemen en de [Vertrouwelijk] (X1, X2 en X3) is geconfigureerd. TM geeft aan dat deze plaatsing van de Firewall tot stand is gekomen door een interne pre-audit alvorens de komst van de geplande sessie met AT. 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 implementatie van de [Vertrouwelijk] aansluiting op de [Vertrouwelijk].⁴⁷

Het is dit gebrek aan een planmatige aanpak bij de installatie van de firewall die heeft geresulteerd in onbevoegde toegang voor 81 personen. Vervolgens heeft Odido de firewall moeten uitschakelen vanwege het gebrek aan stabiliteit op de nieuwe versleutelde verbinding. Deze omstandigheden rechtvaardigen in het geheel de bestempeling van de gang van zaken als misconfiguratie niet.

7.2.2.6 Betwisting evenredigheid boete overtreding 2

Subsidiair aan haar bewijsverweren voert Odido ook een grond aan tegen de evenredigheid van de opgelegde boete. Volgens Odido moet in haar voordeel meewegen dat de VOG's van de [Vertrouwelijk]-medewerkers wel bestonden, ook al waren deze niet bij Odido in bezit. Hetzelfde geldt voor de aangeleverde functieomschrijvingen.

Anders dan Odido betoogt, acht ik de opgelegde boete geenszins onevenredig hoog. Odido heeft gedurende een lange periode – in ieder geval van 5 oktober 2021 tot 14 september 2022⁴⁸ – alle Bbgt-normen met betrekking tot het personeel overtreden. Mijn toezichthouder heeft namelijk vastgesteld dat Odido vier overtredingen van de minimumvereisten uit het Bbgt heeft begaan. Daarmee heeft Odido niet voldaan aan haar plicht om de buitengewoon gevoelige gegevens, waaronder formele staatsgeheimen, te beschermen tegen kennisname door onbevoegden. Het belang van bescherming van staatsgeheimen vergt nu juist dat de beveiliging op elk punt in ieder geval het minimumniveau heeft. Deze

⁴⁷ [Vertrouwelijk]

⁴⁸ 1 november 2021 tot 14 februari 2022 voor wat betreft de overtreding van artikel II, onder c, van de bijlage bij het Bbgt.

overtredingen heb ik in één hoofdovertreding vervat waarvoor één boete is opgelegd. Deze overtredingen zien op alle personeelsonderdelen van het Bbgt en op personeel met toegang tot meerdere LI-systemen.

Voor wat betreft de VOG's van de medewerkers van ^[Vertrouwelijk] heb ik al uiteengezet dat Odido artikel 4, tweede lid, van het Bbgt heeft overtreden. Ik heb daarbij ook het belang van de juiste naleving van deze norm benadrukt. Ik erken evenwel dat de door het Bbgt te dienen belangen door Odido in mindere mate zijn geschonden dan in het geval de VOG's in het geheel niet zou zijn afgegeven. Hoewel de VOG's (en dus de betrouwbaarheid van deze medewerkers) niet bij Odido bekend was, bleken de medewerkers van ^[Vertrouwelijk] wel 'gescreend' te zijn. Hierdoor ging van hen een geringer risico op kennisneming van LI-gegevens door kwaadwillenden uit dan geheel ongescreende medewerkers. Nu ik de overtreding bewezen acht, maar Odido met deze overtreding het beveiligingsbelang in beperktere mate schendt, zie ik grond voor een beperkte boetematiging met € 50.000.

Odido voert aan dat ik in mijn boetevoornemen een groter aantal medewerkers onder de overtreding van artikel II, onder c, bij de bijlage van het Bbgt heb geschaard dan in het bestreden Besluit. Ook nu achteraf is gebleken dat twee functiebeschrijvingen voldoen, acht Odido deze omstandigheid eveneens grond voor boetematiging. Ik kom niet tot dat oordeel.

Zoals ik met betrekking tot de gronden tegen de functiebeschrijvingsverplichting heb overwogen, heeft Odido deze verplichting in ieder geval overtreden met betrekking tot één van haar LI-medewerkers, de ^[Vertrouwelijk] en de vijf medewerkers van ^[Vertrouwelijk]. Deze overtreding heb ik voor de boetetoemeting samengevoegd met de andere overtredingen op personeelsgebied. De aard en ernst van dit samenstel aan overtredingen wordt bepaald door de kans dat de zeer gevoelige LI-gegevens door onbevoegden of kwaadwillenden worden ingezien. Voor een substantieel aantal medewerkers heeft Odido niet aan haar verplichtingen op grond van het Bbgt voldaan. Daaruit blijkt dat de overtredingen structurele systeemfouten zijn die geen incidenteel karakter hadden. De ernst van de overtreding wordt niet verminderd door een afdoende functiebeschrijving van twee LI-medewerkers. De boetetoemeting is tenslotte ook geen mathematische afweging waarbij een berekening per medewerker in een bepaald boetebedrag resulteert. Daarbij heb ik één boete voor alle overtredingen van de eisen voor personeelsbeveiliging opgelegd. Het (grote) aantal medewerkers dat hetzij onbevoegde toegang had of voor wie de personeelsbeveiligingsnormen niet in acht waren genomen is voor mij ook geen aanleiding geweest om de basisboete in dit geval te verhogen. Omgekeerd zie dan ook geen reden voor verlaging.

Odido voert verder aan dat ik het bredere beveiligingsbeeld in de vorm van het bestaan van VGB's niet heb meegewogen. Ik weerspreek die stelling. Het bredere beveiligingsbeeld is, zoals ik al eerder heb overwogen, dat Odido elke norm met betrekking tot de personeelsbeveiliging heeft overtreden. Ik overweeg verder dat gedeeltelijke naleving van artikel 4, tweede lid, van het Bbgt voor de drie LI-medewerkers niet betekent dat andere overtredingen minder ernstig zouden zijn. De overige overtredingen schenden de veiligheid van de staat in dezelfde mate. Zo levert de afwezigheid van een toereikende geheimhoudingsverklaring ook bij een

medewerker aan wie een VGB is verstrekt nog steeds hetzelfde risico op het prijsgeven van staatsgeheimen op. Daarbij komt dat Odido deze norm ten aanzien van de [Vertrouwelijk] en [Vertrouwelijk]-medewerkers wel heeft overtreden, zodat ook niet vooraf gescreende personen van LI-gegevens kennis konden krijgen. Dat Odido aanvoert dat zij wel een goed beeld had van de personele beveiliging onderschrijf ik niet. Odido had voor slechts een deel van de personen die een LI-taak een screeningsdocument in de vorm van een VGB in haar bezit. Deze omstandigheid bewijst het tegendeel van hetgeen Odido stelt: er waren medewerkers die Odido niet in beeld had. Zij had bijvoorbeeld geen zicht op het feit dat de werkzaamheden van de [Vertrouwelijk] binnen de reikwijdte van het Bbgt lagen. Odido had voor [Vertrouwelijk] geen screeningonderzoek laten plaatsvinden. Het bestaan van de VGB's voor de LI-medewerkers heb ik dan ook terecht niet als boetematigingsgrond gekwalificeerd.

7.2.3 Betwisting evenredigheid en opslagen boete overtreding 3

Overtredinggroep 3 ziet op de tekortkomingen met betrekking tot de toegangsbeveiliging van geautomatiseerde informatiesystemen (artikel V van de bijlage bij het Bbgt).

- Op twee systemen was geen sprake van een deugdelijke beveiliging, onder meer doordat persoonsgebonden authenticatie ontbrak en gebruik werd gemaakt van (oude) standaardwachtwoorden.
- Op twee systemen was geen blokkering van kracht bij overschrijding van drie foutieve inlogpogingen.
- Op twee systemen was geen centrale logging en detectie geactiveerd.
- Handelingen met betrekking tot de verwerking van de LI-gegevens werden niet persoonsgebonden vastgelegd om onderzoek mogelijk te maken.

U heeft geen inhoudelijke gronden aangevoerd tegen bovenstaande tekortkomingen.

Vastgesteld en onbetwist is dat de toegangsbeveiliging van geautomatiseerde informatiesystemen waarin LI-gegevens worden verwerkt onvoldoende was gedurende de periode van in ieder geval 17 december 2012 tot 7 februari 2022. Hiervoor hanteer ik een basisboetebedrag van € 450.000,-.

Ik heb het basisboetebedrag van € 450.000,- met 25% verhoogd 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] op 17 december 2012 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 heb ik dit basisboetebedrag van € 450.000,- nogmaals met 25% verhoogd vanwege de verhoogde verwijtbaarheid. Ik reken het Odido zwaar aan dat zij weloverwogen – en zelfs nadat door de leverancier zelf versleuteling werd aangeraden – 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. Odido heeft op 14 december 2021, enkele dagen voor de aangekondigde inspectie, een vergeefse poging gedaan tot het wegnemen van het risico van deze inadequate beveiliging door met spoed een 'firewall' te plaatsen. Echter, door een misconfiguratie van deze 'firewall' hebben nog eens 81 personen tijdelijk toegang gekregen tot de LI-gegevens.

Ik heb in totaal aan Odido voor deze overtredingsgroep een bestuurlijke boete opgelegd van € 675.000,-.

Hieronder reageer ik op de door Odido ingenomen standpunten, zoals weergegeven onder 4.4, ten aanzien van hoogte van de boete van de overtredingsgroep 3, waarbij ik de argumenten die meermaals worden aangevoerd zo goed mogelijk probeer te clusteren onder de hieronder opgenomen subgronden. Ik volg Odido niet in het standpunt dat boeteoplegging niet passend, geboden en (daardoor) evenredig is. Daartoe overweeg ik het volgende.

Effectuering risico's en boeteverhoging 1

In reactie op het verweer van Odido dat niet is vastgesteld dat er gevolgen zijn waargenomen of de gesignaleerde risico's zijn geëffectueerd en dat dit een grond zou zijn voor boetematiging, of het achterwege blijven van boeteverhoging 1, blijf ik bij mijn eerdere overwegingen in mijn bestreden Besluit, met de navolgende aanvullingen.

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 detectiemaatregelen. 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 voert in het bezwaar aan dat er forensisch onderzoek uitgevoerd had kunnen worden door de RDI en dat de RDI ervoor heeft gekozen om dit niet te doen. Dit snijdt echter geen hout. Forensisch onderzoek had namelijk – voor zover het al mogelijk was om dit technisch uit te voeren op een systeem dat al vele jaren draait, waardoor veruit het grootste deel van de data niet valt terug te halen – hooguit

kunnen opleveren dat er via een root-account (dus niet-persoonsgebonden) toegang is verkregen tot LI-gegevens. Maar, nu de root-account werd gebruikt door eenieder die wilde inloggen (een andere manier was er immers niet) zegt dit nog niks. De informatie wordt immers pas echt relevant als je kan achterhalen wie het root-account heeft gebruikt. De vraag of dit een medewerker was van Odido, en zo ja welke medewerker, of een externe partij of persoon met kwade intenties kan daarmee nog niet worden beantwoord. Waar forensisch onderzoek dus in de meest positieve situatie enigszins had kunnen compenseren voor Odido's gebrek aan logging, had het nooit kunnen compenseren voor het gebrek aan persoonsgebonden registratie. Het is tekenend voor de ernstige omissies aan de zijde van Odido dat zelfs forensisch onderzoek nooit uitsluitsel had kunnen geven over de vraag of en zo ja door wie er een inbreuk is gemaakt en welke gegevens zijn geraadpleegd. Het enige dat met zekerheid gezegd kan worden is dat we nooit zullen weten of er sprake is geweest van een inbreuk. Dit is een pijnlijke constatering als het gaat om staatsgeheime informatie en dit bepaalt (mede) de ernst van de overtreding. Het achterwege blijven van forensisch onderzoek kan dus niet door Odido worden aangevoerd als argument 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.

Daarbij merk ik verder op dat de zaak waarnaar Odido verwijst⁴⁹ 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 haar aanvulling op het bezwaar, ik heb kunnen *vaststellen* dat de risico's zich niet geëffectueerd hebben vanwege getroffen mitigerende maatregelen. 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. Nu er in die zaak daarnaast ook nog sprake was van andere zaakspecifieke verzachtende omstandigheden, zoals pseudonimisering van de gegevens, worden hier de spreekwoordelijke appels met

⁴⁹ [Vertrouwelijk]

peren vergeleken en zie ik in Odido's verwijzing naar deze zaak geen aanleiding om in de onderhavige zaak tot een ander oordeel te komen.

Ons kenmerk
[Vertrouwelijk]

Voor zover Odido ook in dit kader heeft aangevoerd dat de LI-gegevens (via de [Vertrouwelijk]) toegankelijk waren via de SSH-ingang, die aldus Odido in de praktijk nooit werd gebruikt, omdat de gebruikers altijd inlogden via een *Graphical User Interface* (GUI) waarbij die gegevens niet toegankelijk waren (en dit niet tot een verhoging van de boete zou moeten leiden), permiteer in mij een analogie. Als de GUI wordt gezien als een voordeur, en de SSH-ingang als een achterdeur, dan is het voor de vraag of er toegang te verkrijgen valt tot de woning niet relevant of de welwillende bezoekers altijd de voordeur gebruiken, als de achterdeur al die tijd open staat voor eenieder met kwade intenties. Het komt erop neer dat toegang tot de woning met daarin de LI-gegevens dus altijd mogelijk is voor eenieder met enige kennis van zaken. Ik zie niet in hoe dit boetematigend zou moeten werken.

'Zelfstandige beëindiging' en bredere beveiligingsbeeld

Odido betoogt dat de boete dient te worden gematigd nu uit vaste jurisprudentie volgt dat het zelfstandig beëindigen van een overtreding een boetematigende omstandigheid is.⁵⁰ Vooropgesteld dient te worden dat van zelfstandige beëindiging geen sprake kan zijn nu er pas ná de interventie van de toezichthouder is ingegrepen. Als Odido de geconstateerde overtredingen na afloop van de periode waar de overtredingen op zien heeft beëindigd – waarbij ik dit standpunt van Odido even voor waar aanneem – dan zie ik hierin bereidwilligheid om aan de geldende regelgeving te gaan voldoen en weeg ik dit conform de lijn in de jurisprudentie mee bij de bepaling van de boetehoogte. Hierbij ken ik echter doorslaggevend gewicht toe aan andere omstandigheden, te weten de ernst en de verwijtbaarheid van de geconstateerde overtredingen. Dat er na afloop van de overtredingen herstelmaatregelen worden getroffen zie ik niet als een boetematigende omstandigheid, maar als een gepaste reactie op het overtreden van de wet: het herstel is niets meer dan wat reeds jarenlang op grond van de wet van Odido werd verwacht. Als ik dit weeg tegen de ernst en de verwijtbaarheid van de geconstateerde overtreding, dan maken de laatstgenoemde factoren maken dat ik geen aanleiding zie om de boete te verlagen. Ook zie ik hierom geen aanleiding om te volstaan met een aanwijzing of met een waarschuwing, zoals door Odido ook in dit verband is aangevoerd, ook niet in verbinding met de overige door Odido daartoe aangevoerde argumenten.

Odido betoogt dat de RDI zich uitsluitend heeft gericht op vermeende tekortkomingen in specifieke beveiligingsmaatregelen, zonder het bredere beveiligingsbeeld in ogenschouw te nemen. Hier heb ik onder 7.1.3 al op gereageerd, gelet waarop ik op dit punt zal volstaan met een verwijzing naar die overweging.

Odido betwist dat de door mij geschetste omstandigheden een verhoging van de basisboete voor overtreding 3 rechtvaardigen op basis van de argumenten zoals uiteengezet onder 4.4.

⁵⁰ Odido verwijst hierbij naar ECLI:NL:RBDHA:2021:3090 (*HagaZiekenhuis*).

Ik volg Odido hierin niet. 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.

De toezichthouder heeft immers vastgesteld dat de X1-, X2- en X3-verbindingen⁵¹ 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 voorts de "[Vertrouwelijk]
" van Odido ontvangen.⁵² 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)"*⁵³

Van deze verplichtingen ziet verplichting nummer 8 uit het [Vertrouwelijk] 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."*⁵⁴

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]

Het is algemeen bekend dat informatiestromen versleuteld dienen te zijn.⁵⁵ Dat geldt tegenwoordig als *good practice* voor iedere informatiestroom, zelfs voor bijvoorbeeld online winkelen of het raadplegen van nieuwsberichten, maar is

⁵¹ 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.

⁵² Rvb, p. 27.

⁵³ Rvb, p. 27.

⁵⁴ Rvb, p. 28.

⁵⁵ Zie bijvoorbeeld de ICT-Beveiligingsrichtlijnen Webapplicaties van het Nationaal Cybersecurity Center uit 2012 en 2015, beveiligingsmaatregel U/WA.05.

absoluut essentieel 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.

Het voorgaande toont al dat de optimale manier om staatsgeheime gegevens te beschermen tegen ongeautoriseerde toegang ligt in het versleutelen van die gegevens. Het achterwege blijven hiervan is niet iets dat kan worden gemitigeerd door te verwijzen naar de zeldzaamheid van het scenario dat het iemand zou lukken om de kabels te lokaliseren en af te tappen. Het beperken van de toegang (via fysieke toegangscontrole of cameratoezicht) is ook geen adequate wijze om gegevens te beschermen en het ontbreken van versleuteling te compenseren.

Ten overvloede merk ik nog op dat ik de mogelijkheid van aftappen, anders dan Odido, niet als uiterst hypothetisch en vergezocht zie. 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. Er kan op iedere plaats data op fysiek niveau getapt worden uit deze kabels, binnen en buiten de datacenters. Netbeheerders, leveranciers en ongetwijfeld nog andere personen kunnen op verschillende momenten toegang hebben tot verschillende onderdelen van het netwerk en de bekabeling.

De informatie over de ligging van de kabels is daarbij deels openbaar toegankelijke informatie, die via het Kadaster te raadplegen is. Beheerders van deze kabels zijn op grond van artikel 11 van de Wet informatie-uitwisseling ondergrondse en bovengrondse netten en netwerken gehouden deze informatie te verstrekken aan eenieder die een graafmelding of oriëntatieverzoek doet. Daarbij wordt ook aangegeven wie de netbeheerder van de betreffende kabel is. Dat vormt dus een concreet eerste aanknopingspunt, waarna met enige zoekslagen de betreffende kabels te achterhalen zijn. Hierbij merk ik op dat het Bbgt niet alleen bedoeld is om bescherming te bieden aan een willekeurige gelegenheidsovertreder, maar in het bijzonder is opgesteld met het oog op statelijke actoren of georganiseerde misdaad en kwaadwillenden, met bijbehorende kennis en middelen. Meer subsidiair overweeg ik dat er naast fysieke aanvallen op de netwerkkabels ook andere mogelijkheden zijn om tot de onversleutelde LI-gegevens te komen. Zo kunnen ook netbeheerders, leveranciers of ander (onderhouds)personeel die een legitieme reden hebben om te werken aan of bij de genoemde verbindingen een zwakke schakel vormen bij het voorkomen van toegang tot de dataverbindingen. Ik geef hiervan een voorbeeld. Als er een storing optreedt in het netwerkverkeer, dan is het maken van een verkeersanalyse een logische eerste stap die een beheerder zet om tot een oplossing te komen. Dit kan bijvoorbeeld door het aanmaken van een PCAP-file. Als dit gebeurt, dan zou dit bestand ook het netwerkverkeer met onversleutelde informatie kunnen bevatten. Hoe wordt deze data in een dergelijk geval beschermd? Het is hierbij voor Odido onmogelijk om dit scenario, maar ook andere scenario's die minder voor de hand liggen maar wel kunnen worden bedacht door (statelijke) actoren met aanzienlijke middelen, af te dekken.

Odido heeft 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.

Ons kenmerk
[Vertrouwelijk]

7.2.3.5 Vervangen aftapsysteem

Dat Odido op last van de overheid het aftapsysteem heeft moeten vervangen, doet aan bovenstaande niets af. Deze procedure staat los van de verwijten die in dit besluit voorliggen en kan en zal hierin niet worden betrokken. Doordat deze zaken los van elkaar moeten worden gezien, heeft de uitkomst van deze zaak geen invloed op de evenredigheid van de boete.

7.3 Conclusie

Ik ben bevoegd om handhavend op te treden, door een bestuurlijke boete op te leggen. Dit volgt uit artikel 15.4 van de Tw.

Op basis van zorgvuldig en deugdelijk onderzoek is vastgesteld dat Odido onvoldoende maatregelen heeft getroffen om ongeoorloofde toegang tot LI-gegevens te voorkomen. Over de gehele linie schoten de door Odido in dezen getroffen maatregelen tekort, met alle mogelijke risico's van dien. Odido heeft aldus het Bbgt overtreden. Voor deze overtredingen heb ik dan ook terecht een bestuurlijke boete opgelegd.

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 hoofdovertradingen:

- I. Vastgesteld is dat Odido in het geheel niet beschikte over een beveiligingsplan (artikel 3 van het Bbgt);
- II. Vastgesteld is dat de beveiligingseisen van Odido ten aanzien van het personeel onvoldoende waren (artikel 4 van het Bbgt en artikel II van de bijlage bij het Bbgt);
- III. Vastgesteld is dat de toegangsbeveiliging van geautomatiseerde informatiesystemen waarin LI-gegevens worden verwerkt onvoldoende was (artikel V van de bijlage bij het Bbgt).

Per hoofdovertrading heb ik een bestuurlijke boete opgelegd, waarbij ik een basisbedrag van € 450.000,- als uitgangspunt heb gehanteerd. Voor overtreding I heb ik gelet op het feit dat een beveiligingsplan bij Odido in het geheel ontbrak, terecht besloten 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,-. Voor overtreding III heb ik het basisbedrag tweemaal met 25% verhoogd vanwege de verhoogde ernst van de overtreding en de verhoogde mate waarin de overtreding aan Odido te verwijten is.

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, heb ik besloten om

de bestuurlijke boete met 10% te matigen tot € 1.518.750,-.

Ons kenmerk
[Vertrouwelijk]

In mijn heroverweging heb ik geoordeeld dat het bestaan van de VOG's voor de medewerkers van ^[Vertrouwelijk] een matiging van de bestuurlijke boete met € 50.000,- rechtvaardigt. Daarmee bedraagt de cumulatieve boete € 1.468.750,-.

Gezien de belangen die gemoeid zijn met de beveiliging van LI-gegevens en de risico's die zich als gevolg van de geconstateerde overtredingen hebben voorgedaan acht ik de boetes niet alleen afzonderlijk, maar ook in samenhang bezien, alleszins evenredig.

7.3.1 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 € 1.468.750,- voor de vastgestelde overtredingen op te leggen. Dit bedrag acht ik passend en geboden.

8. Beslissing op bezwaar

Gelet op het bovenstaande verklaar ik uw bezwaar gedeeltelijk gegrond. Het bestreden Besluit blijft in stand, met dien verstande dat ik de opgelegde bestuurlijke boete matig tot € 1.468.750,-.

9. Beroep

Indien Odido zich niet met deze beslissing kan verenigen, kunt u binnen zes weken na de datum waarop deze beschikking aan u is verzonden beroep instellen. Het beroepschrift moet worden gericht aan de rechtbank te Rotterdam, Sector bestuursrecht, Postbus 50951, 3007 BM ROTTERDAM.

Hoogachtend,

De Staatssecretaris van Economische Zaken - Digitale Economie & Soevereiniteit,
namens deze, ^[Vertrouwelijk]

mr. S.P. Janssen
plv. Teammanager Juridische Zaken
Rijksinspectie Digitale Infrastructuur