Auditdienst Rijk
Ministerie van Financiën

Rapport van bevindingen
Feitenonderzoek eMates

Definitief

Colofon

Titel	Feitenonderzoek eMates
Uitgebracht aan	Ministerie van Justitie en Veiligheid
Datum	26 januari 2023
Kenmerk	2023-00000180031
Referentienummer	2022-JenV-026

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

De berichtenservice eMates (voorheen Emailaprisoner) verzorgt digitaal berichtenverkeer tussen gedetineerden en hun familie, vrienden en andere sociale en zakelijke relaties. eMates is een externe partij zonder formele, schriftelijke overeenkomst met de Dienst Justitiële Inrichtingen (DJI). DJI faciliteert dit digitale berichtenverkeer (hierna berichten-service) sinds het besluit van het MT-Gevangeniswezen in 2014. Begin maart 2022 heeft DJI van het Openbaar Ministerie (OM) een brief ontvangen waarin zij haar zorgen over de beveiliging omtrent eMates beschrijft. Als reactie hierop heeft DJI besloten het gebruik van eMates per direct op te schorten. Er diende eerst een onderzoek uitgevoerd te worden naar de inrichting en de beheersing van eMates alvorens er besloten werd of de berichtenservice gecontinueerd kon worden. Daarnaast ontstond de vraag hoe de huidige situatie met eMates heeft kunnen ontstaan.

Het ministerie van Justitie en Veiligheid - meer specifiek de plaatsvervangend secretaris-generaal (pSG) – heeft de Auditdienst Rijk (ADR) verzocht dit onderzoek uit te voeren.

1.2 Doelstelling en onderzoeksvraag

De doelstelling van het ADR-onderzoek is tweeledig: 1) *het verschaffen van inzicht in de inrichting en beheersing van de informatiebeveiliging van de berichtenservice eMates* en 2) *het verschaffen van inzicht hoe de huidige situatie rond eMates vanaf 2012 heeft kunnen ontstaan*. Uiteindelijk dient de opdrachtgever met deze informatie te kunnen beoordelen of er een probleem is met de wijze waarop de samenwerking met eMates tot stand is gekomen en hoe eMates wordt gebruikt.

Daarbij staan de volgende twee onderzoeksvragen centraal:

1. Welke beheersmaatregelen zijn door DJI en de dienstverlener[1] getroffen voor het inrichten en beheersen van de informatiebeveiliging van de berichtenservice[2] eMates conform een door DJI geselecteerd aantal normen[3] uit de baseline informatiebeveiliging overheid (BIO)?
2. Op welke wijze is de berichtenservice eMates ingevoerd en in gebruik genomen bij de verschillende penitentiaire inrichtingen, en wat was de betrokkenheid van de beleidsdirecties van het ministerie van Justitie en Veiligheid en uitvoeringsorganisatie DJI hierbij?

1.3 Afbakening

Voor onderzoekvraag 1 is het object van onderzoek de inrichting en beheersing van de informatiebeveiliging van de berichtenservice door DJI en de dienstverlener. Hierbij wordt gebruik gemaakt van het met de opdrachtgever overeengekomen referentiekader, i.c. een selectie van toepasselijke normen uit de baseline informatiebeveiliging overheid (BIO). Het onderzoek beperkt zich tot het in opzet en bestaan aantoonbaar inzichtelijk maken van het functioneren van de beheersmaatregelen t.a.v. de informatiebeveiliging van de berichtenservice. De technische afbakening van het object betreft de applicatie eMates, de servers waarop deze applicatie draait en de infrastructuur van deze servers.

Voor de beantwoording van deze onderzoeksvraag is uitgegaan van de beschikbaar gestelde informatie van DJI en van de dienstverlener en leverancier van de

[1] *De dienstverlener betreft het bedrijf eMates.*
[2] *De berichtenservice betreft de service eMates zoals aangeboden door de dienstverlener.*
[3] *Het referentiekader met gehanteerde normen is te vinden in bijlage 1.*

berichtenservice, eMates en Unilink. Documentatie is verzameld in de periode van 14 april 2022 tot en met 21 november 2022.

Voor onderzoeksvraag 2 is het object van onderzoek het proces dat geleid heeft tot de invoering en ingebruikname van de berichtenservice bij de verschillende penitentiaire inrichtingen (PI's). Dit raakt onder andere de beraadslagingen, de overwegingen en de besluitvorming van betrokkenen, blijkend uit zowel documentatie als interviews.

Voor beide onderzoeksvragen worden in dit rapport feitelijke bevindingen gerapporteerd, zonder conclusies of aanbevelingen. De ADR geeft geen aanwijzingen voor het treffen van maatregelen. De opdrachtgever van het rapport zal zelf een oordeel moeten vormen over de werkzaamheden en bevindingen die in het rapport zijn weergegeven en eigen conclusies moeten trekken uit de door ons verrichte werkzaamheden.

In het onderzoek is nadrukkelijk geen aandacht besteed aan juridische en/of criminele risico's (zgn. Voortgezet Crimineel Handelen) zoals die (indirect) opgenomen zijn in de brief[4] van het OM. Een scenarioanalyse rond alternatieve vormen van een emailberichtenservice is eveneens niet in scope van het onderzoek.

Kanttekening aangeleverde informatie

Voor beide onderzoeksvragen geldt dat wij ons in de beantwoording baseren op de informatie die is verstrekt door DJI, eMates en haar IT-serviceprovider Unilink. Wij kunnen niet instaan voor de volledigheid van de aangeleverde informatie. Om deze reden valt niet uit te sluiten dat documenten en/of informatie die wel ter zake doen niet in het onderzoek zijn betrokken.

1.4 Leeswijzer

Allereerst wordt in hoofdstuk 2 een samenvattend antwoord gegeven op de centrale onderzoeksvragen. Hoofdstuk 2 vormt daarmee de managementsamenvatting. In hoofdstuk 3 wordt toegelicht wat de berichtenservice is en hoe deze door de verschillende PI's wordt gebruikt. In hoofdstuk 4 worden de bevindingen rond het onderzoek naar de implementatie en ingebruikname van de berichtenservice weergegeven aan de hand van het feitenrelaas. Ook wordt daarbij de betrokkenheid van het beleidsdepartement van Justitie en Veiligheid, de uitvoeringsorganisatie DJI en eMates toegelicht. Hoofdstuk 5 bevat tot slot een beschrijving van de uitgevoerde werkzaamheden en vormt de verantwoording van het uitgevoerde onderzoek. In de bijlage zijn de bevindingen over informatiebeveiliging en privacy opgenomen.

[4] *Minister van Rechtsbescherming, brief aan de Tweede Kamer van 24 maart 2022 (kenmerk 3923371).*

2 Managementsamenvatting

In dit hoofdstuk beschrijven we de uitkomsten van ons onderzoek op hoofdlijnen. Voor onderzoeksvraag 1 (informatiebeveiliging) geldt dat wij voor de feitelijke bevindingen verwijzen naar de bijlage.

2.1 Kenmerken van het invoerings- en ingebruiknameproces vanaf 2011

In hoofdstuk 4 is de tijdlijn met het feitenrelaas vanaf 2011 weergegeven. Op basis van de daarin opgenomen afzonderlijke feiten kunnen we op hoofdlijnen de navolgende bevindingen geven van de invoering en ingebruikname van de berichtenservice.

Aanleiding van de introductie berichtenservice

De berichtenservice, destijds onder de naam Emailaprisoner[5], is geïntroduceerd als onderdeel van het programma Modernisering Gevangeniswezen (MGW) dat in de periode 2008-2012 liep. Uitgangspunt van het programma was dat iedere gedetineerde de juiste mate van beveiliging, zorg en passende dagprogramma's kon krijgen om zo de kans te vergroten op een geslaagde terugkeer in de maatschappij en recidive te verminderen. De toentertijd moderne berichtenservice (van Emailaprisoner) sloot aan bij de doelstellingen van het programma.

Bij de introductie van de berichtenservice werd vanuit DJI-organisatie een gebruikelijk instrumentarium voor de introductie van nieuwe diensten gehanteerd, zoals het opstellen van een business case met kritische vragen over bijvoorbeeld informatiebeveiliging, eventuele aanbestedingen of het eventueel opstellen van een contract. Geen van deze onderwerpen heeft echter een plaats gekregen in de gehanteerde beleidslijn voor de berichtenservice.

Beleidslijn

Het initiatief voor een berichtenservice ontstond vanuit een aanbod van buiten DJI en niet vanuit een interne vraag van DJI. Het aanbod van buiten werd geadopteerd door enkele van het idee overtuigde DJI-leidinggevenden die voor implementatie van de berichtenservice een *'low profile'* beleidslijn hebben uitgezet. Hoofdpunten van deze beleidslijn zijn dat DJI geen partij is in de overeenkomst tussen Emailaprisoner en haar afnemers en dat DJI slechts verantwoordelijk is voor de vertrouwelijkheid van de (post)processen binnen de inrichtingen. Ook wordt door betrokkenen gesteld dat een geprint emailbericht te beschouwen is als poststuk en het schenden van de vertrouwelijkheid van de post geen veiligheidsrisico vormt voor DJI. In beantwoording van Tweede Kamervragen en behandeling van vraagstukken met betrekking tot de berichtenservice wordt herhaaldelijk teruggegrepen op deze beleidslijn.

Implicaties en verantwoordelijkheid

Na afronden van het programma MGW in 2012 is de verdere uitwerking van het idee van de berichtenservice overgedragen aan de staande organisatie (destijds de sectordirectie Gevangeniswezen) en de directeur van Emailaprisoner. De berichten-service werd door betrokkenen beschouwd als een 'klein' project, zijnde een specifieke vorm van de reguliere postbezorging door een externe partij waarbij informatiebeveiligingsaspecten en mogelijke privacy-problemen als 'nihil' werden ingeschat. Begin 2013 was er ook politieke aandacht voor de introductie van de

[5] *Vanaf 1 november 2016 wordt de naam eMates gebruikt.*

berichtenservice en is de staatssecretaris daarover bevraagd[6]. In april 2014 kwam het formele besluit van het MT Gevangeniswezen (GW) van DJI om de berichtenservice uit te rollen bij alle PI's. In welke mate de staatssecretaris betrokken is geweest bij het geven van deze opdracht is overigens onduidelijk: in maart 2014 informeert de staatssecretaris Kamerleden van de vaste commissie Veiligheid en Justitie nog dat pilots met Emailaprisoner in juni 2014 worden geëvalueerd waarna de service landelijk zou kunnen worden uitgebreid.

De vertegenwoordiging van de in het onderzoek betrokken PI's gaven aan niet betrokken te zijn geweest bij het besluit om Emailaprisoner als berichtenservice in gebruik te nemen. Volgens hen betrof de implementatie van de berichtenservice een opdracht van het hoofdkantoor DJI, waarmee het MT GW wordt bedoeld.

Met de gestage uitbreiding van de berichtenservice vanaf april 2014 nam vanuit de betrokkenen bij de PI's de behoefte toe aan een zekere mate van regie of beleid op de berichtenservice. Het betreft (herhaalde) vragen over informatiebeveiliging, zoals opslag van PI gegevens buiten de PI, de toepasselijkheid van de Wet Bescherming Persoonsgegevens, het maken van afspraken in de vorm van een contract of convenant met eMates en, in het verlengde daarvan, het uitvoeren van een vertrouwelijkheidsonderzoek naar de vertegenwoordiging van eMates. Dergelijke verzoeken zijn binnen DJI aangekaart bij specialisten en leidinggevenden, maar hebben geen (inhoudelijke) opvolging gekregen. Uit het onderzoek blijkt niet of dergelijke signalen op een (hoog) niveau binnen de organisatie van Justitie en Veiligheid terecht zijn gekomen.
Ook doen enkele PI's vanaf 2017 een aantal keren het verzoek om centralere beleidscoördinatie rond de berichtenservice in te richten (zoals het opstellen van een contract). Op deze vraagstukken werd binnen DJI doorgaans gereageerd met de stelling dat DJI geen partij was. De eerdergenoemde beleidslijn werd gevolgd, waarbij DJI louter een faciliterende rol had zonder inkooprelatie. Dat er geen verantwoordelijkheid werd gevoeld voor de werking en de mogelijke informatie-beveiligingseffecten van de berichtenservice eMates blijkt bijvoorbeeld ook uit het feit dat volgens de betrokkenen bij de PI's en eMates nooit evaluatiemomenten zijn geïnitieerd vanuit DJI over de werkwijze met de berichtenservice.

Halverwege 2017 lijkt in deze beleidslijn een kentering te komen: eMates krijgt vanaf augustus 2017 hernieuwde aandacht van de afdeling Beleid van DJI en er worden vaker vragen gesteld over de verantwoordelijkheid van DJI en de werklast bij PI's bij de controle van de berichten. Ook neemt DJI eMates in december 2020 op in haar verwerkingsregister (onder het thema 'Postafhandeling').

Invloed van de externe partij eMates

Bij de introductie en invoering van de berichtenservice is voor regie en coördinatie ruimte gelaten aan de organisatie van Emailaprisoner (later eMates). eMates heeft in 2013 bij haar politieke relaties gevraagd of zij de ingebruikname wilden bevorderen. Vervolgens had de organisatie van eMates bij de operationele ingebruikname van de berichtenservice vanaf april 2014 ruimte om invloed uit te oefenen, met daaraan dienstbare functionele betrokkenheid van DJI-medewerkers. Die ruimte strekte zich soms ook uit tot bemoeienis met de praktische uitvoering van de activiteiten die de PI's rond de berichtenservice verzorgden. Een voorbeeld hiervan is dat volgens betrokkenen bij een PI eMates om motivering vroeg wanneer berichten de interne controle niet doorstonden. Bij sommige PI's leefde het idee dat eMates onderdeel was van de eigen organisatie.
Het karakter van de samenwerking tussen DJI, de PI's en de organisatie van eMates lijkt ook voor de Minister voor Rechtsbescherming voor Nederland te leiden tot een misvatting: op de vraag van een Tweede Kamerlid in augustus 2019 over welke

[6] *Tweede Kamer der Staten-Generaal, verslag van een notaoverleg, 10 april 2013 (kenmerk 33177-6).*

communicatiemiddelen een gedetineerde beschikt antwoordt de Minister dat betrokkene ook beschikt over het 'reguliere DJI-systeem eMates'[7].

In juni 2021 hebben de beloften van eMates aan haar klanten juridische gevolgen voor de leiding van een PI. De PI is volgens de Raad voor Strafrechttoepassing en Jeugdbescherming (RSJ) gehouden aan haar zorgplicht inzake tijdige postbezorging waarvan eMates de specifieke tijden heeft bepaald. De betreffende overeenkomst tussen eMates en haar klanten is voor de PI als derde partij zodoende medebepalend hoe zij aan die zorgplicht invulling en verantwoording geeft.

Eigenaarschap
Tot op heden is het eigenaarschap voor het dossier eMates niet belegd op enig beleidsniveau. Uit het onderzoek blijkt dat dit al door het MT GW is geconstateerd in april 2020. In het verlengde daarvan blijkt uit ons onderzoek dat er bij de PI's geen centraal aanspreekpunt op beleidsniveau bekend is voor het behartigen van een eenduidige benadering van de eMates berichtenservice.

Eerst in augustus 2017 en vooral later vanaf begin 2019 komt er meer aandacht voor informatiebeveiliging rond de berichtenservice op zowel PI niveau als vanuit de afdeling Beleid van DJI. De roep vanuit de PI's om meer centrale kaders intensiveert. Ook de werkdruk rond de controle op de groeiende aantal berichten wordt vaker een issue. Om het aantal berichten te beteugelen neemt de PI Vught in mei 2020 maatregelen, maar wordt daarin door de RSJ in het ongelijk gesteld. Door de RSJ worden digitale berichten (mails) in oktober 2020 gelijkgesteld aan post. Dat betekent dat gedetineerden niet beperkt mogen worden in het ontvangen van het aantal berichten.

Vragen over de informatiebeveiliging van eMates worden wederom in februari 2022 gesteld, maar deze keer door het OM. Deze vragen vormden de aanleiding voor dit onderzoek.

2.2 Hoofdpunten van het onderzoek naar de informatiebeveiligingsaspecten

Onderzoekkader
Het geschetste beeld in paragraaf 2.1 heeft invloed op de beperkte mogelijkheden om onderzoek te doen naar de informatiebeveiligingsaspecten van het IT-systeem dat eMates gebruikt. Zo is al bij de opdrachtaanvaarding geconstateerd dat de berichten-service van eMates buiten de regie van DJI wordt gebruikt. Aangezien er geen contract tussen DJI en eMates is afgesloten en er geen formele klant-leverancier relatie met eMates bestaat, is de medewerking aan het onderzoek afhankelijk van de welwillendheid van eMates en haar IT-serviceprovider Unilink. De PI's zijn als informatieverwerkende partij, in de faciliterende en controlerende rol in het berichtenverkeer, verantwoordelijk voor alle inkomende en uitgaande informatiestromen. Vanwege het beleidsuitgangspunt dat DJI geen partij is en er ook geen zwaarwegend financieel belang is, is de rol van IT-controller, Chief Information Officer (CIO) en beveiligingsautoriteit (BVA) bij DJI rond eMates niet ingevuld.
In dat kader zijn de hoofdpunten van ons onderzoek naar de informatiebeveiliging hierna beschreven. In bijlage 1 is een gedetailleerdere beschrijving van de bevindingen per gehanteerde BIO-norm opgenomen.

DJI heeft geen zicht op de informatiebeveiliging van de berichtenservice eMates
DJI heeft aangegeven dat er geen formele afspraken, overeenkomsten of contracten met eMates zijn gemaakt of gesloten (conform de eerdergenoemde beleidslijn). Daardoor heeft DJI rondom het gebruik van eMates geen aandacht besteed aan vereisten voor informatiebeveiliging en aan de verwerking van gegevens conform de AVG. De standaard werkwijze volgens de BIO is daarom niet gevolgd. Normaliter

[7] *Tweede Kamer der Staten-Generaal, Antwoord op vragen, 20 augustus 2019 (kenmerk 2019Z10764).*

begint deze werkwijze met het uitvoeren van een BBN-toets (risicoanalyse) waaruit een basisbeveiligingsniveau (BBN) volgt. Het BBN bepaalt welke controls vervolgens moeten worden doorlopen. Per control moet worden bepaald welke maatregelen in aanvulling op de verplichte overheidsmaatregelen nodig zijn. Externe dienstenleveranciers zijn geen onderdeel van de overheid en zijn daarmee niet rechtstreeks gebonden aan de BIO. Ze moeten wel voldoen aan de eisen van de opdrachtgever. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom in het contract zijn vastgelegd en dienstleveranciers leggen hierover verantwoording af aan hun opdrachtgever. In dit specifieke geval bestaat vanuit DJI voor de berichtenservice eMates geen opdrachtgeverschap[8], geen contract en als gevolg hiervan geen formele verantwoordingslijn.

eMates heeft zich voorgenomen de informatiebeveiligingseisen te formaliseren

Unilink is de IT-serviceprovider van eMates. De relatie tussen eMates en Unilink is naar aanleiding van dit onderzoek per 1 november 2022 geformaliseerd in een klant-leverancierscontract. Hiervoor was er geen contract. Als reden werd genoemd dat Unilink deels eigenaar is van eMates en er in belangrijke mate sprake is van co-ownership en samenwerking op basis van vertrouwen. Recent heeft eMates aangegeven dat het voornemens is om ook de operationele samenwerking vast te leggen in afspraken middels een Service Level Agreement met Unilink. Ditzelfde geldt voor het opstellen van een eMates Operations en Security Manual, waarin voor een aantal normen de inrichting en beheersing zal worden geformaliseerd.

Tijdens het onderzoek heeft eMates een adviseur informatiebeveiliging ingehuurd om de directeur eMates in het onderzoek bij te staan en deze verbeteringen en formaliteiten door te voeren. Daarnaast zijn tijdens het onderzoek door eMates documenten op het gebied van informatiebeveiliging opgesteld en geformaliseerd.

Beperkt onderzoek mogelijk naar de inrichting en beheersing van de informatiebeveiliging van de berichtenservice eMates

Unilink beschikt over een ISO27001 certificering; evenals Cyber Essentials Plus-certificeringen en geeft aan dat deze certificeringen zijn uitgegeven door geaccrediteerde partijen in het Verenigd Koninkrijk. Daarnaast beschikt Unilink volgens mededeling over een assurance verklaring (SOC2) van de Cloud leverancier. Het Unilink ISO 27001 certificaat en het bijbehorende Statement of Applicability toont volgens Unilink aan dat alle normen in scope van deze audit volgens het certificaat zijn geïmplementeerd door Unilink. eMates en Unilink geven aan dat deze certificaten naar hun mening aantonen dat Unilink voldoet aan alle normen in scope van deze audit. Wij hebben dat niet zelfstandig kunnen vaststellen. De inhoud van de onderliggende stukken voor de certificeringen, verklaringen en diverse bewijsstukken zijn door Unilink als vertrouwelijk aangemerkt, omdat het delen van deze stukken met derde partijen een informatiebeveiligingsrisico voor Unilink vormt. De SOC2 verklaring van de cloudleverancier mag volgens Unilink niet met de ADR gedeeld worden omdat de ADR geen *permitted recipient* is. In de context van deze audit is het volgens Unilink niet wenselijk om een geheimhoudingsverklaring op te stellen, omdat de certificeringen voldoende zekerheid zouden geven en er geen directe aanleiding is dat de systemen van Unilink een risico vormen voor de klanten. Vanwege het ontbreken van een geheimhoudingsverklaring heeft de ADR beperkt inzage in vertrouwelijke stukken. Hierdoor kunnen wij niet herleiden wat de scope en diepgang is van de certificeringen en de assurance verklaring.

Diverse door de ADR ontvangen bewijsstukken zijn niet voorzien van aanvullende informatie die benodigd is om de stukken te kunnen duiden, zoals de context van schermafdrukken en het versiebeheer van documenten. Wij hebben hierdoor beperkt

[8] *MT GW heeft in april 2014 aan PI's de opdracht gegeven mee te werken aan de introductie van de berichtenservice. Dat is intern opdrachtgeverschap. Toezicht op de dienstverlening is daarna niet (centraal) georganiseerd.*

onderzoek kunnen uitvoeren naar de getroffen beheersmaatregelen, waardoor voor meerdere beheersmaatregelen geen of beperkt feitelijke bevindingen zijn gerapporteerd. Dit wil niet altijd zeggen dat de beheersmaatregel niet is ingericht, maar dat wij dit niet hebben kunnen vaststellen.

De feitelijke bevindingen over de inrichting en beheersing van de informatiebeveiliging zijn beschreven in bijlage 1.

3 Wat is eMates en hoe werkt het?

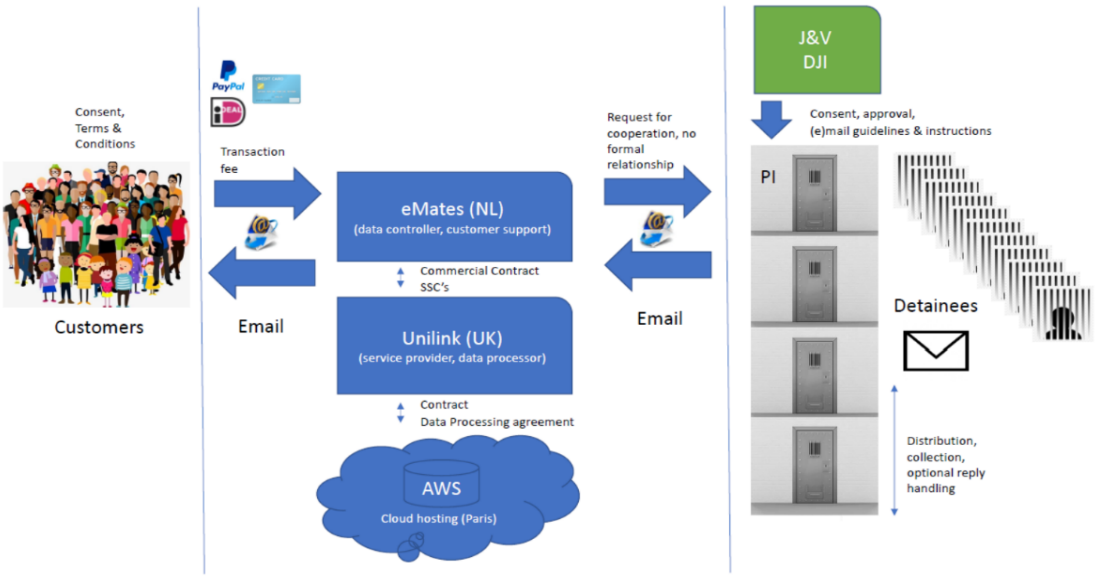
Ter achtergrondinformatie wordt in dit hoofdstuk toegelicht wat de berichtenservice van eMates is. Ook wordt in dit hoofdstuk de werkwijze met de berichtenservice bij de verschillende PI's beschreven.

3.1 Wat is eMates?

De berichtenservice van Emailaprisoner, die later eMates[9] is gaan heten, is een communicatieplatform voor gedetineerden en hun relaties. De berichtenservice is een product van een private onderneming en is zodoende *geen* onderdeel van het ministerie van Justitie en Veiligheid. De PI's verlenen hun medewerking aan het faciliteren van de berichtenservice, maar het gebruik ervan is niet verplicht. DJI heeft geen contract afgesloten met eMates.

De berichtenservice eMates maakt gebruik van de IT-dienstverlening van Unilink. Deze relatie werd tijdens het onderzoek geformaliseerd in een commercieel contract. Hiervoor was deze samenwerking gebaseerd op informele afspraken, aangezien de eigenaar van Unilink mede-eigenaar is van eMates. Unilink maakt gebruik van de dienstverlening van Amazon Web Services (AWS).
De context wordt gevat in figuur 1 afkomstig uit eMates 'Activities, Business Services, Information Security Policy'.

Figuur 1. *Visuele weergave organisatorische context eMates*



Via de website van eMates kunnen relaties van gedetineerden tegen een tarief per bericht, een bericht sturen naar een gedetineerde. Hiervoor dient de relatie van de gedetineerde een account aan te maken. Voor het verzenden van een bericht moet de relatie van de gedetineerde de naam en Strafrechtketennummer van de gedetineerde invoeren. Ook wordt de naam en het adres van de afzender gevraagd. Bij de meeste inrichtingen kunnen de afzenders ook maximaal vier foto's als een bijlage bijvoegen bij hun bericht. De berichten worden per PI in een afzonderlijke

[9] *eMates droeg voor 1 november 2016 nog de naam 'Emailaprisoner'.*

batch opgenomen, waarna één keer per dag de afzonderlijke batch naar de desbetreffende PI wordt doorgestuurd[10].

In oktober 2015 werd de dienstverlening van eMates uitgebreid met een antwoordservice. Bij de PI's die deze service faciliteren kunnen gedetineerden, als zijn of haar relatie dat op de site aangeeft en daarvoor betaalt, een antwoord schrijven op een antwoordformulier. Deze antwoordformulieren worden vervolgens door de PI gescand en weer retour gestuurd naar eMates.

In onderstaande tabel wordt weergegeven welke PI wanneer is gestart met het faciliteren van eMates.

Tabel 1 *Overzicht invoering berichtenservice bij de PI's (in chronologische volgorde)*

Inrichting	Gestart met berichtenservice
PI Heerhugowaard	September 2013
PI Leeuwarden	September 2013
RJJI De Hartelborgt	November 2013
PI Zuidoost (Ter Peel)	November 2013
PI Lelystad	Maart 2014
PI Middelburg	Juni 2014
PI Dordrecht	Juli 2014
PI Zwaag	Juli 2014
JC Schiphol	Augustus 2014
PI Utrecht (Nieuwersluis)	Oktober 2014
PI Vught	Oktober 2014
PI Arnhem	November 2014
PI Zuidoost (Roermond)	November 2014
PI Grave	December 2014
PI Sittard	Maart 2015
PI Alphen aan den Rijn	Juni 2015
PI Zwolle	Juni 2015
PI Achterhoek (Zutphen)	Juli 2015
PI Veenhuizen, locatie Esserheem	Juli 2015
PI Ter Apel	Augustus 2015
PI Krimpen aan den IJssel	Oktober 2015
PI Nieuwegein	Oktober 2015
PI Almere	December 2015
PI Almelo	Januari 2016
PI Rotterdam	Januari 2016
PI Haaglanden	Maart 2016
Detentiecentrum Zeist	December 2016
JC Zaanstad	Februari 2017
Militair Penitentiair Centrum (Stroe)	September 2017
PI Veenhuizen, locatie Klein Bankenbosch	Oktober 2018
PI Veenhuizen, locatie Norgerhaven	April 2019
DC Rotterdam	November 2020

[10] *De attachments worden versleuteld, opnieuw geformatteerd en met een wachtwoord beveiligd. Zie daarover onze bevindingen in de bijlage onder normen 13 en 18.*

3.2 Hoe werkt eMates?

3.2.1 Procesbeschrijving

De verwerking van de (antwoord)berichten is door alle penitentiaire inrichtingen gelijkgesteld aan het reguliere postproces.

PI's die de berichtenservice van eMates faciliteren ontvangen via eMates dagelijks een versleutelde berichtenbatch van Unilink op een algemene, functionele mailbox. Alleen de medewerkers van de inrichtingen gemoeid met de verwerking van eMatesberichten hebben een autorisatie tot deze mailbox. De medewerkers – doorgaans medewerkers van het Bureau Managementondersteuning (BMO)[11] – openen de berichtenbatch meestal door middel van een wachtwoord. Na het openen van de batch worden de berichten uitgeprint, waarna de bovengenoemde medewerkers de berichten controleren. *Goedgekeurde* berichten worden in een eMates-envelop gedaan en worden afgegeven bij de postkamer voor uitreiking aan de gedetineerde. Afgekeurde berichten worden in enveloppen gedaan en bij de persoonlijke eigendommen van de gedetineerden opgeborgen (de preciosa). In geval van een afgekeurd bericht wordt ook het Bureau Inlichtingen en Veiligheid (BIV) op de hoogte gebracht. De berichtenbatches worden voor drie maanden binnen de inrichtingen gearchiveerd.

Wanneer een PI de antwoordservice van eMates faciliteert, worden er antwoordvellen (met een QR-code) meegeleverd bij de aan de gedetineerden uitgereikte berichten. Gedetineerden kunnen op deze antwoordvellen een reactie schrijven, waarna deze weer bij de postkamer wordt afgegeven voor uitgaande post. Op eenzelfde wijze worden de antwoordvellen gecontroleerd door de medewerkers die ook de binnenkomende berichten controleerden. Goedgekeurde antwoordvellen worden ingescand en doorgaans als versleutelde batch teruggestuurd naar eMates.

3.2.2 De controle van de (antwoord)berichten

De mate van controle van eMates-berichten verschilt. Zo geldt voor gedetineerden in de Extra Beveiligde Inrichting (EBI) of de Terroristische Afdeling (TA) dat alle in- en uitgaande berichten volledig worden gecontroleerd. Voor gedetineerden die niet in de EBI of TA verblijven geldt dat berichten alleen worden gecontroleerd als daar een concrete aanleiding voor is. In dat geval wordt een toezichtsmaatregel opgelegd. Berichten gericht aan of van een gedetineerde waarop een toezichtmaatregel van toepassing is, worden volledig doorgelezen en gecontroleerd. Van het BIV vernemen de controlemedewerkers welke gedetineerden een toezichtmaatregel hebben. In sommige gevallen is afgesproken dat de berichten van deze gedetineerden direct aan een BIV-medewerker ter controle worden afgegeven.
Wanneer er geen sprake is van een toezichtmaatregel worden de berichten in sommige gevallen ter controle (diagonaal) doorgelezen, aldus een aantal PI's. Bij vermoedens over voortgezet crimineel handelen worden berichten doorgestuurd naar het Gedetineerden Recherche Informatiepunt (GRIP).

Verschillen tussen PI's

Uit het onderzoek blijkt dat de controle van eMates berichten bij de verschillende inrichtingen verschillend is ingericht. Zo worden de berichten bij de ene PI door de nachtdienst gecontroleerd en verwerkt, terwijl bij de andere PI de berichten worden verwerkt door medewerkers van het BMO. Verder wordt bij een aantal PI's aangegeven dat alle berichten *wel* volledig worden gecontroleerd, ook wanneer geen toezichtmaatregel van toepassing is. Volgens geïnterviewden verschillen de hoeveelheid afgekeurde berichten eveneens (sterk) per inrichting.

[11] *Of bijvoorbeeld (senior) complexbeveiligers.*

4 Feitenrelaas

In dit hoofdstuk wordt een chronologisch overzicht gegeven van de belangrijkste feiten die hebben gespeeld rondom de invoering en ingebruikname van eMates bij de verschillende penitentiaire inrichtingen. Daarbij wordt eveneens de betrokkenheid van de directies van het ministerie van Justitie en Veiligheid, de uitvoeringsorganisatie DJI en eMates toegelicht.

4.1 Tijdlijn

In onderstaande tijdlijn zijn de belangrijkste feiten en gebeurtenissen die wij hebben kunnen achterhalen, chronologisch weergeven. Het feitenoverzicht begint bij het moment waarop de berichtenservice van eMates – toentertijd nog Emailaprisoner – als idee werd geïntroduceerd bij het ministerie van Justitie en Veiligheid en eindigt op het moment dat de berichtenservice is opgeschort.

In onderstaand overzicht zijn zaken zo feitelijk mogelijk beschreven.

Datum	Toelichting event	Betrokkenheid[12]
13 januari 2011 *Introductie van het idee*	Er vindt een presentatie plaats bij het hoofdkantoor van DJI over de berichtenservice van Emailaprisoner, op initiatief van directie bestuursondersteuning SG. Bij deze presentatie zijn een aantal PI directeuren en een vertegenwoordiging van het programma 'Modernisering Gevangeniswezen' aanwezig. Zowel het programma als de PI directeuren reageerden enthousiast op het initiatief.	• *De organisatie Emailaprisoner* heeft een informerende rol bij de introductie van het idee van de berichtenservice. • *Directie bestuursondersteuning SG van het Ministerie van Justitie en Veiligheid* heeft een faciliterende rol bij de presentatie van *Emailaprisoner* van het idee omtrent Emailaprisoner.
14 maart 2011 *Introductie van het idee*	Het programma Modernisering Gevangeniswezen besluit dat het initiatief van een berichtenservice van Emailaprisoner aansluit bij de re-integratie projecten die reeds onderdeel zijn van het programma. Een vertegenwoordiging van het programma verzoekt het MT Gevangeniswezen (GW) in te stemmen met de verdere ontwikkeling van Emailaprisoner in de vorm van een aantal pilots.	• *DJI-programma Modernisering GW* had een besluitvormende rol bij de bepaling dat het initiatief van Emailaprisoner aansluit bij re-integratie projecten. • Het *DJI-programma Modernisering GW* had een voorbereidende rol in het besluitvormingsproces.
6 december 2011 *Uitwerken van een business case*	Het MT GW gaat akkoord met de verdere ontwikkeling van de berichtenservice in de vorm van een aantal pilots. Er wordt gestart met het schrijven van een business case. De business case wordt geschreven door de organisatie van Emailaprisoner en een vertegenwoordiging van het project Terugkeer-activiteiten, onderdeel van het programma Modernisering Gevangeniswezen.	• *MT GW* had een besluitvormende rol bij de verdere ontwikkeling van de berichtenservice in de vorm van een aantal pilots. • Het *project Terugkeeractiviteiten* heeft met het opstellen van een business case een betrokkenheid bij de beleidsontwikkeling omtrent de berichtenservice.
10 februari 2012	Als onderdeel van het schrijven van de business case vindt er overleg plaats tussen medewerkers van de afdeling	• *De organisatie van Emailaprisoner* en *(beleidsdirecties van) DJI* geven

[12] Voor de duiding van de vorm van betrokkenheid worden diverse rollen genoemd. Deze rollen zijn algemeen gedefinieerd, d.w.z. hebben niet een specifieke juridische of bestuurlijke betekenis.

Uitwerken van een business case	Beleid van DJI en van de organisatie van Emailaprisoner. Beveiligingsvraagstukken worden geopperd, maar niet (volledig) beantwoord.	met het schrijven van een business case berichtenservice nadere invulling aan de beleidsontwikkeling omtrent het programma modernisering GW.
Februari – oktober 2012 *Uitwerken van een business case*	Het project Terugkeeractiviteiten heeft de business case onderhanden. Doorlopend worden er vragen gesteld over of er een aanbestedingstraject met Emailaprisoner gestart dient te worden. Geconcludeerd wordt dat er door DJI niets wordt ingekocht en dat de aanbestedingsgrens niet bereikt wordt. Ook wordt besproken of DJI – omwille van beveiligingsmaatregelen – zelf een berichtenservice zou kunnen maken. Wat uit deze discussie komt is onduidelijk. Er wordt nog contact gelegd met een tweede aanbieder, Prisonmail.eu, maar de samenwerking met Emailaprisoner wordt gecontinueerd.	• Het *project Terugkeeractiviteiten* heeft met het opstellen van een business case een betrokkenheid bij de beleidsontwikkeling omtrent de berichtenservice.
19 oktober 2012 *Uitwerken van een business case*	Een vertegenwoordiging van het project Terugkeeractiviteiten verzoekt het MT GW om opdracht te geven de scope van de initiële business case voor de berichtenservice uit te breiden. Meer specifiek wordt toestemming gevraagd voor de ontwikkeling van een berichtenservice die zowel berichten van buiten naar binnen kan sturen, als van binnen naar buiten (tweerichtingsverkeer). Daarbij wordt aangegeven dat de behoefte van tweerichtingsverkeer kenbaar is gemaakt door verschillende PI's. Hoe het MT GW op dit verzoek reageert is onbekend.	• Het *project Terugkeeractiviteiten* is, met het verzoek tot uitbreiding van de business case met een tweerichtingsverkeer, betrokken bij de beleidsontwikkeling.
1 februari 2013 *Pilots*	Bij de PI Heerhugowaard wordt op eigen initiatief gestart met een "papieren" pilot. Hierbij worden berichten uit de berichtenservice door een vrijwilliger uitgeprint en als post bij de PI afgegeven. Het doel van de papieren pilot is het wegnemen van eventuele weerstand tegen de berichtenservice.	• *De leiding PI Heerhugowaard* heeft een initiërende betrokkenheid bij het starten van een 'papieren pilot'.
Februari – april 2013 *Politieke aandacht*	Het initiatief om de berichtenservice te implementeren stokt bij het beleidsdepartement van DJI, omdat de toenmalige staatssecretaris (nog) geen voorstander is. De organisatie van Emailaprisoner neemt daartoe contact op met de vertegenwoordiging van een Tweede Kamerfractie. Op 8 april 2013 wordt er een motie ingediend, waarin de regering wordt verzocht het de berichtenservice van Emailaprisoner te faciliteren bij de verschillende PI's. De motie wordt op 10 april 2013 besproken in een vergadering van de vaste commissie voor Veiligheid en Justitie. De staatssecretaris geeft aan de mogelijkheden aangaande de financiële dekking van de motie te willen onderzoeken. De motie wordt aangehouden; afgesproken wordt dat	• De *organisatie van Emailaprisoner* is betrokken bij de introductie van het initiatief in de Tweede Kamer. • *Tweede Kamerleden* is met het indienen van een motie betrokken bij de introductie van de berichtenservice. • De *staatssecretaris* is met het onderzoeken van de mogelijkheden aangaande de financiële dekking van de motie, betrokken bij de beleidsontwikkeling/-verkenning.

	de Kamerleden voor 1 juli 2013 worden geïnformeerd.	
Mei 2013 *Pilots*	Ongeacht de politieke discussie wordt door de leiding van PI Heerhugowaard besloten te starten met een pilot van Emailaprisoner. Geïnterviewden geven aan dat dit is afgestemd met het MT GW. Het idee is om de pilot 'begin 2014' te evalueren. Door een vertegenwoordiging van het project Terugkeeractiviteiten wordt de Directie Informatievoorziening van DJI betrokken bij de uitrol van de pilot.	• *De leiding van PI Heerhugowaard* is, met het besluit (volgens betrokkenen in afstemming met MT GW) tot het starten van de pilot van Emailaprisoner en het evalueren daarvan, betrokken bij de beleidsontwikkeling van de berichtenservice. • Het *project Terugkeeractiviteiten* en de *Directie Informatievoorziening* ondersteunen bij de uitrol van de pilot bij PI Heerhugowaard.
7 oktober 2013 *Pilots*	Er wordt een presentatie gehouden over de uitbreiding van de pilot naar meer PI's. Onder andere is aanwezig een vertegenwoordiging van PI Leeuwarden, die besluit aan te willen sluiten bij de pilot.	• De *organisatie van Emailaprisoner* is betrokken bij de uitbreiding van de pilot. • *PI Leeuwarden* is met het deelnemen aan de pilot betrokken bij de beleidsontwikkeling van de berichtenservice.
8 oktober 2013 *Feedback*	Een vertegenwoordiging van de Directie Informatievoorziening stuurt per mail een aantal vraagpunten inzake privacy- en informatiebeveiligingsaspecten. De vertegenwoordiging vanuit PI Heerhugowaard antwoordt dat Emailaprisoner *low-profile* gehouden kan worden, omdat het feitelijk een regulier postproces is. Bovendien, zo wordt gesteld, kost het initiatief DJI geen geld en is de familie van gedetineerde klant bij Emailaprisoner (en niet DJI). De vertegenwoordiging van PI Heerhugowaard stemt deze redenering vervolgens op 11 oktober 2013 af met een toenmalige directeur Gevangeniswezen. Zij zijn het erover eens dat Emailaprisoner een dienst betreft die ''simpel georganiseerd en aangeboden kan worden, op een veilige manier, zonder dat daar zoveel energie en uren […] in worden geïnvesteerd''.	• *Directie Informatievoorziening* heeft bij het inrichten van de pilots een toetsende rol, waarbij randvoorwaardelijke informatiebeveiligingsaspecten ter sprake komen. • De leiding van *PI Heerhugowaard* is bij het inrichten van de pilots betrokken bij de beantwoording van vragen vanuit *Directie Informatievoorziening* omtrent de informatiebeveiliging na afstemming met MT-lid GW
12 november 2013 *Pilots*	Een vertegenwoordiging van de Directie Informatievoorziening van DJI deelt een startdocument met de inrichtingen die ook willen aansluiten bij de pilot van Emailaprisoner, zijnde RJJI de Hartelborgt en PI Zuid-Oost (Ter Peel). In dit document staat onder andere beschreven hoe de (controle)processen omtrent de berichtenservice ingericht kunnen worden bij de inrichtingen.	• *Directie Informatievoorziening* heeft met het opstellen van een startdocument een ondersteunende rol bij de inrichting van de pilots bij de PI's.
Begin 2014 *Pilots*	Uit communicatie tussen de Directie Informatievoorziening en de organisatie van Emailaprisoner blijkt dat het plan was de pilots begin 2014 te evalueren. Uit het onderzoek is niet gebleken dat deze evaluatie daadwerkelijk heeft plaatsgevonden.	• *Directie Informatievoorziening* en de *organisatie van Emailaprisoner* hebben een voorbereidende rol bij het plan tot evaluatie van de berichtenservice.

27 maart 2014 *Politieke aandacht*	De vaste commissie voor Veiligheid en Justitie voert een overleg met de staatssecretaris. Besproken wordt dat er op dat moment pilots met de berichtenservice bij de PI's in Ter Peel (Zuidoost), Leeuwarden, Heerhugowaard en RJJI Hartelborgt worden gehouden. De staatssecretaris zegt toe dat de pilots halverwege het jaar, in juni, worden geëvalueerd alvorens een landelijke uitrol kan worden bewerkstelligd.	• De *staatssecretaris* en de *vaste commissie voor Veiligheid en Justitie* hebben politieke aandacht voor de evaluatie van de pilots bij de PI's in Ter Peel, Leeuwarden, Heerhugowaard en JJI Hartelborgt.
16 april 2014 *Besluitvorming*	Een MT-lid GW verzoekt het MT GW om op de korte termijn de PI's de opdracht te geven de berichtenservice te implementeren. Dit besluit wordt door MT GW eind april genomen. Uit het memo ter MT-besluit blijkt dat drie punten van belang worden geacht: 1) privacy, 2) briefgeheim en 3) aanbesteding. Bij de invulling van deze punten wordt de beleidslijn gevolgd dat DJI geen partij is.	• De *Directie Informatievoorziening* heeft (als concipiënt) een voorbereidende rol bij de besluitvorming van het MT GW tot de uitrol van de berichtenservice. • Het *MT GW* is betrokken bij de besluitvorming bij de uitrol van de berichtenservice bij alle PI's.
17 april 2014 *Pilots*	Een vertegenwoordiging van Emailaprisoner vraagt via een email aan de Directie Informatievoorziening naar de uitkomst van de evaluatie van de pilots. Een vertegenwoordiging van de Directie Informatievoorziening reageert niet op de vraag hoe geëvalueerd is, maar geeft op 29 april 2014 aan dat de landelijke uitrol wordt gestart.	• De *vertegenwoordiging van Emailaprisoner* en de *Directie Informatievoorziening* zijn betrokken bij vragen over de evaluatie van de pilots.
2 mei 2014 *Invoering*	Vanuit de Directie Informatievoorziening wordt een email gestuurd naar alle Lokaal Implementatie Coördinatoren bij de inrichtingen aangaande de landelijke uitrol van Emailaprisoner. Verzocht wordt om notie te nemen van de dienst en waar nodig te monitoren of vanuit de vestigingen de gewenste acties in gang worden gezet. Een vertegenwoordiging van PI Limburg Zuid reageert met het signaal dat er mogelijk haken en ogen zitten aan Emailaprisoner. Dit zou namelijk blijken uit een signaal van de Security Afdeling van SSC-ICT DJI.	• De *Directie Informatievoorziening* heeft een voorbereiden rol bij de uitrol van Emailaprisoner. • *PI Limburg Zuid* geeft feedback bij de voorbereiding van de uitrol van Emailaprisoner. • De *Directie Informatievoorziening* en de *organisatie van Emailaprisoner* zijn tijdens de uitrol betrokken bij het beantwoorden van vragen vanuit de PI omtrent privacy- en security-aspecten van de berichtenservice.
16 juni 2014 *Invoering*	Een vertegenwoordiging van de Directie Informatievoorziening van DJI stuurt een mail naar de portefeuillehouders informatievoorziening gevangeniswezen aangaande de landelijke uitrol van Emailaprisoner. In de mail wordt verzocht de vestigingsdirecteuren te attenderen dat de berichtenservice van Emailaprisoner in gebruik genomen dient te worden.	• De *portefeuillehouders informatievoorziening gevangeniswezen* hebben een coördinerende rol bij de uitrol van berichtenservice. • De PI-directeuren worden geïnformeerd over de uitrol van de berichtenservice.
11 juli 2014 *Feedback*	Een vertegenwoordiging vanuit PI Rotterdam communiceert naar de directiesecretaris Gevangeniswezen een aantal bedenkingen over het privacy beleid van Emailaprisoner. Ook wordt aangegeven dat er nog een	• PI Rotterdam is betrokken bij het vragen naar het privacy beleid en de, betrouwbaarheid van de aanbieder alsmede het vragen naar een informatie-beveiligingsonderzoek.

	beoordeling moet plaatsvinden naar de betrouwbaarheid van de aanbieder, zijnde Emailaprisoner. Verzocht wordt om een opdracht te verstrekken voor een informatiebeveiligingsonderzoek	
Juli – september 2014 *Politieke aandacht*	Op 18 juli 2014 stellen Kamerleden van de vaste commissie van Veiligheid en Justitie schriftelijk een aantal vragen aan de staatssecretaris over de pilots van Emailaprisoner. Op 2 september 2014 antwoordt de staatssecretaris dat de pilots bij PI's Heerhugowaard, Leeuwarden, Ter Peel en JJI Hartelborgt positief zijn verlopen. Dit heeft hem doen besluiten om de service verder te implementeren, zo licht hij toe. De staatssecretaris geeft aan dat er momenteel in alle PI's voorbereidingen worden getroffen.	• De *staatssecretaris* heeft, met het beantwoorden van de Tweede Kamervragen over de pilots bij PI's Heerhugowaard, Leeuwarden, Ter Peel en JJI Hartelborgt, een informerende rol. • De *staatssecretaris* heeft een besluitvormende rol bij de verdere implementatie van de berichtenservice.
29 september 2014 *Feedback*	De directiesecretaris Gevangeniswezen stuurt de eerdergenoemde zorgen van PI Rotterdam (zie 11 juli 2014) door naar een vertegenwoordiging van de Directie Bestuursondersteuning. Er wordt geantwoord dat DJI niet verantwoordelijk is voor het privacy beleid van Emailaprisoner. DJI kan zich beperken door te zorgen dat een bericht veilig wordt ontvangen, waarna deze conform de reguliere postprocedure kan worden gecontroleerd.	• De *directie GW* heeft een betrokkenheid inzake de feedback vanuit de PI Rotterdam inzake het privacy beleid, de betrouwbaarheid van de organisatie van eMates, alsmede het verzoek tot informatiebeveiligings-onderzoek • Een vertegenwoordiging van de *Directie Bestuurs-ondersteuning* heeft een (ontzorgende) betrokkenheid in het beantwoorden van de feedback vanuit PI Rotterdam
September 2014 – september 2015 *Ingebruikname*	PI's krijgen het bericht dat de berichtenservice geïmplementeerd kan worden. De organisatie van Emailaprisoner gaat bij verschillende PI's langs om een presentatie te geven over de berichtenservice. Bij elke PI afzonderlijk worden afspraken gemaakt over hoe het werkproces omtrent de berichtenservice ingericht dient te worden. Bij operationele problemen die de techniek betreffen, zoals technische storingen, neemt Emailaprisoner contact op met een vertegenwoordiger van de Directie Informatievoorziening van DJI. In tabel 1 staat het totaaloverzicht van wanneer verschillende inrichtingen zijn gestart met het aanbieden van de berichtenservice.	• De *organisatie van Emailaprisoner* is betrokken bij het informeren, implementeren en faciliteren van de uitrol en de ingebruikname van de berichtenservice bij de PI's. • De *PI's* hebben een implementerende rol bij de ingebruikname van de berichtenservice. • De *Directie Informatievoorziening* heeft een faciliterende rol bij operationele en technische problemen inzake de uitrol en het gebruik van de berichtenservice.
1 oktober 2015 *Ingebruikname*	Een vertegenwoordiging van de Directie Informatievoorziening en een vertegenwoordiging van Emailaprisoner geeft bij PI Lelystad aan dat er voldoende akkoord is vanuit het portefeuillehouders Informatievoorziening Gevangeniswezen overleg voor de start met pilot van de antwoordservice: PI Lelystad start als eerste PI met berichten van binnen naar buiten.	• De *Directie Informatievoorziening* en een *vertegenwoordiging van Emailaprisoner* hebben een betrokkenheid bij de pilot ter invoering van de berichtenservice met berichten van *binnen naar buiten*. • *Verschillende PI's* zijn betrokken bij de implementatie van de berichtenservice met antwoordservice.

	Vanaf dit moment starten verschillende PI's met de antwoordservice van Emailaprisoner.	
1 november 2016	Emailaprisoner heet vanaf dit moment eMates	
9 augustus 2017 *Ingebruikname*	Er vindt overleg plaats tussen eMates, een vertegenwoordiging van de Directie Informatievoorziening en de afdeling Beleid van DJI. Besproken wordt hoe eMates werkt. Daarnaast wordt toegelicht dat de organisatie van eMates inzage heeft tot het volledige berichtenverkeer en persoonsgegevens van alle klanten[13]. Uit het onderzoek blijkt niet dat hier verder afspraken over worden gemaakt.	• Het overleg tussen de *organisatie eMates*, *Directie Informatievoorziening en de afdeling Beleid van DJI* heeft het karakter van een hernieuwde kennismaking omtrent de werking van eMates en de toegang van de organisatie eMates tot het volledige berichtenverkeer en persoonsgegevens van alle klanten.
1 september 2017 *Feedback*	Het directiesecretariaat van PI Zwaag stuurt een memo naar de directiesecretariaten van andere PI's waarin zorgen over de berichtenservice worden geuit. Daarnaast wordt beschreven dat na navraag is gebleken dat de directie Gevangeniswezen geen afspraken heeft gemaakt over o.a. de juridische en financiële begrenzing van de berichtenservice. Ter afsluiting verzoekt het directiesecretariaat van PI Zwaag aan de andere directiesecretariaten om gezamenlijk het MT Gevangeniswezen te verzoeken een contract af te sluiten met eMates. Hoe hieraan opvolging wordt gegeven is onduidelijk.	• *PI Zwaag* geeft met de memo, waarin zorgen over de berichtenservice worden geuit, feedback op de berichtenservice een heeft daarmee een signalerende rol. • *PI Zwaag* heeft, met het verzoek aan andere directiesecretariaten om het MT GW te verzoeken een contract af te sluiten, een signalerende rol in de besluitvorming.
18 februari 2019 *Feedback*	Een vertegenwoordiging van de afdeling Beleid van DJI vraagt aan het MT Gevangeniswezen om de berichtenservice te limiteren óf af te schaffen voor gedetineerden in de Extra Beveiligde Inrichting (EBI) en de Terroristen-afdeling (TA). Reden hiervoor is de hoge controlelast die gepaard gaat met het controleren van alle berichten. Hoe opvolging wordt gegeven aan dit verzoek is onduidelijk.	• *DJI Beleid en Bestuursondersteuning* heeft in deze een besluit-voorbereidende rol.
20 februari 2019 *Jurisprudentie*	De Raad voor Strafrechttoepassing en Jeugdbescherming (RSJ) doet uitspraak in een beroepszaak over het niet uitreiken van een eMates bericht door de directeur van PI Vught. Volgens de RSJ had de gedetineerde het bericht moeten ontvangen. Er wordt een schadevergoeding toegezegd.	• De *RSJ* heeft met de jurisprudentie een corrigerende rol in de beleidsbepaling omtrent de berichtenservice.
29 september 2019 *Feedback*	Een vertegenwoordiging van de afdeling Beleid van DJI vraagt via de mail bij een aantal PI's wat hun ervaringen zijn met de berichtenservice van eMates. De reden van de uitvraag is onduidelijk, alsmede de uitkomsten en de eventuele opvolging hierbij.	• *DJI Beleid en Bestuursondersteuning* heeft een initiërende rol bij de uitvraag van ervaringen met de berichtenservice bij een aantal PI's.

[13] *Voor meer informatie over de toegangsbeveiliging van eMates zie bijlage 1: Toegangs-beveiliging – Bedrijfseisen voor toegangsbeveiliging, BIO 9.1.*

16 maart 2020 *Feedback*	De afdeling Beleid van DJI oppert middels een memo de vraag bij het MT Gevangeniswezen welke strategie wordt gehanteerd ten aanzien van eMates. Meer specifiek wordt gevraagd om een landelijk standpunt in te nemen en beleid te formuleren aangaande het aantal berichten en de werkdruk die gepaard gaat met het faciliteren van de berichtenservice.	• *DJI Beleid en Bestuursondersteuning* heeft, met de vraag aan het MT GW om een landelijk standpunt (inzake aantal berichten en werkdruk) in te nemen en beleid te formuleren, een initiërende/ voorbereidende rol in de besluitvorming.
17 april 2020 *Toezicht*	Het MT GW vergadert over eMates. Besproken wordt dat eigenaarschap nu niet goed is belegd, terwijl er aangaande informatiebeveiliging risico's worden onderkent. Besproken wordt dat wordt bezien wat - binnen de context van corona - de meerwaarde is van de berichtenservice. Indien blijkt dat de berichtenservice van meerwaarde is voor gedetineerden, zal er een marktverkenning worden uitgevoerd. Afgesproken wordt dat hier binnen enkele maanden duidelijkheid over moet komen.	• Het *MT GW* heeft een evaluerend en verkennende overleg ten aanzien van het eigenaarschap van de berichtenservice van eMates, de onderkende risico's in de informatievoorziening en de meerwaarde voor gedetineerden van de berichtenservice.
Mei-oktober 2020 *Bijsturing*	De directie van PI Vught overlegt met de organisatie van eMates over het instellen van een limiet aan het aantal berichten. Reden hiervoor is de hoge controlelast die gepaard gaat met het aantal te controleren berichten. Een limiet wordt ingesteld (maximaal tien eMates berichten per week)	• De *PI Vught* en de *organisatie van eMates* hebben een verkennende rol in de besluitvorming omtrent het instellen van een limiet aan het aantal berichten.
28 oktober 2020 *Jurisprudentie*	De RSJ doet uitspraak in een beroepszaak aangaande PI Vught en stelt dat eMates berichten gelijk zijn aan post. Om deze reden is een limiet op eMates berichten niet rechtmatig. De RSJ besluit tot slot dat gedetineerden recht hebben op een schadevergoeding.	• De *RSJ* heeft met de jurisprudentie een corrigerende rol in de beleidsuitvoering van PI Vught, ten aanzien van het limiteren van het aantal berichten.
17 december 2020 *Ingebruikname*	DJI neemt eMates op in het verwerkingsregister onder het thema 'Postafhandeling'.	
29 december 2020 *Jurisprudentie*	De RSJ doet uitspraak in een beroepszaak aangaande PI Vught en stelt wederom dat een limiet op eMatesberichten niet rechtmatig is. In deze zaak draagt een gedetineerde tevens aan dat hij/zij op vrijdag post moet kunnen ontvangen of versturen. Dit beklag verklaard de RSJ ongegrond.	• De *RSJ* heeft met de jurisprudentie, ten aanzien van het limiteren van het aantal berichten, een corrigerende rol in de beleidsuitvoering van PI Vught.
17 juni 2021 *Jurisprudentie*	Wederom doet de RSJ uitspraak in een zaak aangaande eMates, dit keer bij PI Sittard. Zo stelt de RSJ dat de directeur van PI Sittard niet tijdig een bericht heeft uitgereikt aan een gedetineerde. Immers, zo luidt de uitspraak, staat op de site van eMates dat een bericht voor 22:00 verstuurd nog de volgende dag voor 17:00 wordt ontvangen door de gedetineerde. De gedetineerde heeft volgens de RSJ recht op een schadevergoeding.	• De *RSJ* heeft met de jurisprudentie, ten aanzien van het tijdig uitreiken van berichten aan gedetineerden, een corrigerende rol in de beleidsuitvoering van PI Sittard.

21 juli 2021 *Toezicht*	De limiet aan het aantal eMatesberichten bij PI Vught wordt opgeheven.	• *PI Vught* corrigeert, met het opheffen van de limiet aan berichten, haar eigen beleidsbepaling en beleidsuitvoering.
3 december 2021 *Ingebruikname*	Een vertegenwoordiging van eMates vraagt via mail een motivatie aan medewerkers van een PI waarom specifieke berichten worden tegengehouden en niet door de controle komen.	• *De organisatie van eMates* neemt een toezichthoudende houding aan bij het proces.
11 februari 2022 *Toezicht*	Het OM (Hoofdofficier van Justitie Landelijk Parket) stuurt een brief aan de directeur van de EBI. In deze brief uit het OM o.a. haar zorgen over het gebruik van eMates. In overweging wordt gegeven het gebruik van eMates te beperken. Er vindt op 17 februari 2022 een gesprek plaats tussen DJI en het OM.	• Het *OM* heeft met haar brief aan PI Vught een informerende rol omtrent het gebruik van eMates. • Het *OM* heeft met het in overweging geven het gebruik van eMates te beperken een voorbereidende rol in de uiteindelijke besluitvorming ten aanzien van de opschorting.
23 februari 2022 *Toezicht*	Het OM (Hoofdofficier van Justitie Landelijk Parket) stuurt een bericht naar de directeur van DJI, waarin zorgen worden geuit over eMates. Zo verwoordt het OM haar zorgen over de informatiebeveiliging van de berichtenservice.	• Het *OM* heeft met haar bericht aan de directeur van DJI, een signalerende rol omtrent haar zorgen over eMates.
18 maart 2022 *Toezicht*	DJI neemt het besluit om het gebruik van eMates op te schorten bij de verschillende PI's. PI's en eMates worden hierover bericht middels een brief.	• *DJI* heeft een besluitvormende rol in het besluit om de eMates stil te leggen bij de verschillende PI's. • *DJI* heeft een informerende rol bij het informeren van eMates over het stilleggen van de berichtenservice.
28 maart 2022 *Bijsturing*	Het gebruik van de berichtenservice eMates wordt bij alle PI's stopgezet.	• PI's hebben een uitvoerende rol bij het besluit van DJI om eMates stop te zetten.

Context ten tijde van de invoering van eMates

Meerdere geïnterviewden legden uit dat ten tijde van de invoering van eMates het politieke klimaat anders was dan nu: er was relatief veel aandacht voor het intensiveren van re-integratiebeleid en het digitaliseren van het gevangeniswezen. Zo werd er binnen het Ministerie van Justitie en Veiligheid gewerkt aan een initiatief om gedetineerde van een tablet te voorzien om bijvoorbeeld doktersafspraken te maken of boeken te lenen uit een digitale bibliotheek (de zgn. Zelfbedieningsjustitiabelen; ZBJ). Een berichtenservice zoals die van eMates sloot bij deze ontwikkelingen aan en lange tijd werd gedacht dat eMates aan zou sluiten bij het project van ZBJ.

5 Verantwoording onderzoek

5.1 Werkzaamheden en afbakening

Voor de beantwoording van onderzoeksvraag 1 is uitgegaan van de beschikbaar gestelde informatie van DJI, de dienstverlener (eMates) en serviceprovider (Unilink) over de inrichting en beheersing van de informatiebeveiliging van de berichtenservice eMates. DJI heeft een selectie van normen aangeleverd uit de baseline informatiebeveiliging overheid (BIO), welk gebaseerd is op de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017. Deze selectie diende door de ADR gehanteerd te worden als referentiekader binnen dit onderzoek. De opdrachtgever heeft de opdrachtbevestiging met daarin de onderzoeksvragen en het referentiekader opgestuurd naar de dienstverlener. Op basis van dit referentiekader zijn een aantal Prepared-by-Client lijsten (PBC) opgesteld en opgestuurd.
Het onderzoek heeft grotendeels op afstand plaatsgevonden. Aan de hand van de aangeleverde documenten zijn (online) gesprekken gevoerd en per e-mail en telefonisch aanvullende vragen gesteld over de betekenis ervan ten opzichte van de BIO-norm. Waar dat nodig geacht werd, is naar gedetailleerdere informatie en voorbeelden gevraagd. Op basis hiervan zijn in dit rapport per norm bevindingen gegeven met een feitelijk onderbouwing ter beantwoording van de onderzoeksvraag. De feitelijke bevindingen zijn afgestemd met de betrokkenen.

Voor het opstellen van het feitenoverzicht bij onderzoeksvraag 2 zijn er allereerst interviews afgenomen met betrokkenen bij DJI en eMates. Daaropvolgend is bij beide partijen alle documentatie en correspondentie opgevraagd betrekking hebbend op de invoering en ingebruikname van eMates. Ook zijn een aantal PI's bezocht, te weten:

- PI Alphen aan den Rijn;
- PI Lelystad;
- PI Roermond;
- PI Veenhuizen;
- PI Vught.

Bij de PI's zijn groepsinterviews afgenomen. Met betrokkenen is besproken hoe eMates bij de PI is geïntroduceerd en wat de werkwijze omtrent de berichtenservice is geweest. Ter aanvulling hebben deze PI's eveneens hun documentatie en correspondentie aangaande eMates met het onderzoeksteam gedeeld. Van alle interviews zijn gespreksverslagen gemaakt die voor wederhoor zijn teruggelegd bij de geïnterviewden.

In de tweede onderzoeksvraag is aanvankelijk afgesproken alleen de betrokkenheid van de beleidsdirecties van het Ministerie van Justitie en Veiligheid en uitvoerings-organisatie DJI bij de introductie en ingebruikname te onderzoeken. Gedurende het onderzoek bleek al spoedig dat de organisatie van eMates (i.c. Emailaprisoner) bij meerdere events betrokken was. Waar dit het geval was, hebben wij dit aangegeven. Dit is met de opdrachtgever van ons onderzoek besproken.

5.2 Beperkingen van het onderzoek

Zoals eerder beschreven geldt voor beide onderzoeksvragen dat wij ons hebben gebaseerd op de beschikbare informatie die ons is verstrekt door DJI, eMates en Unilink. Om deze reden moeten er een aantal voorbehouden worden gemaakt.

Allereerst hebben wij met betrekking tot onderzoeksvraag 1 in onze beantwoording niet de gewenste diepgang kunnen bereiken. Zo heeft Unilink niet kunnen voldoen aan ons verzoek om voor een aantal normen additionele documentatie aan te leveren, omdat er geen vertrouwelijkheidsverklaring was afgesloten tussen de

opdrachtgever van ons onderzoek en Unilink. Unilink was tevens niet bereid om – in het kader van dit onderzoek – alsnog een vertrouwelijkheidsverklaring met onze opdrachtgever op te stellen, hoewel wij dit wel nadrukkelijk hadden verzocht. Het gevolg is dat wij niet in alle gevallen bij de toetsing van normen voldoende bewijsvoering hebben waargenomen om feitelijke bevindingen te kunnen vaststellen.

Daarnaast bleek tijdens het veldwerk in het kader van onderzoeksvraag 2 dat meerdere betrokkenen bij DJI de organisatie ondertussen hadden verlaten, waardoor niet alle betrokkenen meer bereikbaar waren voor het inplannen van een interview[14]. Daarnaast gaven de meeste geïnterviewden aan zich niet alles meer precies te kunnen herinneren. Om deze reden is het opgestelde feitenrelaas met name gebaseerd op de door eMates en DJI aangeleverde stukken, zgn. *evidence* (zoals interne correspondentie). De volledigheid van deze aanlevering kon door ons niet worden achterhaald, daar wij geen gestructureerd dossier van de introductie en de ingebruikname van de berichtenservice hebben aangetroffen. Zodoende kan niet zonder meer de aanname worden gedaan dat het feitencomplex volledig is: niet alle feiten en/of omstandigheden zijn vermoedelijk boven water gekomen in dit onderzoek. In de tijdlijn zijn events opgenomen die door meerdere bronnen zijn benoemd dan wel bevestigd en/of door documenten worden ondersteund.

5.3 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

5.4 Verspreiding rapport

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

[14] *Betrokkenen die nog bij het ministerie van Justitie en Veiligheid werkten of waarvan contactgegevens nog beschikbaar waren zijn wel benaderd en geïnterviewd.*

6 Ondertekening

Den Haag, 26 januari 2023

Auditdienst Rijk

Bijlage 1: Feitelijke bevindingen inzake informatiebeveiliging en privacy

In deze bijlage behandelen we per hoofdbeveiligingscategorie (gebaseerd op BIO) de beheersmaatregelen die in scope zijn. De feitelijke bevindingen vatten we samen per betrokken partij (eMates, Unilink, DJI). Voor DJI zijn een select aantal normen in scope.

Inleiding

De relatie tussen eMates en Unilink was tot 1 november 2022 niet geformaliseerd in een contract. Hiervoor wordt als reden aangegeven dat Unilink deels eigenaar is van eMates en er in belangrijke mate sprake is van *co-ownership*. eMates had tijdens het onderzoek al aangegeven dat het voornemens is om deze relatie te formaliseren in een klant-leverancierscontract[15] en de operationele samenwerking vast te leggen in afspraken middels een Service Level Agreement met Unilink. Ditzelfde geldt voor het opstellen van een eMates 'Operations en Security Manual', waarin voor een aantal normen de inrichting en beheersing zal worden geformaliseerd.

Unilink beschikt over een ISO27001 certificering; evenals Cyber Essentials Plus-certificeringen en geeft aan dat deze certificeringen zijn uitgegeven door geaccrediteerde partijen in het Verenigd Koninkrijk. Daarnaast beschikt Unilink volgens mededeling over een SOC2 assurance verklaring van Amazon Web Services (AWS). Het Unilink ISO 27001 certificaat en het bijbehorende Statement of Applicability betekent volgens Unilink dat alle normen in scope van deze audit zijn geïmplementeerd door Unilink.

eMates en Unilink geven aan dat deze certificaten naar hun mening aantonen dat Unilink voldoet aan alle normen in scope van deze audit. De inhoud van de onderliggende stukken voor de certificeringen zijn door Unilink als vertrouwelijk aangemerkt, omdat het delen van deze stukken met derde partijen een informatiebeveiligingsrisico voor Unilink vormt. Deze vertrouwelijke stukken zijn voor ons niet inzichtelijk, omdat het ministerie van Justitie en Veiligheid geen overeenkomst heeft met Unilink. De AWS SOC verklaring mag volgens Unilink niet met de ADR gedeeld worden omdat de ADR geen *permitted recipient* is. In de context van deze audit is het volgens Unilink ook niet wenselijk om een geheimhoudingsverklaring tussen beide partijen op te stellen, omdat de certificeringen voldoende zekerheid zou geven en er geen directe aanleiding is om te veronderstellen dat de systemen van Unilink een risico vormen voor hun klanten.

Het gevolg is dat de ADR in het kader van dit onderzoek geen inzage in vertrouwelijke stukken heeft gekregen. Hierdoor is niet te herleiden op welke wijze (met welke diepgang) de ISO 27001 is getoetst door de ISO-auditor en of de scope van de AWS

[15] In het contract is opgenomen dat Unilink als IT-serviceprovider eMates voorziet van 'secure two-way messaging with optional photo attachments provided over Cloud services including: a) registration services for authorised individuals; b) encrypted communications to and from prison establishments; c) hosting/Software as a Service: Unilink supplies hosting platform (AWS Cloud) as well as the application, including Software Lifecycle Management and technical management; d) services are provided according to industry standards e.g. ISO27001 and ISO9001; e) technical support for eMates staff; f) uptime and maintenance window; g) monthly or 'on demand' reporting on performance, information security (digital resilience, i.e. incidents, security patches); h) encryption of data at rest and in transit.'

SOC 2 rapportage overeenkomt met de scope van deze audit. Voor meerdere normen kunnen wij daarom geen feitelijke bevindingen rapporteren.

In onderstaande paragrafen worden enkel de bevindingen beschreven die door ons zijn vastgesteld. We lichten eerst de betreffende norm toe. Vervolgens beschrijven we per partij welke informatie en argumentatie is aangeleverd voor deze norm. Voor elke norm geldt dat wij vanwege de eerder beschreven beperkte diepgang van het onderzoek geen uitspraken kunnen doen in hoeverre er aan de norm wordt voldaan.

Informatiebeveiligingsbeleid - Aansturing door de directie van de informatiebeveiliging (BIO 5.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

5.1.1 Beleidsregels voor informatiebeveiliging
Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.

eMates
eMates heeft per 9 augustus 2022 een informatiebeveiligingsbeleid (Activities, Business Services, Information Security Policy, versie 1.0, d.d. 9 augustus 2022) opgesteld en geformaliseerd, waarin rollen en verantwoordelijkheden, informatiebeveiligings-doelstellingen en databescherming zijn beschreven. Uit de aangeleverde informatie blijkt niet dat voor deze datum een informatiebeveiligings-beleid was vastgesteld. Specifieke onderwerpen, zoals back-ups of malware beveiliging, zijn geen onderdeel van dit beleid.

Unilink
Unilink beschikt over een beleidsdocument waarin het managementsysteem voor informatiebeveiliging (Information Security Management System; ISMS) wordt beschreven; een versienummer en datum ontbreekt op het document Hierin wordt gedefinieerd hoe informatiebeveiliging opgezet, beheerd, gemeten, gerapporteerd en ontwikkeld wordt. Unilink geeft aan dat het informatiebeveiligingsbeleid bestaat uit meerdere losse procedures. Een overzicht van het ISMS laat zien dat het ISMS-procedures bevat voor onder andere strategische uitgangspunten, het wachtwoordbeleid, awareness, fysieke beveiliging privacy en elektronisch berichtenverkeer beschreven, evenals functionarissen binnen de organisatie. De losse procedures zijn niet ter inzage aangeleverd.

Organiseren van informatiebeveiliging - Interne organisatie (BIO 6.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

6.1.2 Scheiding van taken
Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

eMates
Opzetdocumentatie over de functiescheiding is opgevraagd maar niet ontvangen. eMates geeft aan dat er door de beperkte omvang van de onderneming (twee medewerkers) geen sprake is van een ingerichte functiescheiding en dat dit wordt gecompenseerd via logging door de provider(s) die audittrails faciliteert wanneer dat nodig is De implementatie van functiescheiding bij eMates zou volgens eMates resulteren in een *business continuity* risico.

Unilink
Er is opzetdocumentatie over de inrichting van functiescheiding binnen Unilink opgevraagd, maar niet ontvangen. De functiescheiding in het systeem is door de ADR niet ingezien, omdat dit vertrouwelijke informatie betreft. Unilink geeft aan dat de aangeleverde schermafdrukken de functiescheiding aantonen. De (technische) context en metadata ontbreekt bij de schermafdruk waardoor het niet inzichtelijk is of de aangetoonde functiescheiding de systemen van eMates betreft. Volgens mededeling is de inrichting van functiescheiding van eMates als volgt vormgegeven:

- eMates klantenservice, uitgevoerd door de twee medewerkers van eMates.
    - Beide medewerkers hebben toegang tot de eMates managementsite.
- De ontwikkeling van eMates wordt uitgevoerd door drie medewerkers van Unilink.
    - Twee medewerkers hebben toegang tot de onderliggende technologie database en applicaties. Daarnaast hebben beide Unilink medewerkers toegang tot de eMates managementsite.
    - De Unilink DevOps engineer en heeft toegang tot de Cloud omgeving om eMates uit te rollen, resources te managen en performance te monitoren.

Er wordt gebruik gemaakt van een wachtwoordkluis voor het beheer van wachtwoorden voor het beheer van eMates. Deze kluis is alleen toegankelijk voor de wachtwoordkluis beheerder en de drie Unilink werknemers van het NL admin team. De functiescheiding in het systeem hebben we niet ingezien.

Veilig personeel - Voorafgaand aan het dienstverband (BIO 7.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

7.1.1 Screening
Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.

eMates
De opzetdocumentatie voor wat betreft de verificatie van de achtergrond van kandidaten voor een dienstverband is opgevraagd, maar niet ontvangen. eMates heeft aangegeven dat beide medewerkers beschikken over een Verklaring Omtrent Gedrag (VOG). Deze VOG's zijn door ons uitgevraagd en aangeleverd. Daarnaast heeft eMates aangegeven voor beide rollen (directeur en officemanager) bezig te zijn met het formaliseren van de functieomschrijving, waarin ook expliciet de verantwoordelijkheden t.a.v. beveiliging opgenomen zullen worden. De functieomschrijvingen zullen opgenomen worden in een 'eMates Operations and Security manual'.

Unilink
Opzetdocumentatie voor wat betreft de verificatie van de achtergrond van kandidaten voor een dienstverband is opgevraagd, maar niet ontvangen.
Volgens mededeling van Unilink zijn de achtergronden geverifieerd van alle Unilink medewerkers met toegang tot eMates, door de UK Disclosure and Barring Services (DBS). Dit is een uitvoerende non-departementale publieke organisatie. Voorbeelden hiervan zijn vertrouwelijk en zijn niet gedeeld met de ADR.

Veilig personeel – Tijdens het dienstverband (BIO 7.2)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

7.2.1. Directieverantwoordelijkheden
De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.

eMates
Opzetdocumentatie (Information Security Summary Card, V64, van de datum 27 mei 2021) waarin door de directie van alle medewerkers en contractanten geëist wordt dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie is opgevraagd, maar niet ontvangen. Er is een contract met Unilink per 1 november 2022 waarin wordt verwezen naar internationale standaarden voor informatiebeveiliging. eMates heeft aangegeven dat gezien de aard van het werk beide medewerkers zich bewust zijn van de beveiligingsrisico's.

Unilink
Unilink beschikt over opzetdocumentatie waarin door de directie van alle medewerkers en contractanten geëist wordt dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.
Er worden activiteiten ondernomen om informatiebeveiliging(beleid) onder de aandacht te brengen bij het personeel. Dit is aangetoond met een schermafdruk van een Information Security Bulletin email aan Unilink medewerkers.

Dienst Justitiële Inrichtingen
Een strategisch informatiebeveiligingsbeleid (versie 1.0, definitief, d.d. 16 november 2021) is aangetroffen waarin gesteld wordt dat iedere medewerker zelf verantwoordelijk is voor het naleven van beveiligingsmaatregelen, waardoor zij er als individu op aangesproken kan worden. In het document met de inkoopbeleidskaders wordt verwezen naar o.a. de AVG en de informatiebeveiliging en privacy kaders.

De DJI-beleidskaders zijn niet op de berichtenservice eMates toegepast.

Beheer van bedrijfsmiddelen - Informatieclassificatie - (BIO 8.2)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

8.2.1. Classificatie van informatie
Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.

eMates
eMates heeft aangegeven dat invulling van deze norm nog in uitvoering is en ze overwegen om de classificatie van data te formaliseren door Unilink's classificatie model aan te nemen en op te nemen in een 'eMates Operations and Security Manual'.

Unilink
Het Unilink ISMS bevat een procedure voor de classificatie van informatie (geen versienummer en datum). Hierin is beschreven dat de classificatie van informatie plaats vindt volgens gedefinieerde criteria. Op basis hiervan zijn informatieklassen gedefinieerd, alsmede richtlijnen voor het classificeren van informatie en praktische voorbeelden.
Unilink geeft aan dat een schermafbeelding aantoont dat ze beschikt over een informatiebedrijfsmiddelen register waarin de informatiebedrijfsmiddelen van eMates opgenomen zijn. De classificatie voor eMates data is daarin gesteld op PRIVATE. De (technische) context en metadata ontbreekt bij de schermafdruk waardoor het niet inzichtelijk is of dit een registratie in het bedrijfsmiddelenregister betreft. Het bedrijfsmiddelen register is opgevraagd door de ADR, maar niet ontvangen omdat dit een vertrouwelijk document betreft.

Toegangsbeveiliging - Bedrijfseisen voor toegangsbeveiliging (BIO 9.1)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.

9.1.1 Beleid voor toegangsbeveiliging
Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligings-eisen.

9.1.2 Toegang tot netwerken en netwerkdiensten
Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

eMates
Een beleid voor toegangsbeveiliging is opgevraagd, maar niet ontvangen.

eMates heeft aangegeven dat de twee medewerkers in Nederland toegang hebben tot de clouddiensten van Unilink, benodigd voor klant-/consumentenondersteuning en administratieve doeleinden. In de huidige applicatie is het niet mogelijk om de toegang technisch af te schermen zonder daarmee de mogelijkheid te verliezen om gebruikers te assisteren bij het oplossen van problemen of beantwoorden van vragen. De berichten zijn voor de twee medewerkers van eMates en voor een aantal technische beheerders van Unilink uitsluitend toegankelijk als 'privileged access'. eMates geeft voorts aan dat de toegang geen technische en/of bevoorrechte toegang tot de IT-services inhoudt.

Uit ons onderzoek in het kader van het feitenrelaas blijkt dat eMates in augustus 2017 in een overleg met DJI heeft aangegeven inzage te hebben tot het volledige berichtenverkeer en de persoonsgegevens van alle klanten. Tijdens het onderzoek is dat in gesprekken met de directeur van eMates nogmaals bevestigd.

eMates geeft verder aan dat met leverancier Unilink overeen is gekomen dat de huidige applicatie nog dit jaar wordt vervangen door een modern systeem dat beter voldoet aan de hedendaagse beheer- en informatiebeveiligingseisen.

Unilink
Het aangeleverde toegangsbeleid is gericht op logische toegangsbeveiliging, niet op de fysieke toegangsbeveiliging.

In het toegangscontrolebeleid (V39 van de datum 10 februari 2022) is opgenomen dat het beleid (*policy*) en de implementatie (*design)* gebaseerd moet zijn op de bedrijfsbeveiligingseisen zoals gespecificeerd door de eigenaar van de betrokken bedrijfsmiddelen. Aanvullend op deze specifieke eisen vijf algemene principes bij het ontwerpen van maatregelen aangegeven (in het beleid). In het document staan geen specifieke beveiligingseisen voor eMates beschreven.

De beoogde opzet van de netwerkarchitectuur met daarin o.a. segmentering binnen het netwerk (bv. via subnetten) en de implementatie daarvan is niet ontvangen. Hierdoor is het niet inzichtelijk tot welk netwerk en welke netwerkdiensten medewerkers toegang mogen hebben.

Toegangsbeveiliging - Beheer van toegangsrechten van gebruikers (BIO 9.2)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.

9.2.1 Registratie en afmelden van gebruikers

Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

9.2.2 Gebruikers toegang verlenen
Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

9.2.3 Beheren van speciale toegangsrechten
Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.

9.2.4 Beheer van geheime authenticatie-informatie van gebruikers
Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.

eMates
De volgende procedures en/of (proces)beschrijvingen en de implementatie hiervan zijn opgevraagd, maar niet ontvangen:
- Registratie- en afmeldingsprocedure;
- Gebruikerstoegangsverleningsprocedure;
- Beschrijving van het beheer van speciale toegangsrechten;
- Beheerproces voor het toewijzen van geheime authenticatie-informatie.

Volgens mededeling zullen de bovenstaande procedures en (proces)beschrijvingen worden opgenomen in een 'eMates Operations ad security manual'.

Unilink
Het toegangscontrolebeleid van Unilink (V39 van de datum 10 februari 2022) bevat onder andere:
- Registratie- en afmeldingsprocedure;
- Gebruikerstoegangsverleningsprocedure (RBAC, volgens mededeling geldt dit niet voor eMates medewerkers);
- Beschrijving van het beheer van speciale toegangsrechten;
- Beheerproces voor het toewijzen van geheime authenticatie-informatie.

Een voorbeeld is ingezien waaruit het registreren van het verlenen en intrekken van toegang tot de eMates omgeving blijkt.

De ADR heeft geen bestaansvaststellingen kunnen uitvoeren op role-based access control (RBAC), het beheer en de inrichting van speciale toegangsrechten en het beheerproces en de inrichting voor het toewijzen van geheime authenticatie-informatie, omdat deze informatie is uitgevraagd maar niet opgeleverd.

Toegangsbeveiliging - Toegangsbeveiliging van systeem en toepassing (BIO 9.4)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

9.4.1 Beperking toegang tot informatie
Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging

eMates
De volgende procedures en/of (proces)beschrijvingen en de implementatie hiervan zijn opgevraagd, maar niet ontvangen:
- Registratie- en afmeldingsprocedure;
- Gebruikerstoegangsverleningsprocedure;
- Beschrijving van het beheer van speciale toegangsrechten;

- Beheerproces voor het toewijzen van geheime authenticatie-informatie.

Volgens mededeling zullen de bovenstaande procedures en (proces)beschrijvingen worden opgenomen in een 'eMates Operations and security manual'.

Unilink
Het toegangscontrolebeleid van Unilink (V39 van de datum 10 februari 2022) bevat onder andere:
- Registratie- en afmeldingsprocedure;
- Gebruikerstoegangsverleningsprocedure (RBAC, volgens mededeling geldt dit niet voor eMates medewerkers);
- Beschrijving van het beheer van speciale toegangsrechten;
- Beheerproces voor het toewijzen van geheime authenticatie-informatie.

Een voorbeeld is ingezien waaruit het registreren van het verlenen en intrekken van toegang tot de eMates omgeving blijkt.

De ADR heeft geen bestaansvaststellingen kunnen uitvoeren op role-based access control (RBAC), het beheer en de inrichting van speciale toegangsrechten en het beheerproces en de inrichting voor het toewijzen van geheime authenticatie-informatie, omdat deze informatie is uitgevraagd maar niet opgeleverd.

Cryptografie - Cryptografische beheersmaatregelen (BIO 10.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen
Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

eMates
Volgens mededeling zijn zakelijke apparaten van eMates medewerkers versleuteld en lokale (administratieve en ondersteunende) gegevens/informatie worden opgeslagen in de iCloud. Het voornemen is encryptie en compliance te integreren in een eMates Operations and Security Manual.
De ADR heeft de versleuteling en opslag van de gegevens/informatie niet ingezien omdat dit vertrouwelijke informatie betreft. Zie verder norm 13.1.2 voor de bevinding over de VPN-verbinding.

Unilink
Unilink beschikt over een cryptografisch beleid (geen versienummer en datum). In het beleid zijn onder andere de volgende processen/situaties beschreven en bijbehorende technieken:
- *Protection of Code and Restricted or above data on laptops and removable media (symmetric encryption).*
- *Remote Access (VPN, OpenVPN, remote desktopprotocol, etc.).*
- *Identification - signing and verification (public-, private- and asymmetric key).*
- *Website Verification (SSL, TLS 1.3).*

Een schermafdruk van de AWS-encryptie is ingezien. In de schermafdruk komt tot uitdrukking dat het de AWS-site Paris betreft en de database (DB) instance ID nl-live. De (technische) context en metadata ontbreekt bij de schermafdruk waardoor het niet inzichtelijk is of het de database van eMates betreft en dat de volgens mededeling gebruikte encryptietechniek is geïmplementeerd. Bestaansbewijs over *Protection of Code and Restricted or above data*, Unilink *remote access* en *Identification - signing and verification* is opgevraagd, maar niet opgeleverd. Voor *Website Verification* zie verder norm 14.1.3.

Fysieke beveiliging en beveiliging van de omgeving – Beveiligde gebieden (BIO 11.1)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.

11.1.2 Fysieke toegangsbeveiliging
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.

11.1.3 Kantoren, ruimten en faciliteiten beveiligen
Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.

eMates
Volgens mededeling hebben de externe eMates medewerkers geen vaste werkplek en wordt alleen Cloud-based gewerkt. Een vastgesteld document betreffende fysieke beveiliging met daarin een beschrijving van gedefinieerde beveiligingszones en hoe deze zones moeten worden gebruikt en de implementatie daarvan is opgevraagd, maar niet ontvangen.

Unilink
Een fysiek beveiligingsbeleid waarin beveiligingszones zijn gedefinieerd en hoe deze zones moeten worden gebruikt en de implementatie daarvan is niet ontvangen.

Fysieke beveiliging en beveiliging van de omgeving – Apparatuur (BIO 11.2)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

11.2.3 Beveiliging van bekabeling
Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.

eMates
Volgens mededeling wordt door eMates medewerkers alleen remote in de Cloud gewerkt via een VPN.
Door het werken met een VPN is geen bestaansbewijs (fysiek) voor het beveiligen van de bekabeling door de ADR ontvangen.

Unilink
Een fysiek beveiligingsbeleid waarin maatregelen zijn beschreven om voedings- en telecommunicatiekabels te beschermen tegen interceptie, verstoring of schade, en de implementatie daarvan is niet ontvangen.

Beveiliging bedrijfsvoering - Verslaglegging en monitoren (BIO 12.4)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.

12.4.1 Gebeurtenissen registreren
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

12.4.2 Beschermen van informatie in logbestanden
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

12.4.3 Logbestanden van beheerders en operators
Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.

eMates
Volgens mededeling wordt het beheer van logs en audittrails verzorgd door de provider(s) Unilink/AWS. In het recent opgestelde contract (per 1 november 2022) tussen eMates en Unilink is opgenomen dat periodiek en op aanvraag rapportages over performance en informatiebeveiliging worden gedeeld.

Verder is geen bestaansbewijs over de eMates applicatie ontvangen van:
- De rechten van eMates medewerkers op de applicatiesystemen en dat activiteiten van hen hierop worden gelogd.
- De rechten op de logbestanden (bv. eMates medewerkers met leesrechten).
- Periodieke controle op logbestanden.

Unilink
De procedure monitoring van gebruik van IT-systemen (geen versienummer en datum) beschrijft de volgende onderwerpen:

Loggen en bewaken van gebeurtenissen
De bronnen voor het verzamelen van loggegevens met betrekking tot activiteiten en beveiligingsgebeurtenissen zijn onder andere Firewalls/Intrusion detection systems, antivirus protection systems en Windows servers. Eveneens zijn in dit beleid de minimale logstandaarden voor beveiligingsgebeurtenissen beschreven (datum/tijd, uniek gebruikers-ID per activiteit, bron IP-adres, etc.). Ook is meegedeeld dat sommige gebeurtenissen waarschuwingen sturen naar de systeembeheerder en dat logbestanden periodiek op ad-hoc basis worden gecontroleerd. De ISMS18002 procedure maakt niet inzichtelijk:
- Welke logbestanden concreet worden gegenereerd.
- Dat van Linux-servers eveneens logbestanden worden gegenereerd.
- Dat activiteiten van systeembeheerders en operators worden gelogd.
- Een expliciete risicoafweging dat de bewaarperiode van de logging bepaald en welk bewaartermijn na deze afweging gehanteerd moet worden.
- Na welke periode de logbestanden door de scripts worden gewist.

Voorbeelden van het bestaan (en inhoud) van logbestanden zijn niet ingezien. Van zowel het loggen van beheeractiviteiten als het controleren van logbestanden is geen bestaansbewijs opgeleverd. Een schermafdruk *retention periods* (bewaartermijn) is aangeleverd met de uitleg dat de (minimale) bewaartermijnen voor event logging 365 dagen betreft.

Verder is meegedeeld dat foutlogboeken (*error logs*) gegenereerd worden op de AWS-server, maar met AWS is geen Service Level Agreement die formele periodieke monitoring voor eMates specificeert en deze logbestanden normaal gesproken alleen worden geraadpleegd als er een probleem is. Hiervan is geen bestaansbewijs opgeleverd.

Maatregelen beveiligen logbestanden
In het beleidsdocument is beschreven dat Unilink medewerkers beheerdersrechten hebben op hun lokale computer. Zonder toestemming van de Chief Information Security Officer (CISO) mogen medewerkers in geen geval proberen beveiligingslogbestanden uit te schakelen of te verwijderen. Volgens mededeling kunnen alleen medewerkers van beheersites beheeracties in logboeken bekijken. Alle gebruikers kunnen hun eigen log bekijken.

Bestaansbewijs van de rechten (op operating system-niveau) op de logbestanden en het periodiek controleren van de logging is opgevraagd, maar niet ontvangen.

Communicatiebeveiliging – Beheer van netwerkbeveiliging (BIO 13.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

13.1.2 Beveiliging van netwerkdiensten
Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

eMates
Opzetdocumentatie voor wat betreft de inrichting en/of beveiliging van het netwerk door eMates is opgevraagd, maar niet ontvangen. De medewerkers van eMates zijn volgens mededeling sinds dit jaar alleen medewerkers op afstand, zonder een vaste werkplek.
Het is volgens eMates niet mogelijk om de management interface te benaderen zonder VPN. Een drietal schermafdrukken zijn aangeleverd over het aanloggen van een eMates medewerker via VPN. Uit de schermafdrukken is niet af te leiden dat gebruik wordt gemaakt van een VPN.

Unilink
In het Unilink toegangscontrolebeleid (V39 van de datum 10 februari 2022) is beschreven dat externe toegang vanaf door het bedrijf geleverde apparaten standaard is ingeschakeld voor alle Unilink-gebruikersaccounts. De gebruiker is verplicht een VPN-verbinding te gebruiken. In dit beleid is eveneens beschreven dat wanneer een leverancier toegang nodig heeft tot het netwerk dit verloopt via een 'TeamViewer' of vergelijkbare sessie, waarbij de leverancier toegang op afstand krijgt waarbij de sessie gemonitord wordt door een IT-medewerker van Unilink.
Bestaansbewijs van de beveiliging van netwerkdiensten is opgevraagd, maar niet ontvangen.

Communicatiebeveiliging – Informatietransport (BIO 13.2)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.
13.2.3 Elektronische berichten
Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.

13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.

eMates
Opzetdocumentatie over de inrichting en/of beveiliging van beveiliging van elektronisch berichtenverkeer is opgevraagd, maar niet ontvangen. Het wachtwoord voor de batches met berichten van eMates naar de PI's wordt volgens mededeling eenmalig verstrekt, is naar eigen zeggen complex (11 karakters) en ligt opgeslagen in het Unilink-systeem. Ook is aangegeven dat het wachtwoord voor de batches met berichten van eMates naar de PI's gelijk is voor alle locaties.
Ook wordt meegedeeld dat het wachtwoord voor de batches met antwoordformulieren van de PI's naar eMates door de PI wordt vastgesteld en op verzoek van de PI desgewenst wordt gewijzigd; dit wachtwoord verschilt per PI-locatie en wordt eveneens opgeslagen in het huidige Unilink-systeem. Overigens blijkt uit ons onderzoek naar deelvraag 2 (feitenrelaas) dat hieraan in de praktijk verschillend invulling wordt gegeven. Zie onder *DJI* hieronder en onder norm 18.1.4.

eMates geeft aan dat voor zowel eMates-medewerkers als ingehuurd personeel een vertrouwelijkheids- en/of geheimhoudingsovereenkomst zal worden geformaliseerd in een nog te ontwikkelen eMates Operations and Security Manual.
Vertrouwelijkheids- of geheimhoudingsovereenkomsten zijn niet aangeleverd.
Vertrouwelijkheid maakt onderdeel uit van het recent getekende contract (per 1 november 2022) met leverancier Unilink.

Unilink
Opzetdocumentatie over de inrichting en/of beveiliging van beveiliging van elektronisch berichtenverkeer is opgevraagd, maar niet ontvangen. Het verzenden van berichten naar de PI wordt volgens mededeling als volgt beveiligd:
De klanten van eMates voeren hun bericht in op de eMates website. Deze berichten worden versleuteld opgeslagen in de database op het AWS-platform, tot deze naar de PI worden verzonden. Volgens mededeling worden voor iedere PI de berichten met een script in een versleutelde PDF-batch opgenomen. De batch wordt vervolgens verzonden naar de PI, waarbij gebruik wordt gemaakt van OAUTH2 authenticatie en SSL voor encryptie.

Het ontvangen van berichten vanuit een PI wordt volgens mededeling als volgt beveiligd:
In de PI worden de antwoordformulieren geprint en vervolgens ingevuld door de gevangenen. De formulieren bevatten een *header* waarmee de ontvanger kan worden geïdentificeerd. De formulieren worden gescand door PI personeel, samengevoegd in een PDF en vervolgens verzonden naar de Unilink mailbox. Beveiliging van deze mail is afhankelijk van de configuratie van het emailsysteem van de PI. Een script haalt de e-mails op uit de Unilink mailbox en stuurt de afzonderlijke berichten uit de batches door naar de ontvanger (eMates klanten) met behulp van OAUTH2- en SSL-protocollen.
Er is verder geen bestaansbewijs aangeleverd waaruit het beveiligen van elektronische berichten blijkt.

Voor Unilink medewerkers is volgens mededeling een NDA opgenomen in de arbeidsovereenkomst. Hiervan zijn geen voorbeelden aangeleverd.

Dienst Justitiële Inrichtingen
Tijdens ons onderzoek naar de ingebruikname van de berichtenservice hebben we vijf PI's bezocht. Het blijkt dat de PI's verschillend omgingen met het openen en verzenden van berichtenbatches. Zo openden sommigen PI's de versleutelde berichtenbatches met een reeds lang bestaand wachtwoord, terwijl andere PI's geen wachtwoord hoefden in te typen. Ook verstuurden sommige PI's de antwoordbatches versleuteld met een wachtwoord, terwijl anderen dit niet deden. (Zie ook BIO 18.1).

Acquisitie, ontwikkeling en onderhoud van informatiesystemen - Beveiligingseisen voor informatiesystemen (BIO 14.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.

14.1.3 Transacties van toepassingen beschermen
Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

eMates
Er is geen opzetdocumentatie ontvangen wat betreft het beschermen van eMates transacties.

Unilink

Opzetdocumentatie over het beschermen van eMates transacties, ter voorkoming van bijvoorbeeld onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten of onbevoegd openbaar maken en de implementatie daarvan is niet aangeleverd. Uit analyse van de ADR blijkt:

- dat op de website https://login.emates.nl gebruik gemaakt wordt van een *Let's Encrypt* SSL certificaat.
- dat de website TLS 1.0, 1.1, en 1.2 ondersteunt. In NCSC-richtlijnen[16] worden TLS1.0 en TLS1.1 bestempeld als 'Uit te faseren', TLS 1.2 wordt gekenmerkt als 'voldoende'.

Unilink heeft een schermafdruk aangeleverd waarin voor een door AWS gehoste SQL-database te zien is dat encryptie op 'enabled' staat. De (technische) context en metadata ontbreekt bij de schermafdruk waardoor het niet inzichtelijk is of het de database van eMates betreft.

Acquisitie, ontwikkeling en onderhoud van informatiesystemen - Beveiliging in ontwikkelings- en ondersteunende processen (BIO 14.2)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.

14.2.5 Principes voor engineering van beveiligde systemen
Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.

14.2.8. Testen van systeembeveiliging
Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.

eMates
Uit de aangeleverde documentatie Activities, Business Services, Information Security Policy (versie 1.0, d.d. 9 augustus 2022) blijkt dat eMates gebruik maakt van de *webservices* van Unilink, die deze services levert met behulp van AWS-cloudoplossingen. eMates geeft aan dat zij alleen gebruik maakt van ingekochte Cloud Application Services en niet van op maat gemaakte ontwikkeling van IT-applicaties/systemen. In de opzetdocumentatie wordt niet ingegaan op principes voor engineering van beveiligde systemen.

Ook is geen documentatie over het testen van de systeembeveiliging tijdens de ontwikkelactiviteiten ontvangen. Uit het onderzoek is niet gebleken dat tijdens ontwikkelactiviteiten van het informatiesysteem eMates gebruikers en/of eMates bij het testen van de beveiligingsfunctionaliteit betrokken zijn.

Unilink
Engineeringprocedures voor het toepassen van engineering principes in de eMates omgeving zijn opgevraagd, maar niet ontvangen. Unilink geeft aan gebruik te maken van Agile, OWASP en NCSC 10 Cloud principes; dit is door de ADR niet vastgesteld.
Door Unilink is eveneens aangegeven dat de Agile ontwikkelingsmethodiek een testfase bevat. Interne testrapporten zijn door de ADR niet ingezien vanwege vertrouwelijkheid.

Leveranciersrelaties (BIO 15.1)

In het kader van deze BIO-norm is de volgende beheersmaatregel in scope.
15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

[16] *'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.1'*

Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.

eMates
Opzetdocumentatie waarin gesteld wordt dat overeenkomsten met leveranciers eisen horen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie is opgevraagd, maar niet ontvangen.

Er is per 1 november 2022 een contract tussen eMates en Unilink m.b.t. de overeengekomen dienstverlening. Hierin wordt verwezen naar internationale standaarden voor informatiebeveiliging en het maandelijks (of op aanvraag) rapporteren over informatiebeveiliging en performance. De relatie wordt in belangrijke mate bepaald door '*co-ownership*', wat door eMates en Unilink is uitgelegd als een gezamenlijke ontwikkeling en gedeelde verantwoordelijkheden. Unilink geeft aan dat communicatie over de servicelevels tussen Unilink en eMates tot nu toe ad-hoc is en verloopt via e-mails of via de Service Desk.

Per 8 augustus 2022 is er tussen eMates (controller) en Unilink (processor) een *Standard Contractual Clause* (SCC) opgesteld, wat gelijk staat aan een verwerkersovereenkomst. De SCC bevat in annex III technische en organisatorische maatregelen die genomen worden door de processor (Unilink). De SCC heeft alleen betrekking op de beveiliging van persoonsgegevens. Uit de aangeleverde informatie blijkt niet dat er voor 8 augustus 2022 een SCC tussen beide partijen was opgesteld.

Unilink
Opzetdocumentatie waarin wordt beschreven dat overeenkomsten met leveranciers eisen horen te bevatten met betrekking tot informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie is opgevraagd, maar niet ontvangen.
Er is verder geen bestaansbewijs door Unilink aangeleverd t.a.v. de inrichting van controles op hoe leveranciers met hun informatiebeveiligingsrisico's omgaan, respectievelijk mitigeren.

Dienst Justitiële Inrichtingen
Tussen eMates en DJI bestaan geen formele afspraken, overeenkomsten of contracten.

Een vastgesteld strategisch informatiebeveiligingsbeleid (versie 1.0, d.d. 16 november 2021) is ontvangen. Hierin is de borging van informatiebeveiliging in processen beschreven. Over samenwerkingsverbanden is beschreven dat DJI soms gebruik maakt van externe voorzieningen. Hierbij is aandacht voor informatiebeveiliging en privacy. De invulling daarvan en de mate van toezicht hangen af van de aard van de gegevens en met wie wordt samengewerkt.

Beheer van informatiebeveiligingsincidenten - Beheer van informatiebeveiligingsincidenten en verbeteringen (BIO 16.1)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.
16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging
Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.

16.1.7 Verzamelen van bewijsmateriaal

De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

eMates
eMates heeft per 9 augustus beleid (Activities, Business Services, Information Security Policy, versie 1.0, d.d. 9 augustus 2022) waarin opgenomen staat dat het personeel alle inbreuken op de beveiliging en beveiligingsincidenten, feitelijk of vermoedelijk, moet rapporteren aan de directeur.
eMates geeft aan dat in 2021/2022 geen significante beveiligingsincidenten, kwetsbaarheden of datalekken formeel zijn geregistreerd. Mogelijk relevante rapporten, zoals vragen of klachten van klanten werden behandeld als reguliere klantenondersteuning. Dergelijke afhandelingen zijn niet door ons ingezien.

Procedures voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen voor informatiebeveiligingsincidenten is opgevraagd, maar niet ontvangen. eMates deelt mee dat hiervoor Unilink verantwoordelijk is.

eMates heeft de intentie om de informatie-uitwisseling, vastlegging van en verzoeken om rapportage over relevante gebeurtenissen of incidenten te formaliseren in een eMates 'Operations and Security' handleiding. Voor het melden van incidenten aan Unilink zal eMates de Jira servicedesk gaan gebruiken.

Unilink
Unilink geeft aan dat er een aantal beleidsstukken zijn binnen het ISMS, samengevat in een *Information Security Summary Card* (V64, van de datum 27 mei 2021). In deze samenvatting is o.a. een paragraaf over het rapporteren over beveiligingsincidenten opgenomen. Medewerkers en contractanten moeten alle informatiebeveiligingsincidenten, potentiële incidenten of risico's rapporteren aan de ISB (*Information Security Board*) en informatie die kan helpen bij het onderzoeken van het incident noteren.

Unilink geeft aan:
- Dat elke week kwetsbaarheden van het UK National Cybersecurity Centre worden beoordeeld door het ISB, waarbij patches of andere oplossingen worden toegepast zoals benodigd is.
- Dat minimaal wekelijks Common Vulnerabilities and Exposures (CVEs) lijsten worden beoordeeld en hiervoor gebruik gemaakt wordt van Tenable. Patches worden hierbij toegepast zoals benodigd is.
- Dat kwetsbaarheden gedetecteerd op Unilink's systeem, die niet direct verholpen kunnen worden door te patchen, geregistreerd worden via de incident management procedure als zwakke plek.
- Dat een aangeleverde schermafdruk de zwakke plekken toont die in de afgelopen 12 maanden geregistreerd zijn, waarvan er twee relevant zijn voor o.a. eMates. Deze zijn volgens Unilink gemitigeerd.

Er is verder geen bestaansbewijs aangeleverd over de beoordeling van de kwetsbaarheden en CVE's en de opvolging hiervan.

Unilink heeft een samenvatting aangeleverd van de formele Incident Management procedure. Hierin is beschreven dat nauwkeurige registraties moeten worden bijgehouden van de ondernomen acties en het verzamelde bewijsmateriaal. Eenmaal verzameld, moet het bewijsmateriaal op een veilige plaats worden bewaard waar er niet mee kan worden geknoeid. Een bewaarschema waarin registraties en de periode dat ze moeten worden bewaard zijn vastgelegd is opgevraagd, maar niet ontvangen.

Er is geen bestaansbewijs aangeleverd dat de ondernomen acties en het verzamelde bewijsmateriaal nauwkeurig en veilig in een systeem worden geregistreerd.

Unilink geeft aan dat een aangeleverde schermafdruk de (minimale) bewaartermijnen toont die zijn gespecificeerd. De schermafdruk toont voor 'event logging' 365 dagen en voor e-mailberichten zes jaar voor medewerkers (verwijderd na zes maanden na einde dienstverband). Van mogelijke informatiebeveiligingsincidenten van de eMates omgeving is er geen bestaansbewijs van de registratie en afhandeling aangeleverd.

Naleving - Naleving van wettelijke en contractuele eisen (BIO 18.1)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.
18.1.3 Beschermen van registraties
Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.

18.1.4 Privacy en bescherming van persoonsgegevens
Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

eMates
eMates heeft per 9 augustus 2022 beleid (Activities, Business Services, Information Security Policy, versie 1.0, d.d. 9 augustus 2022) waarin beschreven staat dat eMates hun eigen bedrijfsmiddelen en de gegevens en informatie van klanten zal beschermen tegen alle bedreigingen, zowel intern als extern en zowel opzettelijk als per ongeluk. Verder beschrijft het document dat het management en personeel van eMates zich ervan bewust is dat zij een cruciale rol spelen bij het waarborgen van de bescherming van klantinformatie, de beveiliging van eMates bedrijfsmiddelen en (persoons)gegevens. In het beleid wordt verder niet ingegaan op de manier waarop registraties worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.

Er zijn geen richtlijnen ontvangen voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie; er is geen bewaarschema ontvangen waarin registraties en de periode dat ze moeten worden bewaard, zijn vastgelegd.
In het informatiebeveiligingsbeleid wordt verder niet ingegaan op de manier waarop de privacy en bescherming van persoonsgegevens wordt gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Vanuit eMates is geen bestaansbewijs ontvangen waaruit blijkt dat registraties in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde en de periodieke controle daarop.
eMates deelt mee geen bijzondere- of strafrechtelijke persoonsgegevens te verwerken en daarom tot nu toe geen gegevensbeschermingseffectbeoordeling (GEB), in het Engels Data Protection Impact Assessment (DPIA), uitgevoerd te hebben. eMates heeft aangegeven registraties, waaronder persoonsgegevens, te formaliseren en een DPIA te zullen uitvoeren.

eMates geeft aan dat de grondslag voor de verwerking van persoonsgegevens primair 'uitvoering overeenkomst' is, en secundair op basis van toestemming van de betrokkenen (klanten). Op de website van eMates is het privacy beleid van eMates te vinden, waarin wordt uitgelegd welke gegevens waarom worden verzameld en hoe deze gegevens gebruikt worden. In het beleid staat dat persoonlijke gegevens alleen verwerkt worden in overeenstemming met het privacy beleid en met de Algemene Verordening Gegevensbescherming (AVG). Het privacy beleid bevat een e-mailadres waarmee contact opgenomen kan worden met de afdeling Gegevensbescherming.

Zoals beschreven bij onder beheersmaatregel 15.1.3 is er per 8 augustus 2022 tussen eMates (controller) en Unilink (processor) een *Standard Contractual Clause* (SCC)

opgesteld, wat gelijk staat aan een verwerkersovereenkomst. De SCC bevat in annex II een beschrijving van de verwerking, inclusief welke gegevens dit betreft (o.a. NAW-gegevens, e-mailadres, laatste 4 cijfers van betaalkaart, etc.), of gevoelige gegevens worden verwerkt (aangegeven niet van toepassing), de aard van verwerking (EU-datacenter) en meer. Het SCC beschrijft in clausule 9 hoe te handelen bij een inbreuk op persoonsgegevens. In annex III staan de Technische en organisatorische maatregelen opgenomen die genomen worden door de (sub)processor. Per 1 november 2022 heeft eMates een contract met Unilink gesloten, waarin compliance met wet- en regelgeving en privacy en bescherming van persoonlijke gegevens beschreven zijn opgenomen. In het contract wordt ook verwezen naar de SCC.
De ADR heeft geen inzage gehad in de persoonsgegevens die daadwerkelijk verzameld worden. eMates heeft geen gegevensverwerkingsregister maar geeft aan deze te zullen formaliseren, een verwerkersovereenkomst tussen eMates en de PI's of eMates en DJI is opgevraagd, maar niet ontvangen.

Unilink
Unilink heeft een informatie classificatie beleid (geen versienummer en datum). Het beleid definieert vier informatieklassen en bevat richtlijnen en voorbeelden voor het classificeren van informatie. Ook wordt ingegaan op de omgang (*storage, transmission, destruction*) van de verschillende informatieklassen. Er is geen bewaarschema ontvangen waarin registraties en de periode dat ze moeten worden bewaard zijn vastgelegd.
Unilink geeft aan dat ze beschikt over een informatiebedrijfsmiddelen register waarin de informatiebedrijfsmiddelen van eMates opgenomen zijn. De classificatie voor eMates data zijn daarin gesteld op PRIVATE.
Er is geen bestaansbewijs ontvangen over de opslag en verwerking van (klant)gegevens. Ook is geen bestaansbewijs ontvangen van technische- en organisatorische maatregelen beschreven om de bescherming van registraties te waarborgen.

Unilink geeft aan dat er een aantal beleidsstukken zijn binnen het ISMS die allemaal beschikbaar zijn voor werknemers. Hiervan is een samenvatting ingezien door de ADR (Information Security Summary Card, V64, van de datum 27 mei 2021), waarin o.a. een paragraaf over DPA/GDPR opgenomen staat. Hierin staat dat alle medewerkers ervoor moeten zorgen dat persoonlijke gegevens worden behandeld en verwerkt in overeenstemming met de principes uiteengezet in Unilink's gegevensbeschermingsbeleid (Data protection policy), waarin ook de rechten van betrokkenen worden uiteengezet met betrekking tot de manier waarop het bedrijf met hun persoonsgegevens omgaat. Het gegevensbeschermingsbeleid (Data protection policy) is niet aangeleverd.

Unilink heeft aangegeven registraties bij te houden van data die de organisatie verwerkt. Unilink heeft een schermafdruk opgeleverd van deze registratie voor eMates. De context en metadata ontbreekt bij de schermafdruk waardoor het niet inzichtelijk is of registraties worden bijgehouden.

Dienst Justitiële Inrichtingen
DJI heeft een vastgesteld strategisch informatiebeveiligingsbeleid (versie 1.0, definitief, d.d. 16 november 2021). In dit informatiebeveiligingsbeleid zijn de basisprincipes voor informatiebeveiliging en de overkoepelende aanpak voor informatiebeveiliging beschreven. In de aanpak is onder andere het risicomanagement opgenomen om de organisatie brede informatieveiligheidsrisico's met risicoanalyses in kaart te brengen en aan de verantwoordelijke proces- en systeemeigenaren bekend te stellen en dat deze risico's op een aanvaardbare wijze worden afgehandeld.
Het privacy beleid heeft betrekking op alle verwerkingen van alle persoonsgegevens, op papier en digitaal, waarvoor DJI een verantwoordelijkheid heeft. Dit beleid is ook van toepassing op de PI's. In het beleid wordt ingegaan op: de verantwoordelijkheden, taken en bevoegdheden; de uitgangspunten en principes; borging in processen; mens en gedrag.

Tijdens ons onderzoek naar de ingebruikname van de berichtenservice hebben we vijf PI's bezocht. Aldaar is uitgelegd dat de berichten van familieleden en/of vrienden van gedetineerden in een 'batch' (Pdf-bestand) door eMates naar de functionele mailbox van de PI's worden gestuurd. Vier van de vijf PI's geven aan de batch versleuteld is met een verouderd wachtwoord dat sinds de ingebruikname van eMates (Emailaprisoner) nooit is gewijzigd. Een enkele PI geeft aan dat een ontvangen batch zonder wachtwoord geopend kon worden.
Wanneer gebruik wordt gemaakt van de antwoordservice wordt het antwoordvel dat bij het bericht is meegeleverd door de gedetineerde ingevuld. Dit antwoordvel wordt ingescand en omgezet naar een pdf die teruggestuurd wordt naar eMates. Het verschilt per PI of de teruggezonden pdf met een wachtwoord beveiligd wordt.
De PI's geven aan dat de toegang tot de functionele mailbox beperkt is tot een aantal medewerkers.
De ADR heeft geen waarnemingen uitgevoerd op het versleutelde batchbestand, de rechten op de functionele mailbox en het ICT-beheer hiervan.

Er is geen verwerkersovereenkomst tussen eMates en DJI gesloten.
Een Privacy Impact Assessment (PIA) Postafhandeling van de datum 12 april 2022 is met de ADR gedeeld. De PIA is een extractie direct uit het verwerkingsregister van DJI. DJI geeft aan dat de PIA vigerend is en geldt voor heel DJI. Als er een goede reden voor is kunnen PI's hiervan afwijken. Deze afwijkingen moeten dan in een andere PIA worden vastgelegd.
In de PIA Postafhandeling is beschreven dat de grondslag voor het verwerken van gegevens van verdachten en veroordeelden het voldoen aan een op DJI rustende wettelijke verplichting is.
In de PIA is eMates onder de betrokken partijen opgenomen met als rol 'leverancier' en als verantwoordelijkheid 'verwerker'. Gegevens worden over en weer uitgewisseld met de eMates organisatie via beveiligde e-mail.

Naleving - Informatiebeveiligingsbeoordelingen (BIO 18.2)

In het kader van deze BIO-norm zijn de volgende beheersmaatregelen in scope.
18.2.1 Onafhankelijke beoordeling van informatiebeveiliging
De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.

18.2.3. Beoordeling van technische naleving
Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

eMates
Opzetdocumentatie waar wordt ingegaan op de onafhankelijke beoordeling van informatiebeveiliging van eMates en de beoordeling van informatiesystemen op technische naleving is opgevraagd, maar niet ontvangen.
eMates heeft aangegeven dat de dienstverlening voornamelijk afhankelijk is van de provider(s). De veiligheids- en privacy certificering en Assurance verklaring(en) van de provider volgen, meent eMates, uit audits en beoordeling door internationaal erkende auditors en beoordelaars.

Er is geen bestaansbewijs aangeleverd waaruit blijkt dat eMates periodiek de informatiebeveiliging onafhankelijk laat beoordelen. Ook is er geen bestaansbewijs aangeleverd waaruit blijkt dat eMates periodiek de informatiebeveiliging en technische naleving van de applicatie monitort.

Unilink
Zoals eerder aangegeven beschikt Unilink over een beleidsdocument (geen versienummer en datum) waarin het managementsysteem voor informatiebeveiliging (ISMS) wordt beschreven. Hierin staat dat regelmatig wordt beoordeeld hoe de informatiebeveiligings-processen en -procedures worden nageleefd, via gestructureerde management-beoordeling, interne auditbeoordelingen tegen de ISO/IEC 27001 standaard door de ISB en externe audit tegen de standaard om certificering te verkrijgen en te behouden. In dit beleidsdocument wordt verwezen naar een procedure voor ISMS-audits. Deze procedure is niet ontvangen. In dit beleidsdocument wordt niet ingegaan op de beoordeling van informatiesystemen op technische naleving en de frequentie waarin dit dient te gebeuren.

Unilink heeft een ISO 27001 certificaat en een Cyber Essential Plus certificaat van de datum 28 februari 2022. Unilink geeft aan dat zij in mei 2018 een beveiligingstestorganisatie heeft ingeschakeld om een webapplicatiebeoordeling van eMates hebben uit laten voeren, waarbij geen 'hoge' of 'kritieke' kwetsbaarheden zijn gevonden.
Wij hebben geen rapportage van de ISO 27001 certificering, de cyber essentials plus certificering of de webapplicatiebeoordeling ontvangen.

Bijlage 2: Reactie van eMates op de bevindingen inzake informatiebeveiliging en privacy

Gedurende de afgelopen vier maanden (juli 2022 t/m november 2022) heeft de Auditdienst Rijk (ADR) op verzoek van DJI de IT-beveiligingsmaatregelen van eMates en haar belangrijkste leverancier Unilink getoetst.

De ADR heeft deze opdracht zorgvuldig opgepakt, professioneel uitgevoerd en op een prettige en open manier met mij en mijn team gecommuniceerd.

Voorwaar geen sinecure. Bij het begin van de samenwerking tussen DJI en eMates was het immers de uitdrukkelijke wens van DJI om vooral geen formele opdrachtgever/opdrachtnemer-relatie aan te gaan met eMates. Er waren dus vanuit DJI ook geen formele beveiligingseisen beschikbaar op basis waarvan de ADR kon oordelen over opzet, bestaan en werking.

De ADR heeft er daarom voor gekozen de maatregelen te beoordelen op basis van ISO27001/2 normen; *industry best practices*.

Op hoofdlijnen kan ik mij vinden in de *algemene en samenvattende bevindingen per norm* waar het de verantwoordelijkheden en activiteiten van eMates betreft. De audit heeft voor mijn organisatie duidelijk gemaakt dat de activiteiten rond beheer- en gebruikersondersteuning die mijn collega en ik uitvoeren moeten worden beschreven. Ook moet de feitelijke uitvoering daarvan vaker worden gedocumenteerd zodat duidelijker wordt dat eMates voldoet aan de huidige eisen ten aanzien van informatiebeveiliging en gegevensbescherming.

Ondanks de zeer beperkte omvang van mijn organisatie in Nederland zullen wij (ook de reeds bestaande) verantwoordelijkheden en activiteiten nog dit jaar vastleggen in een *eMates Security Operations Manual.*

Enige tijd na de start van de audit richtte de aandacht van de ADR zich mede op onze belangrijkste IT-dienstverlener: Unilink in het Verenigd Koninkrijk. Deze leverancier is - zoals bekend - actief in verschillende landen in de wereld, waaronder Australië, België, Noorwegen en het Verenigd Koninkrijk, Unilink wordt op verzoek van deze overheden/justitiële opdrachtgevers frequent grondig gecontroleerd door gerenommeerde, internationaal geaccrediteerde auditors en instanties op beveiligingsmaatregelen, integriteit en kwaliteit van de dienstverlening.

Hoewel contractuele *right-to-audit*-afspraken en een auditplan ontbraken, hebben management en medewerkers van deze leverancier professioneel en intensief meegewerkt aan de audit door de ADR. Zonder afbreuk te willen doen aan de formele bevindingen van de ADR, overheerst bij mijn team en mij toch de teleurstelling over de *toonzetting* van de rapportage waar het Unilink betreft. In het rapport wordt herhaaldelijk gesteld dat het *aannemelijk* is dat maatregelen zijn geïmplementeerd maar dat de ADR dit niet formeel vast heeft kunnen stellen.

Deze slag om de arm gaat al te makkelijk voorbij aan de integriteit en kwaliteit van de certificering en *assurance statements* en processen waar Unilink continue aan wordt onderworpen. Als gezegd – de beheers- en beveiligingsmaatregelen van Unilink worden doorlopend getoetst door gerenommeerde, internationaal geaccrediteerde auditors en instanties.

Dat gezegd hebbende is de rapportage voor mij wel reden om verbeteringen aan te brengen in het leveranciersmanagement van eMates, te beginnen met het formaliseren van de samenwerking met Unilink de afgelopen tien jaar, waartoe wij inmiddels een overeenkomst hebben gesloten.

Bijlage 3: Managementreactie

Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Auditdienst Rijk

Postbus 20201
2500 EE DEN HAAG

Directie
Eigenaarsadvisering

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
4427922

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 16 januari 2023
Onderwerp Managementreactie rapport 'feitenonderzoek eMates'

Geachte ,

Allereerst dank voor het opgeleverde rapport en de samenwerking met u en uw collega' s van de ADR. De signalen rondom de informatiebeveiliging van eMates waren voor het ministerie van Justitie en Veiligheid aanleiding om eMates tijdelijk op te schorten en onderzoek uit te laten voeren. Vervolgens heb ik u gevraagd dit onderzoek uit te voeren naar de inrichting en beheersing van de informatiebeveiliging van de berichtenservice eMates en de wijze waarop de huidige situatie rond eMates vanaf 2012 heeft kunnen ontstaan.

Voor mij staat voorop dat de bescherming en beveiliging van gegevens op orde moet zijn en dat het toezicht hierop moet zijn ingeregeld. Helaas moet ik constateren dat er geen sluitende afspraken bestaan met eMates en dat vanuit DJI onvoldoende zicht is op de bescherming en beveiliging van deze gegevens. Ik betreur dit. Ik waardeer dat uw rapport goed inzicht geeft in de wijze waarop de berichtenservice is ingericht en in de praktijk van DJI werd gebruikt. Deze bevindingen worden meegenomen bij het maken van de verdere keuzes richting de toekomst.

Op korte termijn wordt de Tweede Kamer geïnformeerd over de uitkomsten van dit rapport.

Hoogachtend,

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00