

Data Protection Impact Assessment

InternetSpiegel

27 maart 2025



Auteurs

Privacy Management Partners:

mr. drs. Jeroen Terstegge CIPP/E, partner

mr. Selina Kerbusch, CIPP/E, CIPM, CIPT, consultant

Bijdragers

Effectory: Wouter Buzing CISO en Lisette Schuilwerpe, Legal Counsel

ICTU: Catharina Kolar

Opdrachtgever

ICTU, programma management InternetSpiegel

Versie: 7.0

© Privacy Management Partners 2025

Privacy Management Partners biedt praktische oplossingen voor behoorlijke en zorgvuldige gegevensverwerking in overeenstemming met de wet.



Versieoverzicht

Versie 1.0	16 juli 2014	Origineel PIA-rapport
Versie 2.0	20 november 2015	Update n.a.v. implementatie verbetermaatregelen
Versie 3.0	7 oktober 2016	Geheel herziene versie, incl. update n.a.v. de AVG en de implementatie van enkele maatregelen
Versie 3.1	3 maart 2017	Enkele aanpassingen n.a.v. commentaar ICTU en Effectory
Versie 4.0	4 oktober 2019	Herziene AVG versie
Versie 4.1	18 september 2020	Herziene versie naar aanleiding van nieuwe aanbesteding. Aanpassingen aan structuur rapport, introductie van bijlagen en toevoeging: ExitMonitor
Versie 5.0	16 november 2020	Herziene versie
Versie 5.1	16 juni 2021	Bijlage met risico's en maatregelen toegevoegd
Versie 5.2	22 juli 2021	Aanpassing naar Rijksmodel DPIA
Versie 5.3	28 juli 2021	Inhoudelijke update na feedback ICTU en Effectory
Versie 6.0	1 februari 2024	Inhoudelijke update na feedback ICTU en Effectory
Versie 7.0	27 maart 2025	Herziene versie naar aanleiding van nieuwe aanbesteding

Inhoud

Versieoverzicht	1
Inleiding en verantwoording	1
• Informatie voor Werkgevers:	3
• Karakter van deze DPIA	3
• Onderzochte partijen	4
• Rapportagestructuur	4
Management samenvatting	5
• Advies FG ICTU op definitieve versie DPIA	5
• Oordeel PMP	5
1 Beschrijving kenmerken gegevensverwerking	7
1.1 Beleidsdoelstellingen en opzet InternetSpiegel	7
1.2 Persoonsgegevens	9
1.3 Gegevensverwerkingen	13
1.4 Verwerkingsdoelen	14
1.5 Betrokken partijen	14
1.6 Belangen bij de gegevensverwerkingen	19
1.7 Verwerkingslocaties	20
1.8 Technieken en methoden van de gegevensverwerkingen	20
1.9 Juridisch en beleidsmatig kader	21
1.10 Bewaartermijnen	22
2 Beoordeling rechtmatigheid gegevensverwerkingen	23
2.1 Rechtsgrond	23
2.2 Bijzondere persoonsgegevens	26
2.3 Doelbinding	26
2.4 Noodzaak en evenredigheid	28
2.5 Rechten van betrokkenen	29
3 Beschrijving en beoordeling risico's voor de betrokkenen en organisatie	32
3.1 Risico's voor rechten en vrijheden van betrokkenen	32
4 Beschrijving maatregelen	38
4.1 Maatregelen	38

Inleiding en verantwoording

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de verantwoordelijkheid voor de kwaliteit van het openbaar bestuur en de wens om de kwaliteit van overheidsmanagement te verbeteren en, in het verlengde daarvan, de prestaties van overheidsorganisaties. Deze ambitie wordt ook wel het stimuleren van goed werkgeverschap genoemd.

De Directie Ambtenaar en Organisatie (A&O) van het ministerie van BZK heeft InternetSpiegel in het leven geroepen voor het verbeteren van de prestaties van overheidsorganisaties. A&O ontwikkelt beleid en kaders onder andere voor de modernisering van het overheidswerkgeverschap, het Strategisch Personeelsbeleid Rijk, versterking van een integere overheid en de inrichting van de P&O-functie van het Rijk.

Het ministerie van BZK/A&O heeft de uitvoering van het concept InternetSpiegel in 2007 ondergebracht bij Stichting ICTU in een eigen programma (Vensters voor medewerkers (<https://www.venster.nl/venster-voor-medewerkers/>)). De voornaamste taak van dit programma is het bevorderen van goed werkgeverschap en bijdragen aan het werkgeluk van medewerkers voor een optimaal presterende overheid. Hiervoor worden verschillende methoden ingezet, waarvan het InternetSpiegel-medewerkersonderzoek er één is.

Het ministerie van BZK biedt, via Stichting ICTU, het medewerkersonderzoek van InternetSpiegel aan vanuit de visie dat de onderzoeksresultaten enerzijds inzichten bieden aan individuele organisaties (middels feedback van de eigen medewerkers) en anderzijds ook zeer waardevol is als informatie over de sector openbaar bestuur als geheel en zo kan worden gebruikt als input voor kennisontwikkeling en beleidsinformatie (o.b.v. statistisch beleidsonderzoek) voor het ministerie van BZK als werkgever van alle ambtenaren, maar ook voor de gehele sector openbaar bestuur.

Gebruik van InternetSpiegel

Als organisaties binnen de sector openbaar bestuur gebruik willen maken van het concept InternetSpiegel, gebeurt dat onder de volgende constructie:

- Het concept InternetSpiegel is eigendom van het ministerie van BZK die de regie en het beheer hiervan heeft ondergebracht bij het programma Venster voor medewerkers bij Stichting ICTU.
- ICTU heeft voor de uitvoering van InternetSpiegel een Europese aanbesteding uitgezet.
- De aanbesteding is gegund aan Effectory. Zij bieden in opdracht van ICTU het InternetSpiegel medewerkersonderzoek aan bij organisaties binnen de sector openbaar bestuur & veiligheid.

- Tussen Effectory en ICTU is een Raamovereenkomst (ROK) afgesloten, inclusief verwerkersovereenkomst (ARVODI 2018). Deze Raamovereenkomst is ingegaan op 3 december 2024 met een looptijd van vier (4) jaar en een optie tot verlenging van twee (2) maal twee (2) jaar.

Het vervolg van de constructie hangt af van het type organisatie. Er zijn namelijk twee typen afnemers: 'Gebruikers' en '(secundaire) Deelnemers':

1. Met de term 'Gebruiker' wordt bedoeld: een organisatie/werkgever die behoort tot de Staat der Nederlanden, de VNG, het IPO en Unie van Waterschappen ('Gebruiker'): de werkgever sluit een projectovereenkomst met ICTU af, waarmee ICTU op eigen naam een nadere overeenkomst (NOK) sluit met Effectory.
2. Met de term 'Deelnemer' wordt bedoeld: een organisatie/werkgever die zich voorafgaand aan de publicatie van de aanbesteding heeft aangesloten aan de aanbesteding ('(Secundaire) Deelnemer'): de werkgever sluit rechtstreeks een nadere overeenkomst (NOK) af met Effectory.

NB. Het onderscheid is overigens voor de bescherming van de persoonsgegevens niet relevant. De bescherming en het beleid daaromheen is in beide constructies gelijk.

Deze afnemers worden voor het doel van de DPIA hierna gezamenlijk **'Werkgever'** genoemd.

De Raamovereenkomst (met als bijlagen alle onderliggende aanbestedingsdocumenten en de ARVODI-2018), de Nadere Overeenkomsten en/of de Projectovereenkomst vormen samen de in artikel 28 lid 3 AVG bedoelde bindende afspraken (verwerkersovereenkomst). Bovengenoemde documentatie vormen de basis voor de wijze waarop ICTU regie voert over de werkzaamheden van Effectory.

ICTU heeft Privacy Management Partners gevraagd om de privacy- en compliance-aspecten van InternetSpiegel in kaart te brengen.

Scope van deze DPIA

In scope van deze DPIA zijn:

- De omgeving waarin het InternetSpiegel-medewerkersonderzoek wordt uitgevoerd die voor alle Werkgevers gelijk is, zoals de overkoepelende grondslag, het platform, en de beveiligingsmaatregelen;
- De aansturing van Effectory door ICTU;
- Het aanleveren en de inhoud van de standaard (pakketten van-) vragenlijsten uit te voeren door de Werkgever.

Out-of-scope zijn:

- De specifieke aanleiding(en) die spelen binnen een Werkgever om medewerkersonderzoek uit te voeren;
- De wijze waarop de Werkgever omgaat met de rapportages;

- Afwijkingen van de standaard vragenlijsten/vragenlijstmodules en/of de standaard werkwijze;
- De processen waarvoor Effectory de verwerkingsverantwoordelijke is, zoals de helpdesk;
- Het beleidsonderzoek door ICTU.¹

Informatie voor Werkgevers:

- **Aanvullende risico-analyse/DPIA:** De eerste drie bullets die hierboven out-of-scope van deze DPIA zijn geplaatst moeten aanvullend op deze DPIA door uzelf worden beoordeeld, inclusief – waar nodig – het vragen van advies aan de FG over de eventuele afwijkingen van de InternetSpiegel-standaard en instemming van uw ondernemingsraad.
- **Statistisch beleidsonderzoek:** Het leveren van een beperkte, geanonimiseerde dataset na afloop van het onderzoek aan ICTU ten behoeve van statistische beleidsonderzoek in het kader van de systeemverantwoordelijkheid van de Minister van BZK voor het functioneren van het openbaar bestuur en het ambtenarenbeleid is een verplicht onderdeel van InternetSpiegel. Deze levering van de gegevens is volledig in overeenstemming met de AVG (art. 5 lid 1 sub b, tweede volzin). ICTU heeft hierover een separaat memo beschikbaar.
- **Betrokkenheid van uw FG:** ICTU en de Werkgever zijn *gezamenlijke verwerkingsverantwoordelijke* (zie voor de onderbouwing par. 1.5). Volgens de Algemene Voorwaarden Verwerking Persoonsgegevens InternetSpiegel, dat tevens de afspraken tussen ICTU en Werkgever bevat als bedoeld in art. 26 AVG, ligt de aansturing van verwerker Effectory exclusief bij ICTU. Dat geldt ook voor de regie op het aanbod (de vragenlijsten) en de voorwaarden om de geanonimiseerde gegevens na afloop te delen met ICTU.
Dit betekent ook dat het toezicht op de naleving van de AVG binnen InternetSpiegel primair bij de FG van ICTU ligt. De FG van ICTU treedt dus mede namens uw FG op als 'gemeenschappelijke FG'. Het is dus niet nodig om deze DPIA voor advies aan uw FG voor te leggen (u kunt deze wel 'ter informatie' voorleggen). Het oordeel en de aanbevelingen van de FG van ICTU staat hieronder in de Management samenvatting. Mocht uw FG desondanks vragen of opmerkingen hebben over InternetSpiegel, kan deze zich – via ICTU – wenden tot de FG van ICTU .

Karakter van deze DPIA

Deze DPIA is primair een beoordeling van de (privacy)risico's voor de medewerkers (hierna '**Respondenten**') die deelnemen aan een medewerkersonderzoek dat door hun Werkgever via InternetSpiegel wordt uitgevoerd. Naast de (privacy)risico's voor de betrokkenen is

¹ Hiervoor is door PMP separaat het 'Memo Statistisch beleidsonderzoek ICTU InternetSpiegel en de AVG' opgesteld.

tevens de compliance van InternetSpiegel met de Algemene Verordening Gegevensbescherming ('AVG') beoordeeld.

Onderzochte partijen

In onderstaande tabel staan de partijen weergegeven die zijn onderzocht in het kader van het DPIA InternetSpiegel.

Partij	Rol bij InternetSpiegel
ICTU	Programmabureau (verwerkingsverantwoordelijke)
Effectory	Verwerker
Microsoft	Subverwerker
MailJet	Subverwerker

Rapportagestructuur

De rapportage bevat de volgende elementen:

- A. Beschrijving kenmerken gegevensverwerkingen
- B. Beoordeling rechtmatigheid gegevensverwerkingen
- C. Beschrijving en beoordeling risico's voor de betrokkenen
- D. Beschrijving voorgenomen maatregelen

In het hoofddeel van het rapport worden deze onderdelen (A-D) doorlopen voor het algemene overkoepelende 'medewerkersonderzoek', oftewel het concept InternetSpiegel. De verschillende vragenlijsten zijn terug te vinden in de bijlagen. Doordat Werkgevers niet altijd alle mogelijk beschikbare vragenlijsten afnemen of slechts delen ervan inzetten, zijn niet alle bijlagen voor iedereen even relevant. In geval van afwijkende situaties of kenmerken leveren de bijlagen aanvullende conclusies bij de algemene aanbevelingen uit het hoofdrapport. De bijlagen met de beoordeling van de vragenlijsten zijn op aanvraag beschikbaar.

Management samenvatting

Advies FG ICTU op definitieve versie DPIA

De DPIA is, op basis van periodieke actualisering, op 24 maart 2025 beoordeeld door de Functionaris Gegevensbescherming van ICTU. De risico's voor betrokkenen zijn verwaarloosbaar. Hij heeft verder geen opmerkingen op de herziene DPIA behalve dat de aanbevelingen van PMP in het oordeel hier gelijk onder door werkgevers bij hen onder de aandacht worden gebracht.

Oordeel PMP

Naleving AVG

Wij hebben in de naleving van de AVG door ICTU en Effectory **geen tekortkomingen** aangetroffen.

(Privacy)risico's betrokkenen

Het gebruik van en deelname aan InternetSpiegel vormt in het algemeen een **verwaarloosbaar** (netto)risico voor de (privacy)belangen van de Respondenten en overige betrokkenen.

In deze DPIA is het beoogde standaard gebruik van InternetSpiegel door Werkgevers getoetst. Het is van belang dat Werkgevers zich realiseren dat er een aantal risico's overblijven die alleen door hen kunnen worden gemanaged. Deze risico's betreffen:

- het onveilig aanleveren van de persoonsgegevens bij Effectory buiten de beveiligde online omgeving van het My InternetSpiegel platform (*risico op datalekken*). NB. Voor Rijksorganisaties die gegevens aanleveren via de technische voorziening van P-Direkt en Effectory is dit risico praktisch niet aanwezig;
- het laten opnemen van aanvullende vragen, met name als deze bijzondere persoonsgegevens betreffen (*risico op onrechtmatige of disproportionele verwerking*);
- het vragen om afgifte² van de onderzoeksgegevens (ruwe data) voor nader eigen onderzoek (*risico op herleidbaarheid tot individuele respondenten en/of risico op onrechtvaardige behandeling van de Respondent of een andere persoon*); en
- te brede verspreiding van onderzoeksrapporten in de organisatie van de Werkgever met informatie met een hoog risico op spontane herkenning van de Respondent en/of met informatie over andere personen, zoals de leidinggevende (*risico op reputatieschade en/of inbreuk op de persoonlijke levenssfeer*).

² Enkel onder aanvullende voorwaarden, waaronder het uitvoeren van een nadere DPIA en het aanbrengen van passende waarborgen, wordt een dergelijk bestand met de ruwe data geleverd aan een Werkgever. Het uitvoeren van de nadere DPIA is de verantwoordelijkheid van de Werkgever.

Bij deze DPIA horen een aantal – bij ICTU opvraagbare – bijlagen met per vragenlijst concrete adviezen en aanbevelingen die risico's bij de Werkgever mitigeren. Wij adviseren dat voor de inhoud en de scope van een *afwijkend onderzoek* door de Werkgever een **aanvullende** eigen analyse wordt gedaan op de privacy- en compliance-aspecten.

Verder bevelen wij aan dat Werkgevers erop letten dat de gegevens veilig aan Effectory worden aangeleverd. Effectory heeft hiervoor gecertificeerde, beveiligde manieren, die binnen de scope vallen van de technische en organisatorische beveiligingsmaatregelen afgesproken tussen ICTU en Effectory.

1 Beschrijving kenmerken gegevensverwerking

1.1 Beleidsdoelstellingen en opzet InternetSpiegel

Directie Ambtenaar en Organisatie (A&O) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is de Opdrachtgever van InternetSpiegel. A&O ontwikkelt beleid en kaders onder andere voor de modernisering van het overheidswerkgeverschap, het Strategisch Personeelsbeleid Rijk, versterking van een integere overheid en de inrichting van de P&O-functie van het Rijk.

InternetSpiegel is vanuit de directie A&O in het leven geroepen voor het verbeteren van de prestaties van overheidsorganisaties. InternetSpiegel is sinds 2007 ondergebracht bij Stichting ICTU in een apart programma. De voornaamste taak van dit programma is **het bevorderen van goed werkgeverschap en bijdragen aan het werkgeluk van medewerkers voor een optimaal presterende overheid**. Hiervoor worden verschillende methoden ingezet, waarvan het InternetSpiegel-medewerkersonderzoek er een is. Het InternetSpiegel-medewerkersonderzoek is een gedegen medewerkersonderzoek waarbij kwaliteitsborging belangrijk is. Zo wordt gewerkt met gevalideerde, wetenschappelijk en praktisch bewezen onderzoeksmodellen inclusief benchmarks. Werkgevers die gebruik maken van InternetSpiegel-medewerkersonderzoek worden optimaal ondersteund omtrent zaken zoals privacy/AVG, instrumenten worden continue doorontwikkeld zodat de nieuwste ontwikkelingen steeds worden meegenomen.

Het onderzoeksproces is gericht op impact: vragenlijsten zijn device-vriendelijk en goed toegankelijk, rapportages zijn online en interactief en op alle niveaus beschikbaar. Daarnaast worden tips en best practices gedeeld.

De uitvoering van InternetSpiegel-medewerkersonderzoek is via een Europese aanbesteding belegd bij Effectory in Amsterdam. Het programma Venster voor Medewerkers (ICTU) bewaakt de kwaliteit van de uitvoering en verzorgt de regie op de doorontwikkeling van het concept InternetSpiegel. Met het concept InternetSpiegel wordt de aanpak en methode bedoeld waarmee individuele publieke instellingen binnen de sectoren openbaar bestuur en veiligheid en hogescholen belevingsonderzoek kunnen doen onder hun eigen medewerkers, waarbij ze zich ook kunnen vergelijken (spiegelen, benchmarken) met andere organisaties. Onderdeel van het concept InternetSpiegel zijn diverse wetenschappelijk gevalideerde vragenlijsten die Werkgevers kunnen voorleggen aan hun medewerkers. De verschillende af te nemen vragenlijsten zijn op moment van schrijven:

- Agressie en weerbaarheid
- Arbeidsomstandigheden
- Exitmonitor
- Instroommonitor
- Integriteit
- Inzetbaarheidsscan

- Psychosociale arbeidsbelasting (PSA)
- Werkbelevingsscan
- Werkdruk

Naast deze vragenlijsten (die door Werkgever wordt gekozen en ingericht) zijn er binnen InternetSpiegel ook nog losse gevalideerde vraagmodules beschikbaar die een Werkgever aanvullend kan opnemen in de geselecteerde vragenlijst.

Via InternetSpiegel wordt de data verzameld. Deze gegevens worden door Effectory geanalyseerd en verwerkt tot geaggregeerde rapportages voor de Werkgever.

Vanuit het programma Venster voor medewerkers bij ICTU wordt kennisdeling gefaciliteerd, bijvoorbeeld door middel van beleidsonderzoek op de resultaten van InternetSpiegel-medewerkersonderzoek en het delen van best practices. Geanonimiseerde gegevens worden door Effectory ieder kwartaal aan Stichting ICTU geleverd. Dit statistisch beleidsonderzoek vindt altijd geaggregeerd plaats per sector of over sectoren heen. Het doel van de kennisdeling is tweeledig: het dient als input voor beleid voor het ministerie van BZK, maar ook het d.m.v. kennisdeling bevorderen van goed werkgeverschap en bijdragen aan het werkgeluk van medewerkers voor een optimaal presterende overheid.³

In technische zin wordt InternetSpiegel-medewerkersonderzoek uitgevoerd door verwerker Effectory B.V., Rokin 16 te Amsterdam. Effectory zorgt voor de feitelijke uitvoering van medewerkersonderzoek(en) bij een Werkgever en verwerkt de resultaten in een rapportage. Daarnaast voert Effectory de administratie van de projecten en voorziet het ICTU van de benodigde verantwoordingsinformatie. Als ICTU besluit tot veranderingen in het instrumentarium van InternetSpiegel, dan wordt de feitelijke ontwikkeling van nieuwe of de doorontwikkeling van bestaande instrumenten in samenwerking met Effectory gedaan.

Ontwikkelingen binnen de markt hebben ertoe geleid dat het InternetSpiegel-medewerkersonderzoek op verschillende manieren afgenomen kan worden. Daartoe worden verschillende pakketten aangeboden aan de Werkgevers, variërend van een eenmalig medewerkersonderzoek tot een continu onderzoekslandschap waarbij verschillende vragenlijsten voor verschillende doelgroepen kunnen worden ingezet. De basis achter al die pakketten zijn wel veelal dezelfde vragen (of constructen/modules) die gezamenlijk de vragenlijsten vormen.

³ Het beleidsonderzoek door ICTU is out-of-scope van deze DPIA, omdat de gegevens geanonimiseerd zijn. PMP heeft ook hier onderzoek naar gedaan. Een memo met bevindingen is beschikbaar bij ICTU.

Met de combinatie van vragenlijsten (van instroom tot uitstroom en met de verschillende typen medewerkersonderzoek) kan een organisatie inzicht krijgen in de gehele employee journey van hun medewerkers.

Het meest uitgebreide pakket biedt nu ook mogelijkheid tot korte “pulse-onderzoeken” waarin specifieke aspecten van vragenlijsten of andere thema’s worden onderzocht.

InternetSpiegel-medewerkersonderzoek wordt aangeboden als software-as-a-service (SaaS). Medewerkers van de aangesloten overheidsorganisaties kunnen via een unieke link online vragenlijsten invullen. Middels een inlog in een platform genaamd *My InternetSpiegel* via Effectory kunnen de medewerkers vervolgens onder andere hun resultaten vergelijken met de geaggregeerde resultaten van de organisatie. De webapplicatie en data draait op het Azure-platform van Microsoft en wordt gehost in het Microsoft datacenter in Nederland (met Ierland als back-up).

1.2 Persoonsgegevens

In de context van het InternetSpiegel-medewerkersonderzoek worden over de medewerkers van Werkgever onderstaande persoonsgegevens verwerkt.

Categorie betrokkenen	Personalia	Type persoonsgegevens	Bron	Doel
Vereiste gegevens voor uitvoering onderzoek				
Medewerker	Naam	Gewoon persoonsgegevens	Werkgever of Respondent	Uitnodiging deelname
Medewerker	Zakelijk e-mailadres	Gewoon persoonsgegevens	Werkgever	Uitnodiging deelname
Medewerker	Afdeling (organogram)	Gewoon persoonsgegevens	Werkgever	Rapportage
Medewerker	Effectory-ID	Pseudoniem	Effectory	Koppeling antwoorden aan een unieke Respondent
Benodigde (verplicht aan te leveren) demografische gegevens (in categorieën t.b.v. statistisch beleidsonderzoek ICTU en tevens te gebruiken door Werkgever in rapportage (resultaten per groep))				
Medewerker	Leeftijdsgroep ⁴	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Geslacht	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage

⁴ De groepen zijn als volgt ingedeeld: jonger dan 30/30-39;/40-49;/50-59/60 en ouder.

Medewerker	Hoogst voltooide opleiding ⁵	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Wel/niet leidinggevende	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Salarisschaal-categorie (alleen Rijksorganisaties) ⁶	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Respondent	Functiegroep ⁷ (alleen Hogescholen)	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Respondent	Type aanstelling (alleen Hogescholen die gebruik maken van de Exitmonitor) ⁸	Gewoon persoonsgegevens	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Respondent	Soort vertrek/instroom (alleen bij Instroommonitor en Exitmonitor Rijk) ⁹	Gewoon persoonsgegevens	Werkgever	Uitnodiging deelname & Statistisch beleidsonderzoek ICTU
Antwoorden op vragen in vragenlijsten				
Respondent	Antwoorden op gesloten vragen uit InternetSpiegel	Gewoon persoonsgegevens	Respondent	Rapportage, Statistisch beleidsonderzoek ICTU
Respondent, Leidinggeven de	Gedrag leidinggevende ¹⁰	Gewoon persoonsgegevens	Respondent	Rapportage
Respondent	Antwoorden in open tekstvelden	<i>Afhankelijk van de vraag (zie bijlage van het</i>	Respondent	Rapportage

5 De groepen zijn als volgt ingedeeld: Basisonderwijs, vmbo, havo-onderbouw, vwo-onderbouw, mbo 1; Havo, vwo, mbo 2, mbo 3, mbo 4; Hbo-bachelor, wo-bachelor, hbo-master, wo-master, doctor.

6 De groepen zijn als volgt ingedeeld: en wordt aangeleverd in de volgende categorieën: 1-4/5-9/10-13/14-15/16 en hoger.

7 De groepen zijn als volgt ingedeeld: onderwijzend personeel en ondersteunend personeel.

8 De groepen zijn als volgt ingedeeld: Aanstelling voor onbepaalde tijd (D-2)/Aanstelling voor bepaalde tijd met uitzicht op aanstelling voor onbepaalde tijd (D-3)/Aanstelling voor bepaalde tijd (D-4)/Detachering of payrolling.

9 De groepen zijn als volgt ingedeeld: Interdepartementaal, intradepartementaal of buiten Rijk.

10 Het gaat hierbij niet om personalia, maar om persoonsgegevens die mogelijk zijn af te leiden uit de antwoorden van Respondenten op vragen over leidinggevend.

		<i>betreffende onderzoek).</i>		
Respondent	Antwoorden in door Werkgever toegevoegde eigen vragen (dus geen InternetSpiegel-vragen)	<i>Afhankelijk van de vraag (zie bijlage van het betreffende onderzoek).</i>	Respondent	Rapportage
Vereiste gegevens specifiek voor instroom- en of uitstroomonderzoek (*)				
Medewerker	Type vertrekkende (alleen Exitmonitor) ¹¹	Gewoon persoonsgegevens	Werkgever	Uitnodiging deelname & Rapportage
Medewerker	Medewerkers-subgroep, bijv. regulier ambtenaar, stagiair, externe	Gewoon persoonsgegevens	Werkgever of P-Direkt	Uitnodiging deelname & Rapportage (indien gewenst)
Medewerker	Type contract, vast en tijdelijk	Gewoon persoonsgegevens	Werkgever of P-Direkt	Uitnodiging deelname & Rapportage (indien gewenst)
Medewerker	Datum in- en uitdiensttreding (alleen bij Instroommonitor en Exitmonitor)	Gewoon persoonsgegevens	Werkgever	Uitnodiging deelname

(*) NB. Voor ander typen onderzoek zijn geen aanvullende gegevens vereist.

Antwoorden

De antwoorden van Respondenten op de vragenlijsten worden in het My InternetSpiegel platform via Effectory op individueel niveau verzameld en bewaard. Op die manier is het mogelijk om een medewerker een persoonlijke rapportage van zijn of haar antwoorden te verstrekken en om een vergelijkingen mogelijk te maken (bijv. met het vorige onderzoek).

Rapportages

Artikel 5 Gedragscode voor Statistisch onderzoek 2022¹² vereist dat rapportages niet herleidbaar zijn tot individuele respondenten. Conform ICTU's instructies hanteert Effectory een strikte responsregel voor rapportages: per organisatieonderdeel (of andere groep, bijvoorbeeld team) moeten minstens vijf medewerkers de vragenlijst hebben ingevuld, en het responspercentage moet minimaal 40% zijn van het betreffende

¹¹ Categorieën: vrijwillig, onvrijwillig en pensioen.

¹² Gedragscode Onderzoek en Statistiek - MOA Expertise Center voor Marketing-insights, Onderzoek en Analytics.

onderdeel.¹³ Het responspercentage van 40% is een methodologische voorwaarde i.v.m. betrouwbaarheid van de resultaten van het onderzoek. Deze ondergrenzen dragen er aan bij dat gerapporteerde gegevens niet herleidbaar zijn tot individuele Respondenten. Het eventuele singling-out-risico wordt ondervangen door het feit dat de rapportage plaatsvindt door middel van een gemiddelde per vraag. Hierdoor is spontane herkenning vrijwel geheel uitgesloten.

In sommige onderzoeken wordt gewerkt met open tekstvelden. De antwoorden die de Respondenten geven in open tekstvelden worden letterlijk overgenomen in de rapportage. Respondenten worden hiervoor gewaarschuwd in het platform en in de privacyverklaring. InternetSpiegel hanteert in de rapportage dezelfde strikte vertrouwelijkheids grenzen als bij de gesloten vragen. Antwoorden op open vragen worden per groep gebundeld gerapporteerd. Daarnaast is het onduidelijk wie welk antwoord heeft gegeven. De kans op spontane herkenning blijft desalniettemin aanwezig. Zie Hoofdstuk 3 voor een verdere toelichting.

Leidinggevenden

Het kan voorkomen dat informatie in de rapportages (indirect) betrekking heeft op het functioneren van een specifieke leidinggevende. Dat is bijvoorbeeld het geval bij (drill-down) rapportages over een specifieke afdeling. Werkgever dient hier bij het verspreiden van de rapportages binnen de organisatie rekening mee te houden. Indien aan de orde wordt dit behandeld in de betreffende vragenlijsten in de bijlagen bij deze DPIA.

Datakwaliteit

De Werkgever is verantwoordelijk voor de juistheid en compleetheid van de aangeleverde persoonsgegevens. Daarmee valt de datakwaliteit in principe buiten de scope van deze DPIA. Effectory voert wel een marginale controle uit op datakwaliteit, zoals evidente fouten of ontbrekende gegevens.

Als de data door P-Direkt geleverd wordt, is de informatie eerst zichtbaar in My InternetSpiegel. Daardoor worden fouten in gegevens al zoveel mogelijk gedetecteerd voordat de vragenlijst per e-mail wordt verstuurd. Het komt soms voor dat een Respondent het niet eens is met zijn of haar organisatorische indeling. In dat geval wordt dit via de betreffende Werkgever teruggekoppeld aan de contactpersoon van Effectory en worden vervolgstappen bepaald.

¹³ In enkele gevallen, bij bepaalde vragenlijsten of wanneer een organisatie ervoor kiest i.v.m. onvoldoende respons, kan er een aangepaste responsregel gelden m.b.t. de 40% respons. Op dit moment is de 40% responsregel losgelaten bij de Exit- en Instroommonitor. Voor toelichting hierop verwijzen we naar de specifieke bijlage(n).

1.3 Gegevensverwerkingen

1.3.1 Verzameling

De personalia en demografische gegevens worden door de Werkgever via de beveiligde online omgeving My InternetSpiegel via Effectory aangeleverd en opgeslagen in de Microsoft Cloud omgeving.

NB. Rijksorganisaties kunnen voor het aanleveren van de personalia en demografische gegevens gebruik maken van de technische voorziening met P-Direkt en Effectory. Door deze gegevens via deze voorziening aan te leveren wordt het risico op datalekken door het onveilig aanleveren van gegevens door de Werkgever verkleind. P-Direkt zorgt dat gegevens van Werkgever pas worden opgenomen in de technische voorziening nadat Werkgever P-Direct rechtstreeks akkoord geeft via een speciaal hiervoor opgesteld formulier.

1.3.2 Vragenlijst/Antwoorden

Effectory nodigt de medewerkers van de Werkgever uit door een uitnodiging te versturen naar het e-mailadres van de medewerker via grootzakelijke e-maildienst van MailJet (zie paragraaf 1.5.5).

De antwoorden op de vragenlijsten worden door de Respondent zelf aangeleverd via de online link waarmee zij de vragen invullen; zij worden in een web-applicatie (in de Microsoft Azure cloud) opgeslagen en vervolgens gepseudonimiseerd door Effectory. De Respondent is overigens niet verplicht om de (hele) vragenlijst in te vullen en kan binnen de vragenlijst vragen overslaan.

1.3.3 Analyse/Rapportage

De binnengekomen antwoorden worden na pseudonimisering gecalculeerd en gerapporteerd door Effectory waarbij rekening gehouden wordt met de responsregel. Antwoorden op open vragen worden in de rapportage letterlijk overgenomen als er aan de minimumrespons eis wordt voldaan. Respondenten wordt geadviseerd om geen direct identificerende gegevens op te nemen in de antwoorden op hun open vraag. Effectory verricht haar taken met in achtneming van de best practices op het gebied van onderzoek en statistiek (vergelijk art. 89.1 AVG).

De Respondenten ontvangen standaard een persoonlijke rapportage via het My InternetSpiegel platform van Effectory met een overzicht van hun eigen antwoorden (eventueel met een vergelijking met de antwoorden van de vorige keer); inclusief een rapportage per team / organisatie / externe benchmark. Alleen indien een Werkgever dit niet toestaat, ontvangt men geen persoonlijke rapportage.

1.4 Verwerkingsdoelen

Het algemene doel van InternetSpiegel kan worden omschreven als **"het genereren van rapportages om inzicht te krijgen in de werkbeleving in de organisatie teneinde hier als organisatie op te kunnen acteren"**. Het is in dit kader van belang om te begrijpen dat het de Werkgever is die bepaalt welk onderzoek wordt uitgevoerd en waarom. **ICTU biedt een aantal standaardonderzoeken die, indien gewenst, door de Werkgever kunnen worden aangepast binnen de regie van ICTU aan diens eigen behoefte**. De verschillende af te nemen vragenlijsten zijn op moment van schrijven:

- Agressie en weerbaarheid
- Arbeidsomstandigheden
- Exitmonitor
- Instroommonitor
- Integriteit
- Inzetbaarheidsscan
- Psychosociale arbeidsbelasting (PSA)
- Werkbelevingsscan
- Werkdruk

Naast deze vragenlijsten (die door Werkgever wordt gekozen en ingericht) zijn er binnen InternetSpiegel ook nog losse gevalideerde vraagmodules beschikbaar die een Werkgever aanvullend kan opnemen in de geselecteerde vragenlijst.

Ieder van die vragenlijsten heeft derhalve zijn eigen specifieke doeleinde. Zie de bijlagen voor de afzonderlijke vragenlijsten waarin specifieke doeleinden worden uitgewerkt.

1.5 Betrokken partijen

Bij de gegevensverwerkingen binnen InternetSpiegel-medewerkersonderzoek zijn de volgende actoren betrokken:

1.5.1 Werkgever

AVG-rol	Verwerkingsverantwoordelijke gegevensverwerking in het kader van het medewerkersonderzoek (<i>gezamenlijk met Stichting ICTU</i>)
Activiteiten	• Levert de personalia en de demografische gegevens van de Werknemers bij Effectory; • Beheert de projectuitvoering, met ondersteuning van Effectory; • Ontvangt de rapportages van Effectory.
Toegang tot persoonsgegevens	De Werkgever heeft toegang tot de door hem aangeleverde gegevens, maar niet tot de antwoorden van de Respondenten.

	<i>Uitzondering:</i> Op specifiek verzoek van de Werkgever kunnen de ruwe onderzoeksgegevens aan de Werkgever beschikbaar worden gesteld voor eigen analyses. Dit levert alsdan risico's op voor de Respondenten die door de betreffende Werkgever zelf moeten worden gemitigeerd (zie ook onze opmerkingen en conclusies elders in deze DPIA). Die verdere verwerking door de Werkgever is buiten de scope van deze DPIA.
--	---

Toelichting

Uit het feit dat de Werkgever bepaalt wanneer een onderzoek wordt uitgevoerd, binnen welke vestigingen of afdelingen en welke vragenlijst van InternetSpiegel wordt afgenomen (eventueel aangevuld met eigen toegevoegde vragen), volgt dat de Werkgever verwerkingsverantwoordelijke is in de zin van de AVG voor de gegevensverwerking in het kader van de uitvoering van het medewerkeronderzoek.

1.5.2 Stichting ICTU

AVG-rol	Verwerkingsverantwoordelijke (<i>gezamenlijk met Werkgever</i>)
Locatie	Den Haag
Activiteiten	• Stuurt als programmaverantwoordelijke de uitvoering van InternetSpiegel en daarmee ook Effectory aan; • Ontwikkelt en bepaalt de inhoud en het aanbod van de vragenlijsten binnen InternetSpiegel alsmede de 'spelregels' rondom het gebruik van InternetSpiegel.
Toegang tot persoonsgegevens	Nee ¹⁴

Toelichting

ICTU bepaalt als programmabureau hoe InternetSpiegel is ingericht, welke onderzoeken worden aangeboden, inclusief welke vragen worden gesteld, en of, en zo ja hoe, Effectory mag meewerken aan specifieke verzoeken van Werkgever. Verder stelt ICTU de bewaartermijnen vast, alsmede het aggregatieniveau in de rapportages en de minimumbeveiligingsmaatregelen. Ten slotte stelt ICTU de Algemene Voorwaarden Verwerking Persoonsgegevens InternetSpiegel vast. Uit dit alles volgt dat ICTU – gelet op het criterium van 'feitelijke invloed' op de gegevensverwerking van de Werkgever (*Jehovah's Getuigen*-arrest van het Hof van Justitie van de Europese Unie, C25/17) –

¹⁴ Na afloop van het onderzoek worden de gegevens in geanonimiseerde vorm aan ICTU geleverd ten behoeve van beleidsonderzoek en kennisdeling in opdracht van BZK. Dit is out-of-scope van deze DPIA. Voor meer informatie over deze beleidsanalyses heeft ICTU een memo beschikbaar.

gezamenlijke verwerkingsverantwoordelijke is voor de verwerking van persoonsgegevens in het kader van het medewerkersonderzoek via InternetSpiegel.

NB. De Algemene Voorwaarden Verwerking Persoonsgegevens, waarmee de Werkgever akkoord gaat bij ondertekening van de Projectovereenkomst, geldt als regeling tussen de gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26 AVG. **Het belangrijkste gevolg van het feit dat Werkgever gezamenlijk met ICTU verwerkingsverantwoordelijke is, is dat een aantal verplichtingen van de verantwoordelijke genoemd in de AVG op grond van de Algemene Voorwaarden exclusief toevallen aan ICTU die deze *mede namens* Werkgever uitvoert, waardoor de Werkgever ontheven is van de verplichting om die AVG-onderwerpen (ook) zelf te regelen.** Tot de exclusief aan ICTU toekomende verplichtingen behoort onder meer het selecteren van de betrouwbare verwerker ex art. 28 lid 1 AVG, het sluiten van een verwerkersovereenkomst met Effectory ex art. 28 lid 3 AVG, en het melden van een eventueel datalek in de omgeving van Effectory bij de Autoriteit Persoonsgegevens ex art. 33 AVG. Het is derhalve niet meer nodig (en door ICTU ook niet toegestaan) dat een Werkgever nog zelf een verwerkersovereenkomst sluit met Effectory. Ook is het niet nodig dat een eventueel datalek bij Effectory door de Werkgever zelf wordt gemeld bij de AP.

NB. De Algemene Voorwaarden Verwerking Persoonsgegevens leggen ook een aantal AVG-verplichtingen exclusief bij de Werkgever, waaronder het informeren van diens medewerkers ex art. 13 AVG, inclusief het feit dat de gegevens in geanonimiseerde vorm beschikbaar worden gesteld aan ICTU voor statistisch beleidsonderzoek ten behoeve van het Ministerie van BZK, het afhandelen van eventuele AVG-verzoeken van zijn medewerkers en het melden van een eventueel datalek bij de medewerker ex art. 34 AVG.

1.5.3 *Effectory*

AVG-rol	Verwerker
Locatie	Amsterdam
Activiteiten	• Verzamelt de personalia en de demografische gegevens; • Nodigt de medewerkers namens Werkgever uit om aan het onderzoek deel te nemen. Stuurt aankondigingen, herinneringen, enz; • Verzamelt de antwoorden op de vragenlijsten; • Pseudonimiseert binnengekomen antwoorden en slaat de onderzoeksgegevens op in haar datawarehouse; • Calculeert de scores en genereert de rapportages; • Verstrekt de onderzoeksresultaten aan de Werkgever (online).

	• Geeft de Respondent inzicht in diens eigen antwoorden in een persoonlijke online rapportage (tenzij de Werkgever heeft aangegeven dat niet te willen).¹⁵
Toegang tot gegevens	• Het team dat het onderzoek uitvoert heeft toegang tot de onderzoeksgegevens; • De medewerkers van de Helpdesk hebben toegang tot de gegevens die samenhangen met de vragen, klachten, problemen of de uitoefening van de AVG-rechten van individuele Respondenten (voor zover Respondenten direct contact opnemen met Effectory); • Het software development team heeft in uitzonderlijke gevallen toegang tot persoonsgegevens voor zover noodzakelijk voor het creëren, onderhouden en beveiligen van de software.¹⁶

Toelichting

Effectory voert namens de Werkgever het medewerkersonderzoek uit. Omdat de gegevensverwerking een significant en onlosmakelijk onderdeel is van de dienstverlening door Effectory, is Effectory aan te merken als een 'verwerker' in de zin van artikel 4 sub 8 AVG.

Effectory richt in opdracht van ICTU het concept InternetSpiegel technisch in. Ook bepaalt ICTU de algemene verwerkingskaders waarbinnen Effectory opereert en waarbinnen het concept InternetSpiegel in de markt wordt gezet, zoals bewaartermijnen en beveiligingsnormen; Effectory geeft daar namens ICTU uitvoering aan. Effectory dient in dat kader dus ook te worden beschouwd als een verwerker van ICTU.¹⁷

Tussen ICTU en Effectory is een Raamovereenkomst InternetSpiegel gesloten (ingang 3 december 2024 met een looptijd van vier (4) jaar en een optie tot verlenging van twee (2) maal twee (2) jaar). Aanvullend zijn er boven op de Raamovereenkomst tussen ICTU en Effectory afspraken ten aanzien van de bescherming van persoonsgegevens gemaakt. Deze zijn vastgelegd in een verwerkersovereenkomst (als bijlage bij de Raamovereenkomst).

¹⁵ De beslissing van de Werkgever om geen persoonlijk rapport te ontvangen heeft geen invloed op het inzage-recht ex art. 15 AVG.

¹⁶ Normaliter heeft het software ontwikkelingsteam geen toegang tot de onderzoeksgegevens. Dit is zowel in de front-end als de backend geregeld. Ingeval van onvoorziene problemen krijgen de eerste- en tweedelijns support engineers toegang tot de onderzoeksgegevens in het kader van de uitvoering van hun rol en taak. Dit is zowel in de front-end als de backend geregeld.

¹⁷ NB. Het dient een punt van voortdurende aandacht te zijn dat Effectory zonder voorafgaand overleg met ICTU geen beslissingen neemt die het doel en/of de essentiële middelen van de gegevensverwerking raken die leiden tot verwerkingsverantwoordelijkheid (art. 28 lid 10 AVG). Als iets onduidelijk is met betrekking tot de verwerking van persoonsgegevens, zal Effectory dus instructie moeten vragen van ICTU.

De Raamovereenkomst (met als bijlagen alle onderliggende aanbestedingsdocumenten en de ARVODI-2018), de Nadere Overeenkomsten en de Projectovereenkomst vormen samen de in artikel 28 lid 3 AVG bedoelde bindende afspraken (verwerkersovereenkomst). Deze documenten vormen de basis voor de wijze waarop ICTU regie voert over de werkzaamheden van Effectory. In de overeenkomsten wordt specifiek aandacht besteed aan de wijze waarop Effectory aandacht dient te besteden aan privacyaspecten. Bovendien worden er systematisch klantonderzoeken uitgevoerd, controleert ICTU (achteraf) de vragen die door Effectory in een onderzoek zijn meegenomen en onderhoudt ICTU contacten met Werkgevers die gebruik maken van InternetSpiegel.

ICTU en Effectory voeren frequent overleg (minimaal eens in de 4-6 weken) over de uitvoering van de onderliggende contracten, inclusief over het borgen van de bescherming van persoonsgegevens, omdat ICTU en Effectory van mening zijn dat zij een zorgplicht hebben jegens de Werkgever op dit gebied. ICTU geeft hieraan invulling door voorwaarden (kaders) te stellen richting Effectory, door toe te zien op naleving van het contract en door contact te houden met de Werkgevers. Effectory geeft hieraan invulling door haar medewerkers te trainen op het gebied van privacy (bewustwordingssessies, introductiemateriaal voor nieuwe medewerkers en door aandacht aan het onderwerp te geven op intranet). Ook heeft Effectory een CISO (Chief Information Security Officer) aangesteld en beschikt het over diverse informatiebeveiligingscertificeringen.

Voor overige informatie over de informatiebeveiligings- en privacymaatregelen bij Effectory zie <https://security.effectory.com>.

1.5.4 Microsoft

Rol partij	Subverwerker (van Effectory)
Locatie	Nederland (primair) en Ierland (back-up)
Activiteiten	• Hosting van het Effectory platform (dataset/antwoorden)
Toegang tot gegevens	Geen (want versleuteld)

Toelichting

Effectory maakt gebruik van de Microsoft Azure clouddiensten (gehost in Nederland, met Ierland als back-up locatie) en valt onder de 'Microsoft Customer Agreement' raamovereenkomst sinds 2021.¹⁸

Microsoft Azure Services heeft veel ISO certificeringen en SOC assurance. Noemenswaardig voor deze DPIA is in het bijzonder de ISO 27018 ('*Protection of personal*

¹⁸ Voor overige informatie wordt verwezen naar <https://security.effectory.com>.

identifiable information in public clouds active as processors'). Meer informatie over hoe Microsoft omgaat met de gegevens is te vinden op het Microsoft Trust Center (Engels).¹⁹

1.5.5 Mailjet

Rol partij	Subverwerker (van Effectory)
Locatie	België en Duitsland (Google)
Activiteiten	Grootzakelijke e-maildienst voor het in korte tijd versturen van bulk mail (uitnodigingen, etc.)
Toegang tot gegevens	Alleen naam en e-mailadres

Toelichting

Mailjet stelt een softwaretool beschikbaar aan Effectory waarmee Effectory o.a. de uitnodigingen voor het onderzoek binnen een kort tijdbestek kan uitsturen zodat onderzoeken zoveel als mogelijk gelijktijdig starten voor medewerkers bij een Werkgever. Mailjet zorgt er ook voor dat deze mailings niet als spam/phishing worden aangemerkt. Dit draagt er aan bij dat mails met de uitnodigingen daadwerkelijk bij de ontvangers in hun postvak arriveren. Mailjet kan in dit kader worden beschouwd als sub-verwerker (van Effectory). Voor het gebruik van Mailjet heeft Effectory een verwerkersovereenkomst afgesloten. Mailjet is ISO 27001 gecertificeerd.²⁰

1.6 Belangen bij de gegevensverwerkingen

1.6.1 Belang van de Werkgever

Het belang van de Werkgever is gelegen in het goed werkgeverschap, meer in het bijzonder het zorgen voor een prettige en veilige werkomgeving voor hun personeel. Met het uitvoeren van medewerkersonderzoek kunnen sluimerende vraagstukken/problemen van onder de oppervlakte boven water gehaald worden.

1.6.2 Belang van ICTU

ICTU is door het Ministerie van BZK (eigenaar van InternetSpiegel) belast met het programmamanagement van InternetSpiegel en heeft als aanbestedende partij en verkrijger van de geanonimiseerde gegevens belang bij de goede en uniforme werking van InternetSpiegel.

¹⁹ Zie hiervoor de volgende webpagina's <https://azure.microsoft.com/en-us/support/trust-center/>, [Cloud Data Integrity and Compliance | Microsoft Trust Center of Service Trust Portal Home Page \(microsoft.com\)](#).

²⁰ Het Google Cloud Platform waar Mailjet gebruikt van maakt heeft ook ISO certificeringen en SOC 2 assurance.

1.6.3 Belang van de Respondenten

Het is in het belang van de Respondenten om een prettige en veilige werkomgeving te hebben. Zij kunnen hieraan bijdragen door mee te doen aan de medewerkersonderzoek via InternetSpiegel. De Respondent kan zijn/haar werkbeleving en eventuele frustraties of suggesties voor organisatieverbetering op een veilige manier uiten.

1.7 Verwerkingslocaties

De gegevensverwerkingen vinden plaats op de volgende locaties:

Gegevensverwerkingen	Verwerkingslocaties
Verwerkingen binnen Effectory	Amsterdam
Verwerkingen binnen Microsoft	Nederland: hosting Ierland: back-up
Verwerkingen binnen Mailjet (Google Cloud)	Frankfurt (Duitsland), en Saint-Ghislain (België)

Er vindt in de opzet van InternetSpiegel-medewerkersonderzoek **geen** gegevensdoorgifte naar een land buiten de Europese Economische Ruimte plaats. Binnen Microsoft Azure wordt de plaats van de gegevensverwerking volledig door de abonnee (Effectory) bepaald. Medewerkers van Microsoft hebben in beginsel geen toegang tot de gegevens van InternetSpiegel. Voor de verwerkingen binnen Mailjet geldt dat de persoonsgegevens in België en Frankrijk worden verwerkt. Internationaal gegevensverkeer (buiten de EEA) is derhalve niet aan de orde.

1.8 Technieken en methoden van de gegevensverwerkingen

1.8.1 Pseudonimisering

De pseudonimisering van de onderzoeksgegevens vindt als volgt plaats:

Na het invullen van de vragenlijst door de Respondent komen de antwoorden binnen in de database van Effectory. In die database worden de antwoorden direct gekoppeld aan een uniek nummer (pseudoniem), namelijk het Effectory ID, en ontdaan van de personalia van de Respondent. Behoudens de verplicht aangeleverde demografische kenmerken (zoals leeftijd, opleiding, geslacht, salarisschaal (indien sector Rijk) en wel/geen leidinggevende functie) zijn er in deze database geen andere kenmerken gekoppeld aan de antwoorden. Het komt soms voor dat er demografische gegevens worden uitgevraagd op de vragenlijst als een Werkgever deze niet vooraf kan aanleveren. De antwoorden op de vragen komen in dat geval direct gepseudonimiseerd binnen in de database van Effectory.

1.8.2 Analyses en rapportages

Op basis van de gepseudonimiseerde gegevens worden scores berekend en de rapportages opgesteld. Dit door de gegevens weer te koppelen met data uit andere databases met groepsindelingen, eerdere metingen en/of achtergrondkenmerken (zgn. demografische gegevens). Ook deze gegevens zijn uitsluitend gekoppeld aan het unieke nummer. De

benodigde gegevens om resultaten te berekenen worden programmatisch (dus zonder tussenkomst van mensen) berekend in een backend proces. Resultaten worden conform de vertrouwelijkheidscriteria (responsregel) per afdeling/team berekend. Het komt voor dat resultaten van afdeling/teams op de hoogste niveaus worden uitgesplitst naar achtergrondkenmerken (zoals leeftijdscategorieën of geslacht).²¹

De resultaten worden na calculatie in een andere database opgeslagen, waarbij aldaar het unieke individuele nummer niet wordt opgeslagen.²² Effectory bewaart de koppeling tussen de personalia en het unieke nummer in een aparte database, onder meer ten behoeve van het uitsturen van herinneringsmails en het kunnen uitoefenen van de rechten van de betrokkene.

1.9 Juridisch en beleidsmatig kader

1.9.1 Beleidsmatig kader

Zoals eerder naar voren kwam is InternetSpiegel in het leven geroepen door de Directie Ambtenaar en Organisatie (A&O) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Dit is gedaan in het kader van de modernisering van het overheidswerkgeverschap, het Strategisch Personeelsbeleid Rijk, versterking van een integere overheid en de inrichting van de P&O-functie van het Rijk.

InternetSpiegel is sinds 2007 door BZK ondergebracht bij Stichting ICTU in een apart programma. De voornaamste taak van dit programma is het bevorderen van goed werkgeverschap en bijdragen aan het werkgeluk van medewerkers voor een optimaal presterende overheid. Hiervoor worden verschillende methoden ingezet, waarvan het InternetSpiegel-medewerkersonderzoek er een is. Het InternetSpiegel-medewerkersonderzoek is een gedegen medewerkersonderzoek waarbij kwaliteitsborging belangrijk is. Zo wordt gewerkt met gevalideerde, wetenschappelijk en praktisch bewezen onderzoeksmodellen inclusief benchmarks. Werkgevers worden optimaal ondersteund omtrent zaken zoals privacy/AVG, instrumenten worden continue doorontwikkeld zodat de nieuwste ontwikkelingen steeds worden meegenomen.

De Minister van BZK krijgt (via de statistische beleidsanalyses van ICTU) uit InternetSpiegel de benodigde beleidsinformatie om zijn systeemverantwoordelijkheid voor het ambtenarenbeleid in Nederland te kunnen invullen en het Parlement te kunnen informeren.

²¹ Uitsplitsing vindt alleen plaats met inachtneming van de vertrouwelijkheidsgrenzen en in opdracht van de Werkgever voor hun eigen rapportages.

²² De databases hebben elk een eigen functie met eigen toegangsbeveiliging.

1.9.2 Juridisch kader

Op de gegevensverwerkingen in InternetSpiegel is geen specifieke wetgeving van toepassing, anders dan de AVG en de UAVG en het algemene arbeidsrecht (goed werkgeverschap).

1.10 Bewaartermijnen

Effectory bewaart in opdracht van ICTU de onderzoeksgegevens op persoonsniveau gedurende de looptijd van de overeenkomst, inclusief eventuele verlengingen/opvolgende overeenkomsten (hierna: 'klantrelatie'). Een half jaar na afloop van de klantrelatie wordt de data verwijderd, tenzij anders afgesproken in de verwerkingsinstructie zoals gegeven door ICTU.²³

Voor het bewaren van de onderzoeksgegevens op persoonsniveau gedurende de klantrelatie, bestaan een aantal goede redenen:

- Werkgevers vragen Effectory geregeld om een verdere en/of andere uitsplitsing;²⁴
- Het stelt Werkgever in staat om de resultaten te vergelijken met de resultaten uit eerdere onderzoeken, inclusief trendanalyse;
- Werkgevers kunnen voor langere periode bepaalde groepen volgen om het effect van interventies in kaart te brengen;
- Een Respondent kan een persoonlijke rapportage ontvangen (alleen eigen antwoorden), inclusief een vergelijkend overzicht met zijn/haar antwoorden in vorige onderzoeken.

Na het verstrijken van de bewaartermijn worden alle gegevens uit de verschillende databases verwijderd, inclusief rapportages in PDF en PPT-format. De verwijderingscyclus wordt dagelijks in gang gezet.

Gedurende de klantrelatie hebben Werkgevers de mogelijkheid om aan Effectory een verzoek te doen om medewerkers en/of andere gegevenssoorten (zoals oude rapportages) te verwijderen. Effectory volgt dit dan op. Respondenten die vertrekken kunnen door de Werkgever ook zelf in het My InternetSpiegel platform worden verwijderd. Er is dus geen automatische faciliteit om de gegevens actueel te houden met het huidige personeelsbestand.

²³ Met de ingang van de nieuwe aanbesteding in 2025 heeft er een verandering plaatsgevonden in het bewaarbeleid van ICTU/InternetSpiegel. De nieuwe bewaartermijn geldt voor zowel nieuwe onderzoeken als voor de reeds uitgevoerde onderzoeken bij dezelfde Werkgever. Zolang er geen nieuw onderzoek is uitgevoerd, vallen de reeds uitgevoerde onderzoeken onder het oude bewaarbeleid (5 jaar na afloop van het onderzoek).

²⁴ Uitsplitsing vindt alleen plaats met inachtneming van de vertrouwelijkheidsgrenzen.

Verder hanteert Effectory de volgende bewaartermijnen:

- Mailjet: gegevens die door Effectory in de Mailjet tool worden verwerkt, blijven maximaal tot zes maanden bewaard na verzending. Reden voor bewaring van de gegevens in de Mailjet tool is voor troubleshooting en bewijsvoering. Denk bij bewijsvoering aan de aantoonbaarheid rondom het verzenden van e-mails wanneer iemand aangeeft deze email nooit te hebben ontvangen.

Categorie Persoonsgegevens	Bewaartermijn
Personalia.	Tot zes maanden na afloop van de klantrelatie.
Demografische gegevens.	Tot zes maanden na afloop van de klantrelatie.
Antwoorden op gesloten vragen	Tot zes maanden na afloop van de klantrelatie.
Antwoorden in open tekstvelden.	Tot zes maanden na afloop van de klantrelatie.
Contactgegevens	Tot zes maanden na verzending.

2 Beoordeling rechtmatigheid gegevensverwerkingen

2.1 Rechtsgrond

2.1.1 *Werkgever*

De rechtsgronden voor de gegevensverwerking in het kader van medewerkersonderzoek zijn:

Categorie Persoonsgegevens	Rechtsgrond
Personalia	Art. 6 lid 1 sub b AVG: uitvoering arbeidsovereenkomst
Demografische gegevens	Art. 6 lid 1 sub b AVG: uitvoering arbeidsovereenkomst
Antwoorden op de vragen	Art. 6 lid 1 sub f AVG: gerechtvaardigd belang

Toelichting

De verwerking van de personalia en de demografische gegevens vormt een *verdere verwerking* van de gegevens die reeds aanwezig zijn in de personeelsregistratie van de Werkgever. De grondslag voor deze verdere verwerking is gelijk aan de grondslag waarvoor de gegevens zijn verzameld door de Werkgever, te weten: de uitvoering van de arbeidsovereenkomst (zie overweging 50 AVG, tweede volzin). Zie voor de analyse van de doelbinding, paragraaf 2.3.1.

De verwerking van de antwoorden op de vragen is een gerechtvaardigd belang van de Werkgever.²⁵ Om een beroep te kunnen doen op artikel 6(1)(f) AVG moeten aan drie criteria worden voldaan:

1. Het belang moet gerechtvaardigd zijn;
2. De verwerking moet noodzakelijk zijn voor dat belang;
3. Het belang van de verwerkingsverantwoordelijke of een derde waaraan de gegevens worden verstrekt moet zwaarder wegen dan het belang van de betrokkene (belangenafweging).

1. Vindt het medewerkersonderzoek plaats in het kader van een belang van de Werkgever of een derde dat gerechtvaardigd is?

Het medewerkersonderzoek vindt plaats in het kader van het belang van de Werkgever om een goed werkgever te zijn en de organisatie op dit punt waar nodig te verbeteren. Ook dient het onderzoek een aantal gerechtvaardigde belangen van de medewerkers (bijv. veilige werkomgeving). Omdat het zijn van 'goed werkgever' een arbeidsrechtelijke verplichting is, is dit belang een rechtmatig belang. Voorts is dit belang voldoende specifiek en vertegenwoordigt het een werkelijk en aanwezig belang.

2. Is de gegevensverwerking noodzakelijk voor het nastreven van dat belang?

In het Meta Platforms-arrest heeft het Hof van Justitie van de Europese Unie uitleg gegeven aan het begrip 'noodzakelijk' in artikel 6 lid 1: *De gegevensverwerking moet **objectief onontbeerlijk** zijn om het doel te bereiken dat een integraal deel uitmaakt van het belang dat door de verwerkingsverantwoordelijke wordt nagestreefd. Dat wil zeggen dat het doel niet zonder de gegevensverwerking kan worden bereikt.*²⁶

De onderzoeken die via InternetSpiegel worden aangeboden, zijn wetenschappelijk gevalideerd. Het betreffende medewerkersonderzoek, dat ten dienste staat aan het goed werkgeverschap, kan daarom niet zonder de gegevens of met minder/andere gegevens worden uitgevoerd. Derhalve kan worden geconcludeerd dat de gegevensverwerking noodzakelijk is voor de behartiging van het belang. Voor de overige gegevens geldt dat ze noodzakelijk zijn om het onderzoek te kunnen starten dan wel om analyses te kunnen maken (in het onderzoek zelf en/of in het statistisch beleidsonderzoek).

3. Wegen de belangen van de betrokkene niet zwaarder dan de belangen van de Werkgever?

Bij deze vraag zijn de volgende vijf aandachtspunten van belang:

²⁵ NB. Uit het feit dat de Respondent het onderzoek het onderzoek vrijwillig invult, mag niet worden afgeleid dat de grondslag 'toestemming' is. Het doen van onderzoek is een gerechtvaardigd belang, mede omdat de specifieke verwerkingen (de analyses) op voorhand niet steeds vaststaan. Derhalve is het juridisch niet mogelijk om de Respondent om toestemming te vragen. Verder zal toestemming van de medewerker vaak ook niet geldig zijn (zie overweging 43 AVG).

²⁶ Hof van Justitie EU, 4 juli 2023 (C-252/21), randnummers 98 en 125.

- i. *Wat is de gerechtvaardigde (privacy)verwachting van de Respondent op dit punt?*
Antwoord: De rapportages zijn anoniem en dat wordt ook aan de Respondent gecommuniceerd.
(Maatregel: InternetSpiegel hanteert in de rapportage strikte vertrouwelijkheids grenzen a.d.h.v. een vastgestelde responsregel en communiceert hierover richting Respondenten in een privacyverklaring).
- ii. *Wat is de context waarin de gegevens worden verzameld?*
Deelname aan het onderzoek is vrijwillig.
(Maatregel: Vanuit InternetSpiegel vindt geen terugkoppeling plaats over welke medewerkers wel/niet aan het onderzoek hebben deelgenomen. Respondenten kunnen ervoor kiezen om de vragenlijst niet in te vullen. Ook kan men binnen de vragenlijst op afzonderlijke vragen ervoor kiezen om geen antwoord te geven).
- iii. *Is de aard van de gegevens gevoelig?*
Dit is afhankelijk van de vragenlijst (zie bijlagen).
(Maatregel: zie bijlagen).
- iv. *Zijn er persoonlijke gevolgen te verwachten voor de Respondent?*
Omdat de rapportages anoniem zijn, zijn er redelijkerwijs geen persoonlijke gevolgen voor de Respondent te verwachten.
(Maatregel: InternetSpiegel hanteert in de rapportage strikte vertrouwelijkheids grenzen. En voorts zijn er binnen Effectory diverse maatregelen genomen om de onderliggende onderzoeksgegevens vertrouwelijk te houden jegens de Werkgever).
- v. *Zijn er passende waarborgen geïmplementeerd om de belangen van de Respondenten te beschermen (zie ook art. 89 AVG)?*
Ja, zie voornoemde maatregelen.

Alles overziend concluderen wij dat de belangen van de Respondenten niet zwaarder wegen dan de belangen van de Werkgever. Aldus kan artikel 6 lid 1 sub f AVG als grondslag dienen voor de gegevensverwerkingen in het kader van het medewerkeronderzoek.

NB. Dit kan anders liggen (met name punten i, iv en v) als de Werkgever afwijkt van de standaard die door ICTU wordt aangeboden en afwijkende vragen opneemt in de vragenlijst of op verzoek zelf de beschikking krijgt over de ruwe data voor eigen nadere analyse. In dat geval moet de Werkgever zelf een nieuwe belangenafweging maken en beoordelen of deze afwijkingen leiden tot risico's voor de Respondenten. Effectory/ICTU kunnen daarin adviseren. Effectory/ICTU informeert de Werkgever over de noodzaak van het uitvoeren van een aanvullende risicoanalyse door de Werkgever en vraagt om het resultaat daarvan, alvorens de ruwe gegevens ter beschikking te stellen. Het is aan de

Werkgever om in zijn organisatie aanvullende waarborgen voor Respondenten te implementeren. Ook dient de Ondernemingsraad van de Werkgever akkoord te gaan met de verstrekking van de onderzoeksgegevens (art. 27 lid 1 sub K WOR). Zie ook de risico/maatregelen tabel in de Bijlage.

2.1.2 ICTU

Ook voor ICTU is de grondslag voor de gegevensverwerking in het kader van het medewerkersonderzoek het **gerechtvaardigd belang** (art. 6 lid 1 sub f AVG). Het toetsingskader ligt hier echter net even anders:

1. Het belang van ICTU is gelegen in de uitvoering van de programmaovereenkomst met het ministerie van BZK en haar opdrachtgeverschap jegens Effectory (aanbesteding). Ook dit zijn belangen die gerechtvaardigd zijn (want niet verboden of maatschappelijk onbetamelijk).
2. De gegevensverwerking is noodzakelijk voor de correcte uitvoering van het medewerkersonderzoek (conform de programma-eisen die ICTU stelt aan InternetSpiegel).
3. De belangen van de betrokkene wegen niet zwaarder dan de belangen van ICTU. Dit is vooral gelegen in de waarborg dat ICTU geen toegang heeft tot de persoonsgegevens die bij Effectory zijn opgeslagen.

2.2 Bijzondere persoonsgegevens

Voor de vraag of in het medewerkersonderzoek bijzondere persoonsgegevens worden verwerkt, verwijzen wij naar de bijlage betreffende het specifieke onderzoek. InternetSpiegel probeert het verwerken van bijzondere persoonsgegevens zoveel mogelijk te vermijden.

NB. Gegevens die betrekking hebben op situaties zoals de duur van ziekteverzuim, verzuimfrequentie, gezondheid, vitaliteit of antwoorden op vragen over thema's als inclusiviteit, slachtofferschap aan incidenten, kunnen in bepaalde gevallen informatie bevatten die te classificeren is als bijzondere persoonsgegevens.

2.3 Doelbinding

In paragraaf 1.4 staan de doeleinden van InternetSpiegel uitgeschreven. Kort samengevat hebben Werkgevers een belang om te weten wat er onder hun medewerkers leeft. Dit vloeit voort uit de wens om de kwaliteit van overheidsmanagement te verbeteren ('goed werkgeverschap') en in het verlengde daarvan de prestaties van overheidsorganisaties te optimaliseren. Zie de afzonderlijke bijlagen voor een uitweiding van de doeleinden per vragenlijst.

2.3.1 Verenigbaar gebruik

Omdat persoonsgegevens alleen voor nevendoeleinden mogen worden gebruikt als deze “niet onverenigbaar” zijn met het doel waarvoor de persoonsgegevens werden verzameld, moet eventueel nevengebruik worden getoetst aan de eisen van de AVG inzake nevengebruik (art. 5 lid 1 sub b en 6 lid 4 AVG).

Binnen de scope van deze DPIA hebben we het volgende nevengebruik van gegevens geconstateerd:

- Gebruik van personalia en demografische gegevens door Werkgever voor het onderzoek voor de uitvoering van het onderzoek door Effectory;

Gebruik personalia/demografische gegevens

De verstrekking van de personalia en demografische gegevens uit de personeelsadministratie van de Werkgever ten behoeve van het medewerkersonderzoek is een vorm van nevengebruik van de gegevens. Artikel 5(1)(b) stelt dat het gebruik van persoonsgegevens voor statistisch onderzoek *geacht wordt* verenigbaar te zijn, zodat er hier geen belemmeringen liggen om de gegevens daarvoor te gebruiken, mits er passende waarborgen worden genomen (zie art. 89 AVG). De gegevens worden door de Werkgever aangeleverd via de beveiligde omgeving van Effectory (of via een beveiligde faciliteit tussen P-Direkt en Effectory rechtstreeks opgehaald). Voorts moet de rapportage zodanig worden vormgegeven dat de scores niet herleidbaar zijn naar individuele medewerkers. Ook dat is het geval binnen InternetSpiegel.

NB. De hiernavolgende gegevensverwerking is een verdere verwerking waarop geen doelbindingstoets hoeft te worden uitgevoerd.²⁷ Voor de volledigheid noemen wij hem hier wel, omdat er mogelijk risico's aan kleven, die door de Werkgever ex art. 89 AVG moeten worden beoordeeld en gemitigeerd.

- Verstrekking ruwe dataset aan Werkgever op verzoek

Het komt voor dat Werkgevers niet alleen behoefte hebben aan een terugkoppeling van de resultaten uit hun InternetSpiegel-medewerkersonderzoek in de vorm van rapportages (de standaard binnen InternetSpiegel), maar dat zij ook zelf over de ruwe data willen beschikken om zo data-analisten binnen de eigen organisatie nadere statistische analyses te kunnen laten doen.

Het op verzoek verstrekken van de ruwe dataset aan de Werkgever voor aanvullend eigen onderzoek is een **afwijking van de standaard werkwijze** waarbij InternetSpiegel als ‘Chinese Muur’ fungeert tussen de Respondenten en hun Werkgever. Dit is zonder

²⁷ HvJ EU, C-77/21, *Digi*, randnummer 34.

doelbindingstoets dus alleen toegestaan als de Werkgever de gegevens uitsluitend gebruikt voor *hetzelfde doel* (medewerkersonderzoek) en daartoe in de eigen organisatie ex art. 89 AVG de nodige aanvullende waarborgen heeft ingebouwd die minstens vergelijkbaar zijn met de waarborgen die reeds door InternetSpiegel worden geboden. ICTU biedt daarvoor de volgende aanvullende waarborgen reeds aan:

- ICTU c.q. Effectory (namens ICTU) wijst de Werkgever op diens verplichting tot het uitvoeren van een aanvullende risicoanalyse;
- De Werkgever moet een formulier 'Uitleg en levering ruwe data' invullen (awareness), dat ondertekend moet worden door twee personen (vier-ogen-principe);
- Het verstrekken van de ruwe dataset aan onderzoeksgegevens vindt alleen plaats als de Respondenten daarover voorafgaand aan het onderzoek expliciet door de Werkgever zijn geïnformeerd via de daarop aangepaste privacyverklaring.

De Werkgever moet, waar nodig, zelf zorgdragen voor de aanvullende waarborgen in de eigen organisatie (eigen 'Chinese Muur'). Indien de Werkgever voor andere doeleinden wil gebruiken dan aanvullende analyses op het medewerkersonderzoek, dan dient de Werkgever zelf een doelbindingstoets uit te voeren. Afhankelijk van welke gegevens onderdeel zijn van de verstrekking, dient de Werkgever ook zelf na te gaan in welke mate de Ondernemingsraad, en/of Functionaris Gegevensbescherming, en/of andere rollen betrokken moeten zijn bij de besluitvorming over deze verstrekking.

Gegevensverwerkingen	Persoonsgegevens	Doeleinden	Oorspronkelijk doel
Gebruik personalia/demografische gegevens door Effectory	Personalialia, demografische gegevens	Uitvoeren van medewerkers onderzoek	Personeelsadministratie
Bij verzoek van Werkgever: Verstrekking ruwe dataset aan Werkgever	Ruwe dataset aan onderzoeksgegevens	Medewerkersonderzoek	Medewerkersonderzoek

2.4 Noodzaak en evenredigheid

2.4.1 Noodzakelijkheid/Subsidiariteit

In beginsel wordt er in de InternetSpiegel niet meer uitgevraagd aan gegevens dan noodzakelijk is om de beschreven beoogde doeleinden te verwezenlijken (zie ook paragraaf 2.1.1).

2.4.2 Proportionaliteit

De gevoeligheid van de persoonsgegevens varieert van *laag* (personalialia, demografische gegevens) tot *gemiddeld of hoog* (afhankelijk van antwoorden op de vragenlijst). De antwoorden van de medewerker worden niet verder verspreid (met uitzondering van incidentele gevallen op specifiek verzoek in het geval van ruwe datalevering). Een verdere uitweiding over de gevoeligheid van de gegevens voortkomend uit de bevroegde

onderwerpen per vragenlijst, is terug te vinden in de afzonderlijke opvraagbare bijlagen.

Om te kunnen borgen dat de beoogde verwerkingsdoeleinden worden bereikt op een wijze die niet of minder nadelig is voor de Respondenten, hanteert Effectory op instructie van ICTU een strikte responsregel voor de vertrouwelijkheid van de onderzoeksgegevens. Hierdoor is spontane herkenning in de praktijk vrijwel uitgesloten. Door het standaard hanteren van deze strikte regels voldoet de standaarddienstverlening binnen InternetSpiegel naar ons oordeel aan de eis van proportionaliteit.

Gelet op het bovenstaande, alsmede het feit dat Respondenten niet verplicht zijn deel te nemen aan medewerkersonderzoek, staan de beschreven verwerkingsdoeleinden in evenredige verhouding tot de inbreuk op de persoonlijke levenssfeer en de bescherming van persoonsgegevens van Respondenten.

2.5 Rechten van betrokkenen

Betrokkenen (d.w.z.: Respondenten) hebben onder de AVG een aantal rechten bij de verwerking van hun persoonsgegevens in het kader van medewerkersonderzoek:

- Het recht op informatie;
- Het recht op inzage in hun persoonsgegevens;
- Het recht op correctie (verbetering, aanvulling) van hun persoonsgegevens;
- Het recht op verwijdering van hun persoonsgegevens;
- Het recht op beperking van de verwerking;
- Het recht op bezwaar tegen de gegevensverwerking.

NB. Overige rechten zoals beschreven in de AVG zoals het recht op dataportabiliteit en het recht om niet te worden onderworpen aan een geautomatiseerd besluit, inclusief profiling, zijn niet van toepassing op InternetSpiegel-medewerkersonderzoek.

Voordat een verzoek, bezwaar of klacht in behandeling kan worden genomen, moet de identiteit van de betrokkene worden vastgesteld. Effectory neemt de volgende stappen om de betrokkene namens ICTU en Werkgever te identificeren:

- verzoek, bezwaar of klacht per email ontvangen: het emailadres dat is gekoppeld aan het ontvangen bericht wordt vergeleken met het bij Effectory bekende e-mailadres;
- verzoek, bezwaar of klacht telefonisch ontvangen: de Effectory Helpdesk agent stelt twee controlevragen ter verificatie van de identiteit van de betrokkene. Na afronding van het telefoontje wordt ook altijd een e-mail gestuurd naar het bij Effectory bekende e-mailadres over het telefoontje. Indien de ontvanger van de e-mail zich hier niet in herkent, worden hierop corrigerende acties genomen.

2.5.1 *Recht op informatie*

Respondenten moeten worden geïnformeerd over de verwerking van hun persoonsgegevens. Ten minste moeten de Respondenten worden geïnformeerd over de identiteit en contactgegevens van de gezamenlijke verantwoordelijken (Werkgever en ICTU), de doeleinden van het onderzoek waaraan zij deelnemen, het hergebruik van de geanonimiseerde gegevens door ICTU ten behoeve van statistisch beleidsonderzoek, de bewaartermijnen, de pseudonimisering van de gegevens, (indien van toepassing) de eventuele verstrekking van de gegevens aan de Werkgever en de daarvoor ingebouwde extra waarborgen en de wijze waarop zijn hun rechten kunnen uitoefenen.

De verwerkingsverantwoordelijke is verantwoordelijk voor deze informatie. Voor InternetSpiegel-medewerkersonderzoek zijn er echter twee verantwoordelijken: ICTU en de Werkgever. Deze moeten onderling bepalen wie de Respondent waarover informeert. Dit is vastgelegd in de *Algemene Voorwaarden Bescherming Persoonsgegevens InternetSpiegel*. Daarbij zij opgemerkt dat de informatie moet worden verstrekt uiterlijk bij de start van het onderzoek.

- Binnen de InternetSpiegel-omgeving wordt de Respondent geïnformeerd door middel van een algemene privacyverklaring van InternetSpiegel,
- Bij afwijkingen van de standaardwerkwijze kan deze worden aangepast door Werkgever. Daarnaast is er vanuit Effectory materiaal beschikbaar over de borging van de vertrouwelijkheid.²⁸

NB. Wij wijzen erop dat de inhoud van de privacyverklaring bepalend is voor de vraag of de gegevens (in de vorm van ruwe data) op een later tijdstip aan de Werkgever kunnen worden verstrekt. Uitgangspunt bij het gebruik van InternetSpiegel is dat de gegevens niet aan de Werkgever worden verstrekt. Dit wordt ook expliciet zo medegedeeld in de standaard privacyverklaring van InternetSpiegel. Derhalve bepaalt de privacyverklaring de gerechtvaardigde privacyverwachting die de Respondent heeft als hij/zij antwoord geeft op de vragenlijst.

Niettemin komt het geregeld voor dat Werkgevers achteraf vragen om de aanlevering van de gegevens op individueel niveau. Deze functionaliteit is echter om privacyredenen niet beschikbaar binnen InternetSpiegel. De Werkgever, die de gegevens wenst te gebruiken voor het maken van eigen aanvullende analyses, dient zijn medewerkers dus voorafgaand aan de start van het onderzoek expliciet te informeren over deze afwijkende gegevensverstrekking, zodat ze een eigen afweging kunnen maken bij de beantwoording van de vragenlijst. Daarmee dwingt ICTU de Werkgever om vooraf een belangenafweging te maken en binnen zijn organisatie de nodige waarborgen op te tuigen om de belangen van de Respondenten te beschermen.

²⁸ Deze informatie is beschikbaar via <https://helpdeskininternetspiegel.effectory.com/> en <https://support.effectory.com>.

2.5.2 *Recht op inzage*

Het inzage-recht van de betrokkenen wordt (deels) geregeld door het feit dat een Respondent na het invullen van de vragenlijst kan aangeven of hij/zij een persoonlijke rapportage met zijn/haar antwoorden wil ontvangen via de portal. Indien de werkgever deze optie uitsluit, kan de Respondent ook een kopie van de verwerkte gegevens (of een omschrijving hiervan) ontvangen.

2.5.3 *Recht op correctie, verwijdering, beperking of bezwaar*

Respondenten kunnen de helpdesk van Effectory contacteren met een verzoek om de vragenlijst opnieuw te kunnen invullen. Dat kan echter alleen tijdens de meetperiode van het betreffende onderzoek. Ook kan een Respondent de helpdesk tijdens de betreffende meetperiode vragen om de antwoorden te corrigeren, te beperken of te wissen. Dit gaat dan dus om de gegevens uit het medewerkersbestand (denk aan het corrigeren van foutieve contactgegevens, zoals emailadres), maar bijv. ook om de antwoorden die Respondenten gegeven hebben. Ook kunnen eventuele klachten via de helpdesk worden ingediend; indien deze te maken hebben met privacy-gerelateerde zaken die ICTU en/of Werkgever aangaan in hun rol van gezamenlijke verwerkingsverantwoordelijke worden deze rechtstreeks aan hen doorgezet.

2.5.4 *Opmerkingen*

Voor alle rechten geldt dat de Respondent tijdens de meetperiode van een onderzoek via de Effectory Helpdesk zijn/haar verzoek rechtstreeks bij Effectory kan indienen. Na de meetperiode kan de Respondent terecht bij zijn of haar werkgever. Een beroep op het recht op bezwaar of correctie wordt doorgegeven aan de Werkgever, zodat de Werkgever kan beoordelen hoe dit verzoek moet worden afgehandeld. Ook een verzoek met een beroep op het recht op beperking wordt doorgegeven aan de Werkgever.

NB. De inwilliging van een AVG-verzoek (anders dan inzage) kan invloed hebben op de resultaten van het onderzoek. De Werkgever dient dan een afweging te maken tussen het belang van het onderzoek tegenover het belang van de Respondent.²⁹ Als de Werkgever akkoord gaat met het verzoek van de Respondent, licht de Werkgever ICTU in over de praktische uitwerking van het verzoek. ICTU stuurt vervolgens Effectory aan die de instructies van de Werkgever uitvoert.

²⁹ Een scenario dat geregeld voorkomt is dat van een manager die vraagt om bepaalde antwoorden te verwijderen omdat hij/zij negatief in de rapportage voorkomt. In dat geval kan het verwijderingsverzoek gelet op het doel van het onderzoek meestal geweigerd worden.

3 Beschrijving en beoordeling risico's voor de betrokkenen en organisatie

3.1 Risico's voor rechten en vrijheden van betrokkenen

Voor de goede orde herhalen wij hier de opmerking dat de scope van in dit gedeelte van de DPIA slechts het InternetSpiegel-deel wordt besproken, meer in het bijzonder de wijze waarop Effectory de gegevens verwerkt, en dus niet alle privacyaspecten van een medewerkersonderzoek, zoals doel, vragen in de vragenlijst, selectie respondenten, verspreiding van rapportages, etc. Het in kaart brengen van die risico's gebeurt voor een deel in de aparte bijlagen; in hele specifieke gevallen en bij heel specifiek gebruik is mogelijk nog een aanvullende risicoanalyse door de Werkgever zelf vereist.³⁰

Let op: De onderstaande maatregelen zijn van toepassing op de **standaard situatie** waar de gegevens uitsluitend door Effectory worden verwerkt. De standaardsituatie betreft: gebruik standaardvragenlijsten van InternetSpiegel en geen verstrekking van de onderzoeksgegevens aan de Werkgever.

In geval aanvullende vragen worden opgenomen en/of de gegevens worden verstrekt moet de Werkgever een aanvullende risicoanalyse te doen op onderstaande risico's en waar nodig aanvullende maatregelen nemen.

#	Omschrijving Risico	Ernst	Aanbevolen Maatregel (zie voor een toelichting Hoofdstuk 4)	Uitgevoerd (door ICTU/ Effectory)
1.	De Respondent kan spontaan worden herkend aan de hand van de antwoorden op de gesloten vragen in de vragenlijst.	Laag	Standaardvragenlijsten	Ja
			Medewerkers zijn niet verplicht om de vragenlijst in te vullen.	Ja
			Pseudonimisering van de binnengekomen antwoorden door de identiteit van de Respondent te vervangen door een uniek identificerend nummer.	Ja
			Minimumgroepsgrootte in rapportages.	Ja
			Gemiddelde score per vraag <i>NB. Voor zover vragen toelaten dat er gemiddelden berekend kunnen worden (bijvoorbeeld bij stellingen).</i>	Ja

³⁰ Deze DPIA kan daarvoor als input dienen voor wat betreft het deel dat de verwerkingen bij Effectory betreft.

			<i>Bij overige vragen wordt gerapporteerd in percentages.</i>	
			Aanpassen van de antwoorden door Respondent indien een Respondent hiertoe en verzoek doet	Ja
			Procedures voor inzage en correctie na sluiten onderzoek	Ja
2.	De Respondent kan spontaan worden herkend aan de hand van de gegeven antwoorden in open tekstvelden.	Hoog	Medewerkers zijn niet verplicht om de vragenlijst in te vullen.	Ja
			Respondenten wijzen op de letterlijke opname van open antwoorden in de rapportage (in het platform en de privacyverklaring).	Ja
			Beperkte verspreiding van het onderzoeksrapport (<i>need to know</i>)	Deze maatregelen moeten door Werkgever worden genomen
			Weglakken van antwoorden voordat het rapport verder verspreid wordt in de organisatie.	
3.	Beschadiging van reputatie / persoonlijke levenssfeer van Respondent of anderen als gevolg van negatieve feedback in de rapportage.	Laag	Minimumgroepsgrootte in rapportages.	Ja
			Beperkte verspreiding van het onderzoeksrapport (<i>need to know</i>)	Deze maatregelen moeten door Werkgever worden genomen
			Geen/beperkte drill down in de onderzoeksrapporten. ³¹	
4.	Toegang tot gegevens/ onthulling van mensen in mensen in bepaalde veiligheidsfuncties, (<i>onveiligheid van respondenten en/of hun familie</i>).	Hoog	Aanpassen van de maatregelen aan de eisen voor de gegevensverwerking van personen in bepaalde veiligheidsfuncties.	Werkgever moet zelf beoordeling doen

³¹ Vanuit InternetSpiegel wordt hierbij altijd de minimale responsregel bewaakt.

5.	De onderzoeksgegevens worden gebruikt voor doeleinden waarvoor ze niet zijn verzameld (<i>onrechtvaardige behandeling</i>). (**)	Laag	Geen verstrekking van de onderzoeksgegevens aan de Werkgever.	Ja
			ICTU krijgt na afloop van het onderzoek uitsluitend geanonimiseerde gegevens.	Ja
			De toegang tot de gegevens is beperkt tot personen binnen Effectory die de gegevens nodig hebben voor hun taak.	Ja
			Werkafspraken voor het gebruik van de onderzoeksgegevens om te zorgen dat de gegevens uitsluitend gebruikt worden voor de doelstellingen van InternetSpiegel (goed werkgeverschap en gelukkige medewerkers), incl. een toets door de Programmamanager InternetSpiegel.	Ja
6.	Gegevens worden langer bewaard dan nodig	Laag	Vastgesteld bewaarbeleid van een half jaar na afsluiting klantrelatie.	Ja
7.	Er worden meer gegevens verwerkt dan nodig.	Laag	Standaardvragenlijsten (<i>zie losse bijlages bij deze DPIA, opvraagbaar bij ICTU</i>).	Ja
			Bij open antwoorden wordt altijd gewezen op de letterlijke opname. Respondenten bepalen zelf wat ze invullen. Indien een rapportage op een specifiek achtergrondkenmerk wordt gevraagd, blijven de open antwoorden achterwege.	Ja
8.	Datalek bij de aanlevering van de gegevens (personalia, demografische gegevens).	Laag	Beveiligd Extranet (van Effectory) om gegevens aan te leveren. <i>NB. De Werkgever moet er zelf voor zorgen dat de gegevens ook daadwerkelijk via het Extranet worden aangeleverd (en niet bijvoorbeeld via e-mail).</i>	Ja

			Optionele technische voorziening met P-Direkt (Rijk) via API.	Ja
9.	Datalek in de backend van Effectory	Laag	Versleuteling van de gegevens	Ja
			Autorisatiebeheer en toegangscontrole	Ja
			Diverse andere beveiligingsmaatregelen, waaronder een wekelijkse vulnerability scan en een jaarlijkse penetratietest	Ja
			Geheimhoudingsplicht medewerkers Effectory	Ja
			ISO 27001 certificering Effectory	Ja
10.	Datalek door misbruik van toegangsrechten	Laag	Geheimhoudingsplicht voor medewerkers	Ja
			Logging op ongeautoriseerde activiteiten	Ja

Toelichting

Spontane herkenning/ Reputatieschade/Inbreuk op de persoonlijke levenssfeer

In sommige onderzoeken wordt gewerkt met open tekstvelden, waarin de Respondent een toelichting kan geven. Uitgangspunt is dat deze antwoorden letterlijk worden overgenomen in de rapportage ter illustratie van de bevindingen (hier wordt de Respondent ook op gewezen via de vragenlijst en bijbehorende privacyverklaring). Het kan voorkomen dat Respondenten, ondanks de waarschuwing van letterlijke opname, in de open tekstvelden (zeer) privacygevoelige informatie prijsgeven over zichzelf of anderen, ook als daar niet specifiek om gevraagd wordt.³² Het rapport geeft niet aan wie welk antwoord gegeven heeft. Echter, hoe specifieker het commentaar van de Respondent in de open tekstvelden, hoe hoger de kans op spontane herkenning van de Respondent zal zijn.³³ Of dit leidt tot risico's voor de Respondent of een ander zal enerzijds afhangen van de inhoud van

³² Het komt soms ook voor dat een Respondent antwoorden geeft die ook persoonsgegevens vormen over een andere persoon (bijv. het gedrag van de leidinggevende). Het is zowel vanuit het oogpunt van de AVG als vanuit het oogpunt van goed werkgeverschap aan de Werkgever als verwerkingsverantwoordelijke om te zorgen voor verspreiding van een dergelijke rapportage op een 'need-to-know' basis plaatsvindt. Dit betekent dat wellicht alleen een gecensureerde versie van het rapport wordt verspreid (censureren moet de Werkgever zelf doen; wordt niet ondersteund door Effectory).

³³ Op mededelingen in de open tekstvelden is mogelijk de klokkenluidersregeling van de Werkgever van toepassing.

het commentaar, maar anderzijds ook van het onderwerp van het onderzoek en de reactie van het management van de organisatie.

Risico voor de veiligheid van de Respondent en/of zijn familie

NB. InternetSpiegel-medewerkersonderzoek is NIET ingericht conform de eisen die worden gesteld aan omgevingen waar gegevens over mensen met veiligheidsfuncties worden verwerkt! Voor zover medewerkers met dergelijke functies toch deelnemen aan het medewerkersonderzoek geldt dat een eventuele doorbreking van de beveiligingsmaatregelen in InternetSpiegel-medewerkersonderzoek, zoals het op straat liggen van personalia en functies, zou kunnen leiden tot veiligheidsrisico's voor de Respondent en/of diens familie. Hoewel de kans daarop -gelet op de beveiligingsmaatregelen die Effectory heeft genomen- klein is, kan de impact van een dergelijk datalek voor deze Respondenten groot zijn en de gevolgen onherstelbaar. Een Werkgever, die dergelijke veiligheidsfuncties in huis heeft, zal dus specifiek moeten beoordelen of de medewerkers in die functies kunnen worden meegenomen in het onderzoek, en zo ja, of eventuele aanvullende afspraken en/of beschermingsmaatregelen dan wel afwijkende procedures nodig zijn. Binnen de looptijd van InternetSpiegel is er al enige ervaring opgedaan met dergelijke aanvullende beoordelingen, afspraken/maatregelen en afwijkende procedures.

Ongerechtvaardigde behandeling

Zolang de gegevens bij Effectory blijven, achten wij dit risico voor de betrokkene in het algemeen **verwaarloosbaar** (geringe kans, lage impact). Dit is mede ingegeven door het feit dat er binnen InternetSpiegel gerapporteerd wordt door middel van een gemiddelde score per vraag (dus zonder uitsplitsing naar antwoordcategorie), waardoor het risico van uitspraken doen over te kleine populaties wordt geëlimineerd. Een uitsplitsing naar antwoordcategorie is er wel wanneer er wordt gerapporteerd in *tabelvorm*: x% heeft categorie Y aangevinkt. Dit wordt alleen gedaan op verzoek van Werkgever en bij minimaal 50 respondenten. Om het risico van spontane herkenning in de rapportage uit te sluiten hanteert Effectory onder regie van ICTU ook specifieke responsregels.

() NB.** De door ICTU/Effectory geboden bescherming wordt ongedaan gemaakt indien de ruwe data worden verstrekt aan de Werkgever voor eigen nader onderzoek. Dit gebeurt enkel op verzoek van de Werkgever, onder aanvullende voorwaarden, en pas nadat de Respondent hierover voorafgaand aan het onderzoek is geïnformeerd. Echter, het risico van spontane herkenning blijft inherent aanwezig als de Werkgever toegang heeft tot de ruwe data (met name in combinatie met de antwoorden in de open tekstvelden), hetgeen mogelijk kan leiden tot onrechtvaardige behandeling van de Respondent of een ander.

Indien de ruwe data aan de Werkgever worden geleverd achten wij het bruto-risico voor onrechtvaardige behandeling van de Respondent of een ander **substantieel** (significante kans / grote impact), mits de aard van het onderzoek en de antwoorden daar uiteraard aanleiding voor geeft en de gegevens buiten de kring van de onderzoekers worden

verspreid. Het is zowel vanuit het oogpunt van de AVG als vanuit het oogpunt van goed werkgeverschap aan de Werkgever als verwerkingsverantwoordelijke om te zorgen voor passende waarborgen voor de bescherming van de belangen van de Respondenten, zoals zorgen dat de gegevens uitsluitend toegankelijk zijn voor onderzoekers met een geheimhoudingsplicht.

4 Beschrijving maatregelen

In dit hoofdstuk staat een overzicht van de algemene maatregelen beschreven die ICTU c.q. Effectory hebben genomen om de persoonsgegevens te beschermen. Een overzicht van de specifieke maatregelen per relevant risico treft u aan in Bijlage 1.

4.1 Maatregelen

4.1.1 Compliance-maatregelen (art. 5.2/24/25 AVG)

ICTU en Effectory hebben diverse specifieke maatregelen genomen om de gegevensverwerking conform de eisen van de AVG in te richten.

Pseudonimisering

Effectory pseudonimiseert de onderzoeksgegevens met een Effectory-ID alvorens de gegevens te gebruiken voor onderzoek. De ruwe onderzoeksgegevens zijn gescheiden van de gepseudonimiseerde onderzoeksgegevens.

Geen toegang tot de gegevens door de Werkgever

De Werkgever heeft geen toegang tot de onderzoeksgegevens (standaardsituatie). Gebruik van de gegevens door de Werkgever voor doeleinden waarvoor ze niet zijn verzameld is daarmee uitgesloten.

NB. In sommige situaties wordt er op verzoek van de Werkgever van deze standaard binnen InternetSpiegel afgeweken en krijgt de Werkgever een kopie van de ruwe dataset voor eigen nadere analyses. In elk geval moet de Werkgever een risicoanalyse doen waaruit blijkt dat de risico's van deze nadere analyses voor de Respondenten verwaarloosbaar zijn. Als de Werkgever de data voor andere doeleinden wil inzetten, zal de Werkgever een eigen doelbindingstoets moeten doen.

Dataminimalisatie

Er worden door Effectory uitsluitend gegevens verzameld die nodig zijn voor het onderzoek. Dit geschiedt door vooraf vastgestelde InternetSpiegel-modules/vragenlijsten. Indien de Werkgever aanvullende vragen wil toevoegen, wordt in overleg met Effectory bekeken in hoeverre dit toegevoegde waarde heeft voor het onderzoek. Voorts is de Respondent niet verplicht om de vragenlijst (of delen van de vragenlijst) in te vullen.

Datakwaliteit

Via de helpdesk van Effectory kunnen – in overleg met Respondent – de demografische gegevens en/of personalia worden aangepast. Respondenten kunnen gedurende de meetperiode van een onderzoek de vragenlijst opnieuw invullen.

Bij onderzoeken binnen het Rijk kunnen fouten bij de aanlevering van gegevens worden voorkomen door als individuele organisatie gebruik te maken van de P-Direkt-voorziening.

Bewaartermijnen

De bewaartermijn is standaard een half jaar na afloop van de overeenkomst. Gewenste afwijkingen op de standaard bewaartermijn worden in een verwerkinstructie opgenomen door Werkgever en nageleefd door Effectory. Effectory verwijdert alle gegevens uit de verschillende databases na het verstrijken van de bewaartermijn, inclusief rapportages in PDF en PPT format.

Privacymanagement

De verantwoordelijkheid voor naleving van de AVG binnen InternetSpiegel is belegd bij de programmamanager van het programma Venster voor medewerkers werkzaam bij ICTU. Privacy en informatiebeveiliging waren een belangrijk aandachtspunt in de aanbesteding van het InternetSpiegel-medewerkersonderzoek. ICTU stemt met Effectory de procedures af rondom de gegevensverwerking in InternetSpiegel, evenals de eventuele door de Werkgever gevraagde uitzonderingen. De teams van ICTU en Effectory worden geregeld getraind op de aspecten van privacy en gegevensbescherming. ICTU heeft een functionaris gegevensbescherming (FG) die toezicht houdt op de gegevensverwerking binnen het InternetSpiegel-concept. Effectory heeft een Chief Information Security Officer en een jurist die nauw betrokken zijn bij de zorgvuldige gegevensverwerking en de naleving van de AVG. Het management van Effectory vindt privacy en compliance belangrijk en is nauw betrokken bij de naleving van het beleid en de AVG.

Verwerkersovereenkomst

Er is een verwerkersovereenkomst tussen ICTU en Effectory. De Werkgever is via de *Algemene Voorwaarden Verwerking Persoonsgegevens InternetSpiegel*, dat geldt als een regeling als bedoeld in artikel 26 AVG, gebonden aan de verwerkersovereenkomst. Beiden voldoen aan de eisen van de AVG.

Effectory heeft overeenkomsten gesloten met de subverwerkers Microsoft en Mailjet.

4.1.2 *Maatregelen uitoefening rechten betrokkenen (art. 12)*

Informatie

ICTU en Effectory hebben een standaard privacyverklaring opgesteld. Wanneer de Respondent de unieke link naar de vragenlijst aanklikt, krijgt hij/zij de verklaring aangeboden. Deze link staat ook in de uitnodiging die Respondenten per email ontvangen. De privacyverklaring kan waar nodig in overleg met de Werkgever worden aangepast. Dit is vereist als de ruwe data worden geleverd aan de Werkgever voor nadere analyses.

Inzage, correctie, verwijdering

Effectory heeft een helpdesk beschikbaar voor vragen van Respondenten. Effectory controleert de identiteit van de verzoeker middels het vergelijken van het e-mailadres met het reeds bij Effectory bekende e-mailadres (e-mail) of het stellen van een aantal controlevragen (telefoon). E-mails worden alleen verstuurd naar het bij Effectory bekende e-mailadres. Eventuele AVG-verzoeken worden doorgeleid naar de Werkgever.

Beveiligingsbeleid

ICTU hanteert als norm voor de beveiliging van gegevens in aanbestedingen de Baseline Informatiebeveiliging Overheid (BIO) of gelijkwaardig. NEN-ISO/IEC 27001 wordt door ICTU als gelijkwaardig gezien aan de BIO. Effectory's informatiebeveiligingsbeleid is gebaseerd op NEN-ISO/IEC 27001.³⁴

Preventieve maatregelen

Effectory voert wekelijks een vulnerabilityscan uit om kwetsbaarheden te ontdekken. Jaarlijks wordt een penetratietest uitgevoerd.

Certificering

Effectory is ISO 27001 gecertificeerd, waarbij alle beheersmaatregelen van toepassing zijn verklaard, en geïmplementeerd. De scope van de certificering is beveiliging van persoonsgegevens en onderzoeksresultaten. De huidige certificeringscyclus loopt af in oktober 2027, met jaarlijkse controle door een externe auditor. Daarna gaat Effectory verder met de volgende certificeringscyclus.

Effectory is sinds 2022 ook ISO 27701:2019 gecertificeerd. De scope van de certificering is de bescherming van persoonsgegevens van medewerkers van klanten en de onderzoeksresultaten van klanten. De certificeringscyclus loopt af in oktober 2027. Jaarlijks worden er controles uitgevoerd.

Daarnaast is Effectory SOC 2 Type II geaudit.

Geheimhouding

De medewerkers van Effectory en de verwerkers van Effectory (sub-verwerkers) zijn gebonden aan geheimhouding.

Screening

Alle medewerkers van Effectory moeten een Verklaring Omtrent het Gedrag overleggen bij indiensttreding.

Versleuteling

Al het dataverkeer gaat over versleutelde TLS verbindingen (1.3, met fallback naar 1.2 als 1.3 nog niet bij de gebruiker van het platform wordt ondersteund). Dataverkeer tussen Effectory en de Microsoft Azure gaat via een IPSec VPN. De gegevens worden in de Microsoft Azure altijd versleuteld opgeslagen.

Mobiele apparaten zijn versleuteld met en worden beheerd door Microsoft EndPoint Manager (mobile device management). Data die op laptops is opgeslagen is versleuteld met Bitlocker. Voor zover het nodig is om data op een USB-stick op te slaan, worden bij

³⁴ Op de website van Effectory is een recent 'Whitepaper information security and privacy' opvraagbaar met de concrete technische en organisatorische maatregelen die genomen zijn. Het Whitepaper is opvraagbaar via <https://security.effectory.com> net zoals de ISO certificaten.

Effectory bekende versleutelde USB-sticks gebruikt (*NB. USB-poorten zijn normaal gesproken geblokkeerd*).

Autorisaties en toegangscontrole

Binnen Effectory hebben medewerkers alleen toegang tot gegevens die zij nodig hebben voor hun taak.³⁵ Effectory voert logging uit op (on)geautoriseerde activiteiten. Effectory medewerkers gebruiken twee-factor authenticatie voor toegang tot Effectory's portals (Microsoft Azure en customer portal).

Werkgevers kunnen ook via Single Sign-On aansluiten op de portal. De Multi-factor authentication (MFA) voor toegang tot Effectory's portals is verplicht voor bepaalde rollen die toegang hebben tot de vooraf aangeleverde persoonsgegevens.³⁶ Voor de overige rollen is dat een keuze van de Werkgever. Toegang tot de portals wordt geblokkeerd bij zes foutieve inlogpogingen. Effectory maakt gebruik van het Intrusion Detection systeem van Microsoft om aanvallen op haar webapplicaties in Microsoft Azure te detecteren.

Apparaatbeheer

USB-poorten zijn geblokkeerd, behalve voor bij Effectory bekende versleutelde USB-sticks. Opslagmedia (SSD/HDD/etc.) die volledig buiten werking worden gesteld worden, indien nodig, verwijderd uit apparaten en fysiek of door middel van software van Blancco dusdanig onbruikbaar gemaakt op DIN 66399 protection class 2 security level 3 niveau. Hardware vernietiging wordt hiernaast ook aangeboden bij IT-recycling. Apparatuur en opslagmedia wordt op locatie door IT-recycling vernietigd, waarbij een certificaat van vernietiging wordt afgegeven.

Overleg ICTU/Effectory

ICTU en Effectory voeren kwartaaloverleg over het borgen van privacy en informatiebeveiliging, waarbij ook de FG van ICTU evenals de projectleiders van InternetSpiegel bij ICTU en Effectory en de CISO van Effectory aansluit.

Datalekken management

Het risico op datalekken bij Effectory is klein. Eventuele datalekken bij Effectory dienen – conform de verwerkersovereenkomst tussen ICTU en Effectory – door Effectory gemeld te worden bij ICTU. Als het datalek aan ICTU is gemeld worden de Werkgevers daarover door ICTU of in opdracht van ICTU door Effectory geïnformeerd. Op grond van de Algemene Voorwaarden Bescherming Persoonsgegevens InternetSpiegel wordt een datalek aan de zijde van Effectory waarbij de persoonsgegevens van meerdere Werkgevers zijn betrokken door ICTU bij de Autoriteit Persoonsgegevens gemeld en worden in dat geval de

³⁵ Zie verder de opmerkingen in paragraaf 1.5.3.

³⁶ De rollen waarvoor MFA verplicht is, controleren enkel of de Respondent vooraf de juiste vragenlijst ontvangt. Hierbij is geen inzicht in de antwoorden van Respondenten mogelijk. Voor meer informatie, zie de website van Effectory: How to set up Multi-factor authentication (MFA) – Effectory.

betrokkenen door de respectievelijke Werkgevers geïnformeerd. Voor dat laatste is gekozen opdat de Werkgevers vanuit hun werkgeverschap in staat worden gesteld hun verantwoordelijkheid jegens hun medewerkers te kunnen nemen en controle hebben over óf en zo ja de wijze waarop zij hun medewerkers wensen te informeren. Wanneer een datalek is ontstaan binnen de context van een specifiek onderzoeksproject, dan ligt de meldplicht jegens de Autoriteit Persoonsgegevens alsnog bij de betrokken Werkgever.

4.1.4 Audits

Naast de jaarlijkse audits verzorgt de Audit Dienst Rijk (ADR), in het geval dat nodig is, ook audits bij Effectory in opdracht. Naar aanleiding van het bovenstaande, in het bijzonder de ISO-certificeringen en SOC 2 assurance, hebben wij geen reden om aan te nemen dat de beveiligingsmaatregelen bij Effectory niet passend zouden zijn.