Data Protection Impact Assessment

InternetSpiegel

30 oktober 2026



Auteurs

Privacy Management Partners:
mr. drs. Jeroen Terstegge CIPP/E, partner
mr. Jochem Gerritsen, adviseur
Sam Berens, paralegal

Bijdragers

ICTU: Catharina Kolar
Effectory: Wouter Buzing, CISO
Effectory: Lisette Schuilwerve, legal counsel

Opdrachtgever

ICTU: programma management Venster

Versie: 8.0

© Privacy Management Partners 2026
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
Versie 8.0	30 oktober 2026	Inhoudelijke update na feedback ICTU

Inhoud

Versieoverzicht 1

Inleiding en verantwoording 1
- Informatie voor Werkgevers: 3
- Karakter van deze DPIA 5
- Onderzochte partijen 5
- Rapportagestructuur 5

Management samenvatting 7
- Advies FG ICTU op definitieve versie DPIA 7
- Oordeel PMP 7

1 Beschrijving kenmerken gegevensverwerking 9
1.1 Beleidsdoelstellingen en opzet InternetSpiegel 9
1.2 Persoonsgegevens 11
1.3 Gegevensverwerkingen 15
1.4 Verwerkingsdoelen 16
1.5 Betrokken partijen 16
1.6 Belangen bij de gegevensverwerkingen 22
1.7 Verwerkingslocaties 23
1.8 Technieken en methoden van de gegevensverwerkingen 23
1.9 Juridisch en beleidsmatig kader 28
1.10 Bewaartermijnen 29

2 Beoordeling rechtmatigheid gegevensverwerkingen 30
2.1 Rechtsgrond 30
2.2 Bijzondere persoonsgegevens 34
2.3 Doelbinding 34
2.4 Noodzaak en evenredigheid 36
2.5 Rechten van betrokkenen 37

3 Beschrijving en beoordeling risico's voor de betrokkenen en organisatie 41
3.1 Risico's voor rechten en vrijheden van betrokkenen 41

4 Beschrijving maatregelen 47
4.1 Maatregelen 47

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. In het verlengde daarvan is het ook verantwoordelijk voor 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 het concept 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 functie Organisatie & Personeel Rijk (hierna: O&P Rijk).

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

Op deze informatiepagina is meer informatie over het concept InternetSpiegel beschikbaar voor o.a. inkopers, functionarissen gegevensbescherming (FG's) en HR-directeuren. Tevens zijn hier de relevante en meest recente documenten met betrekking tot InternetSpiegel te vinden.

Het ministerie van BZK biedt, via ICTU, het medewerkersonderzoek van het concept InternetSpiegel aan. Dit doet zij enerzijds vanuit de visie dat de onderzoeksresultaten inzichten bieden aan individuele organisaties (middels feedback van de eigen medewerkers) binnen de sector openbaar bestuur & veiligheid. Anderzijds zijn de onderzoeksresultaten ook zeer waardevol als informatie over de sector openbaar bestuur als geheel. Zo kan deze informatie worden gebruikt als input voor kennisontwikkeling en beleidsinformatie (op basis van statistisch beleidsonderzoek) voor het ministerie van BZK als werkgever van alle ambtenaren, maar ook voor de gehele sector openbaar bestuur.

Gebruik van het concept 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 in uitvoering bij ICTU.
- ICTU heeft voor de uitvoering van het concept InternetSpiegel een Europese aanbesteding uitgezet.
- De meest recente aanbesteding is in december 2024 gegund aan Effectory, marktleider als het gaat om medewerkersfeedback. Zij bieden in opdracht van ICTU het concept InternetSpiegel 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 overheidsorganisatie/werkgever die behoort tot de Staat der Nederlanden, Deze organisaties/werkgevers sluiten 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 overheidsorganisatie/werkgever die zich voorafgaand aan de publicatie van de aanbesteding heeft aangesloten aan de aanbesteding middels een volmacht. Ook vallen de organisaties die vertegenwoordigd zijn binnen het bestuur van ICTU onder de groep 'Deelnemers'.
3. Onder de groep 'Secundaire deelnemers' vallen alle organisaties binnen de sector Openbaar bestuur & veiligheid die gedurende de looptijd van de Raamovereenkomst tussen ICTU en Effectory mogelijk kunnen aansluiten op de Raamovereenkomst. Bij (Secundaire) Deelnemers sluit de werkgever rechtstreeks een nadere overeenkomst (NOK) af met Effectory.

Op de informatiepagina van het concept InternetSpiegel is te vinden tot welk type Afnemer overheidsorganisaties/werkgevers behoren.

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

Alle 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 vormt de basis voor de wijze waarop ICTU regie voert over de werkzaamheden van Effectory.

ICTU heeft Privacy Management Partners (PMP) gevraagd om de privacy- en compliance-aspecten van het concept 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 My Internetspiegel-platform waar de medewerkersonderzoeken op plaatsvinden, en de beveiligingsmaatregelen;
- De aansturing van Effectory door ICTU;
- Het aanleveren en de inhoud van de standaard vragenlijsten en/of vraagmodules 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 binnen het concept InternetSpiegel (denk aan het toevoegen van door Werkgevers zelf samengestelde enquêtevragen);
- De processen waarvoor Effectory de verwerkingsverantwoordelijke is, zoals de helpdesk;
- Het statistisch beleidsonderzoek door ICTU.[1]

Informatie voor Werkgevers:

- **Aanvullende risicoanalyse/DPIA:** De eerste drie bullets die hierboven out-of-scope van deze DPIA zijn geplaatst moeten aanvullend op deze DPIA door uzelf worden beoordeeld. Waar nodig dient u advies te vragen aan uw Functionaris Gegevensbescherming (FG) over de eventuele afwijkingen van de InternetSpiegel-standaard en instemming vragen van uw ondernemingsraad.

- **Statistisch beleidsonderzoek:** Het leveren van een beperkte, anonieme dataset aan ICTU na afloop van het onderzoek is een verplicht onderdeel van het concept InternetSpiegel. Deze dataset wordt gebruikt ten behoeve van statistisch beleidsonderzoek in het kader van de systeemverantwoordelijkheid van de Minister

1 Hiervoor is door PMP separaat het 'Memo Statistisch beleidsonderzoek ICTU InternetSpiegel en de AVG' opgesteld. Deze memo bevat de motivatie waarom het statistisch beleidsonderzoek buiten de scope valt. Dit document is te vinden op de informatiepagina van het concept InternetSpiegel.

van BZK voor het functioneren van het openbaar bestuur en het ambtenarenbeleid.

- **Gezamenlijke kennisopbouw binnen het openbaar bestuur:** Door de onderzoeksgegevens van verschillende organisaties en metingen samen te brengen en te analyseren, kan ICTU bredere ontwikkelingen en patronen zichtbaar maken. Die kennis wordt vervolgens gedeeld binnen het openbaar bestuur en kan worden benut voor onderzoek en beleid. Iedere meting levert daarmee niet alleen waardevolle inzichten op voor de organisatie zelf, maar draagt ook bij aan een breder beeld van wat er speelt binnen het openbaar bestuur.

  Deze levering van de gegevens is volledig in overeenstemming met de AVG (artikel 5 lid 1 sub b, tweede volzin) en is geregeld in de Algemene Voorwaarden Verwerking Persoonsgegevens van het concept InternetSpiegel (AVVP). De AVVP en een separaat memo over het statistisch beleidsonderzoek zijn te vinden op de informatiepagina.

- **Betrokkenheid van uw FG:** ICTU en de Werkgever zijn *gezamenlijke verwerkingsverantwoordelijke* (zie voor de onderbouwing par. 1.5), waarbij ICTU als programmamanager de regiefunctie vervult. Volgens de Algemene Voorwaarden Verwerking Persoonsgegevens InternetSpiegel, dat tevens de afspraken tussen ICTU en Werkgever bevat als bedoeld in artikel 26 AVG, ligt de aansturing van verwerker Effectory exclusief bij ICTU. Dat geldt ook voor de regie op het aanbod (de vragenlijsten/vraagconstructen) en de voorwaarden om de geanonimiseerde gegevens na afloop te delen met ICTU.
  De regiefunctie van ICTU betekent ook dat het toezicht op de naleving van de AVG binnen het concept InternetSpiegel primair bij de FG van ICTU ligt. De FG van ICTU treedt dus mede namens uw FG op als een soort '*coördinerend FG'*. Het is dus niet nodig om deze DPIA voor advies aan uw FG voor te leggen (u kunt deze wel 'ter informatie' voorleggen). Zie ook de opmerking hierboven over de aanvullende risicoanalyses/DPIA. Deze is ook relevant voor de rol van uw FG bij alles wat buiten de regiefunctie van ICTU valt.

  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 het concept InternetSpiegel, kan deze zich – via de projectleider van het concept InternetSpiegel bij ICTU (conceptisp@ictu.nl) – wenden tot de FG van ICTU.

  Rol van uw ondernemingsraad
  Uw ondernemingsraad (OR) speelt een belangrijke rol bij de inzet van het concept Internetspiegel. Afhankelijk van de wijze waarop het concept Internetspiegel wordt ingezet, kan de instemming van uw OR vereist zijn. Dit is met name van belang indien er wordt afgeweken van de Internetspiegel-standaard, bijvoorbeeld wanneer een organisatie gepseudonimiseerde individuele antwoordgegevens in de vorm van ruwe

data wil ontvangen voor eigen analyses. In een dergelijk geval dient de organisatie zelf te beoordelen welke aanvullende privacy- en organisatorische maatregelen noodzakelijk zijn, waaronder het eventueel uitvoeren van een aanvullende DPIA en waar van toepassing het verkrijgen van instemming van de OR.

Let op: U hoeft niet voor elk onderzoek opnieuw een DPIA uit voeren, uw FG te raadplegen of instemming van uw OR te vragen. Voldoende is meestal dat de inzet van het instrument InternetSpiegel en uw werkwijze daaromheen als zodanig een keer is beoordeeld en zo nodig met uw FG en OR is besproken. Daar kunt u de volgende keer dus gewoon op voortborduren; ook als u voor die volgende keer een nieuwe overeenkomst moet afsluiten. Alleen als u in een bepaald onderzoek wenst af te wijken van het standaardaanbod of als het standaardaanbod significant is gewijzigd ten opzichte van vorige keer, kan een herbeoordeling van de DPIA, dan wel het wederom inschakelen de FG en de OR geboden zijn.

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 het concept InternetSpiegel wordt uitgevoerd.[2] Naast de (privacy)risico's voor de betrokkenen is tevens de compliance van het concept 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
Kombo Technologies GmbH	Optionele subverwerker

Rapportagestructuur

Deze 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

[2] In het verleden ontving ICTU ook van de medewerkers die niet deelnemen achtergrondkenmerken ten behoeve van statistische analyses. Dat is niet meer zo.

In het hoofddeel van het rapport worden de onderdelen (A-D) doorlopen voor het algemene overkoepelende 'medewerkersonderzoek', oftewel het concept InternetSpiegel. De verschillende modules met vragen 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 28 oktober 2026 als positief beoordeeld door de FG van ICTU.

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 standaardgebruik van het concept 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 beheerd. 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*).
- Het laten opnemen van aanvullende eigen vragen, met name als deze bijzondere persoonsgegevens betreffen (*risico op onrechtmatige of disproportionele verwerking*). Voor de aanvullende eigen vragen is de betreffende Werkgever de zelfstandig verwerkingsverantwoordelijke
- Het op verzoek van de Werkgever afgeven van 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*). Voor de afgifte van ruwe data geldt een afzonderlijke procedure, waarbij de Werkgever vooraf een keuze maakt uit de beschikbare varianten van ruwe data. Afhankelijk van de gekozen variant worden de ruwe data anoniem, gepseudonimiseerd dan wel niet-anoniem verstrekt. Bij de gepseudonimiseerde en niet-anonieme variant is de Werkgever verantwoordelijk voor de beoordeling van de rechtmatigheid en de privacyrisico's van de verdere verwerking en voor het treffen van passende technische en organisatorische maatregelen ter bescherming van de rechten en vrijheden van de Respondenten.[3]

3 De voorwaarden waaronder de ruwe data worden verstrekt en de daarbij te treffen waarborgen worden vastgelegd in het daartoe bestemde keuzeformulier, dat als bijlage bij de Project-/Nadere overeenkomst wordt opgenomen.

- 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*).

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 tussen ICTU en Effectory afgesproken technische en organisatorische beveiligingsmaatregelen.

1 Beschrijving kenmerken gegevensverwerking

1.1 Beleidsdoelstellingen en opzet InternetSpiegel

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

Het concept InternetSpiegel is vanuit de directie A&O in het leven geroepen voor het verbeteren van de prestaties van overheidsorganisaties. Het concept InternetSpiegel is sinds 2007 ondergebracht bij ICTU in een apart programma (Venster). Dit onderzoeks- en adviesteam is een sparringpartner van, voor en door de overheid en richt zich op het verbeteren van de prestaties van overheidsorganisaties. Het biedt een leerplatform met inzichten, kennis, onderzoeken en vergelijkingen op het gebied van heldere bedrijfsvoering, goed werkgeverschap en werkgeluk van medewerkers.
Hiervoor worden verschillende methoden ingezet, waarvan het InternetSpiegel-medewerkersonderzoek er een is. Het concept InternetSpiegel is een gedegen medewerkersonderzoek waarbij kwaliteitsborging belangrijk is. Zo wordt gewerkt met gevalideerde, wetenschappelijk en praktisch bewezen onderzoeksmodellen en vraagconstructen inclusief benchmarks. Werkgevers die gebruik maken van het concept InternetSpiegel worden optimaal ondersteund over zaken zoals privacy/AVG. Vragenlijsten binnen het concept worden continu doorontwikkeld zodat de nieuwste ontwikkelingen steeds kunnen worden meegenomen in de medewerkersonderzoeken van Werkgevers.
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 het concept InternetSpiegel is via een Europese aanbesteding belegd bij Effectory in Amsterdam. Het programma Venster (ICTU) bewaakt de kwaliteit van de uitvoering en verzorgt de regie op de doorontwikkeling van het concept InternetSpiegel.
Met dit concept 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. Hierbij kunnen deze instellingen zich ook vergelijken (spiegelen, benchmarken) met andere organisaties.
Onderdeel van het concept InternetSpiegel zijn diverse wetenschappelijk gevalideerde vragenlijsten die Werkgevers kunnen voorleggen aan hun medewerkers. De onderzoeksinstrumenten die op het moment worden ingezet zijn:

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

- Duurzame inzetbaarheidsscan;
- Psychosociale arbeidsbelasting (PSA);
- Werkbelevingsscan; en
- 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 ingerichte vragenlijst.

Effectory maakt voor het flexibel en continu verzamelen, bewerken, benchmarken en rapporteren van gegevens (via de onderzoeksinstrumenten van het concept InternetSpiegel) gebruik van een eigen onderzoeksplatform ("my InternetSpiegel").[4] Onder het onderzoeksplatform wordt verstaan: de faciliteiten voor het uitvoeren van online medewerkersonderzoeken voor individuele Werkgevers binnen de doelgroep van het concept InternetSpiegel met gebruik van InternetSpiegel-instrumenten en/of vraagmodules. Hieronder valt tevens het rapporteren van de geaggregeerde onderzoeksresultaten (online en offline), inclusief benchmarks op diverse niveaus/structuren, waaronder ook een persoonlijke rapportage voor Respondenten.

Vanuit het programma Venster bij ICTU wordt kennisdeling gefaciliteerd, bijvoorbeeld door middel van beleidsonderzoek op de resultaten van InternetSpiegel-medewerkersonderzoek en het delen van best practices. Geanonimiseerde gegevens op Werkgevers-niveau worden door Effectory ieder kwartaal aan ICTU geleverd. Dit statistisch beleidsonderzoek en de resultaten daarvan in rapportages, artikelen en dergelijke vindt altijd geaggregeerd plaats per sector of over sectoren heen en gaat nooit over individuele organisaties. Het doel van de kennisdeling is tweeledig: het dient als input voor beleid voor het ministerie van BZK, maar ook het door middel van kennisdeling over het bevorderen van goed werkgeverschap en bijdragen aan het werkgeluk van medewerkers voor een optimaal presterende overheid.[5]

In technische zin worden de medewerkersonderzoeken van Werkgevers die gebruik maken van het concept InternetSpiegel 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 digitale 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

4 Zie Venster, *InternetSpiegel informatiepagina*, onderdeel 'Beschrijvend document', https://www.venster.nl/internetspiegel-informatiepagina/#1744203405216-b9f7b658-9296.

5 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 te vinden op de informatiepagina.

binnen het concept InternetSpiegel, 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 concept InternetSpiegel op verschillende manieren kan worden afgenomen. 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.

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 concept InternetSpiegel wordt aangeboden als software-as-a-service (SaaS). Medewerkers van de aangesloten overheidsorganisaties kunnen via een unieke link online vragenlijsten in vullen. 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

Binnen het concept InternetSpiegel- worden van de medewerkers van Werkgever onderstaande persoonsgegevens verwerkt ten behoeve van de uitvoering van de medewerkersonderzoeken. Deze gegevens worden standaard voorafgaand aan de start van het onderzoek aangeleverd in overeenstemming met de procedure vanuit Effectory via het platform.

Categorie betrokkenen	Personalia	Type persoonsgegeven	Bron	Doel
Vereiste gegevens voor uitvoering onderzoek				
Medewerker	Naam	Gewoon persoonsgegeven	Werkgever	Uitnodiging deelname
Medewerker	Zakelijk e-mailadres	Gewoon persoonsgegeven	Werkgever	Uitnodiging deelname
Medewerker	Afdeling (organogram)	Gewoon persoonsgegeven	Werkgever	Rapportage
Medewerker	Medewerker-ID	Gewoon persoonsgegeven	Werkgever	Een uniek identificatienummer dat aan de medewerker is toegewezen

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[6]	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Genderidentiteit	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Hoogst voltooide opleiding[7]	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Wel/niet leidinggevende	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Salarisschaal-categorie (alleen van toepassing bij Rijksorganisaties)[8]	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Functiegroep[9] (alleen Hogescholen)	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU (indien gewenst) de Rapportage
Medewerker	Type aanstelling (alleen Hogescholen die gebruik maken van de Exitmonitor)[10]	Gewoon persoonsgegeven	Werkgever	Statistisch beleidsonderzoek ICTU, (indien gewenst) de Rapportage
Medewerker	Soort vertrek/instroom (alleen bij Instroommonitor	Gewoon persoonsgegeven	Werkgever	Uitnodiging deelname & Statistisch beleidsonderzoek ICTU

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

7 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.

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

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

10 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.

	en Exitmonitor Rijk)[11]			
Antwoorden op vragen in vragenlijsten				
Respondent	Antwoorden op gesloten vragen binnen het concept InternetSpiegel	Gewoon persoonsgegeven	Respondent	Rapportage, Statistisch beleidsonderzoek ICTU
Respondent, Leidinggevende	Gedrag leidinggevende[12]	Gewoon persoonsgegeven	Respondent	Rapportage
Respondent	Antwoorden in open tekstvelden	*Afhankelijk van de vraag (zie bijlage van het betreffende onderzoek).*	Respondent	Rapportage
Respondent	Antwoorden in door Werkgever toegevoegde eigen vragen (dus geen InternetSpiegel-vragen)	*Afhankelijk van de vraag (zie bijlage van het betreffende onderzoek).*	Respondent	Rapportage
Vereiste gegevens specifiek voor instroom- en of uitstroomonderzoek (*)				
Medewerker	Type vertrekker (alleen Exitmonitor)[13]	Gewoon persoonsgegeven	Werkgever	Uitnodiging deelname & Rapportage
Medewerker	Medewerkers-subgroep, bijv. regulier ambtenaar, stagiair, externe	Gewoon persoonsgegeven	Werkgever of P-Direkt	Uitnodiging deelname & Rapportage (indien gewenst)
Medewerker	Type contract, vast en tijdelijk	Gewoon persoonsgegeven	Werkgever of P-Direkt	Uitnodiging deelname & Rapportage (indien gewenst)
Medewerker	Datum in- en uitdiensttreding (alleen bij Instroommonitor en Exitmonitor)	Gewoon persoonsgegeven	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-

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

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

13 Categorieën: vrijwillig, onvrijwillig en pensioen.

platform via Effectory op individueel niveau verzameld en bewaard. Op die manier is het mogelijk om een Respondent een persoonlijke rapportage van zijn of haar antwoorden te verstrekken en om vergelijkingen mogelijk te maken (bijvoorbeeld met het vorige onderzoek).

Rapportages

Artikel 5 Gedragscode voor Statistisch onderzoek 2023[14] 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 Respondenten de vragenlijst hebben ingevuld en het responspercentage moet minimaal 40% zijn van het betreffende onderdeel.[15] Het responspercentage van 40% is een methodologische voorwaarde in verband met de betrouwbaarheid van de resultaten van het onderzoek. Deze ondergrenzen dragen eraan 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 online indienen in open tekstvelden worden letterlijk overgenomen in de rapportage. Respondenten worden hiervoor gewaarschuwd in het platform en in de privacyverklaring. Binnen het concept InternetSpiegel worden in de rapportage dezelfde strikte vertrouwelijkheidsgrenzen gehanteerd 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. Verder kan bij het samenvatten van de open vragen gebruik worden gemaakt van AI. Ook dit wordt verderop gesproken.

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, waarbij vanuit een hoger organisatieniveau wordt ingezoomd op de resultaten van een specifieke afdeling. Werkgever dient hier bij het verspreiden van de rapportages binnen de organisatie rekening mee te houden, omdat de informatie in de rapportage in zo'n geval een persoonsgegeven van de betrokkene vormt. Indien aan de orde, wordt dit behandeld in de betreffende vragenlijsten in de bijlagen bij deze DPIA.

Datakwaliteit

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

15 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).

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.

Voor Rijksorganisaties: Als de data op uw verzoek door P-Direkt geleverd wordt via de technische voorziening (API), 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.

1.3 Gegevensverwerkingen

1.3.1 Verzameling

De personalia en demografische gegevens worden door de Werkgever via de beveiligde online omgeving My InternetSpiegel van Effectory aangeleverd en opgeslagen in Europese locaties van de cloudomgeving van Microsoft (Azure).

NB Rijksorganisaties kunnen voor het aanleveren van de personalia en demografische gegevens gebruik maken van de technische voorziening tussen 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-Direkt 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 de Europese 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 webapplicatie (in de Microsoft Azure-cloud) opgeslagen en vervolgens gepseudonimiseerd door Effectory. De Respondent is niet verplicht om de (hele) vragenlijst in te vullen en kan binnen de vragenlijst vragen overslaan of ervoor kiezen om helemaal niet deel te nemen.

1.3.3 Analyse/Rapportage

De binnengekomen antwoorden worden na pseudonimisering gecalculeerd en gerapporteerd door Effectory waarbij ten allen tijde rekening gehouden wordt met de responsregel. Antwoorden op open vragen worden in de rapportage letterlijk overgenomen als er aan de minimumresponseis wordt voldaan. Respondenten worden geadviseerd om

geen direct identificerende gegevens op te nemen in de antwoorden op hun open vraag. Effectory verricht haar taken met inachtneming van de best practices op het gebied van onderzoek en statistiek (vergelijk artikel 89 lid 1 AVG).

De Respondenten ontvangen standaard een persoonlijke rapportage via My InternetSpiegel 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 als een Werkgever dit niet toestaat, ontvangt men geen persoonlijke rapportage.

1.4 Verwerkingsdoelen

Het algemene doel van het concept 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, hoe deze wordt ingericht 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 instrumenten zijn op moment van schrijven:

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

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

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

1.5 Betrokken partijen

Bij de gegevensverwerkingen van de medewerkersonderzoeken met het concept InternetSpiegel zijn de volgende actoren betrokken:

1.5.1 *Werkgever*

AVG-rol	Verwerkingsverantwoordelijke van de gegevensverwerking in het kader van het medewerkersonderzoek (*gezamenlijk met ICTU*)
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. ***Uitzondering:*** *Op specifiek verzoek van de Werkgever kunnen de ruwe onderzoeksgegevens aan de Werkgever beschikbaar worden gesteld voor eigen analyses. Dit levert in dat geval 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
De Werkgever bepaalt wanneer een onderzoek wordt uitgevoerd, binnen welke vestigingen of afdelingen en welke vragenlijst(modules) van InternetSpiegel wordt afgenomen (eventueel aangevuld met eigen toegevoegde vragen). Hieruit volgt dat de Werkgever verwerkingsverantwoordelijke is in de zin van de AVG voor de gegevensverwerking in het kader van de uitvoering van het medewerkersonderzoek.

1.5.2 *Stichting ICTU*

AVG-rol	Verwerkingsverantwoordelijke (*gezamenlijk met Werkgever)*
Locatie	Den Haag
Activiteiten	• Stuurt als programmaverantwoordelijke de uitvoering van het concept InternetSpiegel en daarmee ook Effectory aan; • Ontwikkelt en bepaalt de inhoud en het aanbod van de vragenlijsten binnen het concept InternetSpiegel en ook de 'spelregels' rondom het gebruik van InternetSpiegel.
Toegang tot persoonsgegevens	Nee[16]

16 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 buiten de scope van deze DPIA. Voor meer informatie over deze beleidsanalyses heeft ICTU een memo beschikbaar.

Toelichting
ICTU bepaalt als programmabureau hoe het concept 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 en ook 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 **gezamenlijke verwerkingsverantwoordelijke** is in de zin van artikel 26 AVG, voor de verwerking van persoonsgegevens in het kader van het medewerkersonderzoek via het concept InternetSpiegel.[17]

NB De Algemene Voorwaarden Verwerking Persoonsgegevens, waarmee de Werkgever akkoord gaat bij ondertekening van de Projectovereenkomst (voor gebruikers) dan wel de nadere overeenkomst (voor secundaire deelnemers), geldt als regeling tussen de gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26 AVG. **De werkgever is met ICTU gezamenlijk verwerkingsverantwoordelijke. Het belangrijkste gevolg hiervan, is dat een aantal verplichtingen van de verantwoordelijke uit de AVG op grond van de Algemene Voorwaarden *exclusief* toevallen aan ICTU die deze *mede namens* Werkgever uitvoert. Hierdoor is de Werkgever ontheven 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 artikel 28 lid 1 AVG en het sluiten van een verwerkersovereenkomst met Effectory ex artikel 28 lid 3 AVG. Ook is uitsluitend ICTU verantwoordelijk voor het melden van een eventueel datalek in de omgeving van Effectory bij de Autoriteit Persoonsgegevens ex artikel 33 AVG. Het is daarom 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 Autoriteit Persoonsgegevens.

NB De Algemene Voorwaarden Verwerking Persoonsgegevens leggen ook een aantal AVG-verplichtingen exclusief bij de Werkgever, waaronder het informeren van diens medewerkers ex artikel 13 AVG. Hieronder valt ook het feit dat de gegevens in geanonimiseerde vorm beschikbaar worden gesteld aan ICTU voor statistisch beleidsonderzoek ten behoeve van het Ministerie van BZK. Dit is ook opgenomen in de privacyverklaring voor medewerkers.[18] Voorts omvat dit het afhandelen van eventuele AVG-verzoeken van zijn medewerkers en het melden van een eventueel datalek bij de medewerker ex artikel 34 AVG.

[17] Dit gelet op het criterium van 'feitelijke invloed' op de gegevensverwerking van de Werkgever: Hof van Justitie EU, 10 juli 2018 (C25/17, Jehova's *Getuigen*).

[18] Deze verklaring is te vinden op de website van InternetSpiegel.

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 en stuurt t.b.v de uitvoering daarvan uitnodigingen en herinneringen. Onder medewerkersonderzoeken wordt verstaan: reguliere medewerkersonderzoeken, pulse onderzoeken en themaonderzoeken. • 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 en offline). • Geeft de Respondent inzicht in diens eigen antwoorden in een persoonlijke online rapportage (tenzij de Werkgever heeft aangegeven dat niet te willen).[19]
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.[20]

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

19 De beslissing van de Werkgever om geen persoonlijk rapport te ontvangen heeft geen invloed op het inzagerecht ex artikel 15 AVG.

20 Normaliter heeft het software ontwikkelingsteam van Effectory 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.

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.[21]

Tussen ICTU en Effectory is een Raamovereenkomst 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 erboven 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). Deze overeenkomst is te vinden op de informatiepagina.

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). Ook bij de selectie van Effectory als verwerker is tijdens de aanbesteding aandacht besteed aan privacyaspecten en diende Effectory aan diverse verplichtingen op dit gebied te voldoen. 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 het concept InternetSpiegel.

ICTU en Effectory voeren frequent overleg (minimaal eens per twee weken) over de uitvoering van de onderliggende contracten, inclusief het borgen van de bescherming van persoonsgegevens. ICTU en Effectory hebben immers een zorgplicht tegenover 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. Ook houdt de FG van ICTU toezicht op de gegevensverwerkingen binnen Internet. 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 Chief Information Security Officer (CISO) aangesteld en beschikt het over de informatiebeveiligingscertificeringen ISO 27001, ISO 27701 en SOC 2 type II.

21 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 (artikel 28 lid 10 AVG). Als iets onduidelijk is met betrekking tot de verwerking van persoonsgegevens, zal Effectory dus instructie moeten vragen van ICTU.

Voor overige informatie over de informatiebeveiligings- en privacymaatregelen bij Effectory, zie https://security.effectory.com.[22]

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 (de gegevens zijn 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.[23]

Microsoft Azure Services heeft veel ISO-certificeringen en SOC assurance. Noemenswaardig voor deze DPIA is in het bijzonder de ISO 27018 ('*Protection of personal 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 (https://www.microsoft.com/en-us/trust-center).[24]

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 bulkmail (uitnodigingen, etc.)
Toegang tot gegevens	Alleen naam en e-mailadres

Toelichting
MailJet stelt een softwaretool beschikbaar aan Effectory waarmee Effectory onder andere de uitnodigingen voor het onderzoek binnen een kort tijdbestek kan uitsturen zodat onderzoeken zoveel als mogelijk gelijktijdig starten voor Respondenten. MailJet zorgt er ook voor dat deze mailingen niet als spam/phishing worden aangemerkt. Dit draagt eraan bij dat mails met de uitnodigingen daadwerkelijk bij de ontvangers in hun postvak arriveren.

22 Zie https://www.venster.nl/internetspiegel-informatiepagina/

23 Voor overige informatie wordt verwezen naar https://security.effectory.com.

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

MailJet kan in dit kader worden beschouwd als subverwerker (van Effectory). Voor het gebruik van MailJet heeft Effectory een verwerkersovereenkomst afgesloten. MailJet is ISO 27001 gecertificeerd.[25]

1.5.6 Kombo Technologies GmbH

Rol partij	Optionele subverwerker (van Effectory)
Locatie	Nederland en Duitsland
Activiteiten	Technische integratie voor de overdracht van personeelsgegevens naar Effectory
Toegang tot gegevens	Ja, enkel personeelsgegevens

Kombo is een optionele subverwerker van Effectory, die Effectory als optie aanbiedt aan de Werkgevers. Werkgevers kunnen Kombo gebruiken om automatisch vanuit hun bronsysteem met medewerkersgegevens naar My Effectory te laten synchroniseren. Net als Microsoft en Mailjet is Kombo volledig geïntegreerd in My Effectory en voor klanten niet als zodanig herkenbaar. Kombo zorgt ervoor dat de persoonsgegevens vanuit het bronsysteem van de klant naar My Effectory worden overgezet om daarna verder in het proces verwerkt te worden. Alle persoonsgegevens worden standaard met minimaal TLS 1.2 versleuteld opgeslagen. Kombo is ISO 27001 gecertificeerd.

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 en problemen van onder de oppervlakte boven water worden gehaald.

1.6.2 Belang van ICTU

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

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 het concept InternetSpiegel dat afgenomen wordt door hun Werkgever. De Respondent kan zijn/haar werkbeleving en eventuele frustraties of suggesties voor organisatieverbetering op een veilige manier uiten.

25 Het Google Cloud Platform waar MailJet gebruikt van maakt heeft ook ISO-certificeringen en SOC 2 assurance.

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)
Verwerkingen binnen Kombo	Nederland en Duitsland

Er vindt in de opzet van het concept InternetSpiegel **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 Europese Economische Ruimte) is daarom 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, die naast de InternetSpiegel-vragen ook eigen vragen van de Werkgever kan bevatten, 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. Met uitzondering van de verplicht aangeleverde demografische kenmerken (zoals leeftijd, opleiding, geslacht,-salarisschaal (indien sector Rijk) en wel/geen leidinggevende functie) en eventuele aanvullende demografische kenmerken die de Werkgever wenst toe te voegen, zijn er in deze database geen andere kenmerken gekoppeld aan de antwoorden. Het komt soms voor dat de verplichte demografische gegevens worden uitgevraagd via de vragenlijst als een Werkgever deze niet vooraf kan of wil 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 gebeurt door bij de analyse gebruik te maken van andere databases met groepsindelingen, eerdere metingen en/of achtergrondkenmerken (zogeheten 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 afdelingen/teams op de hoogste niveaus worden uitgesplitst naar achtergrondkenmerken (zoals leeftijdscategorieën of geslacht).[26]

De resultaten worden na calculatie in een andere database opgeslagen, waarbij aldaar het unieke individuele nummer niet wordt opgeslagen.[27] 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.

1.8.3 Kunstmatige intelligentie binnen InternetSpiegel

Binnen het concept InternetSpiegel wordt gebruikgemaakt van verschillende Kunstmatige intelligentie (AI)-functies die worden geleverd door Effectory. Het gaat om de volgende functies:

AI-Samenvatting van gesloten vragen

Binnen het resultatendashboard van Effectory wordt gebruikgemaakt van een AI-functionaliteit, de zogenoemde 'AI Samenvatting'. Deze functionaliteit wordt ingezet om de resultaten van de InternetSpiegel-vragenlijst op geautomatiseerde wijze samen te vatten en gebruikers van het dashboard te ondersteunen bij de interpretatie van de onderzoeksresultaten.

De AI Samenvatting analyseert de scores op de verschillende thema's binnen de vragenlijst. Daarbij kunnen de actuele resultaten worden vergeleken met resultaten uit eerdere onderzoeken en met beschikbare benchmarks. Op basis hiervan genereert de AI-functionaliteit een samenvatting bestaande uit drie onderdelen: sterke punten, mogelijke verbeterpunten en aanbevolen vervolgacties. De AI Samenvatting wordt alleen gegenereerd wanneer binnen het betreffende onderzoek gebruik wordt gemaakt van de beschikbare thema's in het concept InternetSpiegel.

Voor het genereren van de AI Samenvatting wordt uitsluitend gebruikgemaakt van gegevens afkomstig uit gesloten vragen. Deze functionaliteit moet worden onderscheiden van de AI-samenvatting van open vragen, die verderop wordt besproken.

Voor de AI-functionaliteit worden uitsluitend anonieme en/of gepseudonimiseerde gegevens gebruikt en worden geen direct identificerende persoonsgegevens als ruwe input aan het AI-model verstrekt. Het betreft een eigen, specifiek voor Effectory ingerichte AI-oplossing, die in termen van de AI Act kwalificeert als een AI-systeem met een minimaal risico. De onderzoeksgegevens worden door Effectory niet gedeeld met externe AI-diensten. Daarmee wordt voorkomen dat individuele antwoorden als input worden

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

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

verstrekt aan generieke AI- of LLM-diensten van externe aanbieders en daar bijvoorbeeld voor andere doeleinden of voor het trainen van externe modellen kunnen worden gebruikt. De door AI gegenereerde samenvatting heeft een ondersteunend karakter. De AI-functionaliteit kan sterke punten en verbeterpunten signaleren en mogelijke vervolgacties voorstellen, maar de gegenereerde informatie dient niet zelfstandig als basis voor besluitvorming over individuele Respondenten of teams te worden gebruikt.

Voorafgaand aan het gebruik van de AI Samenvatting wordt in het dashboard door middel van een disclaimer kenbaar gemaakt dat de betreffende informatie door AI is gegenereerd en dat deze door de gebruiker moet worden beoordeeld voordat op basis daarvan actie wordt ondernomen. Dit is van belang omdat AI-gegenereerde output onjuistheden of onjuiste interpretaties kan bevatten. Wanneer dergelijke output zonder menselijke beoordeling wordt overgenomen, kan dit leiden tot onjuiste managementbeslissingen of maatregelen ten aanzien van teams of medewerkers. De verantwoordelijkheid voor de interpretatie van de resultaten en eventuele daaropvolgende besluitvorming blijft daarom bij de gebruiker van het dashboard.

Effectory voorziet daarnaast in een mogelijkheid om feedback te geven op de AI Samenvatting door middel van een *thumbs-up/thumbs-down*-functionaliteit. Deze functie is bedoeld om feedback over de feature als geheel te geven, en wordt alleen gebruikt door productspecialisten van Effectory om te bepalen of de feature als geheel een toegevoegde waarde heeft voor klanten of juist niet. De feedback komt niet in AI terecht.

Daarnaast vindt periodieke beoordeling van mogelijke veranderingen in de werking en kwaliteit van het AI-model (*model drift*) plaats.

Medewerkers worden via de privacyverklaring en een disclaimer voorafgaand aan het invullen van de vragenlijst geïnformeerd over de verwerking van hun gegevens. Daarbij wordt ook voldoende transparant gemaakt dat AI kan worden ingezet voor het analyseren en samenvatten van onderzoeksresultaten.

Datasegmentatie
Binnen het concept InternetSpiegel kan gebruik worden gemaakt van datasegmentatie. Datasegmentatie houdt in dat resultaten van de vragenlijst worden uitgesplitst aan de hand van bepaalde kenmerken, zodat verschillen tussen groepen respondenten inzichtelijk kunnen worden gemaakt. Deze werkwijze wordt ook wel aangeduid als *crossings*. Hierbij kunnen verschillende kenmerken worden gebruikt om groepen binnen de onderzoeksresultaten van elkaar te onderscheiden.

Door middel van segmentatie kunnen geaggregeerde resultaten van verschillende groepen met elkaar worden vergeleken. Het gebruik van segmentatie brengt tegelijkertijd een risico met zich mee voor de vertrouwelijkheid van respondenten. Met name bij kleine groepen of

bij het combineren van verschillende kenmerken kan de kans op herleidbaarheid toenemen. Een combinatie van bijvoorbeeld leeftijd, geslacht en duur van het dienstverband kan binnen een kleine afdeling of een specifieke functie betrekking hebben op slechts één of enkele medewerkers. Hierdoor zou, ondanks het ontbreken van direct identificerende gegevens in de getoonde resultaten, informatie mogelijk alsnog tot een individuele respondent kunnen worden herleid.

Om dit risico te beperken, worden segmenten onderverdeeld in categorieën en past Effectory regels toe met betrekking tot de minimale omvang van de groepen waarvoor resultaten worden getoond. Een belangrijke waarborg daarbij is dat een datasegment alleen wordt weergegeven wanneer iedere categorie binnen dat segment ten minste vijf uitgenodigde medewerkers én vijf Respondenten bevat. Wanneer één van de categorieën niet aan deze ondergrens voldoet, wordt de betreffende segmentatie in zijn geheel niet weergegeven. Hiermee wordt voorkomen dat door het tonen of vergelijken van kleine groepen informatie over individuele respondenten kan worden afgeleid.

Wanneer een categorie helemaal geen respons bevat, wordt uitsluitend de betreffende categorie verborgen. De overige categorieën binnen het segment kunnen wel worden weergegeven, voor zover zij aan de overige vertrouwelijkheidsvoorwaarden voldoen.

De organisatie kan daarnaast configureren tot welk niveau geautomatiseerde segmentatie wordt toegepast. Daarmee kan de mate van detaillering van de segmentatie worden afgestemd op de organisatiestructuur en kan worden voorkomen dat resultaten automatisch op een te gedetailleerd niveau beschikbaar komen.

Effectory beperkt daarnaast de typen antwoorden waarop segmentatie kan worden toegepast. Segmentatie wordt niet toegepast op antwoorden op open vragen. Vrije tekst kan immers informatie bevatten die, zeker in combinatie met kenmerken van een kleine groep, de herkenbaarheid van een individuele respondent vergroot. Ook worden geen gesegmenteerde inzichten verstrekt voor percentagevragen en meerkeuzevragen wanneer dit tot een verhoogd risico op individuele herleidbaarheid kan leiden.

Naast het risico op herleidbaarheid bestaat bij segmentatie een risico dat gegevens onjuist aan segmenten worden gekoppeld, bijvoorbeeld als gevolg van fouten bij het inrichten, koppelen of integreren van gegevens. Een onjuiste indeling kan leiden tot onjuiste of misleidende onderzoeksresultaten. Om dit risico te beperken worden aanbevelingen ten aanzien van datakwaliteit toegepast en blijft menselijke beoordeling noodzakelijk bij de interpretatie van de gesegmenteerde resultaten en de besluitvorming die daarop wordt gebaseerd.

Met deze systematiek wordt beoogd om verschillen tussen groepen inzichtelijk te maken zonder daarbij de vertrouwelijkheid van individuele respondenten uit het oog te verliezen.

De combinatie van minimale groepsgroottes, beperkingen ten aanzien van de beschikbare segmenten, configuratiemogelijkheden voor geautomatiseerde segmentatie, aanvullende voorwaarden voor handmatige segmentatie en menselijke beoordeling moet voorkomen dat de toepassing van segmentatie leidt tot ongewenste herleidbaarheid of onjuiste besluitvorming.

Geavanceerde filters
Binnen het resultatendashboard van Effectory kan gebruik worden gemaakt van 'Advanced Filters'. Met deze functionaliteit kunnen bevoegde gebruikers onderzoeksresultaten nader filteren door verschillende kenmerken en voorwaarden te combineren. Hiermee kunnen specifieke groepen binnen de onderzoeksresultaten worden geselecteerd en geanalyseerd. Het combineren van meerdere filters kan het risico op herleidbaarheid vergroten. Door steeds specifiekere kenmerken te selecteren, zou een gebruiker kunnen proberen een dusdanig kleine groep samen te stellen dat resultaten mogelijk tot één of enkele personen kunnen worden herleid.

Effectory past daarom real-time controles op vertrouwelijkheid toe. Bij het toevoegen van een volgend filter wordt rekening gehouden met de filters die eerder zijn aangemaakt en met de gevolgen van de combinatie van filters voor de vertrouwelijkheid van respondenten. Eerder aangemaakte filters kunnen bovendien niet worden verwijderd. Hiermee wordt voorkomen dat een gebruiker door het achtereenvolgens toepassen en verwijderen van verschillende filters informatie kan afleiden over individuele respondenten.

Daarnaast is het gebruik van Advanced Filters beperkt tot specifieke rollen, namelijk *Central Coordinators*, *Project Coordinators* en *Survey Creators*. Gebruikers worden in het platform tevens geïnformeerd over de mogelijke risico's van het gebruik van Advanced Filters.

Naast het risico op herleidbaarheid kunnen fouten in de koppeling of integratie van gegevens leiden tot onjuiste filterresultaten en daarmee tot onjuiste conclusies. Effectory voorziet hiervoor in aanbevelingen ten aanzien van datakwaliteit binnen *Employee Exchange* en menselijke beoordeling van de resultaten. Eventuele niet eerder geïdentificeerde situaties of risico's kunnen daarnaast via feedback- en incidentmeldingsprocessen worden gesignaleerd en opgevolgd.

AI-samenvatting van open antwoorden
Naast de hiervoor besproken AI-samenvatting op gesloten vragen, bestaat er een vergelijkbare functionaliteit voor open vragen: de AI-gedreven samenvatting van open antwoorden. Als er genoeg antwoorden zijn gegeven, zal er in het dashboard een AI-samenvatting van de open antwoorden van deelnemers bekeken kunnen worden. Deze AI-gegenereerde samenvattingen worden ook gemaakt voor maatwerkvragen. Deze gegevens worden nooit gedeeld met externe AI-diensten.

Open antwoorden kunnen persoonlijke ervaringen en gevoelige details bevatten. AI-samenvattingen volgen dezelfde principes als de strikte vertrouwelijkheidsregels die gelden voor de weergave van open antwoorden. Ook hier geldt dat de anonimiteit van respondenten te allen tijde wordt beschermd. De AI-samenvattingen worden gemaakt op basis van de open en zijn alleen zichtbaar voor gebruikers die sowieso al toegang hebben tot deze antwoorden.

Aan deze functionaliteit zijn enkele risico's verbonden. Het trainen van modellen met gebruikerscontent kan ertoe leiden dat er reacties ontstaan waarin gevoelige informatie onbedoeld wordt onthouden of herhaald. Respondenten hebben hierdoor geen inzicht in of controle over wie toegang heeft tot hun gegevens of hoe deze worden gebruikt. Dit risico wordt gemitigeerd door een standaard 'opt-out' voor het trainen van modellen, wordt er gebruik gemaakt van een generiek voorgetraind AI-model en is er controle op modelafwijkingen.

Een ander risico is dat de geautomatiseerde analyses van AI de toon of intentie verkeerd interpreteren of relevante context buiten beschouwing laat. Dit kan leiden tot een onjuiste rapportage waardoor vervolgens onjuiste maatregelen van het management ten aanzien van de werknemers wordt genomen. Dit risico wordt gemitigeerd door de oorspronkelijke open antwoorden zichtbaar te plaatsen onder de samenvatting, waardoor de gebruiker kan controleren of de samenvatting correct is. Ook wordt er een disclaimer in beeld gebracht met de vermelding dat de samenvatting met AI gegenereerd is.

Ook zou het kunnen dat in de samenvattingen identificerende gegevens worden onthuld zoals specifieke namen of zeldzame projecten. Dit kan leiden tot heridentificatie en maatschappelijke schade. Dit risico wordt gemitigeerd door anonimisering van de betreffende reacties op open vragen vóór de AI-samenvattingsstap. In de prompt worden ook instructies opgenomen om namen in de gegenereerde samenvatting te vermijden. Dit geldt ook ten aanzien van onbedoelde openbaarmaking van antwoorden van individuen. Dit risico wordt gemitigeerd door gebruik te maken van *prompt engineering* zodat parafrasering wordt vermeden.

1.9 Juridisch en beleidsmatig kader

1.9.1 Beleidsmatig kader

Zoals eerder naar voren kwam, is het concept InternetSpiegel in het leven geroepen door de directie A&O van het ministerie van 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 O&P Rijk.

Het concept InternetSpiegel is sinds 2007 door BZK ondergebracht bij 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 en AVG. Instrumenten worden continu doorontwikkeld zodat de nieuwste ontwikkelingen steeds worden meegenomen.

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

1.9.2 Juridisch kader

Op de gegevensverwerkingen in het concept 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 (beeendigde overeenkomst) wordt de data onomkeerbaar verwijderd, tenzij anders afgesproken in de verwerkingsinstructie zoals gegeven door ICTU.

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;[28]
- 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.

28 Uitsplitsing vindt alleen plaats met inachtneming van de vertrouwelijkheidsgrenzen.

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 ICTU als verwerkingsverantwoordelijke een verzoek te doen om medewerkers en/of andere gegevenssoorten (zoals oude rapportages) te verwijderen. ICTU geeft dit verzoek door aan Effectory, waarna Effectory hieraan uitvoering geeft. Medewerkers die vertrekken kunnen door de Werkgever ook zelf in My InternetSpiegel worden verwijderd. Tenzij wordt gewerkt met een integratie met het personeelsbestand van de Werkgever, is er geen automatische faciliteit waarmee wijzigingen in het huidige personeelsbestand worden verwerkt en de gegevens dienovereenkomstig worden geactualiseerd.

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 e-mail 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. Deze gegevens worden bij ICTU niet na afloop van deze termijn verwijderd.
Antwoorden op gesloten vragen.	Tot zes maanden na afloop van de klantrelatie. Deze gegevens worden bij ICTU niet na afloop van deze termijn verwijderd.
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	Artikel 6 lid 1 sub b AVG: uitvoering arbeidsovereenkomst
Demografische gegevens	Artikel 6 lid 1 sub b AVG: uitvoering arbeidsovereenkomst
Antwoorden op de vragen	Artikel 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 al aanwezig zijn in de personeelsregistratie van de Werkgever (HvJ EU, *Digi*). De grondslag voor deze verdere verwerking is gelijk aan de grondslag waarvoor de gegevens zijn verzameld door de Werkgever (overweging 50 AVG), 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.[29] 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*

29 NB Uit het feit dat de Respondent 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 Respondent vaak ook niet geldig zijn (zie overweging 43 AVG).

zonder de gegevensverwerking kan worden bereikt.[30]
De onderzoeken die via het concept 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:

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: het concept InternetSpiegel hanteert in de rapportage strikte vertrouwelijkheidsgrenzen aan de hand van 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 het concept 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 afzonderlijk 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: het concept InternetSpiegel hanteert in de rapportage strikte vertrouwelijkheidsgrenzen. Voorts zijn er binnen Effectory diverse maatregelen genomen om de onderliggende onderzoeksgegevens vertrouwelijk te houden jegens de Werkgever.)

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

v. *Zijn er passende waarborgen geïmplementeerd om de belangen van de Respondenten te beschermen (zie ook artikel 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 medewerkersonderzoek.

NB Dit kan anders liggen (met name punten i, iv en v) als de Werkgever afwijkt van de standaard die door ICTU wordt aangeboden, afwijkende vragen opneemt in de vragenlijst of als de rapportage persoonsgegevens zijn over een leidinggevende. Dit geldt voor de gevallen waarin de Werkgever op verzoek zelf de beschikking krijgt over de ruwe data voor eigen nadere analyse. In dat geval moet de Werkgever, ervan uitgaande dat goed wordt nagedacht over de spreiding van resultaten, zelf een nieuwe belangenafweging maken en beoordelen of deze afwijkingen leiden tot risico's voor de Respondenten. Effectory/ICTU kunnen daarin adviseren. Effectory/ICTU informeren 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 (artikel 27 lid 1 sub K Wet op de ondernemingsraden). Zie ook de risico/maatregelentabel 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** (artikel 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 richting Effectory (aanbesteding). Ook dit zijn belangen die gerechtvaardigd zijn (want ze zijn niet verboden of maatschappelijk onbetamelijk).

2. De gegevensverwerking is noodzakelijk voor de correcte uitvoering van het medewerkersonderzoek (in overeenstemming met de programma-eisen die ICTU stelt aan het concept 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 over het specifieke onderzoek. InternetSpiegel probeert het verwerken van bijzondere persoonsgegevens zoveel mogelijk te vermijden.

Gegevens kunnen in bepaalde gevallen informatie bevatten die te classificeren is als bijzondere persoonsgegevens. Dit is het geval wanneer gegevens betrekking hebben op situaties zoals de duur van ziekteverzuim, verzuimfrequentie, gezondheid, vitaliteit of antwoorden op vragen over thema's als inclusiviteit, slachtofferschap aan incidenten. Internetspiegel staat toe dat werkgevers eigen vragen aanleveren waar gevraagd wordt naar gegevens die gaan over dergelijke situaties. Aangezien het hier gaat om bijzondere persoonsgegevens is het verwerkingsverbod ex artikel 9 lid 1 AVG van toepassing. Dit verbod kan worden doorbroken indien de werknemer uitdrukkelijke toestemming geeft voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden (artikel 9 lid 2 onder a AVG). Ondanks dat binnen het concept InternetSpiegel geen vragen/constructen zijn en worden opgenomen die vragen naar bijzondere persoonsgegevens , faciliteert het dergelijke vragen wél door werkgevers de mogelijkheid te bieden om deze vragen zelf op te nemen in de vragenlijst. In dergelijke gevallen zal de werknemer de mogelijkheid hebben om een dergelijke vraag over te slaan. Wanneer zij de betreffende vraag invullen, geven zij de in de AVG bedoelde expliciete toestemming. Dit gaat altijd in overleg met ICTU als gezamenlijke verwerkingsverantwoordelijke.

Binnen Internetspiegel wordt niet daarbovenop gevraagd om een apart vakje voor toestemming aan te vinken. Een dergelijk vakje heeft immers geen toegevoegde waarde en is enkel dubbelop. De werknemer geeft immers de bedoelde toestemming door de vraag te beantwoorden.

Aangezien de rapporten aan de werkgever vanuit Effectory voldoende geaggregeerd zijn, bevat de door hen verstuurde rapportages geen persoonsgegevens over de Respondenten. Dit geldt evengoed voor de geaggregeerde antwoorden die bijzondere persoonsgegevens behelzen. Hier is de AVG, en daarmee het verwerkingsverbod, dus niet van toepassing.

NB Ondanks het feit dat juridisch de mogelijkheid bestaat voor de Werkgever om dergelijke vragen te stellen, wordt het door ICTU ten strengste afgeraden. De werknemer kan zich bezwaard voelen om op dergelijke vragen antwoord te geven. Dit zal diens vertrouwen in de vragenlijst als geheel kunnen beschadigen. Ook methodologisch zijn er bezwaren. Wanneer er wordt gestimuleerd op het mogen overslaan van de vragen, heeft dat immers ook effect op de uiteindelijke resultaten. Bijvoorbeeld als een groot deel ze niet beantwoord.

2.3 Doelbinding

In paragraaf 1.4 staan de doeleinden van het concept 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

Eventueel nevengebruik moet worden getoetst aan de eisen van de AVG inzake nevengebruik. Dit volgt uit het feit dat persoonsgegevens alleen voor nevendoeleinden mogen worden gebruikt als deze "niet onverenigbaar" zijn met het doel waarvoor de persoonsgegevens werden verzameld (artikel 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. Daarom liggen er hier geen belemmeringen om de gegevens daarvoor te gebruiken, mits er passende waarborgen worden genomen (zie artikel 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 het concept InternetSpiegel.

NB De hiernavolgende gegevensverwerking is een verdere verwerking waarop geen doelbindingstoets hoeft te worden uitgevoerd.[31] Voor de volledigheid noemen wij de verwerking hier wel, omdat er mogelijk risico's aan kleven die door de Werkgever ex artikel 89 AVG moeten worden beoordeeld en gemitigeerd.

- Verstrekking ruwe dataset aan Werkgever op verzoek

Werkgevers hebben soms niet alleen behoefte aan een terugkoppeling van de resultaten uit hun InternetSpiegel-medewerkersonderzoek in de vorm van rapportages (de standaard binnen InternetSpiegel). In sommige gevallen wensen zij ook zelf over de ruwe data te beschikken, zodat data-analisten binnen de eigen organisatie nadere statistische analyses kunnen doen.

31 Hof van Justitie EU, 20 oktober 2022 (C-77/21), *Digi*, randnummer 34.

Het op verzoek verstrekken van de ruwe dataset aan de Werkgever voor aanvullend eigen onderzoek is een **afwijking van de standaardwerkwijze** waarbij InternetSpiegel als 'Chinese Muur' fungeert tussen de Respondenten en hun Werkgever. Dit is zonder doelbindingstoets dus alleen toegestaan als de Werkgever de gegevens uitsluitend gebruikt voor *hetzelfde doel* (medewerkersonderzoek). De Werkgever dient daartoe in de eigen organisatie ex artikel 89 AVG de nodige aanvullende waarborgen hebben ingebouwd die minstens vergelijkbaar zijn met de waarborgen die al 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'). Als de Werkgever de dataset voor andere doeleinden wil gebruiken dan aanvullende analyses op het medewerkersonderzoek, dient de Werkgever zelf een doelbindingstoets uit te voeren. Afhankelijk van welke gegevens onderdeel zijn van de verstrekking, dient de Werkgever zelf na te gaan in welke mate de Ondernemingsraad en/of FG en/of andere rollen betrokken moeten zijn bij de besluitvorming over deze verstrekking.

Gegevensverwerkingen	Persoonsgegevens	Doeleinden	Oorspronkelijk doel
Gebruik personalia/demografische gegevens door Effectory	Personalia, demografische gegevens	Uitvoeren van medewerkersonderzoek	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 het concept 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* (personalia, demografische gegevens) tot *gemiddeld of hoog* (afhankelijk van de antwoorden op de vragenlijst). Het

onderwerp is bepalend voor de gevoeligheid. De maatregelen zijn bedoeld om ex post de herleidbaarheid uit te sluiten. Die maatregelen moeten zo nodig strenger zijn als de gevoeligheid groter is. De antwoorden van de Respondent worden niet verder verspreid (met uitzondering van incidentele gevallen op specifiek verzoek van de eigen Werkgever in het geval van ruwe datalevering). Een verdere uitweiding over de gevoeligheid van de gegevens voortkomend uit de bevraagde onderwerpen per vragenlijst, is terug te vinden in de afzonderlijke opvraagbare bijlagen.

Effectory hanteert op instructie van ICTU een strikte responsregel voor de vertrouwelijkheid van de onderzoeksgegevens. Dit doet zij om te kunnen borgen dat de beoogde verwerkingsdoeleinden worden bereikt op een wijze die niet of minder nadelig is voor de Respondenten. 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 het 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 (Respondenten en andere medewerkers wiens persoonsgegevens worden verwerkt) 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 zijn niet van toepassing op het concept InternetSpiegel. Het gaat om rechten zoals het recht op dataportabiliteit en het recht om niet te worden onderworpen aan een geautomatiseerd besluit, inclusief profilering.

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 e-mail ontvangen: het e-mailadres 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 en andere betrokkenen moeten worden geïnformeerd over de verwerking van hun persoonsgegevens. Ten minste moeten zij worden geïnformeerd over de volgende zaken:

- identiteit en contactgegevens van de gezamenlijke verwerkingsverantwoordelijken (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 (bij Effectory. ICTU verwerkt in deze fase immers geen persoonsgegevens);
- 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. Binnen het concept InternetSpiegel zijn er echter twee verwerkingsverantwoordelijken: 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 uiterlijk bij de start van het onderzoek (elk los onderzoek, dus ook bij pulsemetingen, themametingen etc) moet worden verstrekt.

- 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.[32]

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 het concept InternetSpiegel is dat de gegevens niet aan de Werkgever worden verstrekt. Dit wordt ook expliciet zo medegedeeld in de standaard privacyverklaring van het concept InternetSpiegel. Derhalve bepaalt de privacyverklaring de gerechtvaardigde privacyverwachting die de Respondent heeft als hij/zij antwoord geeft op de

32 Deze informatie is beschikbaar via https://helpdeskinternetspiegel.effectory.com/ en https://support.effectory.com.

vragenlijst.

Niettemin komt het voor dat Werkgevers achteraf vragen om de aanlevering van de gegevens op individueel niveau in de vorm van ruwe data. Deze functionaliteit is echter om privacyredenen niet beschikbaar binnen het concept 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. Hierdoor kunnen de medewerkers een eigen afweging maken bij de beantwoording van de vragenlijst. Daarmee dwingt ICTU de Werkgever om vooraf bij elk onderzoek weer een belangenafweging te maken en binnen zijn organisatie de nodige waarborgen op te tuigen om de belangen van de Respondenten te beschermen.

2.5.2 Recht op inzage

Het inzagerecht 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. Als 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 e-mailadres), maar bijvoorbeeld ook om de antwoorden die Respondenten gegeven hebben. Ook kunnen eventuele klachten via de helpdesk worden ingediend. Als deze klachten te maken hebben met privacygerelateerde zaken die ICTU en/of Werkgever aangaan in hun rol van gezamenlijke verwerkingsverantwoordelijke, worden deze rechtstreeks aan hen doorgezet. Na de opgeleverde rapportage kunnen de gegevens alleen worden verwijderd na toestemming van de Werkgever, omdat een verwijdering of aanpassing van de onderliggende gegevens de onderzoeksresultaten kan beïnvloeden.

2.5.4 Opmerkingen

Voor alle rechten geldt dat de Betrokkene tijdens de meetperiode van een onderzoek via de Effectory Helpdesk zijn/haar verzoek rechtstreeks bij Effectory kan indienen. Na de meetperiode kan de Betrokkene 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 Betrokkene.[33] Als de Werkgever akkoord gaat met het verzoek van de Betrokkene, licht de Werkgever ICTU in over de praktische uitwerking van het verzoek. ICTU stuurt vervolgens Effectory aan die de instructies van de Werkgever uitvoert.

33 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 dit gedeelte van de DPIA slechts het InternetSpiegel-deel wordt besproken. Meer in het bijzonder gaat het om de wijze waarop Effectory de gegevens verwerkt. Het gaat dus niet over alle privacyaspecten van een medewerkersonderzoek zoals doel, vragen in de vragenlijst, selectie respondenten, verspreiding van rapportages et cetera. 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.[34]

Let op: De onderstaande maatregelen zijn van toepassing op de **standaardsituatie** waar de gegevens uitsluitend door Effectory worden verwerkt. De standaardsituatie betreft: het gebruik van alleen de standaardvragenlijsten/of vragen van het concept InternetSpiegel en dus geen toevoeging van eigen vragen door Werkgever en geen verstrekking van de onderzoeksgegevens aan de Werkgever.

In het geval dat aanvullende eigen vragen worden opgenomen en/of de gegevens worden verstrekt, moet de Werkgever een aanvullende risicoanalyse 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 *NB Voor zover vragen toelaten dat er gemiddelden berekend kunnen*	Ja

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

			worden (bijvoorbeeld bij stellingen). Bij overige vragen wordt gerapporteerd in percentages.	
			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.	Gemiddeld	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 (*need to know).*	Deze maatregelen moeten door Werkgever worden genomen.
			In geval van offline rapportages: weglakken van antwoorden in de gedownloade rapportages voordat de rapportage binnen de organisatie beschikbaar wordt gesteld.	
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 (*need to know).*	Deze maatregelen moeten door Werkgever worden genomen.
			Geen/beperkte drill down in de onderzoeksrapporten.[35]	

35 Vanuit het concept InternetSpiegel wordt hierbij altijd de minimale responsregel bewaakt.

4.	Toegang tot gegevens door derden/ onthulling van mensen in mensen in bepaalde veiligheidsfuncties en politiek prominente personen, *(onveiligheid van respondenten en/of hun familie).*	Hoog	Aanpassen van de maatregelen aan de eisen voor de gegevensverwerking van personen in bepaalde veiligheidsfuncties.	Werkgever moet zelf beoordeling doen en keuzes maken die passen binnen de spelregels van het concept InternetSpiegel.
			(Bepaalde) veiligheidsfuncties en politiek prominente personen uitsluiten van deelname.	
5.	De onderzoeksgegevens worden gebruikt voor doeleinden waarvoor ze niet zijn verzameld (*onrechtvaardige behandeling)*. (**)	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 het concept 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 *(zie losse bijlages bij deze DPIA, opvraagbaar bij ICTU).*	Ja
			Bij open antwoorden wordt altijd gewezen op de letterlijke opname. Respondenten bepalen zelf wat ze invullen. Indien een rapportage op	Ja

			een specifiek achtergrondkenmerk wordt gevraagd, blijven de open antwoorden achterwege.	
8.	Datalek bij de aanlevering van de gegevens (personalia, demografische gegevens) (*verlies van controle)*.	Laag	Beveiligd Extranet binnen My InternetSpiegel om gegevens aan te leveren. *NB De Werkgever moet er zelf voor zorgen dat de gegevens ook daadwerkelijk via het Extranet worden aangeleverd (en niet bijvoorbeeld via e-mail).*	Ja
			Optionele technische voorziening met P-Direkt (Rijk) via API.	Ja
9.	Datalek in de backend van Effectory (*verlies van controle*).	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 27701-certificering Effectory.	Ja
			ISO 27001-certificering Effectory.	Ja
10.	Datalek door misbruik van toegangsrechten (*verlies van controle*)	Laag	Geheimhoudingsplicht voor medewerkers.	Ja
			Logging op ongeautoriseerde activiteiten.	Ja

<u>Toelichting</u>

Spontane herkenning/Reputatieschade/Inbreuk op de persoonlijke levenssfeer

In sommige onderzoeken wordt gewerkt met open tekstvelden waarin de Respondent een toelichting kan geven. Het 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). De gedachte hierachter is om recht te doen aan de oorspronkelijke intentie van de Respondent. 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.[36] 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.[37] Of dit leidt tot risico's voor de Respondent of een ander zal enerzijds afhangen van de inhoud van het commentaar. Anderzijds hangt het ook af 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 en politiek prominente personen worden verwerkt! Voor zover medewerkers met dergelijke functies toch deelnemen aan het medewerkersonderzoek, geldt dat een eventuele doorbreking van de beveiligingsmaatregelen binnen het concept InternetSpiegel zou kunnen leiden tot veiligheidsrisico's voor de Respondent en/of diens familie. Hoewel de kans daarop -gelet op de beveiligingsmaatregelen die zowel Effectory als ICTU hebben 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. Zo ja, dient de Werkgever te beoordelen of eventuele aanvullende afspraken en/of beschermingsmaatregelen dan wel afwijkende procedures nodig zijn. Binnen de looptijd van het concept 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 het concept InternetSpiegel gerapporteerd wordt door middel van een gemiddelde score per vraag. In beginsel geschiedt dit zonder uitsplitsing naar antwoordcategorie, waardoor het risico van uitspraken doen over te kleine populaties wordt geëlimineerd. Bij bepaalde vragen van InternetSpiegel, waaronder meerkeuzevragen

36 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).

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

en enkelvoudige vragen die niet in stellingvorm worden voorgelegd, vindt echter wel een uitsplitsing naar antwoordcategorie plaats. Een uitsplitsing naar antwoordcategorie vindt eveneens plaats wanneer in tabelvorm wordt gerapporteerd, waarbij bijvoorbeeld wordt weergegeven dat x% van de respondenten antwoordcategorie Y heeft 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 als 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. Het risico van spontane herkenning blijft echter inherent aanwezig als de Werkgever toegang heeft tot de ruwe data (met name in combinatie met de antwoorden in de open tekstvelden). Dit leidt mogelijk 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). Dit geldt alleen indien de aard van het onderzoek en de antwoorden daar uiteraard aanleiding voor geeft en de gegevens buiten de kring van de onderzoekers worden verspreid. Vanuit de oogpunten van zowel de AVG als die van het goed werkgeverschap is het aan de Werkgever als verwerkingsverantwoordelijke om te zorgen voor passende waarborgen voor de bescherming van de belangen van de Respondenten. Bijvoorbeeld dat de gegevens uitsluitend toegankelijk zijn voor onderzoekers met een geheimhoudingsplicht.

4 Beschrijving maatregelen

In dit hoofdstuk staat een overzicht beschreven van de algemene maatregelen 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 (artikel 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). Het is daarmee uitgesloten dat de Werkgever de gegevens gebruikt voor andere doeleinden dan waarvoor ze zijn verzameld.

NB In sommige situaties wordt er op verzoek van de Werkgever van deze standaard binnen het concept 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 eerder gegeven antwoorden uit de vragenlijst aanpassen.

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.

Ook andere organisaties kunnen op eigen verzoek gebruikmaken van API voor de aanlevering van gegevens.

Bewaartermijnen
De bewaartermijn is standaard een half jaar na afloop van de overeenkomst. Indien de Werkgever de data wil bewaren, bijvoorbeeld wanneer gedurende een jaar geen meting plaatsvindt, wordt er gebruik gemaakt van dataretentie. Gewenste afwijkingen van de standaardbewaartermijn worden door de Werkgever opgenomen in een verwerkinstructie en door Effectory nageleefd. Na het verstrijken van de bewaartermijn verwijdert Effectory alle gegevens uit de verschillende databases, inclusief rapportages in PDF- en PPT-formaat.

Privacymanagement
De verantwoordelijkheid voor naleving van de AVG binnen het concept InternetSpiegel is belegd bij de programmamanager van het programma Venster werkzaam bij ICTU. Privacy en informatiebeveiliging waren een belangrijk aandachtspunt in de aanbesteding van het concept InternetSpiegel. ICTU stemt met Effectory de procedures af rondom de gegevensverwerking in het concept 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 FG die toezicht houdt op de gegevensverwerking binnen het concept InternetSpiegel. Effectory heeft een CISO en een jurist die nauw betrokken zijn bij de zorgvuldige gegevensverwerking en de naleving van de AVG. Het management van Effectory en ICTU hechten belang aan privacy en compliance en zijn nauw betrokken bij de naleving van het privacybeleid 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. Beide voldoen aan de eisen van de AVG.

Effectory heeft overeenkomsten gesloten met de subverwerkers Microsoft, Mailjet en Kombo Technologies GmbH.

4.1.2 Maatregelen uitoefening rechten betrokkenen (artikel 12)

Informatie
ICTU en Effectory hebben een standaardprivacyverklaring opgesteld. Wanneer de Respondent de unieke link naar de vragenlijst aanklikt, krijgt hij/zij de verklaring aangeboden. Deze link staat in de uitnodiging die Respondenten per e-mail 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 medewerkers van Werkgever (ook voor zij die geen vragenlijst invullen). 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.

4.1.3 Beveiligingsmaatregelen (artikel 32)

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.[38]

Preventieve maatregelen
Effectory voert wekelijks een *vulnerability scan* 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 de 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 geauditeerd.

Geheimhouding
De medewerkers van Effectory en de verwerkers van Effectory (subverwerkers) zijn gebonden aan geheimhouding.

Screening
Alle medewerkers van Effectory moeten een Verklaring Omtrent het Gedrag overleggen bij indiensttreding en daarna elke drie jaar.

Versleuteling

38 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.

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 Microsoft Azure gaat via een IPSec VPN. De gegevens worden in Microsoft Azure altijd versleuteld opgeslagen.

Mobiele apparaten zijn versleuteld met en worden beheerd door Microsoft EndPoint Manager (mobile device management). Data die op laptops zijn opgeslagen zijn versleuteld met Bitlocker. Het is niet mogelijk om data te kopiëren of te verplaatsen naar draagbare media zoals USB-sticks.

Autorisaties en toegangscontrole

Binnen Effectory hebben medewerkers alleen toegang tot gegevens die zij nodig hebben voor hun taak.[39] Effectory voert logging uit op (on)geautoriseerde activiteiten. Effectory-medewerkers gebruiken MFA voor toegang tot Effectory's portals (Microsoft Azure en customer portal).

Werkgevers kunnen ook via Single Sign-On aansluiten op de portal. De MFA voor toegang tot Effectory's portals is verplicht voor bepaalde rollen die toegang hebben tot de vooraf aangeleverde persoonsgegevens.[40] 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 and prevention*-systeem van Microsoft om aanvallen op haar webapplicaties in Microsoft Azure te detecteren.

Apparaatbeheer

USB-poorten zijn geblokkeerd,
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 securitylevel 3-niveau. Hardwarevernietiging 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 het concept 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 –

39 Zie verder de opmerkingen in paragraaf 1.5.3.

40 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.

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. In dat geval worden de betrokkenen door de respectievelijke Werkgevers geïnformeerd. Voor dat laatste is gekozen om de Werkgevers vanuit hun werkgeverschap in staat te stellen hun verantwoordelijkheid tegenover hun medewerkers te nemen. Zo hebben de werkgevers controle 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 richting 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.