**Wereldwijde privacyverklaring m.b.t. medewerkers van externe partijen**

|  |  |
| --- | --- |
| **Contact privacyverklaring:**  Wereldwijde functionaris voor gegevensbescherming | **Datum: 1 januari 2023**   |
|  (pgprivacyofficer.im@pg.com) **Regio:** Wereldwijd | **Toepassingsgebied:**  Alle medewerkers van externe partijen |

# **D****oel**

Deze verklaring informeert alle medewerkers van externe partijen (External Party Resources, EPR's) (hieronder gedefinieerd) over hoe The Procter & Gamble Company, haar dochterondernemingen en/of gelieerde ondernemingen (‘P&G’ of het ‘Bedrijf’) uw persoonsgegevens zullen verzamelen en beheren.

# **Status van onafhankelijke aannemer**

Deze verklaring creëert geen arbeidsrelatie tussen P&G en een EPR. EPR's leveren diensten aan P&G als onafhankelijke aannemers, ongeacht of dergelijke diensten rechtstreeks aan P&G worden geleverd of op grond van een overeenkomst tussen P&G en de werkgever van de EPR.

1. **Begrippen**

**Medewerker van een externe partij:** Elke persoon die P&G werk of diensten levert voor wie P&G niet de geregistreerde werkgever is op het moment dat het werk of de diensten worden geleverd, zoals aannemers.

**Persoonlijke Informatie:** Alle informatie met betrekking tot een geïdentificeerde of identificeerbare persoon, zoals hun naam, andere identificatoren, contactgegevens, professionele informatie en persoonlijke kenmerken.

**Het bedrijf of P&G:** Binnen deze verklaring verwijst het bedrijf of P&G naar The Procter & Gamble Company, haar dochterondernemingen en/of vestigingen.

1. **Principes**

De fundamentele principes voor gegevensbescherming van P&G zijn:

* De minimale hoeveelheid persoonsgegevens van EPR’s verzamelen en beheren.
* Respecteren van individuele privacy.
* Voldoen aan onze doelstellingen, waarden en principes (Purposes, Values and Principles, PVP’s), deze verklaring en relevante wetten.
* Volgen van gepaste normen en procedures bij het verzamelen en/of beheren van persoonsgegevens van EPR’s.
1. **Meldingen**

P&G respecteert uw privacy. Deze kennisgeving beschrijft hoe we persoonsgegevens van EPR’s verwerken, de soorten informatie die we rechtstreeks van u en/of uw werkgever verzamelen, de doeleinden waarvoor we de informatie gebruiken, de categorieën ontvangers met wie we de informatie delen en de keuzes die u kunt maken over ons gebruik van de informatie. We beschrijven ook de maatregelen die we nemen om de veiligheid van persoonsgegevens van EPR’s te beschermen en hoe u contact met ons kunt opnemen over onze privacy praktijken.

* 1. **Voor welke doeleinden verzamelen en gebruiken we persoonsgegevens van EPR’s?**

P&G verzamelt persoonsgegevens over zijn EPR’s in het kader van de serviceovereenkomst en de relatie met een onafhankelijke aannemer die P&G met u en/of uw werkgever heeft. Over het algemeen verzamelen en gebruiken wij persoonsgegevens van EPR’s van u en/of uw werkgever voor de volgende diensten en/of activiteiten:

* Gezondheid/veiligheid op het werk, met inbegrip van gezondheidsgerelateerde screenings en medische programma's in verband met COVID-19 of vergelijkbare medische noodsituaties
* Site-toegangsbeheer
* Identiteits- en referentiebeheer, waaronder identiteitsverificatie en -authenticatie, uitgifte van ID-kaarten en -badges, systeembeheer, registratie van in- en uitloggen en beheer van toegangsgegevens, informatiebeveiliging en cybersecurity
* Noodplanningsdoeleinden, waaronder bedrijfscontinuïteit, personeelsbezetting, ploegendienst en nood-/veiligheidsprotocollen
* Registratie en beheer van elektronische apparaten en optimalisering van het gebruik van netwerken en apparatuur
* Fysieke en cyberveiligheidscontroles, waaronder bewaking van elektronische apparatuur en netwerken en beveiligingsvideo-opname zoals een gesloten televisiecircuit
* Procesvoering en interne/externe onderzoeken, audits en geschillenbeslechting
* Dagelijkse verwerking van werk (bijv. het authentificeren van en inloggen op onze systemen)
* Deelname aan vergaderingen, trainingen en evenementen
* Naleving van de wet- en regelgeving en beleidslijnen van het Bedrijf met betrekking tot anti-omkoping, kinderarbeid, anticorruptie, sancties, exportcontroles, mensenrechten en andere vereisten voor corporate governance en stewardship
* Onderzoeken onder leiding van P&G en/of uw werkgever met betrekking tot wangedrag op de werkplek of schendingen van de rechtsgang
* Handhaving en controle van onze serviceovereenkomsten met u en/of uw werkgever, inclusief het beoordelen van de prestaties van de services
* Naleving van alle wettelijke, regelgevende, gerechtelijke of overheidsvereisten en het reageren op en voldoen aan gerechtelijke bevelen, dagvaardingen, ontdekkingsverzoeken of andere gegevensverzoeken van de overheid
	+ Beveiliging en risicobeheer, inclusief beveiliging en bewaking van personeel en gebouwen, en bescherming van P&G, onze werknemers en onze klanten tegen diefstal, wettelijke aansprakelijkheid, fraude of misbruik.
	1. **Welke soorten persoonsgegevens verzamelen we van EPR’s?**

We zullen altijd de soorten en de hoeveelheid persoonsgegevens van EPR’s die we van of over u kunnen verzamelen, tot een minimum beperken. De onderstaande tabel beschrijft in meer detail de categorieën van persoonsgegevens van EPR’s die P&G verzamelt in verband met haar bedrijfsprocessen.

Het verzamelen van informatie en de toegang tot informatie zal variëren afhankelijk van de landspecifieke wettelijke en/of zakelijke vereisten.

De zakelijke of rechtsgrond voor het verzamelen en verwerken van persoonsgegevens van EPR’s verschilt per soort gegevens en beoogd gebruik, zoals beschreven in paragraaf 5.3 hieronder.

|  |  |
| --- | --- |
| **Welke soorten persoonsgegevens van EPR’s verzamelen en verwerken we?** | **Waarom verzamelen en verwerken we dit soort persoonsgegevens van EPR’s?***We verzamelen en verwerken deze soorten gegevens voor meerdere organisatorische en zakelijke processen zoals beschreven in paragraaf 5.1 en zoals hieronder verder uitgelegd:* |
| *Contactgegevens en persoonlijke kenmerken* * Volledige naam of eerdere namen (zoals meisjesnamen)
* Andere unieke identificatoren, zoals door P&G uitgegeven identificatienummers of toegangsgegevens (bijv. inloggen via e-mail) of een identificatienummer dat door uw werkgever is verstrekt.
* Postadres
* E-mailadres
* Telefoonnummer
 | * Toegang tot de locatie en het elektronische netwerk
* Communicatie met u met betrekking tot bedrijfsnoodplannen, inclusief ploegendienst
* Deelname aan vergaderingen, trainingen en evenementen
* Dagelijkse verwerking van werk (bijv. het authentificeren van en inloggen op onze systemen)
* Wettelijke en beleidsnaleving
* Corporate governance en rentmeesterschap
* Verplichte externe rapportage
* Onderzoek en incidentmanagement
	+ Beveiliging en risicobeheer, inclusief beveiliging en bewaking van personeel en gebouwen, en bescherming van P&G, onze werknemers en onze klanten tegen diefstal, wettelijke aansprakelijkheid, fraude of misbruik
* Gezondheid/veiligheid op het werk, met inbegrip van gezondheidsgerelateerde screenings en medische programma's in verband met COVID-19 of vergelijkbare medische noodsituaties
* Handhaving en controle van onze serviceovereenkomsten met u en/of uw werkgever, inclusief het beoordelen van de prestaties van de services
* Naleving van alle wettelijke, regelgevende, gerechtelijke of overheidsvereisten en het reageren op en voldoen aan gerechtelijke bevelen, dagvaardingen, ontdekkingsverzoeken of andere gegevensverzoeken van de overheid
 |
| *Overheids-ID/Informatie over werkvergunning/Werkgevers-ID** Nationaal identiteitsbewijs (zoals paspoort, visa, burgerservicenummer/sociale zekerheidsnummer, rijbewijs en andere door de overheid uitgegeven identificatiebewijzen)
* Staatsburgerschap
* Woonplaats
* Nationaliteit
* Geboorteland
* Militaire en/of veteranenstatus
* Unieke ID als werknemer van het bedrijf waarmee P&G een contract heeft afgesloten
 | * U wettelijk identificeren en de integriteit van onze dossiers handhaven
* Voldoen aan immigratie- en andere werkvergunningsvereisten
* Beveiligings- en risicobeheer, zoals het verzamelen van rijbewijsgegevens voor EPR’s die bedrijfsauto's besturen, verificatie van professionele licenties, fraudepreventie en soortgelijke doeleinden
* Wettelijke en beleidsnaleving
* Corporate governance en rentmeesterschap
* Beveiliging en noodplanning
* Verplichte externe rapportage
* Onderzoek en incidentmanagement
 |
| *Financiële informatie* * Bankrekeningnummer en -gegevens
* Informatie over persoonlijke betaalkaarten, indien verstrekt voor vergoedingen
 | * Faciliteren van onkostenvergoedingen
* Wettelijke en beleidsnaleving
* Corporate governance en rentmeesterschap
* Beveiliging en noodplanning
* Verplichte externe rapportage
* Onderzoek en incidentmanagement
 |
| *Gezondheidsinformatie* * Informatie met betrekking tot de fysieke of emotionele gezondheid van een persoon, waaronder eventuele handicaps of beperkingen om werktaken of functies uit te voeren
* Drugstests en andere soorten gezondheidsonderzoeken
 | * Voldoen aan de vereisten voor gezondheid op het werk en veiligheid op de werkplek en rapportage aan de overheid
* Beheren van de veiligheids- en bedrijfsrisico's voor EPR’s in verband met de COVID-19-pandemie of soortgelijke noodsituaties op gezondheidsgebied
* Wettelijke en beleidsnaleving
* Corporate governance en rentmeesterschap
* Beveiliging en noodplanning
* Verplichte externe rapportage
* Onderzoek en incidentmanagement
 |
| *Elektronische identificatiegegevens/unieke identificaties/afbeelding en stem** Systeemidentificaties van P&G (bijv. gebruikersnamen of online inloggegevens)
* Digitale handtekening
* Elektronische identificatiegegevens, logboeken en dossiers met betrekking tot toegang tot en gebruik van apparaten, systemen, applicaties, licenties en databases van P&G en het netwerk van P&G (zoals uw gebruik van e-mail, internet en social media).
* Informatie verzameld door beveiligingssystemen van P&G, waaronder de Closed Circuit Television (“CCTV”), toegangssystemen op de locatie, lijnproces- of taakcamera's
* Elektronische identificatiegegevens, logboeken en dossiers met betrekking tot toegang tot fysieke vestigingen van P&G en gebieden met beperkte toegang, waaronder badgenummer/badge-identificatiekenmerk en foto
* Video, foto's en andere beeld-/spraakopnamen in het kader van bijeenkomsten/trainingen
* Elektronische identificatiegegevens met betrekking tot opnamen vanuit callcenters
 | * Toegang en beheer van systemen, technologie en IT-middelen
* Ondersteunen van onze belangen met betrekking tot fysieke beveiliging, informatie- en cyberbeveiliging tegen interne en/of externe bedreigingen
* Beheren van verliespreventie en -herstel in onze kantoren en productielocaties
* Interne administratie en rapportage, waaronder matching en analyse van gegevens
* Toegang tot websites, netwerken, tools, applicaties en andere bedrijfssystemen en -middelen van P&G mogelijk maken
* Bevorderen van de zichtbaarheid van het gebruik en de kosten voor het verbruik van tools, -licenties, -diensten en -applicaties van P&G voor optimalisatie-, kwaliteits-, audit- en kostendoeleinden
* Vastleggen van trainingen en vergaderingen
* Wettelijke en beleidsnaleving
* Corporate governance en rentmeesterschap
* Beveiliging en noodplanning
* Verplichte externe rapportage
* Onderzoek en incidentmanagement
 |
| *Cookies -* Cookies zijn kleine bestanden die naar uw computer worden verzonden wanneer u op het internet surft. Ze slaan nuttige informatie op over uw interactie met de websites die u bezoekt. Cookies verzamelen geen informatie die op uw computer of apparaat of in uw bestanden is opgeslagen. Cookies bevatten geen informatie die u rechtstreeks zou kunnen identificeren. Cookies tonen uw computer en apparaat alleen als willekeurig toegewezen nummers en letters (bijv. cookie-ID ABC12345) en bijvoorbeeld nooit als Jan E. Smit. Dit zijn de soorten cookies die we gebruiken: * *Sessiecookies*.Sessiecookies onthouden u (met behulp van een willekeurig gegenereerd ID) terwijl u van pagina naar pagina gaat, zodat u niet wordt gevraagd om informatie die u al eerder hebt verstrekt. Deze cookies worden verwijderd zodra u onze website verlaat of uw browser sluit.
* *Permanente cookies*. Permanente cookies stellen websites in staat om te onthouden waar u de voorkeur aan geeft wanneer u opnieuw een website bezoekt. Als u er bijvoorbeeld voor kiest om de website bij uw eerste bezoek in het Frans te lezen, zal de website de volgende keer dat u een bezoek brengt automatisch in het Frans verschijnen.
* *Analytische cookies*. Deze cookies vertellen ons hoe onze websites werken. In sommige gevallen gebruiken we cookies van Google Analytics om de prestaties van onze websites te controleren. Onze mogelijkheid om door Google Analytics verzamelde informatie over uw bezoeken aan onze websites te gebruiken en te delen, wordt beperkt door de [Gebruiksvoorwaarden van Google Analytics](https://www.google.com/analytics/terms/us.html) en het [Privacy beleid van Google](https://policies.google.com/privacy).
 | We gebruiken cookies op de P&G-websites voor EPR’s om een aantal redenen, waaronder: * om meer te weten te komen over de manier waarop u omgaat met onze websites en de P&G-inhoud
* om ons te helpen uw ervaring te verbeteren wanneer u onze websites bezoekt
* om de website aan te passen aan uw voorkeuren
* om fouten te identificeren en op te lossen
* om te analyseren hoe goed onze websites presteren
 |
| *Andere persoonlijke kenmerken** Biometrische gegevens, zoals vingerafdrukken of gezichtsscans
* Strafblad/achtergrondcontroles
 | * Faciliteren van uw toegang tot bedrijfslocaties en -systemen via biometrische gegevens
* Wettelijke en beleidsnaleving
* Corporate governance en rentmeesterschap
* Beveiliging en noodplanning
* Verplichte externe rapportage
* Onderzoek en incidentmanagement
 |

* 1. **Op grond van welke zakelijke en/of rechtsgrond verwerken we persoonsgegevens van EPR’s?**

We verzamelen en beheren de minimale persoonsgegevens van EPR’s die nodig zijn om: te voldoen aan onze contractuele en/of wettelijke verplichtingen gerelateerd aan onze aannemersrelatie met u en/of uw werkgever; om de legitieme zakelijke belangen van het Bedrijf te ondersteunen op een manier die in verhouding staat tot uw privacybelangen; en om, indien van toepassing, persoonsgegevens te verwerken die met uw toestemming zijn verstrekt voor de beoogde doeleinden.

De zakelijke en/of rechtsgrond voor het verwerken van persoonsgegevens van EPR’s kan de naleving door P&G zijn van de toepasselijke wet- en regelgeving; naleving van haar contractuele verplichtingen; de legitieme zakelijke belangen van het Bedrijf; belangen voor de volksgezondheid; en/of uw toestemming.

De zakelijke en/of rechtsgrond voor het verwerken van persoonsgegevens van EPR’s kan variëren per rechtsgebied, evenals per gegevenscategorie/-type en per doeleinde waarvoor we dergelijke informatie verzamelen en gebruiken.

Dit zijn de rechtsgrondslagen waarop we ons over het algemeen zullen baseren voor de verwerking van deze categorieën gegevens:

|  |  |
| --- | --- |
| **Soort persoonsgegevens** | **Zakelijke en/of rechtsgrond voor verwerking** |
| Contactgegevens, overheids-ID, financiële informatie, gezondheidsinformatie | Naleving van contractuele en wettelijke verplichtingen door P&G  |
| Overheids-ID / werkvergunning | Naleving door P&G van toepasselijke wetgeving |
| Professionele gegevens, contactgegevens | Legitieme zakelijke belangen van P&G |

* 1. **Hoe delen we persoonsgegevens van EPR’s?**

P&G deelt alleen persoonsgegevens van EPR’s met partijen die een legitieme zakelijke behoefte hebben om die gegevens te kennen.

P&G deelt uw informatie mogelijk met uw werkgever (en andere entiteiten in opdracht van uw werkgever), aannemers, leveranciers, agentschappen en uitzendkrachten van P&G of andere partijen die namens P&G optreden (‘Externe partijen’).

Persoonsgegevens van EPR’s worden mogelijk gedeeld met ons hoofdkantoor en gelieerde ondernemingen wereldwijd als dat nodig is om de verwerkingsdoeleinden te bereiken die uiteengezet zijn in sectie 5.2 hierboven.

We maken mogelijk ook persoonsgegevens van EPR’s openbaar als we daartoe wettelijk of door een gerechtelijke uitspraak verplicht zijn; om de rechten en het beleid van P&G uit te voeren of te beschermen; en/om te assisteren bij onderzoek naar mogelijk of daadwerkelijk wangedrag of illegale activiteiten.

* 1. **Wat zijn uw privacy rechten?**

U hebt het recht om contact met ons op te nemen en toegang te vragen tot de persoonsgegevens van EPR’s die we van u verwerken. Waar toegestaan door de toepasselijke wetgeving, kunt u verzoeken dat onjuiste, verouderde of onnodige gegevens worden gecorrigeerd, gewist of afgeschermd, en kunt u P&G vragen om uw gegevens te verstrekken in een formaat waarin u uw gegevens kunt overdragen aan een serviceprovider, zoals in dat geval van toepassing. Wanneer de verwerking van persoonsgegevens van EPR’s is gebaseerd op toestemming, hebt u het recht om uw toestemming op elk gewenst moment in te trekken. Wanneer de verwerking van persoonsgegevens van EPR’s is gebaseerd op een legitiem belang, hebt u het recht om onder bepaalde omstandigheden bezwaar te maken tegen de gegevensverwerking.

Wanneer u deze rechten uitoefent, raden we u aan om uw zorgen eerst te bespreken met de P&G-medewerker die optreedt als uw sitesponsor. U kunt ook contact opnemen met onze Functionaris voor gegevensbescherming op het onderstaande adres. Als u niet tevreden bent met ons antwoord op uw verzoek of onze verwerking van uw persoonsgegevens, kunt u een klacht indienen bij de autoriteit voor gegevensbescherming in uw land.

* 1. **Hoe dragen we persoonsgegevens van EPR’s over?**

P&G is een wereldwijd bedrijf en heeft EPR’s in talloze landen. Indien wettelijk toegestaan en behoudens landspecifieke verplichtingen en/of beperkingen, worden persoonsgegevens van EPR’s mogelijk overgedragen naar landen buiten het land waarin de gegevens zijn verzameld. Persoonsgegevens van EPR’s worden mogelijk opgeslagen op systemen in de Verenigde Staten, geopend vanuit andere P&G-vestigingen wereldwijd, waaronder hun dienstverleners, of overgedragen naar andere landen, voor zover nodig om de relevante bedrijfsactiviteiten te kunnen verrichten. Deze landen hebben wellicht niet dezelfde wetten voor gegevensbescherming als uw thuisland. Als uw persoonsgegevens worden overgedragen naar of geopend worden vanuit landen buiten uw thuisland, hanteren we gepaste maatregelen en alle wettelijk verplichte administratieve, technische en/of contractuele vereisten om uw gegevens te beschermen. We voeren overdrachten uit buiten de Europese Economische Ruimte (EER), het Verenigd Koninkrijk (VK) en Zwitserland, zowel tussen P&G-entiteiten als naar onze dienstverleners, waarbij we vertrouwen op de standaardcontractbepalingen. Als u een kopie van deze bepalingen wilt ontvangen, neem dan contact op met corporateprivacy.im@pg.com. P&G zal ook voldoen aan andere landspecifieke verplichtingen die de overdracht van gegevens buiten het land van verzameling beperken.

* 1. **Hoe beveiligen we persoonsgegevens van EPR’s?**

Wij implementeren gepaste fysieke, administratieve en technische maatregelen, zoals anonimisering, encryptie en toegangscontroles, ontworpen ter bescherming van persoonsgegevens van EPR’s tegen ongeplande, onrechtmatige of ongeautoriseerde vernietiging, verlies, wijziging, openbaarmaking of toegang of gebruik en alle andere onrechtmatige vormen van verwerking. Wanneer Externe Partijen persoonsgegevens van EPR’s namens P&G verwerken, gaan we ook contracten aan met die Externe Partijen om ervoor te zorgen dat ze de juiste fysieke, administratieve en technische maatregelen implementeren voor het verwerken van dergelijke gegevens.

**5.8 Hoelang bewaart u mijn persoonsgegevens?**

We bewaren persoonsgegevens van EPR’s zo lang als nodig is om de doeleinden te vervullen waarvoor ze zijn verzameld, tenzij een langere bewaartermijn is vereist of toegestaan door de toepasselijke wetgeving. Dit zal over het algemeen zijn voor de periode dat u ons diensten verleent. In sommige gevallen moeten we persoonsgegevens van EPR’s gedurende een bepaalde periode na de beëindiging van uw relatie met P&G bewaren om te voldoen aan wettelijke of contractuele verplichtingen.

* 1. **Controleert P&G het gebruik van het netwerk en de apparatuur?**

Het Bedrijf controleert het gebruik van netwerken en apparaten van P&G. P&G heeft de verplichting om haar werknemers, bedrijfsmiddelen en faciliteiten te beschermen. P&G controleert haar bedrijfsnetwerken en apparaten voor drie doeleinden: i) om de veiligheid (die vertrouwelijkheid, integriteit en beschikbaarheid omvat) van de medewerkers, gegevens, netwerken, bedrijfsmiddelen, faciliteiten, reputatie en concurrentiebelangen van P&G te beschermen; ii) om vermoed of bevestigd wangedrag of schendingen van de wet te onderzoeken (waaronder ter ondersteuning van procesvoering); en iii) om de integriteit van bedrijfsprocessen en financiële rapportage te garanderen.

P&G controleert het P&G-netwerk en de apparaten van een specifiek individu niet, tenzij er een legitieme reden voor is of als we hiertoe wettelijk verplicht zijn, inclusief op verzoek van wetshandhavers. We behouden ons het recht voor om, met inachtneming van de toepasselijke wetgeving, elektronische bestanden, gegevens en berichten die zijn gecreëerd, opgeslagen, verzonden of ontvangen via onze netwerken en apparaten te openen, te inspecteren, openbaar te maken en te verwijderen, voor zover nodig voor de bovengenoemde doeleinden. Deze controle voldoet altijd aan relevante wetten en regelgeving. P&G zal waar nodig aanvullende procedures, normen, beleidslijnen en/of actieve maatregelen implementeren om te voldoen aan lokale wettelijke verplichtingen.

P&G zal met name passieve en actieve controle uitvoeren van P&G-netwerken en P&G-apparaten die zijn toegewezen aan EPR’s om potentiële bedreigingen voor de belangen van P&G te identificeren. De ‘passieve controle’ zal niet actief het gedrag van een individu onderzoeken, maar zoekt in plaats daarvan naar indicatoren van risico's. Deze risico-indicatoren zijn vooraf gedefinieerd door P&G en gespecialiseerde beveiligingsleveranciers en zijn afgestemd op de beveiligingsbehoeften van P&G. Wanneer een dergelijke risico-indicator wordt geactiveerd (een ‘gebeurtenis’), registreren de systemen de gerelateerde gegevens en bewaren ze deze voor latere beoordeling en/of onderzoek. In het bijzonder zullen de onderstaande technieken voor passieve controle worden gebruikt voor P&G-netwerken en apparaten die eigendom zijn van P&G en zijn toegewezen aan EPR’s:

1. **Controle van gebruikspatronen** is een controletechniek waarbij software of hardware geanonimiseerde netwerk- en webgegevens van P&G controleert op een vooraf gedefinieerde set risico-indicatoren. Deze techniek zoekt naar verdachte patronen in het *gebruik* van het netwerk van P&G en/of apparaten die eigendom zijn van P&G en zijn toegewezen aan EPR's. P&G kan bijvoorbeeld de controle van gebruikspatronen instellen om te zoeken naar risico-indicatoren per P&G-inloglocatie. P&G Security kan de tool zo afstemmen dat deze een waarschuwing genereert als de inloggegevens van een gebruiker sneller op twee verschillende P&G-locaties worden ingevoerd dan een persoon redelijkerwijs van de ene naar de andere locatie zou kunnen reizen.
2. **Scannen van binnenkomend verkeer** is een controletool die inkomende webgebaseerde communicatie (inclusief e-mail) scant op risico-indicatoren wanneer deze communicatie het netwerk van P&G binnenkomt. Antivirus- en firewallsoftware is het meest voorkomende voorbeeld van deze tool, omdat dergelijke software voortdurend inkomend verkeer scant op indicatoren van malware in bijlagen, links, websites, enz.
3. **Periodiek scannen** is een controletool die scant op het niveau van het P&G-netwerk en het P&G-apparaat om specifieke risico-indicatoren op te sporen die mogelijk voorbij de perimeterscans van het Scannen van binnenkomend verkeer zijn geglipt. Deze tool is handig omdat gebeurtenissen soms gemakkelijker te identificeren zijn wanneer ze worden bekeken met aanvullende context. Een antivirusscan van de volledige harde schijf is een goed voorbeeld van deze optie.
4. **Scannen van uitgaand verkeer** P&G heeft de mogelijkheid om uitgaand webverkeer te scannen op specifieke, vooraf gedefinieerde risico-indicatoren. De tool scant het uitgaande verkeer om te zien of een gebeurtenis is geactiveerd volgens de gespecificeerde risico-indicatorregels. P&G kan bijvoorbeeld een regel schrijven die grote bestandsuploads naar plaatsen buiten het P&G-netwerk rapporteert die hoogst vertrouwelijke gegevens of bepaalde trefwoorden bevatten, zoals een specifieke chemische verbinding die wordt gebruikt in een nieuwe productformule

Op basis van de aard van een risico dat is geïdentificeerd door de tools voor passief toezicht of anderszins onder de aandacht van P&G is gebracht (bijv. rechtszaak, vermeend wangedrag, wetshandhaving, enz.) bepaalt P&G of verder onderzoek/analyse van het risico nodig is. Bij die beoordeling houdt P&G rekening met de mogelijke schade voor werknemers, consumenten, andere belanghebbenden en/of het bedrijf, evenals met de juridische en privacybelangen van alle betrokken personen. P&G bepaalt mogelijk ook of verdere analyse vereist is op basis van wettelijke of beleidsvereisten om activa te beschermen en de integriteit van bedrijfsprocessen te garanderen. Op basis van deze analyse zal P&G ofwel geen verder onderzoek verrichten of overgaan op een proportioneel onderzoek met behulp van actieve controletools.

P&G gebruikt vijf basistypen van actieve controletools: (1) Apparaat scannen, (2) Internet scannen, (3) Zachte controle, (4) Hardware controle en (5) Preventie van gegevensverlies.

1. **Apparaat scannen:** Met deze tools kan P&G, soms via een derde partij, de *volledige* inhoud van een computer of ander apparaat van P&G in één keer ophalen voor gebruik in een onderzoek. Tools voor het scannen van apparaten halen niet alleen de bestanden en applicaties op die zijn opgeslagen op het P&G-apparaat, maar kunnen ook het geheugen oppikken dat op dat apparaat aanwezig was op het moment van vastleggen. Afhankelijk van de tool kan P&G ervoor kiezen om alleen fysieke bestanden op te halen (d.w.z. geen geheugen) of een gedeeltelijk beeld van het apparaat op te halen, waardoor het onderzoek zich uitsluitend kan richten op specifieke bestandstypen of toepassingen in overeenstemming met de principes van proportionaliteit.
2. **Internet scannen:** P&G maakt gebruik van een cloudgebaseerde webproxytool van derden met drie primaire functies. Ten eerste beschikt het over de mogelijkheid om het openbare internetgebruik te volgen op URL-niveau (d.w.z. de namen van de bezochte webpagina's) wanneer het EPR een apparaat van P&G gebruikt. Deze functie volgt en registreert internetactiviteit door gebruik te maken van gehashte persoonlijke identificatiegegevens (waardoor de gebruiker wordt geanonimiseerd) voor mogelijk gebruik in een goedgekeurd onderzoek. Ten tweede beschikt het over de mogelijkheid om inzicht te geven in de gegevens die zijn ingevoerd op een niet-versleutelde webpagina en de bestanden die zijn geüpload of gedownload bij het bezoeken van niet-versleutelde websites. Ten derde beschikt het over de mogelijkheid om een beperkte subgroep van webverkeer te ontsleutelen die vooraf is gedefinieerd als een hoog risico (bijvoorbeeld uitgaande verbindingen naar bekende schadelijke webpagina's, webpagina's waarvan bekend is dat ze malware naar apparaten sturen of niet-goedgekeurde sites voor het delen van bestanden). Deze oplossing is geconfigureerd om verkeer dat bestemd is voor websites die mogelijk gevoelige persoonlijke informatie over de eindgebruiker verwerken niet te ontsleutelen (bijvoorbeeld websites van banken en zorgdiensten).
3. **Zachte controle:** Dit zijn technieken die worden ingezet als onderdeel van een onderzoek waarbij identificeerbare personen betrokken zijn, waarbij (a) de persoon op de hoogte wordt gebracht van het onderzoek en (b) de persoon niet het onderwerp van het onderzoek is. Een zachte controletool kan bijvoorbeeld een telefoontje of een e-mail zijn om te bepalen waar een *geïdentificeerde* EPR zich momenteel bevindt/ingelogd is om te bepalen of een geografisch geactiveerde Gebeurtenis legitiem is.
4. **Hardware- en applicatiecontrole**: Tools voor hardware- en applicatiecontrole zijn registratie- en controlemogelijkheden die fabrikanten inbouwen in de hardware en/of applicaties die, in combinatie met een identificeerbare EPR, actieve controle vormen. Veelgebruikte voorbeelden zijn serverlogboeken, SAP-logins, gebruiksrapporten van ID-badges, netwerkauthenticatie, enz.
5. **Preventie van gegevensverlies:** P&G of een goedgekeurde serviceprovider scant e-mails die bestemd zijn voor niet-P&G-adressen op indicatoren van gegevensverlies. Als een EPR bijvoorbeeld een niet-versleutelde e-mail met een hoogst vertrouwelijke bijlage naar een niet-P&G-e-mailadres verzendt, rapporteert de oplossing voor het voorkomen van gegevensverlies die e-mail als een informatiebeveiligingsrisico en kan de gebruiker worden geïnformeerd dat voor toekomstige communicatie een goedgekeurde versleutelingsoplossing moet worden gebruikt. Als een uitgaande e-mail die is geclassificeerd als hoogst vertrouwelijk of geheim (inclusief specifiek aangewezen sleutelwoorden) wordt gerapporteerd, wordt die e-mail op vergelijkbare wijze beoordeeld op beveiligingsrisico's. Eventueel kan een onderzoek worden ingesteld. P&G scant geen berichten die zijn geclassificeerd als ‘Persoonlijk’ of ‘Privé’ of die zijn aangeduid als ‘Persoonlijk’ of ‘Privé’ in de onderwerpregel.
6. **Toekomstige wijzigingen**

P&G behoudt het recht om deze Verklaring aan te passen indien nodig, bijvoorbeeld om te voldoen aan wijzigingen in wetten, regelgeving, bedrijfspraktijken en procedures, of om te reageren op nieuwe dreigingen of nieuwe vereisten ingesteld door gegevensbeschermingsautoriteiten. Als dergelijke wijzigingen in materieel opzicht onze verwerking van uw persoonsgegevens als EPR beïnvloeden, zullen we u daarvan overeenkomstig in kennis stellen.

1. **Contactgegevens**

Als u vragen of bedenkingen hebt in verband met onze verwerking van uw persoonlijke informatie/persoonsgegevens als EPR, of uw privacy rechten wenst uit te oefenen, kunt u contact opnemen met onze Global Data Protection Officer via – e-mail: pgprivacyofficer.im@pg.com, telefoon: +1 (513) 622-0103, Postadres: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, VS

Als u zich zorgen maakt over een mogelijke inbreuk van gegevens betreffende de persoonsgegevens van EPR’s of persoonlijke informatie die wordt verwerkt door P&G, neem dan contact met ons op door een e-mail te sturen naar securityincident.im@pg.com.