**Datenschutzerklärung für Mitarbeiter globaler Drittparteien**

|  |  |
| --- | --- |
| **Kontakt Datenschutzerklärung:**  Beauftragter für globalen Datenschutz | **Datum: 1. Januar 2023**   |
|  (pgprivacyofficer.im@pg.com) **Region:** Global | **Geltungsbereich:**  Alle Mitarbeiter von Drittparteien |

# **Zi****elsetzung**

Diese Erklärung informiert alle Mitarbeiter von Drittparteien („EPRs“) (im Folgenden definiert) darüber, wie die „The Procter & Gamble Company“, deren Tochtergesellschaften und/oder verbundene Unternehmen (im Folgenden als „P&G“ oder „Unternehmen“ bezeichnet) Ihre personenbezogenen Daten erhebt und verwaltet.

# **Status als unabhängiger Auftragnehmer**

Aus dieser Erklärung entsteht kein Beschäftigungsverhältnis zwischen P&G und einem EPR. EPRs erbringen ihre Dienstleistungen für P&G als unabhängige Auftragnehmer. Dies gilt ungeachtet dessen, ob die entsprechenden Dienstleistungen direkt für P&G erbracht werden, oder gemäß einer von P&G und dem jeweiligen Arbeitgeber des EPR geschlossenen Vereinbarung.

1. **Definitionen**

**Mitarbeiter einer Drittpartei:** Jegliche Personen, die für P&G Arbeiten oder Dienstleistungen erbringen, ohne dass P&G zum Zeitpunkt der Leistung der Arbeiten bzw. der Erbringung der Dienstleistungen der eingetragene Arbeitgeber ist, wie beispielsweise Auftragnehmer.

**Personenbezogene Daten:** Alle Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen, wie etwa der Name, andere Identifizierungsmerkmale, Kontaktangaben, berufsbezogene Informationen oder persönliche Merkmale.

**Unternehmen oder P&G:** Im Rahmen dieser Erklärung ist mit Unternehmen oder P&G „The Procter & Gamble Company“ sowie deren Tochtergesellschaften und/oder verbundenen Unternehmen gemeint.

1. **Prinzipien**

Die fundamentalen Prizipien der Datenverbarbeitung von P&G sind:

* Das Minimum an personenbezogenen Daten von EPRs zu erheben und zu verwalten.
* Respektieren der Privatsphäre jedes Einzelnen.
* Die Übereinstimmung unserer Ziele, Werte und Prinzipien („Purposes, Values and Principles“, PVPs), dieser Erklärung und den entsprechenden Gesetzen.
* Befolgen der maßgeblichen Standards und Verfahren bei der Erhebung und/oder Verwaltung personenbezogener Daten von EPRs.
1. **Erklärung**

P&G achtet Ihre Privatsphäre. Diese Erklärung erläutert, wie wir personenbezogene Daten von EPRs verarbeiten, welche Arten von Daten wir direkt bei Ihnen und/oder Ihrem Arbeitgeber erfassen, für welche Zwecke wir sie erfassen, an welche Kategorien von Empfängern wir sie weitergeben, und welche Wahlmöglichkeiten Sie im Hinblick auf unsere Nutzung Ihrer Daten haben. Ferner erläutern wir die Maßnahmen, die wir zur Gewährleistung der Sicherheit personenbezogener Daten von EPRs ergreifen, sowie die Art und Weise, in der Sie uns hinsichtlich unserer Datenschutzpraktiken kontaktieren können.

* 1. **Für welche Zwecke erheben und verwenden wir die personenbezogenen Daten von EPRs?**

P&G erfasst die personenbezogenen Daten seiner EPRs im Kontext der Dienstleistungsvereinbarung und dem Verhältnis als unabhängigem Auftragnehmer, die zwischen P&G und Ihnen und/oder Ihrem Arbeitgeber besteht. Im Allgemeinen sammeln und nutzen wir die bei Ihnen und/oder Ihrem Arbeitgeber erfassten personenbezogenen Daten von EPRs für die folgenden Dienstleistungen und/oder Tätigkeiten:

* Gesundheit und Sicherheit am Arbeitsplatz, einschließlich gesundheitsbezogener Reihenkontrollen und medizinischer Programme im Zusammenhang mit COVID-19 oder ähnlicher gesundheitlicher Ausnahmesituationen
* Zugangsmanagement
* Für die Identitäts- und Berechtigungsverwaltung, einschließlich der Verifizierung und Authentifizierung der Identität, der Ausstellung von Ausweisen und Zugangskarten, der Systemadministration, der Erfassung von An- und Abmeldungen und der Verwaltung von Zugangsdaten, der Informationssicherheit und Cybersicherheit
* Für die Zwecke der Notfallplanung, einschließlich der Geschäftskontinuität, der Personalplanung, der Schichtverwaltung und von Notfall- und Sicherheitsprotokollen
* Für die Registrierung und Verwaltung elektronischer Geräte sowie die Optimierung der Netzwerk- und Gerätenutzung
* Für die physische und Cyber-Sicherheitskontrollen, einschließlich der Überwachung elektronischer Geräte und Netzwerke und der Erfassung von Überwachungsvideos, wie etwa von CCTV
* Rechtsstreitigkeiten und interne/externe Ermittlungen, Prüfungen und Streitbeilegung
* Tägliche Verfahren im Zusammenhang mit der Arbeit (z. B. Authentifizierung und Anmeldung in unseren Systemen)
* Teilnahme an Besprechungen, Schulungen und Veranstaltungen
* Compliance zu Gesetzen, Vorschriften und Unternehmensrichtlinien in Bezug auf Anti-Korruption, Kinderarbeit, Sanktionen, Exportkontrollen und Menschenrechten, sowie anderen Anforderungen an Corporate Governance und Unternehmensverantwortung
* Von P&G und/oder Ihrem Arbeitgeber geführte Untersuchungen im Hinblick auf das Fehlverhalten am Arbeitsplatz oder Verstöße gegen Verfahrensverordnungen
* Umsetzung und Prüfung unserer mit Ihnen und/oder Ihrem Arbeitgeber geschlossenen Dienstleistungsverträge, einschließlich einer Leistungsbewertung der Dienstleister,
* Compliance zu allen rechtlichen, behördlichen, richterlichen oder staatlichen Vorgaben und die Reaktion auf bzw. die Erfüllung von Gerichtsbeschlüssen, Vorladungen, Offenlegungsaufforderungen oder anderen behördlichen Datenanfragen
	+ Sicherheits- und Risikomanagement, einschließlich der Sicherheit und Überwachung von Personal und Betriebsgelände, sowie dem Schutz von P&G, unserer Arbeitskräfte und unserer Kunden vor Diebstahl, gesetzlicher Haftung, Betrug oder Missbrauch.
	1. **Welche Arten personenbezogener Daten von EPRs werden von uns erfasst?**

Wir halten die Art und Menge personenbezogener Daten von EPRs, die wir bei Ihnen oder über Sie erfassen, immer so gering wie möglich. Die folgende Grafik geht detaillierter auf die Kategorien personenbezogener Daten von EPRs ein, die P&G im Zusammenhang mit seinen Geschäftsabläufen erfasst.

Die Erfassung von Informationen und der Zugriff auf Informationen variieren je nach den jeweiligen länderspezifischen, rechtlichen und/oder geschäftlichen Anforderungen.

Die rechtliche oder geschäftliche Grundlage für die Erfassung und Verarbeitung personenbezogener Daten von EPRs variiert je nach dem Datentyp und der beabsichtigten Verwendung, wie in Abschnitt 5.3 weiter unten beschrieben.

|  |  |
| --- | --- |
| **Welche Arten personenbezogener Daten von EPRs erfassen und verarbeiten wir?** | **Warum erheben und verarbeiten wir diese Art personenbezogener Daten von EPRs?***Wir erheben und verarbeiten diese Datentypen für mehrere organisatorische und geschäftliche Prozesse, wie die in Abschnitt 5.1 beschrieben ist, und im Weiteren näher erläutert wird:* |
| *Kontaktinformationen und persönliche Merkmale* * Vollständiger Name oder frühere Namen (wie etwa der Geburtsname)
* Sonstige einmalige Kennungen, wie von P&G ausgegebene Identifikationsnummern oder Zugangsdaten (z. B. Anmeldedaten für das E-Mail-Postfach) oder jedwede andere von Ihrem Arbeitgeber vergebene Identifikationsnummer.
* Physische Adresse/Postanschrift
* E-Mail-Adresse
* Telefonnummer
 | * Zugang zu Einrichtungen und elektronischem Netzwerk
* Kommunikation mit Ihrer Person im Hinblick auf die betriebliche Notfallplanung, einschließlich der Schichtverwaltung
* Teilnahme an Besprechungen, Schulungen und Veranstaltungen
* Tägliche Arbeitsabläufe (z. B. Authentifizierung und Anmeldung in unseren Systemen)
* Compliance mit rechtlichen Vorgaben und Richtlinien
* Unternehmensführung und Kontrolle
* Erforderliche externe Berichterstattung
* Untersuchungen und Vorfallsmanagement
	+ Sicherheits- und Risikomanagement, einschließlich der Sicherheit und Überwachung von Personal und Betriebsgelände, sowie der Schutz von P&G, unserer Arbeitskräfte und unserer Kunden vor Diebstahl, gesetzlicher Haftung, Betrug oder Missbrauch
* Gesundheit und Sicherheit am Arbeitsplatz, einschließlich gesundheitsbezogener Reihenkontrollen und medizinischer Programme im Zusammenhang mit COVID-19 oder ähnlicher gesundheitlicher Ausnahmesituationen
* Umsetzung und Prüfung unserer mit Ihnen und/oder Ihrem Arbeitgeber geschlossenen Dienstleistungsverträge, einschließlich einer Leistungsbewertung der Dienstleistungen
* Compliance zu allen rechtlichen, behördlichen, richterlichen oder staatlichen Vorgaben und die Reaktion auf bzw. die Erfüllung von Gerichtsbeschlüssen, Vorladungen, Offenlegungsaufforderungen oder anderen behördlichen Datenanfragen
 |
| *Behördliche Dokumente zur Identifikation/Arbeitsberechtigung/Identifikation des Arbeitgebers** Nationale Ausweisdokumente (wie Reisepass, Visa, Sozialversicherungsnummer, Führerschein oder andere behördlicherseits ausgestellte Ausweise)
* Staatsbürgerschaft
* Wohnsitz
* Nationalität
* Land der Geburt
* Militärischer und/oder Veteranenstatus
* Einmalige ID als Mitarbeiter des Unternehmens, mit dem P&G einen Vertrag hat
 | * Rechtliche Identifizierung und Aufrechterhaltung der Integrität unserer Unterlagen
* Einhaltung der Anforderungen für Visa und andere Arbeitsgenehmigungen
* Sicherheits- und Risikomanagement, wie das Erfassen von Führerscheindaten von EPRs, die Geschäftsfahrzeuge benutzen, Verifizierung der Berufskraftfahrerlizenz, Betrugsprävention und ähnliche Zwecke
* Compliance mit rechtlichen Vorgaben und Richtlinien
* Unternehmensführung und Kontrolle
* Sicherheit und Notfallplanung
* Erforderliche externe Berichterstattung
* Untersuchungen und Vorfallsmanagement
 |
| *Finanzielle Informationen* * Bankkontonummer und Details
* Angaben zur persönlichen Zahlungskarte, wenn diese für Erstattungen bereitgestellt wurde
 | * Erleichterung der Spesenerstattung
* Compliance mit rechtlichen Vorgaben und Richtlinien
* Unternehmensführung und Kontrolle
* Sicherheit und Notfallplanung
* Erforderliche externe Berichterstattung
* Untersuchungen und Vorfallsmanagement
 |
| *Informationen zur Gesundheit* * Informationen im Zusammenhang mit der körperlichen oder emotionalen Gesundheit einer Person, einschließlich aller Behinderungen oder Einschränkungen zur Erfüllung von Arbeitsaufgaben oder Funktionen
* Drogentests und andere Arten von gesundheitlichen Untersuchungen
 | * Einhaltung der Anforderungen an Arbeitsschutz und Sicherheit am Arbeitsplatz und behördliche Berichterstattung
* Umgang der EPRs mit Sicherheits- und Geschäftsrisiken im Zusammenhang mit COVID-19 oder ähnlichen gesundheitlichen Notfällen
* Compliance mit rechtlichen Vorgaben und Richtlinien
* Unternehmensführung und Kontrolle
* Sicherheit und Notfallplanung
* Erforderliche externe Berichterstattung
* Untersuchungen und Vorfallsmanagement
 |
| *Elektronische Identifikationsdaten/ Besondere Identifikatoren/ Bild und Stimme** P&G System-Identifikatoren (z. B. Benutzernamen oder Online-Anmeldedaten)
* Digitale Unterschrift
* Elektronische Identifikationsdaten, Protokolle und Aufzeichnungen bezüglich des Zugriffs auf und der Nutzung von unternehmenseigenen Geräten, Systemen, Anwendungen, Lizenzen und Datenbanken von P&G und des unternehmenseigenen Netzwerks von P&G (wie z. B. Ihre Nutzung des E-Mail-Systems, des Internets, der sozialen Medien).
* Von P&G erfasste Informationen von Sicherheitssystemen, einschließlich des Closed Circuit Television („CCTV“), der Zugangssysteme für den Standort, und von Prozesslinien- oder Aufgabenkameras
* Elektronische Identifikationsdaten, Protokolle und Aufzeichnungen in Bezug auf den Zugang zu physischen P&G-Standorten und zu zugangsbeschränkten Bereichen, einschließlich Zugangskartennummer/ Zugangskartenkennung und Foto
* Videos, Fotografien und andere Bild-/Stimmaufnahmen im Zusammenhang mit Meetings/Schulungen
* Elektronische Identifikationsdaten für Call Center-Aufzeichnungen
 | * Systemadministration, Technologie und Zugang zu und Verwaltung von IT-Gütern
* Unterstützung unserer physischen Sicherheit, sowie der Informationssicherheits- und Cybersicherheitsinteressen gegen interne und/oder externe Bedrohungen
* Verwaltung der Verhütung von und Wiederherstellung nach Schäden in unseren Büros und Produktionsstätten
* Interne Aufzeichnungen und Berichte, einschließlich Datenabgleich und Datenanalyse
* Ermöglichen des Zugriffs auf Standorte, Netzwerk, Tools, Anwendungen und andere Systeme und Vermögenswerte des Unternehmens P&G
* Erhöhund der Transparenz bezüglich der Nutzung und der Kosten für den Verbrauch der Tools, Lizenzen, Dienste und Anwendungen von P&G für Optimierungs-, Qualitäts-, Audit- und Kostenzwecke
* Protokollierung von Schulungen und Meetings
* Compliance mit rechtlichen Vorgaben und Richtlinien
* Unternehmensführung und Kontrolle
* Sicherheit und Notfallplanung
* Erforderliche externe Berichterstattung
* Untersuchungen und Vorfallsmanagement
 |
| *Cookies -* Cookies sind kleine Dateien, die beim Surfen im Web an Ihren Computer gesendet werden.  Sie speichern nützliche Informationen darüber, wie Sie mit den von Ihnen besuchten Websites interagieren.  Cookies sammeln keine Informationen, die auf Ihrem Computer oder Gerät oder in Ihren Dateien gespeichert sind.  Cookies enthalten keine Informationen, die Sie direkt identifizieren würden. Cookies zeigen Ihren Computer und Ihr Gerät immer nur als zufällig zugewiesene Zahlen und Buchstaben (z. B. Cookie-ID ABC12345) an, und niemals z. B. als „Thomas Schmitt“. Wir verwenden folgende Arten von Cookies: * *Sitzungs-Cookies*.Sitzungs-Cookies erinnern sich an Sie und Ihre Bewegungen von Seite zu Seite (unter Verwendung einer zufällig generierten ID), damit Sie nicht aufgefordert werden müssen, Daten bereitzustellen, die Sie zuvor bereits eingegeben haben. Diese Cookies werden gelöscht, sobald Sie unsere Website verlassen oder Ihren Browser schließen.
* *Dauerhafte Cookies*. Dauerhafte Cookies ermöglichen es Websites, Ihre Vorlieben für den Fall zu speichern, wenn Sie die Seite erneut besuchen. Wenn Sie sich beispielsweise bei Ihrem ersten Besuch dafür entscheiden, die Website auf Französisch zu lesen, wird die Website beim nächsten Mal automatisch auf Französisch angezeigt.
* *Analyse-Cookies*. Diese Cookies sagen uns, wie unsere Websites funktionieren. In einigen Fällen verwenden wir Cookies von Google Analytics, um die Leistung unserer Websites zu überwachen. Unsere Möglichkeit, von Google Analytics erfasste Informationen über Ihre Besuche auf unseren Websites zu verwenden und weiterzugeben, wird durch die [Nutzungsbedingungen von Google Analytics](https://www.google.com/analytics/terms/us.html) und die [Datenschutzrichtlinie von Google](https://policies.google.com/privacy) eingeschränkt.
 | Wir verwenden Cookies auf Websites von P&G, die von EPRs besucht werden, aus Reihe von Gründen wie z. B.: * um mehr über die Art und Weise zu erfahren, wie Sie mit unseren Websites und P&G-Inhalten interagieren
* um uns zu helfen, Ihre Erfahrung beim Besuch unserer Websites zu verbessern
* zur individuellen Anpassung der Website an Ihre Präferenzen
* um Fehler zu identifizieren und sie zu beheben
* um zu analysieren, wie gut unsere Websites funktionieren
 |
| *Andere persönliche Merkmale** Biometrische Daten, wie Fingerabdrücke oder Gesichtsscans
* Überprüfung auf Vorstrafen/Hintergrundprüfungen
 | * Ermöglichen Ihres Zugangs zu Standorten und Systemen des Unternehmens anhand von biometrischen Daten
* Compliance mit rechtlichen Vorgaben und Richtlinien
* Unternehmensführung und Kontrolle
* Sicherheit und Notfallplanung
* Erforderliche externe Berichterstattung
* Untersuchungen und Vorfallsmanagement
 |

* 1. **Auf welchen rechtlichen und/oder geschäftlichen Grundlagen erfolgt der Verarbeitung personenbezogener Daten von EPRs?**

Wir erheben und verwalten das Minimum an personenbezogenen Daten von EPRs, das erforderlich ist: um unseren vertraglichen und/oder gesetzlichen Verpflichtungen nachzukommen, die uns im Rahmen unserer Beziehung zu Ihnen und/oder Ihrem Arbeitgeber als unabhängigem Auftragnehmer obliegen, um die legitimen Geschäftsinteressen des Unternehmens in einer Weise zu unterstützen, die in einem angemessenen Verhältnis zu Ihren Datenschutzinteressen steht, und um die personenbezogenen Daten, die mit Ihrer Einwilligung für die beabsichtigten Zwecke bereitgestellt wurden, auch verarbeiten zu können.

Die rechtliche und/oder geschäftliche Grundlage für die Verarbeitung personenbezogener Daten von EPRs können die Einhaltung der geltenden Gesetze und Vorschriften durch P&G, die Einhaltung von vertraglichen Verpflichtungen, die legitimen geschäftlichen Interessen des Unternehmens, die Interessen der öffentlichen Gesundheit und/oder Ihre Einwilligung sein.

Die rechtliche und/oder geschäftliche Grundlage für die Verarbeitung personenbezogener Daten von EPRs kann je nach Rechtsraum sowie nach Datenkategorie/-typ und den Gründen für die Erfassung und Verwendung der jeweiligen Daten variieren.

Dies sind die rechtlichen Grundlagen, auf die wir uns bei der Verarbeitung dieser Kategorien von Daten im Allgemeinen stützen:

|  |  |
| --- | --- |
| **Art der personenbezogenen Daten** | **Rechtliche/geschäftliche Grundlage für die Verarbeitung** |
| Kontaktinformationen, behördliche Dokumente zur Identifikation, finanzielle Informationen, gesundheitsbezogene Informationen | Einhaltung vertraglicher und rechtlicher Verpflichtungen durch P&G  |
| Behördliche Dokumente zur Identifikation/Arbeitsberechtigung | Compliance mit geltendem Recht durch P&G |
| Berufsbezogene Daten, Kontaktinformationen | Die legitimen Geschäftsinteressen von P&G |

* 1. **Wie geben wir personenbezogene Daten von EPRs weiter?**

P&G gibt personenbezogene Daten von EPRs nur an diejenigen Personen weiter, die diese aus legitimen geschäftlichen Gründen kennen müssen.

P&G kann Ihre Daten an Ihren Arbeitgeber (und an andere juristische Personen, sofern von Seiten Ihres Arbeitgebers eine entsprechende Anweisung erfolgt) weitergeben, sowie an P&G-Auftragnehmer, Lieferanten, Agenturen, Zeitarbeitskräfte oder alle anderen Parteien weitergeben, die im Namen von P&G tätig sind („Drittparteien“).

Die personenbezogenen Daten von EPRs können an unseren Hauptsitz und an verbundene Unternehmen in aller Welt weitergegeben werden, wenn dies notwendig ist, um die in Abschnitt 5.2 weiter oben ausgeführten Verarbeitungszwecke zu erreichen.

Wir sind zudem zur Offenlegung personenbezogener Daten von EPRs berechtigt, wenn wir gesetzlich oder im Rahmen eines Rechtsverfahrens dazu aufgefordert werden, um die Rechte und Richtlinien von P&G durchzusetzen oder zu schützen, und/oder um bei der Untersuchung mutmaßlichen oder tatsächlichen Fehlverhaltens oder illegaler Aktivitäten zu helfen.

* 1. **Was sind Ihre Datenschutzrechte?**

Sie haben das Recht, sich an uns zu wenden und Zugang zu den personenbezogenen EPR-Daten zu verlangen, die wir von Ihnen verarbeiten und nutzen. Wenn dies nach geltendem Recht zulässig ist, können Sie erbitten, dass ungenaue, veraltete oder unnötige Informationen korrigiert, gelöscht oder beschränkt werden. Weiterhin können Sie P&G auffordern, Ihre Daten in einem Format zugänglich zu machen, das Ihnen den Transfer der Daten an einen Service-Provider ermöglicht, soweit dies den Umständen nach sachgerecht ist. Wenn die Verarbeitung personenbezogener Daten von EPRs auf Ihrer Zustimmung basiert, haben Sie die Möglichkeit, diese Zustimmung jederzeit zurückzuziehen. Wenn die Verarbeitung personenbezogener Daten von EPRs auf einem berechtigten Interesse beruht, haben Sie das Recht, der Datenverarbeitung unter bestimmten Umständen zu widersprechen.

Wenn Sie diese Rechte ausüben wollen, möchten wir Sie darum bitten, Ihre Anliegen zunächst mit jenem Mitarbeiter von P&G zu besprechen, der an Ihrem Standort als Auftraggeber fungiert. Alternativ können Sie sich unter der unten genannten Adresse auch an Ihren Datenschutzbeauftragten wenden. Wenn Sie mit unserer Antwort auf Ihr Ersuchen oder der durch uns erfolgenden Verarbeitung Ihrer personenbezogenen Daten nicht zufrieden sind, können Sie bei der Datenschutzbehörde Ihres Landes eine diesbezügliche Beschwerde einreichen.

* 1. **Wie übertragen wir personenbezogene Daten von EPRs in andere Länder?**

P&G ist ein weltweit tätiger Konzern, der mit EPRs in vielen Ländern zu tun hat. Wenn es rechtlich zulässig ist, können personenbezogene Daten von EPRs im Rahmen der länderspezifischen Vorschriften und/oder Einschränkungen in Länder übermittelt werden, die von jenem Land abweicht, in dem sie erfasst wurden. Personenbezogene Daten von EPRs können in Systemen in den USA gespeichert sein, und von anderen mit P&G verbundenen Unternehmen, sowie deren Service-Providern, in aller Welt abgefragt oder in andere Länder transferiert werden, soweit dies für die Abwicklung der jeweiligen Geschäftsvorgänge notwendig ist. Die Datenschutzgesetze in diesen Länder entsprechen möglicherweise nicht den Datenschutzgesetzen im Land ihres Wohnsitzes. Für den Fall, dass Ihre personenbezogenen Daten in andere Länder als Ihr Heimatland transferiert werden, oder diese von dort aus abgerufen werden, implementieren wir ausreichende Sicherheitsvorkehrungen, und erfüllen sämtliche gesetzlich vorgeschriebene administrative, technische und/oder vertragliche Bestimmungen, um Ihre Daten zu schützen. Wir transferieren Daten außerhalb des Europäischen Wirtschaftsraums (EEA), des Vereinigten Königreichs (UK) und der Schweiz sowohl zwischen den einzelnen Organisationen von P&G, wie auch, unter Berufung auf die Standardvertragsklauseln, an unsere Service Provider. Wenn Sie eine Kopie dieser Klauseln wünschen, wenden Sie sich bitte an corporateprivacy.im@pg.com. P&G hält daneben auch die weiteren länderspezifischen Vorschriften ein, die die Datenübermittlung einschränken, sobald diese außerhalb des Landes ihrer Erhebung erfolgen.

* 1. **Wir sichern wir die personenbezogenen Daten von EPRs?**

Wir ergreifen sachgerechte physische, administrative und technische Maßnahmen wie zum Beispiel Pseudonymisierung, Verschlüsselung und Zugangskontrollen, die den Zweck verfolgen, personenbezogene Daten von EPRs vor Vernichtung, Verlust, Veränderung, Offenlegung, Zugriff oder Nutzung schützen, und zwar unabhängig davon, ob diese versehentlich, rechtswidrig oder unbefugt erfolgen, und schützen diese auch vor allen weiteren rechtswidrigen Formen der Verarbeitung. Wenn Drittparteien personenbezogene Daten von EPRs im Namen von P&G verarbeiten, schließen wir auch Verträge mit diesen Drittparteien ab, um sicherzustellen, dass sie die entsprechenden physischen, administrativen und technischen Maßnahmen im Umgang mit solchen Daten umsetzen.

**5.8 Wie lange werden meine personenbezogenen Daten von Ihnen aufbewahrt?**

Wir bewahren personenbezogene Daten von EPRs so lange auf, wie dies für die Erfüllung der Zwecke notwendig ist, für die sie erfasst wurden, solange nach geltendem Recht keine längere Aufbewahrungsfrist vorgeschrieben oder gestattet ist. Hierbei handelt es sich im Allgemeinen um den Zeitraum, in dem Sie Dienstleistungen für uns erbringen. In manchen Fällen ist es möglich, dass wir personenbezogene Daten von EPRs nach dem Ende Ihrer geschäftlichen Beziehung zu P&G für einen bestimmten Zeitraum weiterhin aufbewahren müssen, um gesetzlichen oder vertraglichen Verpflichtungen nachkommen zu können.

* 1. **Überwacht P&G die Netzwerk- und Geräteverwendung?**

Das Unternehmen überwacht die Nutzung der Netzwerke und Geräte von P&G. P&G hat die Verpflichtung, seine Mitarbeiter, Vermögenswerte und Anlagen zu schützen. P&G überwacht seine unternehmenseigenen Netzwerke und Geräte zu drei Zwecken: i) um die Sicherheit (einschließlich Vertraulichkeit, Integrität und Verfügbarkeit) von P&G-Mitarbeitern, Daten, Netzwerken, Vermögenswerten, Einrichtungen, Reputation und Wettbewerbsinteressen zu schützen, ii) um vermutetes oder bestätigtes Fehlverhalten oder Rechtsverstöße (einschließlich von Rechtsstreitigkeiten) zu untersuchen und iii) um die Integrität von Geschäftsprozessen und Finanzberichterstattung zu gewährleisten.

P&G überwacht das unternehmenseigene Netzwerk und die Geräte bestimmter Mitarbeiter nur dann, wenn ein berechtigter Grund dazu besteht oder wir dazu nach geltendem Recht verpflichtet sind, insbesondere auch auf Antrag der Strafverfolgungsbehörden. Wir behalten uns im Rahmen des geltenden Rechts das Recht vor, alle elektronischen Dateien, Daten und Nachrichten, die in unseren Netzwerken bzw. auf unseren Geräten erstellt und gespeichert, oder über diese verschickt werden, einzusehen, zu inspizieren, offenzulegen und zu vernichten, wenn dies im Sinne der oben genannten Zwecke erforderlich ist. Diese Überwachung erfolgt stets in Übereinstimmung mit den entsprechenden Gesetzen und Vorschriften. P&G wird zusätzliche Verfahren, Standards, Richtlinien und/oder aktive Maßnahmen implementieren, wann immer dies für die Erfüllung lokaler gesetzlicher Vorschriften erforderlich ist.

Konkret wird P&G eine passive und aktive Überwachung von unternehmenseigenen Netzwerken und im Besitz von P&G befindlicher Geräte durchführen, die bestimmten EPRs zugewiesen wurden, um mögliche Gefahren für die Interessen von P&G zu erkennen. Die „passive Überwachung“ nimmt nicht in aktiver Form eine Überprüfung der Verhaltensweisen von Mitarbeitern vor, sondern stellt vielmehr bestimmte Risikoindikatoren fest. Diese Risikoindikatoren werden von P&G und spezialisierten Sicherheitsanbietern vorab festgelegt, und sind auf die Sicherheitsbedürfnisse des Unternehmens abgestimmt. Wenn ein solcher Risikoindikator ausgelöst wird („Risikoereignis“), zeichnen die Systeme die zugehörigen Daten auf, und speichern diese zur anschließenden Überprüfung und/oder Untersuchung. In den unternehmenseigenen Netzwerken von P&G und bei den im Besitz von P&G befindlichen Geräten, die EPRs zugewiesen wurden, kommen konkret die im Folgenden genannten passiven Überwachungstechniken zum Einsatz:

1. **Die Überwachung von Nutzungsmustern** ist eine Überwachungstechnik, bei der pseudonymisierte Netzwerk- und Internetdaten von P&G durch Software oder Hardware auf eine vordefinierte Reihe von Risikoindikatoren hin untersucht werden. Diese Technik sucht nach verdächtigen Verhaltensmustern bezüglich der Art und Weise, in der unternehmenseigene Netzwerke von P&G oder im Besitz von P&G befindliche Geräte, die bestimmten EPRs zugewiesen wurden, *genutzt* werden. Das Unternehmen kann zum Beispiel das Instrument für die Nutzungsmuster-Überwachung so einstellen, dass nach Risikoindikatoren je nach P&G-Anmeldeort gesucht wird. Die Sicherheitsabteilung von P&G kann das Instrument so abstimmen, dass ein Warnhinweis angezeigt wird, wenn die Anmeldedaten eines Nutzers an zwei verschiedenen P&G-Standorten schneller eingegeben werden, als eine Person sich vernünftigerweise zwischen diesen beiden Orten bewegen kann.
2. Das **Inbound Traffic Scanning** ist ein Überwachungsinstrument, das die eingehenden internetbasierten Kommunikationen (einschließlich der E-Mails) bei deren Eintritt in das Netzwerk von P&G auf Risikoindikatoren überprüft. Antivirus- und Firewall-Software sind die geläufigsten Beispiele für dieses Instrument, das den eingehenden Datenverkehr kontinuierlich auf Malware-Indikatoren wie Anhänge, Links, Websites usw. überprüft.
3. Das **Periodic Scanning** ist ein Überwachungsinstrument, das Kontrollen auf der Ebene des Netzwerks und der Geräte von P&G durchführt, um spezifische Risikoindikatoren zu erfassen, die möglicherweise durch die Maschen der Überprüfung des eingehenden Verkehrs geschlüpft sind. Dieses Instrument ist nützlich, da Risikoereignisse manchmal leichter zu erkennen sind, wenn sie in einem erweiterten Kontext gesichtet werden. Ein Virenscan der gesamten Festplatte ist ein Hauptbeispiel für diese Funktionalität.
4. Das **Outbound Traffic Scanning** von P&G hat die Fähigkeit, den ausgehenden Internetverkehr auf spezifische vordefinierte Risikoindikatoren zu überprüfen. Das Instrument prüft den ausgehenden Verkehr, um zu erkennen, ob ein Risikoereignis nach Maßgabe der spezifizierten Risikoindikatorregeln ausgelöst worden ist. P&G kann etwa eine Regel verfassen, die den Upload großer Dateien an Orte außerhalb des Unternehmensnetzwerks anzeigt, wenn Daten mit der Klassifizierung „Zugriff stark eingeschränkt“ oder mit bestimmten Schlüsselwörtern, wie etwa dem Namen einer spezifischen chemischen Verbindung, verwendet werden, die in neuen Produktformulierungen verwendet werden.

P&G analysiert auf Basis der Art des Risikos, wie sie von den passiven Überwachungsinstrumenten gemeldet oder dem Unternehmen auf andere Weise zur Kenntnis gebracht wurde (z. B. aufgrund eines Gerichtsverfahrens, mutmaßlichen Fehlverhaltens, strafrechtlicher Verfolgung, usw.), ob eine weitere Untersuchung/Analyse dieser Risiken erforderlich ist. Im Rahmen dieser Analyse berücksichtigt P&G den potenziellen Schaden für Mitarbeiter, Verbraucher, andere Stakeholder und/oder das Unternehmen sowie rechtliche und den Schutz der Privatsphäre betreffende Interessen betroffener Personen. Zudem kann P&G festlegen, ob basierend auf rechtlichen Vorgaben oder Richtlinien weitere Analysen erforderlich sind, um Vermögenswerte zu schützen und die Integrität der geschäftlichen Prozesse zu garantieren. Auf der Grundlage dieser Analyse führt P&G entweder keine weiteren Ermittlungstätigkeiten aus, oder nimmt mit Hilfe von aktiven Überwachungsinstrumenten eine im angemessenen Verhältnis stehende Untersuchung vor.

P&G setzt fünf Grundtypen von Instrumenten für die aktive Überwachung ein: (1) Geräteüberprüfung, (2) Internet-Überprüfung, (3) Soft-Überwachung, (4) Hardware-Überwachung und (5) Data Loss Prevention.

1. **Geräteüberprüfung:** Diese Instrumente ermöglichen es P&G, manchmal mit Hilfe eines externen Anbieters, die *gesamten* Inhalte eines im Besitz von P&G befindlichen Computers oder eines anderen unternehmenseigenen Geräts zu einem bestimmten Zeitpunkt für Untersuchungszwecke zu erfassen. Instrumente zum Geräte-Scanning erfassen nicht nur die auf dem unternehmenseigenen Gerät gespeicherten und installierten Dateien und Anwendungen, sondern sind außerdem in der Lage, den zum Zeitpunkt der Erfassung auf diesem Gerät befindlichen Speicher zu erfassen. Je nach verwendetem Instrument kann P&G wählen, nur physische Dateien (also Dateien ohne Speicher) oder nur ein Teilabbild des Geräts zu erfassen; dies macht es möglich, im Einklang mit dem Prinzip der Verhältnismäßigkeit den Schwerpunkt der Untersuchung nur auf bestimmte Dateitypen oder Anwendungen zu richten.
2. **Internet-Überprüfung:** P&G setzt ein externes, Cloud-basiertes Web-Proxy-Tool ein, das über drei Haupteigenschaften verfügt. Erstens hat es die Fähigkeit, die Nutzung des öffentlichen Internets auf URL-Ebene (d. h. aufgrund der Namen der besuchten Webseiten) nachzuverfolgen, wenn ein EPR ein Gerät verwendet, das sich im Besitz von P&G befindet. Diese Eigenschaft verfolgt und protokolliert Internetaktivitäten durch den Einsatz „gehashter“ personenbezogener Identifikatoren (wodurch der Nutzer pseudonymisiert wird) für die mögliche Verwendung im Rahmen einer genehmigten Untersuchung. Zweitens hat es die Fähigkeit, die in unverschlüsselte Webseiten eingegebenen Daten und die beim Besuch unverschlüsselter Webseiten hoch- bzw. heruntergeladenen Dateien sichtbar zu machen. Drittens hat es die Fähigkeit, eine eingeschränkte Teilmenge des Internetverkehrs zu entschlüsseln, die nach einer vorherigen Definition als mit einem zu hohem Risiko behaftet gilt (z. B. ausgehende Verbindungen zu bekanntermaßen schädlichen Webseiten, Webseiten, die bekanntermaßen Malware auf Geräte spielen, oder nicht genehmigten Dateifreigabeseiten). Diese Lösung ist so konfiguriert, dass sie keinerlei Verkehr entschlüsselt, der an Webseiten gerichtet ist, auf denen unter Umständen sensible personenbezogene Daten der Endnutzer verarbeitet werden (z. B. Bankseiten oder gesundheitsbezogene Seiten).
3. **Soft-Überwachung:** Hierbei handelt es sich um Techniken, die im Rahmen einer Untersuchung eingesetzt werden, die eine identifizierbare Personen betreffen, und bei der die Person (a) von der Untersuchung in Kenntnis gesetzt wurde und (b) nicht selbst Gegenstand der Untersuchung ist. Ein Soft-Überwachungsinstrument kann beispielsweise ein Telefonanruf oder eine E-Mail sein, mit dem bzw. der man herausfinden möchte, an welchem Ort ein *identifizierter* EPR derzeit anwesend/angemeldet ist, um so festzustellen, ob ein geografisch ausgelöstes Risikoereignis einen legitimen Hintergrund hat.
4. **Überwachung von Hardware und Anwendungen**: Überwachungsinstrumente für Hardware und Anwendungen sind Aufzeichnungs- und Überwachungskapazitäten, die die Hersteller in die Hardware und/oder Anwendungen einbauen, und die eine aktive Überwachung darstellen, sofern sie bei einem identifizierbaren EPR eingesetzt werden,. Häufig verwendete Beispiele sind Server-Logs, SAP-Logins, Aufzeichnungen zur Benutzung magnetischer Ausweiskarten, Netzwerk-Authentifizierung, usw.
5. **Data Loss Prevention (DLP, Verhinderung von Datenverlust):** P&G oder ein zugelassener Dienstleister prüft E-Mails, die an nicht zu P&G gehörende Adressen gerichtet sind, auf Hinweise für einen Datenverlust. Sendet ein EPR beispielsweise eine nicht verschlüsselte E-Mail mit einem Anhang, der mit „Zugriff stark eingeschränkt“ klassifiziert ist, an eine nicht zu P&G gehörende Adresse, kennzeichnet die DLP-Lösung diese E-Mail als Risiko für die Informationssicherheit. Der Benutzer wird möglicherweise darüber informiert, dass bei zukünftiger Kommunikation eine zugelassene Verschlüsselungslösung zu verwenden ist. Wenn eine ausgehende E-Mail als „Zugriff stark eingeschränkt“ oder „geheim“ klassifiziert wird (einschließlich besonders ausgewiesener Schlüsselworte), wird diese E-Mail in Hinsicht auf ihr Sicherheitsrisiko überprüft. Sofern es angebracht ist, wird unter Umständen eine Ermittlung in die Wege geleitet. P&G überprüft keine Nachrichten, die als „persönlich“ oder „privat“ klassifiziert oder in der Betreffzeile mit „persönlich“ oder „privat“ gekennzeichnet sind.
6. **Künftige Änderungen**

P&G behält sich das Recht vor, diese Erklärung bei Bedarf zu ändern, um Compliance zu Änderungen bei Gesetzen und Vorschriften sowie Unternehmenspraktiken und -verfahren herzustellen, oder um auf neue Bedrohungen oder von den Datenschutzbehörden auferlegte Anforderungen zu reagieren. Wenn sich solche Änderungen wesentlich auf unsere Verarbeitung Ihrer personenbezogenen EPR-Daten auswirken, werden wir Sie entsprechend informieren.

1. **Kontaktinformationen**

Wenn Sie Fragen oder Bedenken hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten oder personenbezogener EPR-Daten haben, oder Ihre Rechte auf Datenschutz ausüben möchten, können Sie unseren Beauftragten für globalen Datenschutz gerne auf den folgenden Wegen kontaktieren – E-Mail: pgprivacyofficer.im@pg.com, Telefonnummer: +1 (513) 622-0103, Postanschrift: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, USA

Sollten Sie Bedenken bezüglich einer möglichen Verletzung das Datenschutzes Ihrer personenbezogenen EPR-Daten oder sonstiger personenbezogener Daten haben, soweit diese von P&G verarbeitet wurden, kontaktieren Sie uns bitte per E-Mail an securityincident.im@pg.com.