**Globalna informacja o zasobach stron trzecich**

|  |  |
| --- | --- |
| **Osoba kontaktowa ds.  informacji o prywatności:**  Globalny inspektor ochrony danych | **Data: 1 stycznia 2023** |
| ([pgprivacyofficer.im@pg.com](mailto:pgprivacyofficer.im@pg.com))  **Region:** Cały świat | **Zasięg:** Wszystkie zasoby stron trzecich |

# **Cel**

Niniejsza Informacja zawiera informacje dla Zasobów stron trzecich („EPR”, External Party Resources) (określonych poniżej) na temat tego, w jaki sposób firma The Procter & Gamble Company, jej podmioty zależne i/lub stowarzyszone („P&G” lub „Firma”) gromadzą i przetwarzają Państwa dane osobowe.

# **Status niezależnego kontrahenta**

Niniejsza Informacja nie tworzy stosunku pracy pomiędzy P&G oraz EPR. EPR świadczą usługi na rzecz P&G jako niezależni kontrahenci, niezależnie od tego, czy takie usługi są świadczone bezpośrednio na rzecz P&G, czy na mocy umowy pomiędzy P&G oraz pracodawcą EPR.

1. **Definicje**

**Zasoby stron trzecich:** Każda osoba wykonująca pracę lub świadcząca usługi na rzecz P&G, w przypadku których to osób P&G nie jest formalnym pracodawcą w chwili wykonywania danej pracy lub świadczenia określonych usług, np. kontrahenci.

**Dane osobowe:** Wszelkie dane dotyczące osób fizycznych zidentyfikowanych lub możliwych do zidentyfikowania, np. imię i nazwisko, inne identyfikatory, dane kontaktowe, informacje służbowe oraz cechy osobowe.

**Firma lub P&G:** na potrzeby niniejszej Polityki termin „Firma” lub „P&G” będzie oznaczać The Procter & Gamble Company oraz jej jednostki zależne i stowarzyszone.

1. **Zasady**

Podstawowe zasady ochrony prywatności i przetwarzania danych przez P&G są następujące:

* Gromadzenie i zarządzanie minimalną ilością Danych osobowych EPR;
* Szanowanie prywatności osób fizycznych;
* Postępowanie w sposób zgodny z naszymi Celami, wartościami i zasadami (PVP, Purposes, Values and Principles), niniejszą Informacją oraz obowiązującymi przepisami prawa;
* Przestrzeganie obowiązujących standardów i procedur podczas gromadzenia Danych osobowych EPR lub zarządzania nimi.

1. **Informacja**

P&G szanuje prywatność kandydatów. Niniejsza Informacja zawiera informacje na temat tego, w jaki sposób przetwarzamy Dane osobowe EPR, rodzaju informacji gromadzonych przez nas bezpośrednio od Państwa i/lub Państwa pracodawcy, celów, w jakich je wykorzystujemy, kategorii podmiotów, którym je udostępniamy, oraz wyborów, których mogą Państwo dokonać w związku z wykorzystywaniem przez nas tych danych. Opisano w niej również środki, jakie podejmujemy w celu ochrony bezpieczeństwa Danych osobowych EPR oraz w jaki sposób można się z nami kontaktować odnośnie naszych praktyk dotyczących ochrony prywatności.

* 1. **W jakich celach gromadzimy i wykorzystujemy Dane osobowe EPR?**

Firma P&G gromadzi Dane osobowe o jej EPR w kontekście umowy o świadczenie usług i relacji z niezależnym kontrahentem, która istnieje między P&G oraz Państwem i/lub Państwa pracodawcą. Ogólnie gromadzimy i wykorzystujemy Dane osobowe EPR od użytkownika i/lub jego pracodawcy do celów wykonania poniższych usług i/lub działań:

* bezpieczeństwo i higiena pracy, w tym badania przesiewowe oraz programy medyczne powiązane z COVID-19 lub podobnymi zagrożeniami zdrowia;
* zarządzanie dostępem do obiektów;
* zarządzanie tożsamością i danymi uwierzytelniającymi, w tym weryfikacja i potwierdzenie tożsamości, wydawanie kart identyfikacyjnych oraz identyfikatorów, administracja systemu, rejestrowanie logowania/wylogowania, jak również zarządzanie danymi logowania, bezpieczeństwem informacji oraz cyberbezpieczeństwem;
* cele w zakresie planowania awaryjnego, w tym zachowanie ciągłości pracy, obsada etatów, zarządzanie zmianami i protokoły awaryjne/bezpieczeństwa;
* rejestrowanie urządzeń elektronicznych i zarządzanie nimi oraz optymalizacja wykorzystania sieci i urządzeń;
* kontrole bezpieczeństwa fizycznego i cybernetycznego, w tym monitorowanie urządzeń elektronicznych i sieci, jak również rejestracja wideo z monitoringu, np. telewizja przemysłowa;
* postępowania sądowe i wewnętrzne/zewnętrzne dochodzenia, audyty i rozstrzyganie sporów;
* przetwarzanie dla celów codziennej pracy (np. uwierzytelnianie i logowanie do naszych systemów);
* Udział w spotkaniach, szkoleniach i wydarzeniach;
* zachowanie zgodności z przepisami prawa, regulacjami i politykami Firmy w zakresie przeciwdziałania łapownictwu, pracy dzieci i korupcji, sankcji, kontroli eksportu, praw człowieka i innych wymogów ładu korporacyjnego i zarządzania;
* postępowania wyjaśniające prowadzone przez P&G i/lub pracodawcę, dotyczące niewłaściwego zachowania w miejscu pracy lub naruszeń procesów;
* wdrożenie i audyt naszych umów o świadczenie usług z Państwem i/lub Państwa pracodawcą, w tym ocena wyników usług;
* zachowanie zgodności z wszelkimi wymogami prawnymi, regulacyjnymi, sądowymi lub rządowymi oraz odpowiedź i stosowanie się do nakazów sądowych, wezwań, żądań ujawnienia dowodów lub innych rządowych wniosków dotyczących danych;
  + zarządzanie bezpieczeństwem i ryzykiem, w tym bezpieczeństwo i monitorowanie personelu i obiektu, jak również ochrona P&G, naszych pracowników i klientów przed kradzieżą, odpowiedzialnością prawną, oszustwem lub nadużyciem.
  1. **Jakiego rodzaju Dane osobowe EPR gromadzimy?**

Zawsze będziemy maksymalnie ograniczać rodzaje i ilość Danych osobowych EPR, które możemy zbierać od niego lub na jego temat. W poniższej tabeli opisano bardziej szczegółowo kategorie Danych osobowych EPR, które P&G gromadzi w związku z procesami biznesowymi.

Gromadzenie informacji i dostęp do nich będą różnić się w zależności od wymogów prawnych i/lub biznesowych obowiązujących w danym kraju.

Podstawa prawna lub biznesowa gromadzenia i przetwarzania Danych osobowych EPR będzie się różnić w zależności od rodzaju danych i ich przeznaczenia, jak opisano w punkcie 5.3 poniżej.

|  |  |
| --- | --- |
| **Jakie rodzaje danych EPR gromadzimy i przetwarzamy?** | **Dlaczego gromadzimy i przetwarzamy tego rodzaju Dane osobowe EPR?**  *Gromadzimy i przetwarzamy te rodzaje danych w ramach wielu procesów organizacyjnych i biznesowych, jak opisano w sekcji 5.1 i jak objaśniono poniżej:* |
| *Dane kontaktowe i informacje personalne*   * Imię i nazwisko lub poprzednie nazwiska (np. nazwiska panieńskie) * Inne unikalne identyfikatory, takie jak numery identyfikacyjne P&G lub dane uwierzytelniające (np. login e-mail) lub inne numery identyfikacyjne wydane przez Państwa pracodawcę * Adres fizyczny/adres korespondencyjny * Adres e-mail * Numer telefonu | * Dostęp do obiektów i sieci elektronicznych * Komunikacja z Państwem w związku z biznesowymi planami awaryjnymi, w tym zarządzanie zmianami * Udział w spotkaniach, szkoleniach i wydarzeniach * przetwarzanie dla celów codziennej pracy (np. uwierzytelnianie i logowanie do naszych systemów); * Zachowanie zgodności z przepisami prawa i polityką * Ład korporacyjny i zarządzanie * Wymagana sprawozdawczość zewnętrzna * Postępowania wyjaśniające i zarządzanie incydentami   + Zarządzanie bezpieczeństwem i ryzykiem, w tym bezpieczeństwo i monitorowanie personelu i obiektu, jak również ochrona P&G, naszych pracowników i klientów przed kradzieżą, odpowiedzialnością prawną, oszustwem lub nadużyciem * Bezpieczeństwo i higiena pracy, w tym badania przesiewowe oraz programy medyczne powiązane z COVID-19 lub podobnymi zagrożeniami zdrowia * Wdrożenie i audyt naszych umów o świadczenie usług z Państwem i/lub Państwa pracodawcą, w tym ocena wyników usług * Zachowanie zgodności z wszelkimi wymogami prawnymi, regulacyjnymi, sądowymi lub rządowymi oraz odpowiedź i stosowanie się do nakazów sądowych, wezwań, żądań ujawnienia dowodów lub innych rządowych wniosków dotyczących danych |
| *Dokument tożsamości wydany przez organ rządowy/ informacja o kwalifikowalności do pracy/ identyfikator pracodawcy*   * Krajowy dokument tożsamości (taki jak paszport, wiza, numer ubezpieczenia społecznego, prawo jazdy, inne dokumenty tożsamości wydane przez organ rządowy) * Obywatelstwo * Miejsce zamieszkania * Narodowość * Kraj urodzenia * Status wojskowy i/lub weterana * Unikatowy identyfikator pracownika, który został zakontraktowany przez P&G | * Zgodne z prawem identyfikowanie Państwa i zachowanie integralności naszych rejestrów * Zachowanie zgodności z wymogami imigracyjnymi i innymi wymogami dotyczącymi pozwoleń na pracę * Zapewnienie bezpieczeństwa i zarządzanie ryzykiem, takie jak gromadzenie danych dotyczących praw jazdy EPR, którzy prowadzą samochody Firmy, weryfikacja licencji zawodowych, zapobieganie oszustwom i podobne cele * Zachowanie zgodności z przepisami prawa i polityką * Ład korporacyjny i zarządzanie * Bezpieczeństwo i tworzenie planów awaryjnych * Wymagana sprawozdawczość zewnętrzna * Postępowania wyjaśniające i zarządzanie incydentami |
| *Informacje finansowe*   * Numer i dane rachunku bankowego * Informacje o osobistej karcie płatniczej, jeśli zostały podane na potrzeby zwrotów kosztów | * Ułatwianie zwracania wydatków * Zachowanie zgodności z przepisami prawa i polityką * Ład korporacyjny i zarządzanie * Bezpieczeństwo i tworzenie planów awaryjnych * Wymagana sprawozdawczość zewnętrzna * Postępowania wyjaśniające i zarządzanie incydentami |
| *Informacje zdrowotne*   * Informacje związane ze zdrowiem fizycznym lub emocjonalnym danej osoby, w tym wszelkie niepełnosprawności lub ograniczenia w wykonywaniu obowiązków lub pełnieniu funkcji zawodowych * Testy na obecność narkotyków i inne rodzaje badań zdrowotnych | * Przestrzeganie wymogów dotyczących zdrowia i bezpieczeństwa w miejscu pracy oraz wymagań rządowych w zakresie sprawozdawczości * Zarządzanie bezpieczeństwem EPR i ryzykiem biznesowym związanym z pandemią COVID-19 lub podobnymi stanami zagrożenia zdrowia * Zachowanie zgodności z przepisami prawa i polityką * Ład korporacyjny i zarządzanie * Bezpieczeństwo i tworzenie planów awaryjnych * Wymagana sprawozdawczość zewnętrzna * Postępowania wyjaśniające i zarządzanie incydentami |
| *Elektroniczne dane identyfikacyjne/unikatowe identyfikatory/wizerunek i głos*   * Identyfikatory systemowe P&G (np. nazwy użytkownika lub dane uwierzytelniające online) * Podpis cyfrowy * Elektroniczne dane identyfikacyjne, dzienniki i rejestry dotyczące dostępu i korzystania z urządzeń P&G, systemów, aplikacji, licencji, baz danych i sieci P&G (takiego jak korzystanie z poczty elektronicznej, Internetu i mediów społecznościowych) * Informacje gromadzone przez systemy bezpieczeństwa P&G, w tym telewizję przemysłową („CCTV”), systemy dostępu do obiektów, kamery ciągów technologicznych lub kamery do zadań szczególnych * Elektroniczne dane identyfikacyjne, dzienniki i zapisy dotyczące dostępu do obiektów P&G i obszarów o ograniczonym dostępie, w tym numer przepustki/identyfikator przepustki oraz zdjęcie * Nagrania wideo, fotografie i inne nagrania wizerunku/głosu w kontekście spotkań/szkoleń * Dane identyfikacji elektronicznej dotyczące nagrań z centrów telefonicznych | * Administracja systemu, dostęp do technologii i zasobów IT oraz zarządzanie nimi * Wspieranie naszych interesów związanych z bezpieczeństwem fizycznym, bezpieczeństwem informacji i bezpieczeństwem cybernetycznym w ramach ochrony przed zagrożeniami wewnętrznymi i/lub zewnętrznymi * Zarządzanie zapobieganiem utratom i odzyskiwaniem w naszych biurach i zakładach produkcyjnych * Prowadzenie rejestrów wewnętrznych i sprawozdawczość, w tym dopasowywanie danych i analityka * Zapewnianie dostępu do obiektów, sieci, narzędzi, aplikacji oraz innych systemów i zasobów Firmy * Zapewnianie widoczności wykorzystania i kosztów zużycia narzędzi, licencji, usług i aplikacji P&G w celu optymalizacji, poprawy jakości oraz w celach audytowych i związanych z kosztami * Utrwalanie szkoleń i spotkań * Zachowanie zgodności z przepisami prawa i polityką * Ład korporacyjny i zarządzanie * Bezpieczeństwo i tworzenie planów awaryjnych * Wymagana sprawozdawczość zewnętrzna * Postępowania wyjaśniające i zarządzanie incydentami |
| *Pliki cookie –* to niewielkie pliki przesyłane na Państwa komputer podczas przeglądania witryn internetowych. Przechowują one użyteczne informacje na temat interakcji użytkownika z odwiedzanymi witrynami internetowymi. Pliki cookie nie gromadzą żadnych informacji przechowywanych na Państwa komputerze lub urządzeniu ani w Państwa plikach. Pliki cookie nie zawierają żadnych informacji, które mogłyby bezpośrednio identyfikować Państwa jako osobę. Pliki cookie pokazują Państwa komputer i urządzenie wyłącznie jako losowo przypisany ciąg numerów i liter (np. identyfikator pliku cookie ABC12345), a nigdy jako np. Jana Kowalskiego. Wykorzystujemy poniższego rodzaju pliki cookie:   * *Sesyjne pliki cookie*.Sesyjne pliki cookie zapamiętują użytkownika (przy użyciu losowo wygenerowanego identyfikatora) podczas przechodzenia pomiędzy stronami, dzięki czemu nie jest on proszony o podanie tych samych informacji, które już wcześniej podał. Te pliki cookie są usuwane niezwłocznie po opuszczeniu naszej witryny lub zamknięciu przeglądarki. * *Trwałe pliki cookie*. Trwałe pliki cookie umożliwiają witrynom zapamiętywanie preferencji Pracownika przy ponownym odwiedzeniu witryny. Jeśli np. przy pierwszej wizycie Pracownik zdecyduje się czytać stronę w języku francuskim, wówczas przy następnej wizycie witryna ta będzie automatycznie wyświetlana w tym języku. * *Analityczne pliki cookie.* Pliki te informują nas o działaniu naszych witryn internetowych. W niektórych przypadkach używamy plików cookie usługi Google Analytics do monitorowania wydajności naszych witryn. Nasza zdolność do wykorzystywania i udostępniania informacji gromadzonych przez Google Analytics na temat wizyt Pracownika w naszych witrynach jest ograniczona przez [Warunki korzystania z Google Analytics](https://www.google.com/analytics/terms/us.html) oraz [Politykę prywatności Google](https://policies.google.com/privacy). | Używamy plików cookie w witrynach P&G skierowanych do EPR z wielu powodów, w tym:   * aby dowiedzieć się więcej o sposobie interakcji Pracownika z naszymi witrynami i treściami P&G; * aby pomóc nam poprawić wrażenia Pracownika podczas odwiedzania naszych witryn internetowych; * aby spersonalizować witrynę pod kątem preferencji użytkownika; * aby wykrywać i naprawiać błędy; * aby analizować to, jak dobrze działają nasze witryny internetowe. |
| *Inne cechy osobiste*   * Dane biometryczne, takie jak odciski palców lub skany twarzy * Informacje o karalności/ kontrole podstawowych danych | * Ułatwianie dostępu do obiektów i systemów Firmy za pomocą danych biometrycznych * Zachowanie zgodności z przepisami prawa i polityką * Ład korporacyjny i zarządzanie * Bezpieczeństwo i tworzenie planów awaryjnych * Wymagana sprawozdawczość zewnętrzna * Postępowania wyjaśniające i zarządzanie incydentami |

* 1. **Na jakiej podstawie prawnej i/lub biznesowej przetwarzamy Dane osobowe EPR?**

Gromadzimy i zarządzamy minimalną ilością Danych osobowych EPR, niezbędną do wypełnienia naszych zobowiązań umownych i/lub prawnych związanych z naszą relacją jako niezależnego kontrahenta z Państwem i/lub Państwa pracodawcą; w celu wspierania uzasadnionych interesów biznesowych Firmy w sposób proporcjonalny do Państwa interesów związanych z prywatnością oraz do przetwarzania Danych osobowych dostarczonych za Państwa zgodą, w stosownych przypadkach, do zamierzonych celów.

Podstawą prawną i/lub biznesową przetwarzania Danych osobowych EPR może być przestrzeganie przez P&G obowiązujących przepisów prawa i regulacji, przestrzeganie zobowiązań umownych, uzasadnione interesy biznesowe Firmy, interesy związane ze zdrowiem publicznym i/lub zgoda Pracownika.

Podstawa prawna i/lub biznesowa przetwarzania Danych osobowych EPR może być różna w zależności od jurysdykcji, a także kategorii/rodzaju danych oraz powodów, dla których je gromadzimy i wykorzystujemy.

To podstawy prawne, na których będziemy zwykle polegać w przypadku przetwarzania poniższych kategorii danych:

|  |  |
| --- | --- |
| **Rodzaj Danych osobowych** | **Podstawa prawna/biznesowa przetwarzania** |
| Dane kontaktowe, dokument tożsamości wydany przez organ rządowy, informacje finansowe, informacje zdrowotne | Zgodność P&G z zobowiązaniami umownymi i prawnymi |
| Dokument tożsamości wydany przez organ rządowy/ kwalifikowalność do pracy | Przestrzeganie przez P&G obowiązujących przepisów prawa |
| Dane związane z pracą, dane kontaktowe | Uzasadnione interesy biznesowe P&G |

* 1. **W jaki sposób udostępniamy Dane osobowe EPR?**

P&G będzie udostępniać dane osobowe EPR wyłącznie tym osobom, które posiadają uzasadnioną potrzebę biznesową, aby je poznać.

P&G może udostępniać Państwa dane Państwa pracodawcy (i innym jednostkom po otrzymaniu upoważnienia Państwa pracodawcy), kontrahentom P&G, dostawcom, agencjom, pracownikom tymczasowym lub wszelkim innym stronom działającym w imieniu P&G („Podmioty zewnętrzne”).

Dane osobowe EPR mogą być udostępniane do naszej siedziby głównej oraz podmiotom stowarzyszonym na całym świecie wedle potrzeb związanych ze spełnieniem celów przetwarzania, które określono w Sekcji 5.2 powyżej.

Jeżeli wymagają tego przepisy prawa lub procedury prawne, możemy udostępniać Dane osobowe EPR; w celu egzekwowania lub ochrony praw i polityk P&G; i/lub w związku z postępowaniem wyjaśniającym, a także z domniemaną lub faktyczną działalnością niezgodną z prawem.

* 1. **Prawa do prywatności przysługujące kandydatom**

Mają Państwo prawo skontaktować się z nami i zażądać dostępu do dotyczących Państwa Danych osobowych EPR, które przetwarzamy i wykorzystujemy. W sytuacjach, w których zezwalają na to stosowne przepisy prawa, mogą Państwo zażądać, aby niedokładne, nieaktualne lub niepotrzebne informacje zostały poprawione, usunięte lub zastrzeżone, jak również przekazania Państwa danych w formacie, który pozwoli Państwu na przesłanie tych danych do usługodawcy, wedle potrzeb podyktowanych przez daną sytuację. W przypadkach, w których przetwarzanie Danych osobowych EPR jest uzależnione od uzyskania zgody, mają Państwo prawo wycofać swoją zgodę w dowolnym momencie. Jeżeli przetwarzanie Danych osobowych EPR opiera się na uzasadnionym interesie, w pewnych okolicznościach mają Państwo prawo do wniesienia sprzeciwu wobec przetwarzania danych.

Podczas korzystania z tych praw zachęcamy do uprzedniego omówienia swoich obaw z pracownikiem P&G, który działa w roli sponsora Państwa witryny. Mogą Państwo również skontaktować się z naszym Inspektorem ochrony danych, korzystając z adresu podanego poniżej. W przypadku braku zadowolenia ze sposobu, w jaki rozpatrzymy żądania, lub przetwarzania przez nas Państwa Danych osobowych można złożyć skargę do organu ochrony danych działającego w danym kraju.

* 1. **W jaki sposób przesyłamy Dane osobowe EPR?**

P&G jest firmą o zasięgu globalnym i ma EPR w wielu krajach. Jeśli jest to zgodne z prawem, w zależności od wymogów i/lub ograniczeń prawnych obowiązujących w danym kraju, Dane osobowe EPR mogą być przesyłane do krajów innych niż ten, w którym je zgromadzono. Dane osobowe EPR mogą być przechowywane w systemach znajdujących się w Stanach Zjednoczonych, dostęp do nich może być uzyskiwany przez podmioty stowarzyszone P&G w innych krajach, w tym przez ich usługodawców, lub przekazywane do innych krajów wedle potrzeb w celu realizacji istotnych działań biznesowych. Kraje te mogą nie stosować takich samych reguł ochrony danych jak kraj zamieszkania kandydata. W przypadkach, w których Dane osobowe są przesyłane do krajów innych niż Państwa kraj rodzinny lub dostęp do nich uzyskują podmioty z krajów innych niż Państwa kraj rodzinny, wdrażamy odpowiednie środki ochrony oraz spełniamy wszelkie wymagane przez prawo wymogi administracyjne, techniczne i/lub umowne w celu ich ochrony. Przekazujemy dane poza Europejski Obszar Gospodarczy (EOG), Wielką Brytanię (UK) oraz Szwajcarię, zarówno pomiędzy podmiotami P&G, jak i pomiędzy P&G a naszymi dostawcami usług odbywa się zgodnie ze Standardowymi klauzulami umownymi. W przypadku chęci otrzymania kopii tych Standardów prosimy o kontakt pod adresem [corporateprivacy.im@pg.com](mailto:corporateprivacy.im@pg.com). P&G będzie również przestrzegać wymogów określonych krajów, które to wymogi ograniczają przekazywanie danych poza kraj ich gromadzenia.

* 1. **W jaki sposób zabezpieczamy Dane osobowe EPR?**

Wdrażamy odpowiednie fizyczne, administracyjne i techniczne środki ochrony, takie jak pseudonimizacja, szyfrowanie i kontrola dostępu, zaprojektowane w celu ochrony Danych osobowych EPR przed przypadkowym, niezgodnym z prawem lub nieupoważnionym zniszczeniem, utratą, zmianą, ujawnieniem, wykorzystaniem lub dostępem, a także przed wszelkimi innymi formami przetwarzania niezgodnymi z prawem. W przypadku gdy Podmioty zewnętrzne przetwarzają Dane osobowe EPR w imieniu P&G, zawieramy również umowy z tymi Podmiotami zewnętrznymi w celu zapewnienia, że stosują one odpowiednie środki fizyczne, administracyjne i techniczne przy przetwarzaniu takich danych.

**5.8 Jak długo przechowywane są moje dane osobowe?**

Przechowujemy Dane osobowe EPR wyłącznie przez okres niezbędny do realizacji celów, do których zostały zgromadzone, chyba że dłuższy okres przechowywania jest wymagany lub dopuszczony przez prawo. Zazwyczaj oznacza to okres, w którym świadczą nam Państwo usługi. W niektórych przypadkach możemy musieć zachować Dane osobowe EPR przez pewien czas po zakończeniu Państwa relacji z P&G, aby zapewnić zgodność z zobowiązaniami prawnymi lub umownymi.

* 1. **Czy P&G monitoruje wykorzystanie sieci i urządzeń?**

Firma monitoruje wykorzystanie sieci P&G i urządzeń P&G. P&G ma obowiązek chronić swoich Pracowników, zasoby i obiekty. P&G monitoruje swoje sieci korporacyjne i urządzenia w trzech celach: i) w celu ochrony bezpieczeństwa (obejmującego poufność, integralność i dostępność) osób, danych, sieci, aktywów, obiektów, reputacji i interesów konkurencyjnych firmy P&G; ii) w celu badania podejrzewanych lub potwierdzonych wykroczeń lub przypadków naruszenia prawa (w tym w celu wspierania postępowania sądowego) oraz iii) w celu zapewnienia integralności procesów biznesowych i sprawozdawczości finansowej.

P&G nie monitoruje sieci P&G ani urządzeń pojedynczych osób bez uzasadnionych przyczyn, chyba że wymagają tego przepisy prawa, w tym na wniosek właściwych organów. Zastrzegamy sobie prawo, zgodnie ze stosownymi przepisami ustawowymi, do uzyskania dostępu, sprawdzania, ujawniania i pozbywania się wszelkich elektronicznych plików, danych i wiadomości tworzonych, przechowywanych, wysyłanych lub otrzymywanych za pośrednictwem naszych sieci i urządzeń w stopniu koniecznym dla celów wymienionych powyżej. Monitorowanie to zawsze odbywa się zgodnie ze stosownymi przepisami prawa i regulacjami. P&G będzie stosować dodatkowe procedury, standardy i polityki lub w razie potrzeby inne środki aktywnie zmierzające do spełnienia lokalnych wymogów prawnych.

Dokładniej mówiąc, P&G przeprowadzi pasywne i aktywne monitorowanie sieci P&G oraz urządzeń będących własnością P&G przydzielonych EPR w celu oznaczenia potencjalnych zagrożeń dla interesów P&G. Takie „bierne monitorowanie” nie jest czynnym sprawdzaniem działań poszczególnych osób, a jedynie szukaniem wskaźników ryzyka. Wskaźniki ryzyka zostały określone przez firmę P&G oraz dostawców specjalistycznych usług w zakresie bezpieczeństwa i dopasowano je do potrzeb bezpieczeństwa P&G. W przypadku, gdy taki wskaźnik ryzyka się pojawi („Zdarzenie”), system zapisuje odpowiednie dane i zachowuje je do późniejszego przejrzenia i/lub postępowania wyjaśniającego. W szczególności poniższe techniki monitorowania biernego zostaną wykorzystane w sieciach P&G oraz urządzeniach będących własnością P&G przydzielonych EPR.

1. **Monitorowanie wzorców użytkowania** jest techniką monitorowania, w ramach której oprogramowanie bądź urządzenie sprawdza zanonimizowane dane z sieci P&G i sieci web pod kątem określonego wcześniej zestawu wskaźników ryzyka. Technika ta polega na wyszukiwaniu podejrzanych wzorców w *użytkowaniu* sieci P&G i/lub urządzeń będących własnością P&G przydzielonych EPR. Na przykład P&G może ustawić narzędzie do monitorowania wzorców użytkowania w taki sposób, aby wyszukiwało wskaźniki ryzyka po miejscu logowania do sieci P&G. Dział bezpieczeństwa firmy P&G może dostosować narzędzie tak, że będzie wysyłało alert, jeśli te same dane logowania zostaną użyte w dwóch różnych lokalizacjach sieci P&G w krótszym odstępie czasu niż czas niezbędny do przebycia tej odległości przez człowieka.
2. **Skanowanie ruchu przychodzącego** to narzędzie monitorujące służące do skanowania komunikacji przychodzącej w oparciu o sieć web (w tym poczty e-mail) w momencie wejścia do sieci P&G pod kątem wskaźników ryzyka. Oprogramowanie antywirusowe i zapory to najpopularniejsze przykłady narzędzia, które nieustannie skanuje ruch przychodzący pod kątem wskaźników występowania złośliwego oprogramowania w załącznikach, hiperłączach, na stronach internetowych itp.
3. **Skanowanie okresowe** to narzędzie monitorujące służące do skanowania na poziomie sieci P&G i urządzeń P&G w poszukiwaniu szczególnych wskaźników ryzyka, które mogły wymknąć się Skanowaniu ruchu przychodzącego. Jest to pożyteczne narzędzie, ponieważ czasami Zdarzenia łatwiej rozpoznać w kontekście. Skanowanie całego dysku programem antywirusowym jest dobrym przykładem takiego narzędzia.
4. **Skanowanie ruchu wychodzącego** Firma P&G ma możliwość skanowania sieciowego ruchu wychodzącego pod kątem konkretnych, określonych wcześniej wskaźników ryzyka. Narzędzie skanuje ruch wychodzący w celu sprawdzenia, czy według reguł określonych w ramach wskaźników ryzyka nie miało miejsca Zdarzenie. Na przykład P&G może napisać regułę sygnalizującą przesyłanie na zewnątrz sieci P&G dużych plików zawierających ściśle zastrzeżone dane lub określone słowa kluczowe, na przykład nazwy substancji chemicznych stosowanych w składzie nowego produktu.

P&G, w oparciu o rodzaj zagrożenia wskazanego przez bierne narzędzia monitorujące lub na podstawie informacji z innych źródeł (np. proces sądowy, domniemanie niewłaściwego postępowania, organy porządkowe itp.), ocenia, czy konieczne są dalsze czynności wyjaśniające/analizy ryzyka. Podczas oceny P&G rozważa potencjalną szkodę dla pracowników, konsumentów, innych interesariuszy lub dla Firmy, a także interes prawny i związany z ochroną prywatności wszystkich osób, których sprawa dotyczy. Firma P&G może również ustalić, czy dalsza analiza jest wymagana zgodnie z wymogami prawnymi lub firmowymi, mającymi na celu ochronę zasobów i zagwarantowanie integralności procesów biznesowych. W oparciu o tę analizę P&G albo powstrzyma się od prowadzenia dalszych czynności wyjaśniających, albo będzie prowadzić w sposób proporcjonalny czynności wyjaśniające, wykorzystując aktywne narzędzia monitorujące.

Firma korzysta z narzędzi aktywnego monitorowania pięciu podstawowych typów: (1) skanowanie urządzeń, (2) skanowanie aktywności internetowej (3) monitorowanie miękkie, (4) monitorowanie sprzętu i (5) zapobieganie utracie danych.

1. **Skanowanie urządzeń:** Narzędzia te pozwalają firmie P&G, czasami za pośrednictwem podmiotów zewnętrznych, wydobyć *całą* zawartość komputera będącego własnością P&G lub innego urządzenia P&G w danym punkcie czasowym do wykorzystania w dochodzeniu. Narzędzia do skanowania urządzeń nie tylko wydobywają pliki i aplikacje zapisane i przechowywane na dysku urządzenia będącego własnością P&G, ale mogą też uchwycić zapis pamięci urządzenia w danej chwili. Zależnie od narzędzia, P&G może wydobyć tylko pliki fizycznie znajdujące się na komputerze (np. z pominięciem pamięci) lub wydobyć częściowy obraz urządzenia – co umożliwia skoncentrowanie czynności wyjaśniających tylko na konkretnych typach plików lub aplikacji, zgodnie z zasadami proporcjonalności.
2. **Skanowanie aktywności internetowej:** Firma P&G używa narzędzia web proxy od dostawcy zewnętrznego działającego w oparciu o chmurę, które posiada trzy podstawowe funkcje. Pierwsza to zdolność śledzenia korzystania z zasobów internetowych na poziomie adresów URL (tj. po nazwach odwiedzanych witryn internetowych), gdy EPR korzysta z urządzenia będącego własnością P&G. Funkcja ta śledzi i rejestruje aktywność internetową poprzez szyfrowane identyfikatory osobiste (a zatem anonimizujące użytkownika) do ewentualnego wykorzystania w zatwierdzonym postępowaniu wyjaśniającym. Druga to możliwość wglądu do danych wpisywanych na nieszyfrowanych stronach internetowych oraz plików wysyłanych lub pobieranych podczas odwiedzin na nieszyfrowanych stronach. Trzecia to możliwość odszyfrowania ograniczonego podzbioru ruchu w sieci, który został wstępnie określony jako wysokiego ryzyka (np. połączenia wychodzące do znanych złośliwych stron internetowych, stron internetowych, o których wiadomo, że zapisują złośliwe oprogramowanie na urządzeniach, lub niezatwierdzonych stron do udostępniania plików). Rozwiązanie to jest skonfigurowane tak, aby nie odszyfrowywało ruchu na witrynach, które mogą przetwarzać wrażliwe dane osobowe na temat użytkownika końcowego (np. strony bankowości i ochrony zdrowia).
3. **Monitorowanie miękkie:** Są to techniki stosowane jako część postępowania wyjaśniającego dotyczącego konkretnych osób, w przypadku gdy (a) dana osoba została poinformowana o toczącym się postępowaniu oraz (b) postępowanie wyjaśniające nie jest prowadzone w stosunku do tej osoby. Na przykład narzędziem monitorowania miękkiego może być połączenie telefoniczne lub e-mail w celu stwierdzenia, gdzie *konkretny* EPR się aktualnie znajduje/jest zalogowany, aby ustalić, czy Zdarzenie związane z położeniem geograficznym jest uzasadnione.
4. **Monitorowanie sprzętu i aplikacji**: Narzędzia do monitorowania sprzętu i aplikacji to narzędzia monitorujące i logujące wbudowane w sprzęt przez producenta lub aplikacje, które w powiązaniu z konkretnym EPR stanowią aktywne monitorowanie. Powszechnie stosowanymi przykładami są dzienniki serwerów, listy loginów SAP, raporty użycia identyfikatorów zbliżeniowych, uwierzytelnienie sieciowe itp.
5. **Zapobieganie utracie danych:** Firma P&G lub zatwierdzony usługodawca skanuje wiadomości e-mail wysyłane na adresy spoza P&G pod kątem wskaźników utraty danych. Jeśli na przykład EPR wysyła niezaszyfrowaną wiadomość e-mail ze ściśle poufnym załącznikiem na adres e-mail spoza P&G, rozwiązanie mające na celu zapobieganie utracie danych oznaczy taką wiadomość e-mail jako zagrażającą bezpieczeństwu danych, a użytkownik może zostać poinformowany o konieczności zastosowania zatwierdzonego rozwiązania szyfrującego w przypadku przyszłych wiadomości. Podobnie będzie, jeśli wysyłana wiadomość e-mail sklasyfikowany jako Ściśle poufne lub Tajne (obejmujący specjalnie wyznaczone słowa kluczowe) zostanie oznaczona – zostanie ona sprawdzona pod kątem ryzyka dla bezpieczeństwa. W stosownych przypadkach wszczęte może zostać postępowanie wyjaśniające. Firma P&G nie skanuje wiadomości sklasyfikowanych jako „Osobiste” lub „Prywatne” ani tych oznaczonych jako „Osobiste” lub „Prywatne” w temacie wiadomości.
6. **Przyszłe zmiany**

P&G zastrzega sobie prawo do modyfikowania niniejszej Informacji wedle potrzeb, na przykład z powodów podyktowanych zmianami w przepisach prawa, regulacjach, praktykach i procedurach Firmy lub w celu reagowania na nowe zagrożenia lub nowe wymagania narzucone przez organy ds. ochrony danych. Jeżeli zmiany te wywierać będą poważny wpływ na przetwarzanie Danych osobowych EPR, zostanie on stosownie powiadomiony.

1. **Dane kontaktowe**

W razie pytań bądź wątpliwości dotyczących przetwarzania Państwa danych osobowych / Informacji osobowych EPR lub w przypadku chęci skorzystania z przysługującego Państwu prawa do prywatności można również skontaktować się z Generalnym Inspektorem Ochrony Danych, pisząc na adres e-mail [pgprivacyofficer.im@pg.com](mailto:pgprivacyofficer.im@pg.com), telefonicznie pod numerem: +1 (513) 622-0103 lub pisząc na adres: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, U.S.A.

W razie wątpliwości związanych z potencjalnym naruszeniem Danych osobowych EPR lub innych danych osobowych wykorzystywanych przez P&G należy przesłać wiadomość na adres e-mail [securityincident.im@pg.com](mailto:securityincident.im@pg.com).