**Повідомлення про конфіденційність щодо Сторонніх ресурсів у всьому світі**

|  |  |
| --- | --- |
| **Контактна особа щодо Повідомлення про конфіденційність:**  Міжнародний спеціаліст із захисту даних | **Дата: 1 січня 2023 року**   |
|  (pgprivacyofficer.im@pg.com) **Регіон:** Для всього світу | **Сфера застосування:** Всі Сторонні ресурси |

# **Намір**

У цьому Повідомленні міститься інформація для всіх сторонніх ресурсів («СР») (згідно із визначенням нижче) про те, як компанія Procter & Gamble, її дочірні та (або) афілійовані компанії («P&G» чи «Компанія») збиратимуть ваші Персональні дані та керуватимуть ними.

# **Статус незалежного підрядника**

Це Повідомлення не створює трудових відносин між компанією P&G та СР. СР надають послуги компанії P&G у якості незалежних підрядників, незважаючи на те, чи такі послуги надаються безпосередньо компанії P&G, чи шляхом укладення угоди між компанією P&G та роботодавцем СР.

1. **Визначення**

**Сторонній ресурс.** Будь-яка фізична особа, яка виконуватиме роботу або надаватиме послуги компанії P&G, для якої компанія P&G не є офіційним роботодавцем на час виконання робіт або надання послуг, як, наприклад, підрядники.

**Персональні дані.** Будь-яка інформація щодо визначеної фізичної особи або фізичної особи, яку можна визначити, як, наприклад, П.І.Б., інші ідентифікаційні дані, контактна інформація, професійна інформація та особисті характеристики.

**Компанія або P&G.** Для цілей цього повідомлення «Компанія», або «P&G», стосується компанії Procter & Gamble, її дочірніх і (або) афілійованих компаній.

1. **Принципи**

Нижче наведено основні принципи P&G, пов’язані з обробкою персональних даних:

* збір мінімальної кількості Персональних даних СР і керування ними;
* повага до приватного життя;
* дотримання нашої мети, цінностей та принципів (МЦП), цього Повідомлення та відповідного законодавства;
* дотримання відповідних стандартів і процедур під час збору та (або) керування Персональними даними СР.
1. **Повідомлення**

Компанія P&G поважає вашу конфіденційність. Це повідомлення описує, як ми обробляємо Персональні дані СР, типи інформації, збір якої ми здійснюємо напряму від вас та (або) від вашого роботодавця, мету використання такої інформації, категорії одержувачів, з якими ми нею ділимось, а також вибір, який ви можете зробити щодо використання нами цієї інформації. Ми також описуємо заходи, яких вживаємо для захисту Персональних даних СР, і способи, у які ви можете звертатися до нас щодо наших практик дотримання конфіденційності.

* 1. **Для яких цілей ми збираємо та використовуємо Персональні дані СР?**

Компанія P&G збирає Персональні дані про своїх СР у контексті договору про надання послуг та відносин із незалежним підрядником, які виникають у компанії P&G із вами та (або) вашим роботодавцем. Загалом, ми збираємо та використовуємо Персональні дані СР, отримані від вас та (або) вашого роботодавця, для наступних послуг та (або) видів діяльності:

* безпека та охорона праці, включаючи скринінги, пов’язані з оцінкою стану здоров’я, та медичні програми щодо COVID-19 або подібних криз у сфері охорони здоров’я;
* керування доступом на об’єктах;
* управління ідентифікаційними та обліковими даними, включаючи перевірку та автентифікацію особи, видачу облікових карток та бейджів, системне адміністрування, запис входів у систему та виходів із неї та управління обліковими даними щодо доступу, інформаційну безпекою та кібербезпеку;
* планування дій у надзвичайних ситуаціях, включаючи безперервність бізнес-процесів, кадрове забезпечення, управління змінами та протоколами дій в надзвичайних ситуаціях / протоколами безпеки;
* реєстрація електронних пристроїв і керування ними, оптимізація використання мережі й пристроїв;
* забезпечення роботи засобів контролю фізичної та кібербезпеки, включно з моніторингом електронних пристроїв і мереж та запис відео забезпечення безпеки, наприклад система відеоспостереження;
* судовий розгляд спорів і внутрішні чи зовнішні розслідування, аудиторські перевірки й вирішення суперечок;
* щоденна обробка даних робочих процесів (як-от автентифікація та вхід у наші системи);
* участь у зборах, тренінгах і подіях;
* дотримання законів, нормативних актів і політик Компанії щодо боротьби з хабарництвом, дитячою працею та корупцією, а також санкцій, вимог експортного контролю, прав людини й інших вимог щодо корпоративної поведінки та відповідального керівництва;
* розслідування, які проводить компанія P&G та (або) ваш роботодавець щодо неналежних дій на робочому місці або порушення процесів;
* виконання та аудит наших договорів про надання послуг із вами та (або) вашим роботодавцем, включаючи оцінку виконання цих послуг;
* дотримання всіх законодавчих, нормативних, судових або урядових вимог, реагування на судові накази, повістки, запити на надання відомостей або запити на надання інших урядових даних та дотримання їх;
	+ керування безпекою та ризиками, включаючи забезпечення безпеки та контроль за персоналом та приміщеннями та захист компанії P&G, наших працівників та наших клієнтів від крадіжки, юридичної відповідальності, обману чи зловживання.
	1. **Які типи Персональних даних СР ми збираємо?**

Ми завжди мінімізуємо типи та кількість Персональних даних СР, які ми одержуємо від вас або про вас. У наведеній нижче таблиці більш детально описані категорії Персональних даних СР, які збирає компанія P&G у зв’язку з процесом керування своєю діяльністю.

Збір інформації й доступ до неї відрізнятимуться залежно від юридичних і (або) бізнес-вимог у конкретній країні.

Юридична або комерційна основа для збору й обробки Персональних даних СР буде відрізнятися залежно від типу даних і цільового використання, як описано в нижченаведеному розділі 5.3.

|  |  |
| --- | --- |
| **Які типи даних СР ми збираємо та обробляємо?** | **Чому ми збираємо та обробляємо різні типи Персональних даних СР?***Ми збираємо та обробляємо ці типи даних для різних організаційних і бізнес-процесів, що докладно описується в розділі 5.1 і більш детально пояснюється нижче.* |
| *Контактна інформація та персональні характеристики* * П. І. Б. або попередні імена (як-от дівоче прізвище);
* інші унікальні ідентифікатори, як-от ідентифікаційні номери чи облікові дані, видані компанією P&G (наприклад, логін до електронної пошти) або будь-який ідентифікаційний номер, виданий вашим роботодавцем;
* фізична/поштова адреса;
* адреса ел. пошти;
* номер телефону.
 | * доступ до об’єктів і електронної мережі;
* обмін інформацією з вами щодо планування комерційних дій у надзвичайних ситуаціях, включаючи керування змінами;
* участь у зборах, тренінгах і подіях;
* щоденна обробка даних робочих процесів (як-от автентифікація та вхід у наші системи);
* дотримання законів, вимог політик;
* дотримання норм корпоративної поведінки й відповідального керівництва;
* підготовка обов’язкової зовнішньої звітності;
* розслідування та контроль інцидентів;
	+ керування безпекою та ризиками, включаючи забезпечення безпеки та контроль за персоналом та приміщеннями та захист компанії P&G, наших працівників та наших клієнтів від крадіжки, юридичної відповідальності, обману чи зловживання;
* безпека та охорона праці, включаючи скринінги, пов’язані з оцінкою стану здоров’я, та медичні програми щодо COVID-19 або подібних криз у сфері охорони здоров’я;
* виконання та аудит наших договорів про надання послуг із вами та (або) вашим роботодавцем, включаючи оцінку виконання цих послуг;
* дотримання всіх законодавчих, нормативних, судових або урядових вимог, реагування на судові накази, повістки, запити на надання відомостей або запити на надання інших урядових даних та дотримання їх.
 |
| *Інформація про посвідчення особи / дозвіл на виконання робіт / ідентифікаційні дані роботодавця** державний ідентифікаційний документ (як-от паспорт, візи, номер соціального страхування, посвідчення водія, інші державні ідентифікаційні документи);
* громадянство;
* місце проживання;
* національність;
* країна народження;
* військовий статус і (або) статус ветерана;
* унікальний ідентифікаційний номер у якості працівника компанії P&G, який зазначений у договорі із вами.
 | * юридична ідентифікація вашої особи та підтримання цілісності наших кадрових записів;
* дотримання імміграційних вимог та інших вимог щодо дозволів на виконання робіт;
* керування безпекою та ризиками, наприклад збір даних водійських посвідчень для СР, які керують автомобілями Компанії, перевірка професійних ліцензій, запобігання шахрайству та досягнення подібних цілей;
* дотримання законів, вимог політик;
* дотримання норм корпоративної поведінки й відповідального керівництва;
* забезпечення безпеки та планування дій у надзвичайних ситуаціях;
* підготовка обов’язкової зовнішньої звітності;
* розслідування та контроль інцидентів.
 |
| *Фінансова інформація* * номер і реквізити банківського рахунку;
* інформація про особисту платіжну картку, якщо її дані надаються для відшкодування.
 | * сприяння відшкодуванню супутніх витрат;
* дотримання законів, вимог політик;
* дотримання норм корпоративної поведінки й відповідального керівництва;
* забезпечення безпеки та планування дій у надзвичайних ситуаціях;
* підготовка обов’язкової зовнішньої звітності;
* розслідування та контроль інцидентів.
 |
| *Медична інформація* * інформація, пов’язана з фізичним або емоційним здоров’ям особи, зокрема про будь-які обмеження для виконання робочих обов’язків або функцій;
* аналізи на лікарські препарати та інші види медичних обстежень.
 | * дотримання вимог щодо безпеки й охорони праці на робочому місці та державних вимог до звітності;
* керування ризиками, пов’язаними з безпекою СР, і бізнес-ризиками у зв’язку з пандемією COVID-19 або подібними надзвичайними ситуаціями у сфері охорони здоров’я;
* дотримання законів, вимог політик;
* дотримання норм корпоративної поведінки й відповідального керівництва;
* забезпечення безпеки та планування дій у надзвичайних ситуаціях;
* підготовка обов’язкової зовнішньої звітності;
* розслідування та контроль інцидентів.
 |
| *Електронні ідентифікаційні дані / унікальні ідентифікатори / зображення й голосові дані** ідентифікатори системи P&G (як-от імена користувачів або облікові дані);
* цифровий підпис;
* електронні ідентифікаційні дані, журнали та записи щодо доступу й використання пристроїв, систем, програм, ліцензій, баз даних компанії P&G та мережі P&G (наприклад, використання вами електронної пошти, Інтернету, соціальних мереж);
* інформація, зібрана системами безпеки компанії P&G, включно із системою відеоспостереження («CCTV»), системою доступу до об’єктів, камерами спостереження за лінійними процесами або виконанням завдань;
* електронні ідентифікаційні дані, журнали та записи, що стосуються вашого доступу до сайтів P&G й обмежених зон доступу, зокрема номер значка/фотографія значка;
* відео, фотографії та інші зображення / записи голосу в контексті зустрічей/навчань;
* електронні ідентифікаційні дані щодо записів кол-центру.
 | * системне адміністрування, доступ до технологій та ІТ-ресурсів і керування ними;
* відстоювання наших інтересів у сфері фізичної, інформаційної та кібербезпеки задля протистояння внутрішнім і (або) зовнішнім загрозам;
* керування запобіганням втратам і відновленням у наших офісах та на виробничих майданчиках;
* внутрішнє ведення обліку та звітування, зокрема зіставлення та аналітика даних;
* надання доступу до об’єктів, мережі, інструментів, програм та інших систем і ресурсів компанії P&G;
* забезпечення видимості використання та витрат на використання інструментів, ліцензій, послуг і програм P&G для оптимізації, забезпечення якості, аудиту й контролю витрат;
* зйомка процесу навчання та зустрічей;
* дотримання законів, вимог політик;
* дотримання норм корпоративної поведінки й відповідального керівництва;
* забезпечення безпеки та планування дій у надзвичайних ситуаціях;
* підготовка обов’язкової зовнішньої звітності;
* розслідування та контроль інцидентів.
 |
| *Файли cookie -* Файли cookie — це невеликі файли, які надсилаються на ваш комп’ютер під час перегляду вебсайту. Вони зберігають корисну інформацію про те, як ви взаємодієте з вебсайтами, які відвідуєте. Файли cookie не збирають інформацію, яка зберігається на вашому комп’ютері чи пристрої або у ваших файлах. Файли cookie не містять жодної інформації, яка безпосередньо ідентифікує вас як особу. Ці файли показують ваш комп’ютер і пристрій лише як номери та букви, призначені у випадковий спосіб (наприклад, ідентифікатор cookie «ABC12345»), і ніколи як, наприклад, «Джон Е. Сміт». Нижче наведено типи файлів cookie, які ми використовуємо: * *Файли cookie сеансу*.Файли cookie сеансу запам’ятовують вас (за допомогою випадково згенерованого ідентифікатора), коли ви переходите зі сторінки на сторінку, щоб вам не доводилося надавати ту саму інформацію, яку ви вже надали на сайті. Ці файли cookie видаляються, щойно ви покинете наш сайт або закриєте браузер.
* *Постійні файли cookie*. Постійні файли cookie дають сайтам змогу запам’ятовувати ваші вподобання, коли ви повертаєтесь. Наприклад, якщо ви вирішите переглянути сайт французькою мовою під час першого візиту, то наступного разу, коли ви повернетесь, сайт автоматично відобразиться французькою мовою.
* *Аналітичні файли cookie*. Ці файли cookie показують нам, як працюють наші вебсайти. У деяких випадках ми використовуємо файли cookie Google Analytics для моніторингу роботи наших вебсайтів. Наші можливості використання та передачі інформації, зібраної Google Analytics про відвідування вами наших вебсайтів, обмежуються [Умовами використання Google Analytics](https://www.google.com/analytics/terms/us.html) і [Політикою конфіденційності Google](https://policies.google.com/privacy).
 | Ми використовуємо файли cookie на вебсайтах, призначених для СР компанії P&G, із низки причин, зокрема, щоб: * дізнатися більше про те, як ви взаємодієте з нашими вебсайтами та контентом P&G;
* допомогти нам покращити ваш досвід під час відвідування наших вебсайтів;
* налаштовувати вебсайт згідно з вашими вподобаннями;
* виявити помилки та виправити їх;
* аналізувати ефективність наших вебсайтів.
 |
| *Інші особисті характеристики** біометричні дані, як-от відбитки пальців або скани обличчя;
* перевірка щодо наявності судимостей / перевірка попередньої діяльності.
 | * сприяння доступу до сайтів і систем Компанії за допомогою біометричних даних;
* дотримання законів, вимог політик;
* дотримання норм корпоративної поведінки й відповідального керівництва;
* забезпечення безпеки та планування дій у надзвичайних ситуаціях;
* підготовка обов’язкової зовнішньої звітності;
* розслідування та контроль інцидентів.
 |

* 1. **На яких юридичних і (або) комерційних підставах ми обробляємо Персональні дані СР?**

Ми збираємо мінімальну кількість Персональних даних СР (і керуємо ними), які необхідні для виконання наших договірних і (або) юридичних зобов’язань щодо відносин із незалежним підрядником, які виникають із вами та (або) вашим роботодавцем; задля забезпечення законних ділових інтересів Компанії у спосіб, пропорційний інтересам конфіденційності наших працівників, а також для обробки персональних даних, наданих за вашою згодою (у відповідних випадках) для визначених цілей.

Правовими та (або) комерційними підставами для обробки Персональних даних СР можуть бути дотримання компанією P&G застосовних законів і норм, виконання своїх договірних зобов’язань; забезпечення дотримання законних ділових інтересів Компанії чи інтересів органів охорони громадського здоров’я та (або) ваша згода.

Правові та (або) комерційні підстави для обробки Персональних даних СР можуть відрізнятися залежно від юрисдикції, категорії чи типу даних і причин, із яких ми збираємо й використовуємо таку інформацію.

Ось на які правові підґрунтя ми, загалом, покладаємось при обробці цих категорій даних:

|  |  |
| --- | --- |
| **Тип персональних даних** | **Правова/комерційна підстава для обробки** |
| контактна інформація, інформація про посвідчення особи, фінансова інформація, інформація про стан здоров’я; | дотримання компанією P&G контрактних та правових зобов’язань;  |
| інформація про посвідчення особи / дозвіл на виконання робіт; | дотримання компанією P&G чинних законів і нормативно-правових актів; |
| професійні дані, контактна інформація. | законні ділові інтереси P&G. |

* 1. **Як ми розкриваємо Персональні дані СР?**

Компанія P&G розкриватиме Персональні дані СР лише тим особам, які мають законні ділові інтереси їх знати.

Компанія P&G може передавати вашу інформацію вашому роботодавцю (та іншим організаціям за вказівкою вашого роботодавця), підрядникам, постачальникам, агенціям, тимчасовим працівникам або будь-яким іншим сторонам, які діють від імені P&G («Сторонні сторони»).

Персональними даними СР можна ділитися із нашими головними офісами і з філіями по всьому світі, якщо необхідно досягнути цілей обробки даних, які зазначені в розділі 5.2 вище.

Ми також можемо розкривати Персональні дані СР, якщо це вимагається законом або судовим процесом, а також для забезпечення дотримання чи захисту прав і політик компанії P&G, сприяння розслідуванню імовірних чи фактичних неналежних дій або незаконної діяльності та (або) у рамках продажу бізнесу P&G іншій компанії.

* 1. **Які ви маєте права на конфіденційність?**

Ви маєте право зв’язатися з нами та попросити надати доступ до Персональних даних СР, які ми обробляємо та використовуємо стосовно вас. Якщо дозволено чинним законодавством, ви можете подати запит щодо виправлення, видалення чи обмеження неточної, застарілої чи непотрібної інформації, та ви можете попросити компанію P&G надати свої дані у форматі, що дає змогу передати їх постачальнику послуг за певних обставин. Якщо обробка Персональних даних СР ґрунтується на згоді, ви маєте право будь-коли відкликати свою згоду. Якщо обробка Персональних даних СР ґрунтується на законному інтересі, ви маєте право за певних обставин заперечувати проти обробки даних.

При застосуванні цих прав ми рекомендуємо вам спершу обговорити свої проблеми із працівником компанії P&G, який виступає спонсором на місці. Або ж ви можете звернутися до нашого спеціаліста із захисту даних за адресою нижче. Якщо вас не влаштовують відповіді, надані нами на ваш запит або ж обробка нами ваших Персональних даних, ви можете подати скаргу до органу нагляду за дотриманням законодавства про захист персональних даних у своїй країні.

* 1. **Як ми передаємо Персональні дані СР?**

Компанія P&G є міжнародною компанією та має СР у багатьох країнах. Якщо це дозволено згідно із законом та з врахуванням бізнес-вимог та (або) обмежень у конкретній країні, Персональні дані СР дозволяється передавати у країни за межами країни їх збору. Персональні дані СР можуть зберігатися в системах у Сполучених Штатах Америки, доступ до яких здійснюється з інших філій компанії P&G у всьому світі, зокрема з боку постачальників послуг. Крім того, дані можуть передаватися в інші країни, якщо це необхідно для здійснення відповідних операцій згідно з чинним законодавством. У цих країнах закони про захист даних можуть відрізнятися від законів вашої країни проживання. Коли ваші Персональні дані передаються до країн за межами вашої країни проживання або, коли до них здійснюється доступ із таких країн, ми вживаємо належних заходів безпеки, а також дотримуємося будь-яких обов’язкових (відповідно до законодавства) адміністративних, технічних і (або) договірних вимог щодо захисту вашої інформації. Ми передаємо ці дані за межі Європейської економічної зони (ЄЕЗ), Великої Британії та Швейцарії, як між організаціями компанії P&G, так і нашим провайдерам послуг покладаючись на стандартні статті угоди. Якщо ви хочете отримати копію цих пунктів угоди, надішліть звернення на адресу corporateprivacy.im@pg.com. P&G також буде дотримуватися інших особливих вимог країни, які обмежують передачу даних за межі країни збору інформації.

* 1. **Як ми захищаємо Персональні дані СР?**

Ми вживаємо належних фізичних, адміністративних і технічних заходів, як-от псевдонімізація, шифрування та контроль доступу, призначених для захисту Персональних даних СР від випадкового, незаконного або несанкціонованого знищення, втрати, змінення, розкриття чи використання, а також всіх інших незаконних форм обробки. Якщо Сторонні сторони обробляють Персональні дані СР від імені компанії P&G, ми також укладаємо договори з цими Сторонніми сторонами, щоб гарантувати реалізацію ними відповідних фізичних, адміністративних і технічних заходів під час роботи з такими даними.

**5.8 Як довго ви зберігаєте мої Персональні дані?**

Ми зберігаємо Персональні дані СР протягом періоду, який необхідний для досягнення цілей, для яких цю інформацію зібрано, якщо чинним законодавством не вимагається або не допускається триваліший термін зберігання. Загалом, це триває впродовж періоду, поки ви використовуєте ці послуги. У деяких випадках нам може знадобитися зберегти Персональні дані СР протягом певного періоду часу після припинення ваших відносин з P&G для виконання юридичних або договірних зобов’язань.

* 1. **Чи здійснює компанія P&G моніторинг мережі й використання пристроїв?**

Компанія здійснює моніторинг мережі та використання пристроїв компанії P&G. Компанія P&G зобов’язана захищати своїх співробітників, активи й об’єкти. Компанія P&G здійснює моніторинг своєї корпоративної мережі та пристроїв для трьох цілей: i) захист безпеки (забезпечення конфіденційності, цілісності та доступу) працівників, даних, мережі, активів, об’єктів, репутації та конкурентних інтересів Компанії; ii) розслідування імовірних або підтверджених неправомірних дій чи порушень законодавства (зокрема в рамках судових процесів); і iii) забезпечення безперервності ділових процесів і фінансової звітності.

Компанія P&G не контролює мережу P&G та прилади конкретної фізичної особи, окрім наявності законної причини чи вимоги виконувати ці дії згідно із законодавством, включно на вимогу правоохоронних органів. З врахуванням вимог діючого законодавства ми залишаємо за собою право доступу до, перевірки, розголошення та утилізації будь-яких електронних файлів, даних та повідомлень, які створили, зберігали, надсилали чи отримували через наші мережі та пристрої з метою зазначеною вище. Цей моніторинг завжди відповідає відповідним законам та нормам. Компанія P&G застосовуватиме додаткові процедури, стандарти, політику та (або) будь-які активні міри за необхідності, щоб відповідати місцевим законодавчим вимогам.

А саме, компанія P&G здійснюватиме пасивний і активний моніторинг мереж P&G та пристроїв, якими володіє P&G, які передані СР для того, щоб повідомляти про потенційні загрози інтересам P&G. «Пасивний моніторинг» не вивчатиме активно поведінку фізичних осіб, а, натомість, відстежуватиме індикатори ризиків. Ці індикатори ризиків уже визначені P&G та спеціалізованими постачальниками рішень в сфері безпеки та налаштовані, щоб відповідати безпековим потребам P&G. Коли такий індикатор ризику спрацьовує (далі «Подія»), системи реєструють відповідні дані та зберігають їх для подальшого перегляду та (або) вивчення. А саме, методи пасивного моніторингу, зазначені нижче, використовуватимуться у мережах P&G та приладах, якими володіє P&G та які видані СР:

1. **Моніторинг особливостей використання** — це метод моніторингу, коли за допомогою програмного і апаратного забезпечення здійснюється перевірка мережі P&G без ідентифікуючої особистість інформації та вебданих на попередньо визначений набір індикаторів ризику. Цей метод шукає підозрілі шаблони того, яким чином *використовуються* мережа P&G та (або) пристрої, якими володіє P&G та які передали СР. Наприклад, компанія P&G може встановити інструмент для Моніторингу особливостей використання, щоб відстежувати індикатори ризику за допомогою розташування місця входу в системи P&G. Відділ безпеки P&G може налаштувати цей інструмент таким чином, щоб він генерував тривогу, якщо вводяться облікові дані користувача для входу на двох різних об’єктах P&G швидше, ніж ця особа могла б обґрунтовано переміститись між цими місцями.
2. **Перевірка вхідного трафіку** — це інструмент для моніторингу, який сканує вхідні вебкомунікації (включаючи електронну пошту) щодо індикаторів ризику, коли вони потрапляють у мережу P&G. Найзагальнішим прикладом цього інструменту є антивірусне програмне забезпечення та шлюз безпеки, оскільки воно постійно сканує вхідний трафік щодо індикаторів наявності шкідливого програмного забезпечення у вкладеннях, посиланнях, на вебсайтах тощо.
3. **Періодична перевірка** — це інструмент моніторингу, який перевіряє на рівні мережі P&G та пристрою P&G, щоб вловити конкретні індикатори ризику, які могли вислизнути із поля зору при скануванні периметру при Перевірці вхідного трафіку. Цей інструмент є корисним, оскільки інколи Події легше визначити при їх розгляді із додатковим контекстом. Повна перевірка диску на наявність вірусів — це основний приклад такої здатності.
4. **Перевірка вихідного трафіку** — компанія P&G може перевіряти вихідний вебтрафік щодо певних попередньо визначених індикаторів ризику. Цей інструмент перевіряє вихідний трафік, щоб побачити, чи певна Подія спрацьовує згідно з вказаними правилами індикатора ризику. Наприклад, компанія P&G може написати правило, що сигналізуватиме про попередження при вивантаженні великих файлів у місця за межами мережі P&G, які включають інформацію суворо обмеженого доступу чи певні ключові слова, наприклад, певна хімічна сполука, яка використовується у формулі нового продукту.

Компанія P&G оцінює, на основі характеру ризику, який сигналізували інструменти для пасивного моніторингу або який іншим чином потрапив до уваги P&G (наприклад, судовий позов, розслідування зловживань, забезпечення правопорядку тощо), чи потрібне ретельніше дослідження/аналіз цього ризику. Здійснюючи таку оцінку компанія P&G враховує потенційну шкоду для працівників, споживачів, інших акціонерів та (або) Компанії, а також законних інтересів та інтересів, які стосуються недоторканості приватного життя будь-яких залучених фізичних осіб. Компанія P&G також може визначити, чи потрібен детальніший аналіз на основі законодавчих вимог чи вимог політики, щоб забезпечити безпеку активам та гарантувати цілісність бізнес-процесів. На основі цього аналізу компанія P&G не застосовуватиме подальших дій для розслідування чи продовжить пропорційне розслідування застосовуючи засоби для активного моніторингу.

Компанія P&G застосовує п’ять основних типів інструментів для Активного моніторингу: (1) сканування пристрою, (2) сканування інтернету, (3) моніторинг програмного забезпечення, (4) моніторинг апаратного забезпечення, та (5) запобігання втраті даних.

1. **Сканування пристрою:** Ці інструменти дозволяють компанії P&G, іноді за допомогою сторонньої особи, отримати *весь* вміст комп’ютера чи іншого пристрою, яким володіє P&G на певній точці в часі для використання у розслідуванні. Інструменти сканування пристрою не тільки отримують файли та додатки, які збережені та зберігаються на пристрої P&G, але можуть також отримати пам’ять з того пристрою на час її фіксації. Залежно від інструмента, компанія P&G може обрати отримання тільки фізичних файлів (тобто без вмісту пам’яті) або ж отримання часткового зображення пристрою, що дозволяє вивчити концентрацію тільки на певних типах файлів чи додатків згідно із принципами пропорційності.
2. **Сканування інтернету:** Компанія P&G застосовує сторонній хмарний інструмент проксі-сервера, який має три первинні характеристики. По-перше, він має здатність відстежувати використання інтернету загального користування на рівні URL (тобто назв відвідуваних вебсторінок), коли СР використовує пристрій, яким володіє P&G. Ця характеристика відстежує і реєструє інтернет-активність шляхом використання хешованих персональних ідентифікаторів (таким чином знеособлюючи користувача) щодо потенційного використання при схваленому розслідуванні. По-друге, він має здатність забезпечувати видимість даних, які вводяться на зашифрованій вебсторінці, та файлів, які вивантажуються та завантажуються при відвідуванні зашифрованих вебсайтів. По-третє, у нього є здатність декодувати обмежену підгрупу інтернет-трафіку, який попередньо розподілили до категорії високого ризику (наприклад, вихідні підключення до відомих шкідливих вебсторінок, вебсторінок, про які відомо, що вони доставляють шкідливі програми на пристрої, або несанкціонованих сайтів обміну файлами). Це рішення налаштоване не розшифровувати обмеження трафіку для вебсайтів, які можуть обробляти конфіденційні персональні дані про кінцевого користувача (наприклад, банківські сайти та сайти охорони здоров’я).
3. **Моніторинг програмного забезпечення:** Це методи, які застосовуються як частина розслідування, що включає осіб, яких можна ідентифікувати, коли: (a) особі повідомили про це розслідування, та (b) особа не підпадає під це розслідування. Наприклад, інструментом для моніторингу програмного забезпечення може бути телефонний дзвінок або електронний лист, щоб визначити, де знаходиться в даний момент *визначений* СР, який виконав вхід, щоб переконатися, чи певна Подія визначена за географічним тригером має законні підстави.
4. **Моніторинг програмного забезпечення та додатків**: Моніторинг програмного забезпечення та додатків — це можливості реєстрації та моніторингу, які виробники вбудовують в апаратне забезпечення та (або) додатки, що, при поєднанні із СР, яких можна ідентифікувати, складають Активний моніторинг. Поширеними прикладами є журнали сервера, логіни в SAP, звіти про проведення ідентифікаційними бейджами при реєстрації входу, мережева автентифікація тощо.
5. **Запобігання втраті даних:** Компанія P&G або схвалений провайдер послуг сканує електронні листи, які надсилають на адреси, які не належать P&G, на наявність ознак втрати даних. Наприклад, якщо СР надсилає незашифрований електронний лист із вкладенням матеріалів із суворою конфіденційністю на адресу електронної пошти, яка не належить компанії P&G, — то рішення для запобігання втрати даних сигналізуватиме цей електронний лист як інформаційний безпековий ризик, а користувачу можуть повідомити, що слід використовувати схвалене рішення для шифрування для майбутнього обміну повідомленнями. Аналогічно, якщо спрацював тригер щодо вихідного листа, якого класифіковано як суворо конфіденційний або таємний (включаючи спеціально розроблені ключові слова), то цей електронний лист перевірятимуть щодо безпекового ризику. У разі необхідності ініціюють розслідування. Компанія P&G не сканує повідомлення, які класифіковано як «особисті» або «приватні» або які позначені як «особисті» або «приватні» у темі листа.
6. **Майбутні зміни**

Компанія P&G залишає за собою право вносити зміни до цього Повідомлення, наприклад, для забезпечення відповідності змінам у законах, положеннях, практиках і процедурах Компанії або для реагування на нові загрози чи нові вимоги, встановлені органами захисту даних. Якщо такі зміни істотно впливають на здійснювану нами обробку Персональних даних СР, ми відповідним чином повідомимо вас про це.

1. **Контактна інформація**

Із запитаннями чи занепокоєннями щодо обробки ваших персональних даних / Персональних даних СР або якщо ви бажаєте реалізувати своє право на конфіденційність, звертайтеся до нашого Міжнародного інспектора із захисту даних за електронною адресою: pgprivacyofficer.im@pg.com; за телефоном: +1 (513) 622-0103; або за поштовою адресою: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, U.S.A. (США).

Якщо ви занепокоєні потенційним порушенням, пов’язаним із Персональними даними вашого СР або будь-якою особистою інформацією, яка обробляється компанією P&G, надішліть нам електронного листа на адресу: securityincident.im@pg.com.