

	<p>Посилання: CI- XX</p>
<p>Загальна політика конфіденційності КОРПОРАТИВНА ІНСТРУКЦІЯ</p>	<p>Дата останньої редакції: 01 березня 2024 року</p> <p>Дата нової редакції: XX – XX - XXXX</p> <p>Дата набрання чинності: 01 березня 2024 року</p>

Зміст

Заява про положення Політики.....	3
Сфера застосування.....	3
Основні терміни.....	3
Обробка Персональних даних	4
Мінімізація даних, конфіденційність за задумом, зниження чутливості	4
Ведення записів про обробку	5
Оцінка впливу на захист даних (DPIA) і ризики.....	5
Правові підстави обробки Персональних даних	6
Безпека даних.....	6
Конфіденційність і дозвіл	6
Шифрування й псевдонімізація	7
Регулярні аудити безпеки й тестування	7
Відстежування	7
Соціальні мережі.....	7

Керування мобільними пристроями (MDM).....	7
Зберігання даних	7
Права суб'єктів даних.....	8
Спеціальні категорії та чутливі Персональні дані.....	8
Обмін даними й треті особи	8
Повідомлення про порушення безпеки даних.....	9
Транскордонне передавання даних	9
Відповідність законам і правилам	9
Навчання, обізнаність і забезпечення виконання	9
Уповноважений із питань захисту даних (DPO).....	10
Функції і зобов'язання	Error! Bookmark not defined.
Контроль редакцій	10

Заява про положення Політики

Компанія Graphic Packaging прагне захищати Персональні дані своїх співробітників і клієнтів. З метою забезпечення прозорості й дотримання вимог міжнародних нормативних актів у галузі захисту конфіденційної інформації в цій Політиці конфіденційності встановлені такі положення:

- типи Персональних даних, які збирає Graphic Packaging;
- навіщо Graphic Packaging збирає Персональні дані;
- як використовуються й обробляються Персональні дані;
- права й варіанти дій щодо Персональних даних;
- захист Персональних даних; і
- контактні дані органу з питань конфіденційності.

Сфера застосування

Ця Політика стосується всього персоналу, усіх офісів та інших ресурсів компанії Graphic Packaging, зокрема, серед іншого:

- усіх структурних підрозділів Graphic Packaging, її відділів і груп;
- усіх підрядників, консультантів та інших сторонніх постачальників послуг для компанії, за винятком випадків, коли вказано особливі вимоги до співробітників;
- усіх орендованих чи власних приміщень, де працює компанія Graphic Packaging; і
- усієї технологічної й мережевої інфраструктури Graphic Packaging, у тому числі її інформаційних систем, застосунків, системних платформ і комп'ютерних операцій, які виконуються в процесі роботи Graphic Packaging.

Певні політики, які згадуються або на які є посилання в цьому документі, є такими, що призначені для внутрішнього користування, і є доступними лише для призначених співробітників. Якщо ви — співробітник і не можете відкрити посилання на відповідну політику, надішліть запит на отримання копії за електронною адресою law.department@graphicpkg.com.

Основні терміни

«Суб'єкт персональних даних» — це жива фізична особа, чії персональні дані оброблялися або обробляються.

«Персональні дані» включають будь-яку інформацію стосовно ідентифікованої фізичної особи або фізичної особи, яку можна ідентифікувати, наприклад, ім'я і записи в трудовій книжці співробітника, ім'я і робочі контактні дані представника клієнта, ім'я і робочі контактні дані представника постачальника, а також дані, що стосуються вподобань відвідувачів нашого веб-сайту щодо його перегляду.

«Обробка» має дуже широке визначення й по суті означає будь-які дії щодо Персональних даних або операції з ними (у тому числі просте збирання, зберігання, здійснення доступу або видалення).

Обробка Персональних даних

Компанія Graphic Packaging прагне дотримуватись прозорих процедур обробки персональних даних. Особи будуть проінформовані про те, які їхні Персональні дані збираються, навіщо вони збираються та як використовуватимуться, за допомогою чітких і лаконічних повідомлень про конфіденційність і механізмів надання згоди. Персональні дані можуть збиратися лише для конкретних, явних і законних цілей та не можуть далі оброблятися всупереч їм. Зміна цілей обробки допускається лише за згодою особи або іншим чином, як передбачено законом.

Graphic Packaging збирає лише ті Персональні дані, що необхідні для досягнення заявлених цілей, і не збирає надмірну або нерелевантну інформацію. Процеси збору даних включатимуть належні заходи безпеки для захисту даних від несанкціонованого доступу, розголошення, зміни й знищення.

Мінімізація даних, конфіденційність за задумом, зниження чутливості

Один із найкращих способів захистити конфіденційність особи — це взагалі не збирати її Персональні дані. Обробка Персональних даних, якими володіє Graphic Packaging, має бути справді необхідною для запланованої мети, і ми збиратимемо лише мінімальний об'єм таких даних, необхідний для досягнення цілей обробки. Іншими словами, ми ніколи не будемо збирати Персональні дані, які нам не потрібні.

Крім того, чіткою метою Graphic Packaging є впровадження нових програм, послуг і продуктів на основі принципів конфіденційності за задумом і конфіденційності за замовчуванням. Конфіденційність за задумом означає, що конфіденційність має враховуватися із самого початку й протягом усього життєвого циклу будь-якої системи, послуги, продукту, функції чи процесу, що вимагає проактивного застосування технологічних інновацій, визначення ризиків і їх пом'якшення на етапі планування та проектування, а також тривалого перегляду й переоцінки. Конфіденційність за замовчуванням означає, що кожна ІТ-система, послуга, продукт або метод ведення бізнесу в нашій організації налаштовані на захист Персональних даних. Це означає, що суб'єктам даних не потрібно вживати жодних додаткових заходів для захисту своєї конфіденційності, а параметри у відповідних системах мають бути за замовчуванням налаштовані на найбільший рівень захисту.

Graphic Packaging додатково мінімізує ризик розкриття даних, за можливості знижуючи чутливість інформації шляхом:

- зниження точності даних, що зберігаються після їх збору. Приміром, якщо номер телефону клієнта буде використано для статистичного аналізу, то зберігатиметься лише частина цифр, наприклад код міста.
- перетворення Персональних даних у менш конфіденційну форму. Наприклад, якщо для статистичного аналізу за IP-адресою клієнта визначається місцезнаходження, то IP-адресу буде видалено після зіставлення її з містом або селищем.

- обмеження доступу до великих обсягів Персональних даних. Наприклад, співробітники, яким потрібен доступ до окремих записів Персональних даних, не мають автоматично доступу до пакетів Персональних даних.

Ведення записів про обробку

Певні закони й нормативні акти вимагають від Graphic Packaging зберігати точні записи про те, як і навіщо Персональні дані використовуються, зберігаються й обробляються (такі записи про обробку даних і процес їхнього створення також відомі як зіставлення даних). Зокрема, записи про обробку даних мають містити категорії Персональних даних, які ми обробляємо, перелік відповідних постачальників товарів і послуг, яких ми використовуємо, цілі використання Персональних даних і будь-яку передачу таких Персональних даних за кордон (наприклад, постачальникам, зареєстрованим в інших країнах). Зіставлення даних є основоположним зобов'язанням Загального регламенту ЄС і Великої Британії із захисту даних (GDPR). Закони деяких штатів США про конфіденційність також зазвичай вимагають, щоб такі компанії, як Graphic Packaging, могли продемонструвати, як вони використовують Персональні дані, і за допомогою зіставлення даних можна легко задовольнити цю вимогу. Graphic Packaging прагне підтримувати точне, актуальне й вичерпне відображення даних.

Оцінка впливу на захист даних (DPIA) і ризики

Програма керування конфіденційністю в компанії Graphic Packaging спрямована на контроль і пом'якшення ризиків для конфіденційності. Ці ризики насамперед стосуються впливу обробки Персональних даних на особу, чиї дані обробляються Graphic Packaging. Це частина більш широкої оцінки бізнес-ризиків, яку проводить компанія Graphic Packaging.

Для забезпечення прозорості й контролю в тих юрисдикціях, де це вимагається, Graphic Packaging проводить оцінку впливу на конфіденційність (PIA) або оцінку впливу на захист даних (DPIA). PIA або DPIA проводяться в межах контрольного списку вимог щодо допуску відповідно до календаря реалізації проекту, якщо це вимагається згідно з політикою компанії Graphic Packaging або відповідними нормативно-правовими актами.

Терміни PIA і DPIA часто використовуються як взаємозамінні, але зазвичай DPIA стосується певних юридичних зобов'язань згідно з GDPR ЄС і Великої Британії, тоді як PIA часто стосується загальної оцінки ризиків для конфіденційності, яка проводиться відповідно до вимог певного закону про конфіденційність або у межах передового досвіду щодо запровадження програм із захисту конфіденційності. У компанії Graphic Packaging ми використовуємо термін PIA для позначення початкової оцінки ризику, яка виконується на OneTrust — нашому порталі відповідності нормативним вимогам, і за результатами якої визначається, чи потрібно проводити повну оцінку (DPIA).

Проведення DPIA є обов'язковим не для всіх проектів, які може реалізовувати Graphic Packaging. Згідно із законом DPIA вимагається тоді, коли проект може призвести до високого ризику для прав і свобод людей, зокрема, якщо використовуються нові технології.

Таким чином, DPIA — це, по суті, оцінка ризику, яка має враховувати характер, обсяг, контекст і цілі обробки Персональних даних, і має проводитися до початку такої обробки. Незалежно від того, чи конкретний проект, який реалізується Graphic Packaging, є внутрішнім, чи є процесом, продуктом або системою, які надаються третьою особою, DPIA слід розпочинати якомога раніше на стадії закупівлі чи розробки проекту, навіть якщо деякі роботи в межах проекту все ще не визначені.

Докладнішу інформацію можна знайти за посиланням на **Політику й процедуру проведення DPIA** компанії Graphic Packaging (DPIA Policy and Procedure): [Data Privacy Impact Assessment Policy](#).

Правові підстави обробки Персональних даних

Обробка персональних даних дозволяється лише у разі, якщо Graphic Packaging має для цього дійсну правову підставу. Існує кілька правових підстав для обробки Персональних даних. Важливо визначити правову підставу, яка буде використана для будь-якої обробки Персональних даних, до початку такої обробки.

У наших повідомленнях про конфіденційність буде зазначено правову підставу обробки Персональних даних для конкретних цілей. Щоб засвідчити відповідність чинним законам і нормам щодо конфіденційності даних, Graphic Packaging також має задокументувати рішення щодо того, на якій правовій підставі виконуються конкретні дії з обробки Персональних даних.

Типові правові підстави для обробки Персональних даних включають такі:

- **Згода.** Це коли фізична особа (суб'єкт даних) дала чітку згоду на обробку своїх Персональних даних для конкретної цілі. Згода повинна бути заявлена в письмовій формі або іншим способом, дозволеним законом, при цьому особа повинна бути заздалегідь проінформована про ціль такої обробки й будь-яке можливе передавання Персональних даних. Якщо заява про згоду включена до інших заяв особи, то для правильного розуміння вона має бути чітко виділена.
- **Договір.** Це коли обробка Персональних даних необхідна в межах договору, який Graphic Packaging укладає з іншою організацією чи особою.
- **Обов'язок, установлений законом.** Це коли обробка Персональних даних з боку Graphic Packaging необхідна для дотримання вимог закону (договірні зобов'язання сюди не входять).
- **Законні інтереси.** Це коли обробка Персональних даних необхідна для задоволення законних інтересів компанії Graphic Packaging або законних інтересів третьої особи, якщо немає вагомих причин для захисту Персональних даних, які переважають такі законні інтереси.

Безпека даних

Конфіденційність і дозвіл

Обробку персональних даних дозволяється проводити лише уповноваженим співробітникам компанії Graphic Packaging, які зобов'язані дотримуватися вимог щодо конфіденційності даних. Таким співробітникам забороняється використовувати Персональні дані для власних приватних цілей, передавати Персональні дані неуповноваженим особам або в будь-який інший неналежний спосіб робити їх доступними для неуповноважених осіб.

«Неуповноваженим» у цьому контексті вважається будь-який доступ або інше використання Персональних даних співробітниками поза межами їхніх професійних обов'язків. Зобов'язання щодо конфіденційності діють і після припинення трудових відносин.

Шифрування й псевдонімізація

Анонімізація або псевдонімізація Персональних даних використовується за можливості на ранній стадії та якщо їх вартість у відношенні до передбачуваної мети захисту є розумною. Можливість псевдонімізації досягається за допомогою збалансованого набору заходів, зокрема маскування (статичного та/або динамічного), токенизації та/або шифрування.

Регулярні аудити безпеки й тестування

Graphic Packaging проводить регулярні аудити й оцінки безпеки, щоб виявити вразливі місця, оцінити ризики й посилити заходи безпеки. Тестування на можливість проникнення й сканування вразливостей виконуються з метою проактивного виявлення й усунення потенційних слабких місць безпеки. Додаткову інформацію можна знайти в Політиці аудиту й оцінки нормативно-правової відповідності (Audit and Compliance Assessment Policy) за посиланням: [Audit and Compliance Assessment Policy](#).

Відстежування

Graphic Packaging залишає за собою право відстежувати поштовий та інтернет-трафік у межах, дозволених законом. Додаткову інформацію можна знайти в Політиці щодо прийнятного використання ресурсів (Acceptable Use of Assets Policy) за посиланням: [Acceptable Use of Assets Policy](#).

Соціальні мережі

Компанія Graphic Packaging визнає, що її співробітники використовують соціальні мережі. Компанія залишає за собою право відстежувати їхню діяльність у соціальних мережах в межах, дозволених законом, але при цьому вона також намагатиметься за можливості захищати конфіденційність співробітників. Докладнішу інформацію можна знайти в Політиці щодо прийнятного використання соціальних мереж (Acceptable Use of Social Networking Policy) за посиланням: [Acceptable Use of Social Networking Policy](#).

Керування мобільними пристроями (MDM)

Співробітники Graphic Packaging використовують мобільні пристрої, такі як смартфони й планшети. Graphic Packaging намагатиметься захищати Персональні дані там, де це можливо, і де дозволено використання цих пристроїв для особистих цілей. Додаткову інформацію можна знайти в таких політиках:

- Політика щодо управління ресурсами (Asset Management Policy) за посиланням: [Asset Management Policy](#)
- Політика щодо безпеки мобільних обчислень (Mobile Computing Security Policy) за посиланням: [Mobile Computing Security Policy](#)
- Політика щодо особистих пристроїв (Personally Owned Devices Policy) за посиланням: [Personally Owned Devices Policy](#)

Зберігання даних

Чим довше зберігаються Персональні дані, тим вище ймовірність випадкового розголошення, втрати, крадіжки та/або старіння інформації. Іншими словами, час є критично важливим фактором для порушення безпеки даних. Компанія Graphic Packaging має на меті зберігання Персональних даних

лише протягом мінімального періоду часу, потрібного для реалізації бізнес-цілей або через необхідність відповідності вимогам законодавства.

Будь-які персональні дані, які зберігає компанія Graphic Packaging, обробляються відповідно до Програми ведення діловодства, у якій зазначено, чому й протягом якого часу зберігаються дані, а також спосіб їх видалення з усіх сховищ даних.

Докладнішу інформацію можна знайти в Політиці щодо Програми ведення діловодства (Records Management Program Policy) компанії Graphic Packaging за посиланням: [Records Management Program Policy](#).

Права суб'єктів даних

Компанія Graphic Packaging прагне дотримуватися найвищих стандартів захисту даних і конфіденційності. Невід'ємним аспектом нашої прозорості й підзвітності є дотримання, визнання та повага до прав суб'єктів даних відповідно до чинних законів і правових норм про захист даних.

Спеціальні категорії та чутливі Персональні дані

Спеціальні категорії Персональних даних можуть включати інформацію про расове походження, сексуальну орієнтацію, політичні погляди, релігійні чи філософські переконання, громадянство й імміграційний статус, членство в профспілках, а також дані про здоров'я чи статеве життя. Така чутлива особиста інформація регулюється й обробляється відповідно до чинних місцевих законів про конфіденційність даних.

Залежно від контексту й джерела, обсягу та передбачуваного використання, інші дії з обробки Персональних даних у Graphic Packaging також можуть вважатися чутливими відповідно до оцінки ризику конфіденційності. Фінансова інформація в контексті адміністрування зарплати в Graphic Packaging, наприклад, вимагає додаткового захисту й контролю безпеки.

Докладнішу інформацію про класифікацію даних можна знайти в Політиці щодо класифікації інформації (Information Classification Policy) за посиланням: [Information Classification Policy](#).

Обмін даними й треті особи

Graphic Packaging може вирішити укласти договір із третьою особою щодо збору, зберігання або обробки даних, зокрема Персональних даних. Третя особа може пропонувати такі послуги як хостинг, аутсорсинг або обчислення в приватній чи загальнодоступній хмарі.

Якщо Graphic Packaging вирішить укласти договір із третьою особою на обробку Персональних даних, то до його укладання це питання має бути розглянуто Офісом управління ІТ-проектами (РМО). Після схвалення певної третьої особи для надання послуг з обробки даних відносини з такою третьою особою мають регулюватися письмовою угодою, в якій зазначаються права та обов'язки Graphic Packaging і субпідрядника. Має бути обраний той субпідрядник, який гарантуватиме застосування необхідних технологічних та організаційних заходів безпеки згідно з цією Політикою щодо конфіденційності, і надасть достатні гарантії щодо захисту Персональних даних і реалізації прав суб'єктів даних.

У договорі має бути прописаний обов'язок субпідрядника обробляти Персональні дані лише в межах такого договору і вказівок, виданих компанією Graphic Packaging. До будь-якого договору, пов'язаного з

обробкою Персональних даних, має бути укладена затверджена юридичним відділом Додаткова угода про захист даних. Обробка Персональних даних не може здійснюватися з будь-якою іншою метою. Graphic Packaging продовжує нести відповідальність за Персональні дані, які обробляються її контрагентом.

Повідомлення про порушення безпеки даних

Запобігання порушенню безпеки Персональних даних є обов'язком усіх співробітників і підрядників компанії Graphic Packaging. Крім того, кожному пропонується повідомити юридичного консультанта з питань конфіденційності, а у певних регіонах — уповноваженого з питань захисту даних — у разі виявлення порушень щодо обробки Персональних даних.

Положення щодо своєчасного виявлення, реагування, усунення й сповіщення (як регуляторних органів, так і потенційно постраждалих осіб) викладені в Політиці реагування на порушення безпеки даних (Data Breach Response Policy) компанії Graphic Packaging за посиланням: [Data Breach Response Policy](#) і в Політиці реагування на інциденти інформаційної безпеки (Security Incident Response Policy) за посиланням: [Security Incident Response Policy](#).

Транскордонне передавання даних

Передавання Персональних даних усередині компанії або за її межі має здійснюватися в безпечний спосіб із використанням затверджених протоколів і захищених каналів. Graphic Packaging дотримується відповідних законодавчих і нормативних вимог щодо транскордонного передавання даних і забезпечує застосування належного чинного механізму, перш ніж розпочати транскордонне передавання Персональних даних. Це включає забезпечення того, щоб усі договори, що Graphic Packaging укладає зі сторонніми постачальниками товарів чи послуг, які можуть обробляти Персональні дані від імені Graphic Packaging, відповідали застосовним законам і нормам про захист даних.

Відповідність законам і правилам

Graphic Packaging дотримується відповідних міжнародних, загальнодержавних і місцевих законів та норм, що регулюють обробку й захист Персональних даних, зокрема, але не виключно, GDPR ЄС, GDPR Великобританії, Загального закону Бразилії про захист даних, а також федеральних законів і законів штатів США про конфіденційність.

Навчання, обізнаність і забезпечення виконання

Graphic Packaging забезпечить дотримання загальних принципів, викладених у цій Політиці конфіденційності. Задля цього управлінський персонал Graphic Packaging має забезпечити виконання цієї Політики, яка передбачає, зокрема, надання співробітникам інформації про неї.

Співробітники також мають підтвердити своє розуміння цієї Політики конфіденційності й зобов'язання дотримуватися її.

Якщо необхідне додаткове навчання, слід подати запит до Комітету з питань конфіденційності. Інформація про Політику конфіденційності також має містити нагадування про те, що порушення її

загальних принципів може за певних обставин призвести до юридичних наслідків, таких як кримінальне покарання, фінансова відповідальність і наслідки для працевлаштування.

Уповноважений із питань захисту даних (DPO)

Graphic Packaging призначила загальнокорпоративного DPO для нагляду та забезпечення дотримання законів і норм щодо захисту даних. Якщо це можливо чи необхідно, Graphic Packaging також призначає регіональних DPO для виконання місцевих вимог щодо захисту даних. Контактна інформація DPO, зокрема, повне ім'я, посада й дані для зв'язку, надається особам для звернення з будь-якими проблемами, питаннями чи запитамі щодо захисту даних. DPO співпрацює з керівництвом, співробітниками й відповідними зацікавленими особами, щоб забезпечити комплексний підхід до захисту даних у всій компанії, і є контактною особою для запитів щодо захисту даних у Graphic Packaging.

Контроль редакцій

Дата	Опис змін	Автор
XX	XX	XX