Відділ закупівлі корпорації Майкрософт

Гарантування безпеки та конфіденційності для постачальників (SSPA) посібник із програми

Версія 8

Червень 2022

Вступ

Корпорація Майкрософт вважає право на дотримання конфіденційності – основним. Наша місія – надихати кожну людину та організацію у світі досягати більшого, ми щодня працюємо над тим, щоб заслуговувати на довіру наших клієнтів і постійно підтримувати її.

Суворі вимоги до конфіденційності та безпеки є вирішальними для нашої місії, суттєво важливими для підтримання довіри клієнтів, а в деяких країнах – ще й вимогою закону. Стандарти, встановлені політиками конфіденційності та безпеки корпорації Майкрософт, відображають наші корпоративні цінності. Ці стандарти поширюються також на наших постачальників (таких як ваша компанія), які оброблюють дані від імені корпорації Майкрософт.

Корпоративна програма Майкрософт із гарантування безпеки та конфіденційності для постачальників (Supplier Security and Privacy Assurance, далі – **SSPA**) передбачає основні настанови щодо обробки даних для наших постачальників у вигляді Вимог до захисту даних постачальниками корпорації Майкрософт (Data Protection Requirements, далі – **DPR**). Вони доступні на сторінці SSPA on Microsoft.com/Procurement. Зверніть увагу, що на постачальників можуть розповсюджуватися додаткові вимоги на рівні організації. Ці вимоги розробляються та комунікуються поза програмою SSPA групою Майкрософт, яка є відповідальною за взаємодію з постачальником.

Основні умови SSPA визначено в DPR. Додаткові відомості щодо програми дивіться у розділі Запитань і відповідей (FAQs). Крім того, ви можете звернутися до нашої глобальної команди, надіславши листа на адресу SSPAHelp@microsoft.com.

Огляд програми SSPA

SSPA – це спільна організована робота відділу закупівь (Procurement), зовнішніх корпоративних та юридичних справ (Corporate External Legal Affairs) і відділу корпоративної безпеки (Corporate Security) корпорації Майкрософт. Її мета – забезпечувати дотримання постачальниками принципів конфіденційності та безпеки даних.

Вимоги SSPA розповсюджуються на всіх постачальників, які оброблюють персональні та/або конфіденційні дані корпорації Майкрософт у зв'язку з виконанням своїх зобов'язань (наприклад надання послуг, ліцензій на програмне забезпечення, хмарних служб) відповідно до умов договору між постачальником і корпорацією Майкрософт (наприклад умов замовлення на придбання, основної угоди), (далі – **виконувати зобов'язання**, **виконує зобов'язання, виконання зобов'язань**).

SSPA дає змогу постачальнику вибрати профіль обробки даних, що відповідає продуктам і/або послугам, відповідно до умов договору. Залежно від вибору буде встановлено певні правила щодо забезпечення відповідності вимогам корпорації Майкрософт.

Усі зареєстровані постачальники щорічно виконуватимуть самоатестацію на відповідність DPR. Від вашого профілю обробки даних залежатиме обсяг застосовування DPR – усі або їх частина. Якщо постачальник оброблює дані, що за умовами корпорації Майкрософт становлять підвищений ризик, до нього можуть застосовувати додаткові вимоги, такі як: незалежна перевірка відповідності вимогам. Постачальникам, які входять до затвердженого списку підрядних обробників корпорації Майкрософт буде запропоновано пройти незалежну перевірку відповідності вимогам.

Важливо: За результатами перевірки визначається статус SSPA: «Зелений» (відповідає вимогам) або «Червоний» (не відповідає вимогам). Засобами закупок Майкрософт у всіх постачальників перевіряється наявність «Зеленого» статусу в межах програми SSPA, перед тим як розпочати взаємодію з постачальником.

Схема процесу SSPA. Реєстрація нового постачальника

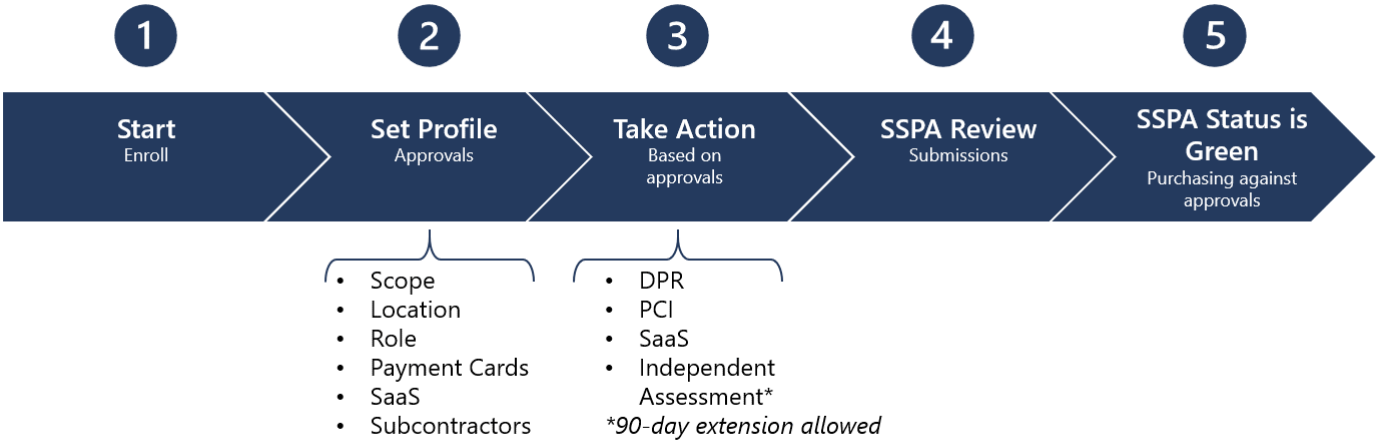
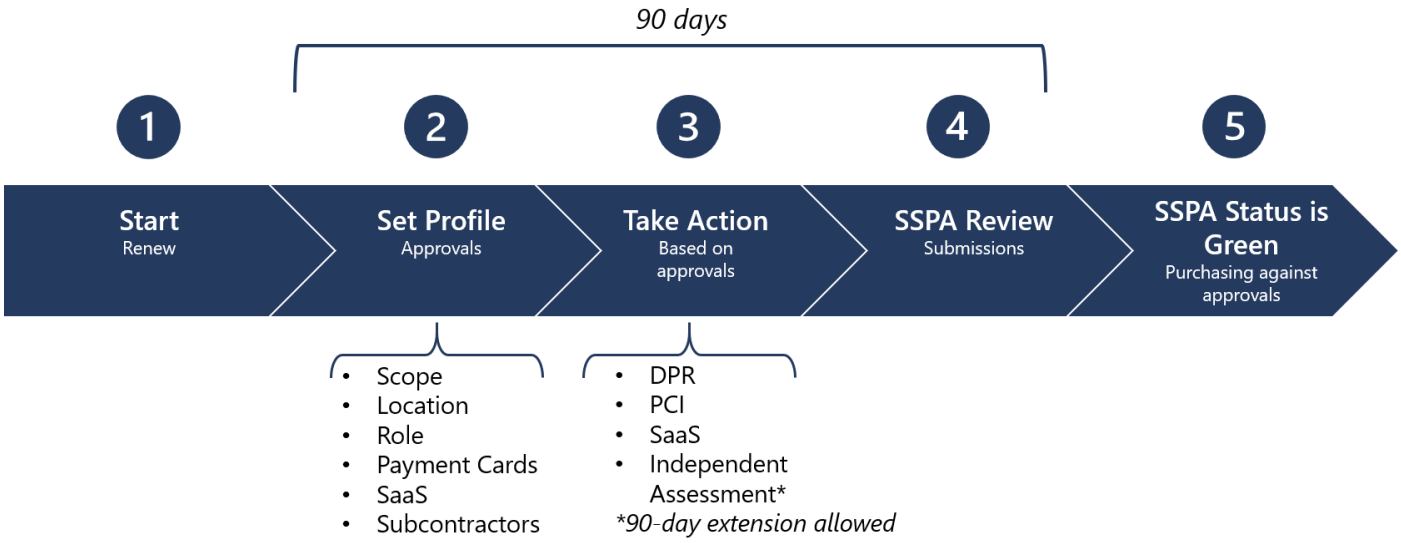


Схема процесу SSPA. Щорічне оновлення статусу постачальника



Обсяг програми SSPA

Щоб визначити, чи оброблює ваша компанія (постачальник) персональні та/або конфіденційні дані корпорації Майкрософт, ознайомтесь з переліком прикладів у наведених нижче таблицях. Зверніть увагу, що список не є вичерпним.

Примітка. Беручи до уваги конфіденційність даних, що оброблюються, представник Майкрософт може запросити реєстрацію, що не передбачена даним списком.

Персональні дані за типом даних

Приклади (список не є вичерпним):

Конфіденційні дані
дані, що стосуються дітей
генетичні, біометричні дані та інформація про стан здоров’я
расове або етнічне походження
політичні, релігійні або філософські погляди, та належність до таких груп
членство у профспілках
статеве життя або сексуальна орієнтацію особи
імміграційний статус (віза, дозвіл на роботу тощо)

дані документів, що посвідчують особу (паспорт, водійські права, віза, номери соціального захисту, персональний ідентифікаційний код)
дані про точне місцезнаходження користувача (у межах 300 метрів)
номери персональних банківських рахунків
номер кредитної карти та термін її дії
Дані, які публікує або якими користується клієнт
документи, фотографії, відео, музика тощо
відгуки та/або оцінки, залишені щодо продукту або послуги
відповіді в опитуваннях
історія пошуку, інтереси та вподобання
висловлювання в рукописному, друкованому та усному форматі (голосовий/аудіо пошук і/або чат/бот)
облікові дані (паролі, підказки паролів, ім’я користувача, біометричні дані, що використовуються для ідентифікації)
дані клієнтів щодо звернень до служб підтримки
Отримувані та створені дані
неточні дані про розташування
IP-адреса
параметри пристроїв і персоналізації
використання служб для відстеження відвідувань веб-сайтів, веб-сторінок
дані із соціальних мереж, профілів сторінок у них
дані про дії, отримані з підключених пристроїв, наприклад для фітнесу
контактні дані, такі як: ім’я, адреса, номер телефону, адреса електронної пошти, дата народження та екстрені контакти
дані з оцінки шахрайства та ризиків, перевірка минулих даних
відомості про страхування, пенсійне забезпечення та пільги
резюме кандидатів, записи та відгуки зі співбесід
Metadata and telemetry
Дані рахунків
дані платіжних інструментів
номер кредитної карти та термін її дії
інформація про банківські перекази

номер банківського рахунку
відомості заявок на кредитні кошти та про кредитні лінії
податкові документи та ідентифікаційні номери
відомості про інвестиції та витрати
дані корпоративних карток
Псевдонімізовані дані користувачів (ідентифікатори, створені корпорацією Майкрософт для ідентифікації користувачів продуктів і послуг Майкрософт)
глобальні унікальні ідентифікатори (GUID)
номер карти користувача чи унікальні ідентифікатори (PUID)
гешовані ідентифікаційні дані користувачів (EUII)
ідентифікатори сеансів
ідентифікатори пристроїв
діагностичні дані
дані журналів
Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Конфіденційні дані Майкрософт за класом

Приклади (список не є вичерпним):

Висококонфіденційні
Інформація, що стосується або пов’язана з розробкою, тестуванням, випуском продуктів Майкрософт або їх компонентів ***Продукти Майкрософт*** *– це програмне забезпечення, онлайн сервіси або обладнання корпорації Майкрософт, реалізовані будь-яким каналом збуту*
маркетингові матеріали щодо пристроїв Майкрософт, що не були опубліковані
нерозголошені фінансові дані корпорації Майкрософт, на які розповсюджуються правила Комісії з цінних паперів і бірж США (SEC)

Конфіденційні
ліцензійні ключі продуктів, надані від імені корпорації Майкрософт для поширення будь-яким способом
інформація щодо розробки й тестування внутрішніх бізнес-програм Майкрософт (LOB)
неопубліковані маркетингові матеріали корпорації Майкрософт, призначені для програмного забезпечення та служб Майкрософт, наприклад Office, SQL, Azure тощо
написана від руки, електронна або надрукована документація стосовно продуктів або послуг Майкрософт, наприклад пристроїв (посібники з експлуатації та процедур, дані конфігурації тощо)

Важливо: корпорація Майкрософт може вимагати реєстрацію, якщо дані, які оброблює постачальник, не передбачено в цьому переліку.

Профіль обробки даних

Постачальникам корпорації Майкрософт надається контроль над своїми профілями обробки даних SSPA.

Це дає їм змогу вирішувати, на які типи взаємодій необхідне право для здійснення діяльності. Приділіть особливу увагу вибору та врахуйте дії необхідні для відповідності вимогам, щоб отримати затвердження. **Дивіться розділ «Вимоги щодо гарантії» нижче та Додаток А.**

Робочі групи Майкрософт зможуть контактувати з постачальниками лише в тому випадку, якщо діяльність з обробки даних відповідає погодженням, що були отримані постачальником.

За відсутності відкритих завдань постачальники зможуть оновити свій профіль з обробки даних будь-коли протягом року. Після внесення змін буде визначено відповідні дії, які необхідно виконати для отримання затвердження. Наявні завершені затвердження будуть застосовуватися, допоки не буде виконано нові встановлені вимоги.

Якщо щойно виконані завдання не будуть завершені протягом дозволеного 90-денного терміну, статус SSPA зміниться на «Червоний» (не відповідає вимогам), а рахунок може бути деактивовано в платіжних системах корпорації Майкрософт (Microsoft Accounts Payable).

Затвердження для обробки даних	
1	Область обробки даних ▪ Конфіденційні ▪ Персональні, конфіденційні
2	Місце обробки даних ▪ В корпорації Майкрософт або у клієнта ▪ У постачальника

3	Роль для обробки даних ▪ Контролер (незалежний або співконтролер) ▪ Обробник ▪ Підрядний обробник (призначений корпорацією Майкрософт)
4	Обробка даних платіжних карт ▪ Так ▪ Не застосовується
5	Програмне забезпечення як послуга ▪ Так ▪ Не застосовується
6	Залучення субпідрядників ▪ Так ▪ Не застосовується

Положення щодо затвердження

Область обробки даних

Конфіденційні дані

Цей профіль необхідно обирати для затвердження, якщо діяльність постачальника передбачає обробку лише конфіденційних даних корпорації Майкрософт.

Обираючи цей профіль затвердження, ви не матимете права на обробку персональних даних.

Персональні, конфіденційні дані

Цей профіль необхідно обирати для затвердження, якщо діяльність постачальника передбачає обробку персональних і конфіденційних даних корпорації Майкрософт.

Місце обробки

В корпорації Майкрософт або у клієнта

Цей профіль необхідно обирати для затвердження, якщо виконання зобов'язань постачальника передбачає обробку даних у мережованому середовищі Майкрософт, де співробітники використовують облікові дані *@microsoft.com* для доступу, або в середовищі клієнта Майкрософт.

Не обирайте цей варіант за наведених нижче умов:

- Якщо постачальник працює з офшорною установою (OF), що призначена корпорацією Майкрософт.
- Якщо постачальник надає ресурси корпорації Майкрософт, які час від часу використовуються в мережі Майкрософт і поза її межами. Місце обробки даних поза мережею визначається як обробка у постачальника.

У постачальника
Якщо умова «в корпорації Майкрософт або у клієнта» (як описано вище) не може бути застосована, оберіть цей варіант.

_____

Роль обробки даних

Контролер (розповсюджуються на незалежних контролерів і співконтролерів)

Цей профіль необхідно обирати для затвердження, якщо **всі** умови здійснюваних зобов'язань постачальника відповідають визначенню ролі контролера з обробки даних (див. DPR).

Обравши це затвердження, ви не матимете права на обробку персональних даних із зазначенням ролі «Обробник». Якщо постачальник має обидві ролі – обробника й контролера даних Майкрософт, не слід вибирати роль «Контролер», оберіть – «Обробник».

Обробник

Це найпоширеніша роль з обробки, яка надає змогу постачальникам оброблювати дані від імені корпорації Майкрософт. Перегляньте визначення терміну «Обробник» в DPR.

Підрядний обробник

Підрядний обробник – це третя сторона, яку корпорація Майкрософт залучає до діяльності з обробки персональних даних Майкрософт, при виконанні якої Майкрософт виступає в ролі обробника. Постачальники не можуть себе ідентифікувати як підрядні обробники в Майкрософт через те, що це потребує попереднього узгодження внутрішніми групами із конфіденційності. Постачальники виступають підрядними обробниками лише в тих випадках, коли корпорація Майкрософт виконує роль обробника даних, а постачальник оброблює відповідні типи персональних даних, що відповідають вимогам корпорації. Підрядні обробники можуть мати додаткові вимоги до контракту та відповідності вимогам, що містять Додаток про захист даних і незалежне оцінювання (див. нижче).

Обробка даних платіжних карт

Цей профіль необхідно обирати для затвердження, якщо будь-яка частина даних, які оброблює постачальник від імені корпорації Майкрософт, містить відомості про оплату за допомогою кредитних або інших платіжних карт.

Це затвердження надає право постачальнику брати участь в операціях з обробки даних платіжних карт.

_____

Програмне забезпечення

Відділ закупівлі корпорації Майкрософт направляє покупців на процес прийому для всіх покупок програмного забезпечення, що включає різні перевірки, в тому числі SSPA для прийняття рішення чи підпадає під дію управління SSPA постачальник, що

надає програмне забезпечення. (Щоб дізнатися більше інформації, покупці Майкрософт можуть переглянути етапи, розміщені на внутрішній сторінці ProcureWeb Software and Cloud Service). Якщо SSPA необхідний, постачальникам також може знадобитися впевнитися, що обрано профіль "Програмне забезпечення як послуга" (SaaS). Для зареєстрованих постачальників SSPA це можна зробити під час заповнення профілю з обробки даних на порталі відповідності постачальників корпорації Майкрософт (Microsoft Supplier Compliance Portal).

Для дотримання цілей SSPA, SaaS розглядають в широкому сенсі, включно з платформою як послугою (PaaS) та інфраструктурою як послугою (IaaS). (Щоб дізнатися більше про SaaS, будь ласка, див. це пояснення.)

Програмне забезпечення як послуга (SaaS)

Програмне забезпечення як послуга (SaaS) дозволяє користувачам підключатися до хмарних програм і використовувати їх через Інтернет.

Корпорація Майкрософт визначає **Програмне забезпечення як послугу (SaaS)** як програмне забезпечення на основі загального коду, що використовується в моделі «один для багатьох» на основі оплати за використання , або як передплата залежно від показників використання. Постачальник хмарних послуг розробляє та обслуговує хмарне програмне забезпечення, забезпечує автоматичне оновлення програмного забезпечення та робить програмне забезпечення доступним для своїх клієнтів через інтернет за принципом «один для багатьох» за принципом оплати за використання. Цей метод надання програмного забезпечення та ліцензування дозволяє отримати доступ до програмного забезпечення онлайн через оформлення передплати, а не купувати та встановлювати на кожному окремому комп'ютері.

Примітка: Більшості постачальників SaaS потрібно буде додати погодження субпідрядника на порталі відповідності постачальників корпорації Майкрософт (Microsoft Supplier Compliance Portal). Це необхідно в разі розміщення персональних або конфіденційних даних Майкрософт на платформі третьої сторони.

Використання субпідрядників

Цей профіль необхідно обирати для затвердження, якщо постачальник користується послугами субпідрядників для виконання своїх зобов'язань (див. визначення в DPR).

Це поняття також охоплює Фрілансерів (див. DPR).

Вимоги щодо гарантії

Вимоги залежно від затвердженого профілю

За затверджуваним профілем обробки даних в SSPA оцінюється ступінь ризику, який постачальник може становити в процесі обробки даних корпорації Майкрософт. Вимоги щодо відповідності умовам SSPA відрізняються залежно від затверджень профілів постачальників. У цьому розділі докладно описано різні вимоги програми SSPA.

Існують також комбінації дій, які можуть збільшити або зменшити обсяг вимог до відповідності стандартам. Ці дії наведено в Додатку А. Ви можете виконати їх на порталі відповідності постачальників при заповненні свого профіль. Ви завжди можете перевірити відповідність вашого сценарію вимогам, надіславши команді SSPA запит на перевірку.

Потрібні дії. Знайдіть свій профіль затвердження в Додатку А і перегляньте вимоги щодо забезпечення відповідності, а також відповідні варіанти незалежної перевірки відповідності, якщо такі доступні.

Важливо: якщо в своєму профілі ви обираєте такі варіанти як: SaaS, субпідрядники, хостинг веб-сайту або платіжні карти - вимагається проходження додаткової перевірки відповідності вимогам.

Самоатестація на відповідність DPR

Усім постачальникам, зареєстрованим у програмі SSPA, необхідно виконати самоатестацію на відповідність DPR протягом 90 днів після отримання запиту. Цей запит надсилається щорічно. Якщо профіль обробки даних буде оновлюватися протягом року, то запит буде надіслано додатково. Статус SSPA рахунків постачальників стане «Червоним» (не відповідає вимогам) після завершення 90-денного терміну. Нові замовлення на придбання не оброблюватимуться, доки не буде отримано «Зелений» статус SSPA (відповідає вимогам).

Щоб розпочати роботу, нові зареєстровані постачальники мають виконати вимоги за вибраними затвердженнями й отримати «Зелений» статус SSPA (відповідає вимогам).

Важливо: Команда програми SSPA не має повноважень подовжувати це завдання.

Уповноважені представники, які будуть проходити самоатестацію, повинні отримати достатньо інформації від галузевих експертів, щоб обдумано виконати всі вимоги. Крім того, реєструючи своє ім’я у формі участі в програмі SSPA, особа цим підтверджує, що вона прочитала та розуміє DPR. Постачальники завжди можуть додати в онлайн-інструмент контактні дані інших осіб, які допомагатимуть їм із виконанням вимог.

Уповноважений представник (див. визначення в DPR) має такі обов’язки:

1. Визначати, які вимоги застосовуються;

2. Надавати відповіді на кожну застосовувану вимогу;

3. Підписати та надіслати атестаційні дані на Порталі відповідності постачальників корпорації Майкрософт.

Застосовність

Постачальники мають відповідати всім застосовуваним вимогам DPR, установленим відповідно до профілю обробки даних. Деякі вказані вимоги можуть не застосовуватися до товарів або послуг, які постачальник надає корпорації Майкрософт. У них буде позначка «не застосовується» з обґрунтуванням, що будуть перевірені спеціалістами програми SSPA.

Команда SSPA перевіряє всі надіслані дані DPR щодо вибраних умов із позначками «не застосовується», «конфлікт з місцевим законодавством» або «договірний конфлікт» для встановлених вимог. Команда SSPA може витребувати додаткові відомості щодо одного вибраного пункту й більше. Конфлікти з місцевим законодавством та договірні конфлікти враховуються лише при наданні додаткових документів і якщо конфлікт не викликає сумнівів.

Вимоги до незалежного оцінювання

Щоб дізнатися докладні відомості про затвердження обробки даних, які вимагають виконання цієї вимоги, див. розділ вимог за затвердженнями в Додатку А.

Постачальники можуть змінювати затверджені види діяльності й оновлювати профілі обробки даних. Однак, якщо постачальник має роль «Підрядний обробник», він не може змінити це погодження та зобов'язаний проходити незалежне оцінювання щорічно.

Щоб отримати затвердження, що потребують незалежної перевірки відповідності вимогам, постачальнику потрібно вибрати незалежного аудитора, який перевірить його на дотримання DPR. Аудитор має підготувати дорадчий лист для надання корпорації Майкрософт підтвердження щодо відповідності вимогам. Цей лист повинен бути безумовно позитивним, всі невідповідності вимогам необхідно вирішити та усунути до надсилання даного листа-підтвердження на Портал відповідності постачальників корпорації Майкрософт на перевірку команді SSPA. Аудитори повинні завантажити затверджений шаблон листа, що додається до PDF-документу «рекомендовані аудитори», що доступний тут.

У **Додатку А** зазначено дозволені альтернативні варіанти сертифікацій, якщо ви вирішите не залучати незалежного аудитора для перевірки відповідності DPR, за умови, що це прийнятно (наприклад для постачальників SaaS, хостингу веб-сайтів або постачальників, які працюють із субпідрядниками). В основі відповідностей DPR використано стандарти ISO 27701 (конфіденційність) та ISO 27001 (безпека).

Якщо постачальник є постачальником медичних послуг на території США чи організацією, що підпадає під їх юрисдикцію, ми приймемо звіт HITRUST для забезпечення конфіденційності та безпеки.

За обставин, що потребують додаткової обачності, SSPA може провести незалежне оцінювання силами власних спеціалістів. Це стосується запитів щодо збереження конфіденційності або забезпечення захисту даних від відповідальних відділів, перевірки виправлення порушень безпеки даних або вимоги щодо автоматизованого виконання прав суб'єкта даних.

Рекомендації щодо виконання цієї вимоги:

1. Процедуру має виконувати аудитор із достатнім рівнем технічної підготовки та спеціальними знаннями для належного оцінювання відповідності вимогам.
2. Аудитор має бути членом Міжнародної федерації бухгалтерів (International Federation of Accountants - IFAC) або Американського інституту сертифікованих присяжних бухгалтерів (American Institute of Certified Public Accountants - AICPA), або мати сертифікати інших організацій із питань безпеки та конфіденційності, наприклад

Міжнародної асоціації фахівців з питань конфіденційності (International Association of Privacy Professionals - IAPP) або Асоціації аудиту та контролю інформаційних систем (Information Systems Audit and Control Association - ISACA).

3. Аудитор має керуватися актуальною версією DPR, яка містить обов'язкове підтвердження відповідності кожній вимозі. **Постачальники повинні надати аудитору свої останні затверджені відповіді атестації на відповідність DPR.**
4. Для нещодавно зареєстрованих постачальників аудитор перевірить схему роботи засобів керування процесами. У всіх інших випадках аудитор перевірить ефективність засобів керування.
5. Область перевірки обмежена персональними та/або конфіденційними даними корпорації Майкрософт, які постачальник обробляє для виконання своїх зобов'язань.
6. Процедура обмежується всіма операціями з обробки відповідних даних, вказаних для номера облікового запису постачальника, який отримав запит. Якщо постачальник вирішив оцінити кілька облікових записів одночасно**, лист атестації має містити перелік облікових записів постачальників, що включені до оцінювання, та відповідні адреси.**

Лист, надісланий до SSPA, не повинен містити жодних тверджень щодо невідповідності постачальника вимогам з обробки даних (DPR). Всі невідповідності необхідно вирішити до надсилання листа.

У системі SSPA доступний список рекомендованих аудиторів. Ці компанії мають досвід із проведення оцінювання SSPA. Послуги аудиторів оплачують постачальники. Вартість залежатиме від обсягу та області обробки даних.

Вимоги до сертифікації за стандартом PCI DSS

Стандарт безпеки даних у галузі платіжних карт (Payment Card Industry Data Security Standard, PCI DSS) – це основний документ, що дає змогу запровадити надійний процес гарантування безпеки даних платіжних карт і передбачає профілактику, виявлення інцидентів, пов'язаних із безпекою, і належне реагування на них. Цю систему розробила Рада з питань стандартів безпеки в галузі платіжних карт (PCI Security Standards Council) – організація, яка встановлює правила ведення діяльності у своїй галузі. Метою вимог PCI DSS є визначення технології та усунення вразливих місць, які становлять загрозу для безпеки даних власника карти, що оброблюється.

Корпорація Майкрософт має дотримуватися цих стандартів. Якщо постачальник виконує обробку інформації платіжних карт від імені корпорації Майкрософт, ми вимагаємо доказового дотримання цих стандартів. Щоб отримати роз'яснення щодо вимог, встановлених організацією в галузі PCI, зверніться до Ради з питань стандартів безпеки в галузі платіжних карт.

Залежно від обсягів транзакцій, що повинні бути обробленими, постачальник повинен пройти або кваліфіковану аудиторську перевірку відповідності вимогам або заповнити форму самостійної атестації.

Емітенти платіжних карт зазвичай встановлюють порогові значення для типу оцінювання:

- Рівень1: надання сертифіката PCI DSS від стороннього аудитора, що провів оцінювання.
- Рівень 2 або 3: надання анкети самооцінювання (Self-Assessment Questionnaire (SAQ) на відповідність стандартам PCI DSS, підписаної посадовою особою постачальника.

Надішліть відповідний сертифікат, що відповідає вимогам PCI.

Вимога для SaaS

Постачальники, що підпадають під визначення SaaS, що міститься в профілі обробки даних, можуть бути зобов'язані надати дійсний сертифікат ISO 27001, якщо це передбачено Договором з хмарних послуг Майкрософт (Microsoft Cloud Services Agreement).

SSPA спеціалісти підтвердять, що ваша заявка відповідає контрактним зобов'язанням.

Будь ласка, не надсилайте сертифікат центру обробки даних. Ми очікуємо сертифікат ISO 27001 щодо надання послуг програмного забезпечення, зазначених у вашому контракті з Майкрософт.

Залучення субпідрядників

Корпорація Майкрософт вважає участь субпідрядників у роботі фактором високого ризику. Постачальники зобов'язані повідомляти корпорацію Майкрософт про залучення третіх сторін для обробки персональних та/або конфіденційних даних Майкрософт та надати відомості про цих субпідрядників. Крім того, постачальник повинен надати відомості про країни, де будуть оброблюватись особисті дані.

Порушення при обробці даних

За наявності порушень, пов'язаних із конфіденційністю або безпекою даних, постачальники повинні повідомляти про них корпорацію Майкрософт відповідно до процедури, визначеної в DPR.

Повідомте про порушення обробки даних, використовуючи SupplierWeb або надіславши листа на електронну пошту SuppIR@microsoft.com

У листі вкажіть наведені нижче дані:

- Дата порушення конфіденційності та безпеки даних:
- Назва постачальника:
- Номер постачальника:
- Контактні дані представників Майкрософт, яких слід сповістити:
- Пов'язане замовлення на придбання, якщо застосовано/доступно:
- Опис порушення при обробці даних:

Додаток A

Вимоги залежно від затвердженого профілю

#	Профіль	Вимоги до забезпечення відповідності	Варіанти незалежної перевірки відповідності
1	**Область**: персональні, конфіденційні дані **Місце обробки:** у Майкрософт чи у клієнта **Роль з обробки:** обробник або контролер **Клас даних:** конфіденційні **або** висококонфіденційні **Платіжні карти:** не застосовуються **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинг веб-сайту:** не застосовується	Самоатестація на відповідність DPR	
2	**Область:** конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** не застосовується **Клас даних:** конфіденційні **Платіжні карти:** не застосовуються **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинг веб-сайту:** не застосовується	Самоатестація на відповідність DPR	

#	Профіль	Вимоги до забезпечення відповідності	Варіанти незалежної перевірки відповідності
3	**Область:** конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** обробник **Клас даних:** висококонфіденційні **Платіжні карти:** не застосовуються **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинг веб-сайту:** не застосовується	Самоатестація на відповідність DPR ***та*** незалежна перевірка відповідності вимогам	Варіанти незалежної перевірки відповідності вимогам: 1. Заповнення форми незалежного оцінювання у відповідності до DPR, **або** 2. Надання сертифікації ISO 27001
4	**Область:** персональні, конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** обробник **Клас даних:** висококонфіденційні **Платіжні карти:** не застосовуються **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинг веб-сайту:** не застосовується	Самоатестація на відповідність DPR ***та*** незалежна перевірка відповідності вимогам	Варіанти незалежної перевірки відповідності вимогам: 1. Проходження незалежного оцінювання у відповідності до DPR, 2. Незалежне оцінювання у відповідності до Секцій A-I DPR та ISO 27001 **або** 3. Надання сертифікації ISO 27701 **та** ISO 27001
5	**Область:** персональні, конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** обробник **Клас даних:** конфіденційні **Платіжні карти:** не застосовуються **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинг веб-сайту:** не застосовується	Самоатестація на відповідність DPR	

#	Профіль	Вимоги до забезпечення відповідності	Варіанти незалежної перевірки відповідності
6	**Область:** персональні, конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** контролер **Клас даних:** висококонфіденційні або конфіденційні **Платіжні карти:** не застосовується **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинг веб-сайту:** не застосовується	Самоатестація на відповідність DPR	
7	**Область:** персональні, конфіденційні дані **Місце обробки:** будь-де **Роль з обробки:** підрядний обробник (ця роль визначена корпорацією Майкрософт – в профілі буде зазначено: «Затвердження підрядного обробника: Так» (“Subprocessor Approval: Yes”) **Клас даних:** висококонфіденційні або конфіденційні **Платіжні карти:** не застосовуються **SaaS:** не застосовується **Залучення субпідрядників:** не застосовується **Хостинги веб-сайту:** не застосовується	Самоатестація на відповідність DPR ***та*** незалежна перевірка відповідності вимогам	Варіанти незалежної перевірки відповідності вимогам: 1. Проходження незалежного оцінювання у відповідності до DPR, 2. Незалежне оцінювання у відповідності до Секцій A-I DPR та ISO 27001 **або** 3. Надання сертифікації ISO 27701 **та** ISO 27001

#	Профіль	Вимоги до забезпечення відповідності	Варіанти незалежної перевірки відповідності
Наслідки додавання SaaS, субпідрядників, хостингу веб-сайту			
8	**Область:** персональні, конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** обробник **Клас даних:** висококонфіденційні або конфіденційні **Платіжні карти:** не застосовуються **Залучення субпідрядників:** ТАК або **SaaS:** ТАК або **Хостинги веб-сайту:** ТАК	Самоатестація на відповідність DPR ***та*** незалежна перевірка відповідності вимогам	Варіанти незалежної перевірки відповідності вимогам: 1. Проходження незалежного оцінювання у відповідності до DPR, 2. Незалежне оцінювання у відповідності до Секцій A-I DPR та ISO 27001 **або** 3. Надання сертифікації ISO 27701 **та** ISO 27001
9	**Область:** персональні, конфіденційні дані **Місце обробки:** у постачальника **Роль з обробки:** контролер **Клас даних:** високонфіденційні або конфіденційні **Платіжні карти:** не застосовуються **Залучення субпідрядників:** ТАК або **SaaS:** ТАК або **Хостинги сайту:** ТАК	Самоатестація на відповідність DPR	

#	Профіль	Вимоги до забезпечення відповідності	Варіанти незалежної перевірки відповідності
Додаткова перевірка відповідності для платіжних карт та SaaS			
10	Будь-який з вказаних вище профілів та **платіжні карти**	Відповідність вищевказаним вимогам **і** галузевим стандартам платіжних карт	Надайте сертифікацію PCI DSS
11	Будь-який з вказаний вище профілів та **SaaS**	Відповідність вищевказаним вимогам і надання сертифікації ISO 27001, з описом функціональних служб, відповідно до умов договору	Надайте сертифікат ISO 27001 з описом функцій, що надаються службами