Вимоги до захисту даних постачальниками корпорації Майкрософт

Застосування

Вимоги до захисту даних постачальниками корпорації Майкрософт («**Вимоги**») застосовуються до кожного постачальника корпорації Майкрософт, що обробляє особисті або конфіденційні дані корпорації Майкрософт у зв'язку з виконанням постачальником своїх зобов'язань (наприклад, наданням послуг, ліцензій на програмне забезпечення, хмарних послуг) відповідно до умов договору між цим постачальником і корпорацією Майкрософт (наприклад, умови замовлення на придбання, основною угодою) («**виконувати**», «**зобов'язання**» або «**виконання зобов'язань**»).

- У разі виникнення протиріч між цими Вимогами і вимогами, що вказані в угодах між постачальником і корпорацією Майкрософт, перевагу матимуть ці Вимоги, якщо постачальник не зазначить інше положення в договорі, що замінює відповідну вимогу щодо захисту даних (у цьому випадку перевагу матимуть положення договору).
- У разі виникнення протиріч між вимогами, наведених у цьому документі, з вимогами будь-якого закону або статуту, перевагу мають юридичні чи законодавчі вимоги.
- Якщо постачальник корпорації Майкрософт виступає контролером, до нього може бути застосований скорочений перелік даних Вимог.
- Якщо постачальник корпорації Майкрософт обробляє лише конфіденційні дані Майкрософт, а не -особисті, до нього можуть бути застосовані скорочений перелік Вимог.

Міжнародна передача даних

Не обмежуючи свої інші зобов'язання, постачальник зобов'язується не здійснювати будь-яку міжнародну передачу персональних даних Майкрософт без попереднього письмового погодження зі сторони корпорації Майкрософт. У будь-якому випадку постачальник має дотримуватися Вимог щодо захисту даних, зокрема стандартних договірних положень, або, на розсуд корпорації Майкрософт, інших відповідних механізмів транскордонного передавання даних, які затвердив відповідний орган із захисту даних або Європейська Комісія в залежності від ситуації; які прийняті або з якими погодилася корпорація Майкрософт. Стандартні договірні положення, прийняті (i) Європейською Комісією або прийняті Європейським наглядовим органом із захисту даних та схвалені Європейською Комісією, (ii) Сполученим Королівством згідно з Загальним федеральним законом Великобританії про захист даних, (iii) Швейцарією згідно з федеральним законом про захист даних Швейцарії, або (iv) положеннями, що регулюють міжнародну передачу персональних даних, офіційно прийнятими урядом у юрисдикції, що не є юрисдикцією Швейцарії, Великобританії або не входять до складу Європейського Союзу або Європейської економічної зони, мають бути включені й бути юридично обов'язковими для постачальника на дату їх прийняття. Постачальник також повинен забезпечити дотримання цих положень усіма учасниками процесу (як визначено в стандартних договірних положеннях).

Основні визначення

Нижче вказано визначення термінів, що використовуються в цих Вимогах. Перелік прикладів, зазначених у цих Вимогах, який наведено після слів «в тому числі», «зокрема», «наприклад» або подібних слів, слід тлумачити із значенням «без обмежень» або «але не виключно», крім випадків, коли відсутні уточнюючі слова, такі як: «тільки» або «виключно». Інші визначення наведено в глосарії наприкінці цього документа.

«**Контролер**» означає юридичну особу, яка визначає мету й значення обробки персональних даних. Поняття також охоплює підприємство, контролера (відповідно до визначення в GDPR) та еквівалентні терміни, зазначені в законах про захист даних, залежно від контексту.

«Файли cookie» — невеликі текстові файли, які зберігаються на пристроях веб-сайтами та/або програмами; містять інформацію, що використовується для розпізнавання суб'єкта даних або пристрою.

«**Порушення безпеки даних**» означає (1) порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розголошення або доступу до персональних або конфіденційних даних Майкрософт, що передаються, зберігаються або іншим чином обробляються постачальником або його субпідрядниками, або (2) уразливість системи безпеки, що пов'язана з обробкою постачальником персональних або конфіденційних даних Майкрософт.

«**Суб'єкт даних**» — це фізична особа, яку можна ідентифікувати прямо або опосередковано, зокрема за допомогою ідентифікатора, наприклад імені, ідентифікаційного номера, даних про розташування, онлайн-ідентифікатора або одного чи декількох факторів, характерних для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної або соціальної ідентичності цієї особи.

«**Право суб'єкта даних**» означає право суб'єкта на отримання, видалення, редагування та експорт особистих даних корпорації Майкрософт, обмеження доступу до них або заперечення проти такої обробки, як це передбачено законом.

«**Закон**» означає всі застосовані закони, правила, статути, укази, рішення, накази, постанови, вироки, кодекси, правові акти, резолюції та вимоги будь-яких державних органів (федеральних, штатних, місцевих чи міжнародних) з відповідною юрисдикцією.
«**Протизаконний**» означає будь-яке порушення закону.

«**Конфіденційні дані корпорації Майкрософт**» – будь-яка інформація, розкриття якої внаслідок порушення конфіденційності або цілісності може завдати корпорації Майкрософт значних репутаційних або фінансових збитків. До них належать обладнання та програмне забезпечення корпорації Майкрософт, внутрішні бізнес-програми, попередні версії маркетингових матеріалів, ліцензійні ключі продуктів, а також технічна документація щодо продуктів і послуг корпорації Майкрософт.

«**Персональні дані корпорації Майкрософт**» — будь-які персональні дані, що обробляються корпорацією Майкрософт або від її імені.

«**Персональні дані**» — будь-яка інформація, що стосується суб'єкта даних, і будь-яка інша інформація, що охоплюється поняттям «персональні дані» або «особиста інформація» відповідно до закону.

«**Обробка**» — будь-яка операція або сукупність операцій, що виконуються з персональними або конфіденційними даними корпорації Майкрософт, за допомогою автоматизованих засобів або без них, зокрема збирання, записування, упорядкування, структурування, зберігання, адаптація або внесення змін, отримання, використання для довідки або інших цілей, розкриття через передавання, розповсюдження або надання доступу до інформації іншим способом, групування або комбінування, обмеження доступу, видалення або знищення. Терміни «обробка» й «оброблений» мають відповідні значення.

«**Обробник**» означає юридичну особу, що обробляє персональні дані від імені іншої юридичної особи, в тому числі постачальника послуг, обробника (згідно з терміном, зазначеним у GDPR) та еквівалентні терміни, що використовуються в законах про захист даних, залежно від контексту.

«**Субпідрядник**» — третя сторона, якій постачальник делегує свої зобов'язання відповідно до договору, що охоплює їх виконання, в тому числі дочірнє підприємство постачальника, яке не укладає додаткові договори безпосередньо з корпорацією Майкрософт.

«**Підрядний обробник**» — це третя сторона, яку корпорація Майкрософт зобов'язує виконувати дію, коли таке виконання передбачає обробку персональних даних Майкрософт, щодо яких корпорація Майкрософт виступає обробником.

Відповідні дії постачальника

Постачальники повинні щороку засвідчувати відповідність наведеним Вимогам, використовуючи онлайн-службу під керівництвом корпорації Майкрософт. Детальніше про те, як здійснюється управління перевіркою відповідності вимогам, вказано в Посібнику програми SSPA.

#	Вимоги до захисту даних постачальниками корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ А. Управління	
1	Кожна чинна угода між корпорацією Майкрософт і постачальником (наприклад, генеральний договір, технічне завдання, замовлення на поставку та інші замовлення) містить відповідні положення щодо захисту конфіденційності та безпеки конфіденційних і персональних даних корпорації Майкрософт, залежно від того, що застосовано, зокрема положення щодо заборони продажу персональних даних корпорації Майкрософт і їх обробку поза прямими діловими відносинами між корпорацією Майкрософт і постачальником. Для компаній, що виступають обробниками або підрядними обробниками персональних даних корпорації Майкрософт у зв'язку з виконанням ними своїх зобов'язань, в угоді має бути вказано предмет, тривалість, характер і мету обробки, тип персональних даних корпорації Майкрософт і категорії суб'єктів даних, а також зобов'язання й права корпорації Майкрософт.	Постачальник повинен надати відповідний договір між корпорацією Майкрософт і постачальником. В чинних угодах з обробниками й підрядними обробниками повинні бути зазначені описи процедур обробки (наприклад, у технічному завданні, замовленні на придбання). Примітка: для компаній, що здійснюють оперативні замовлення на постачання, можлива додача необхідного опису видів процедур обробки на більш пізньому етапі процедури закупівлі.
2	Якщо Майкрософт підтверджує, що ви виконуєте роль підрядного обробника даних, постачальник повинен мати чинні угоди про захист прав, укладені з Майкрософт. Примітка: Майкрософт опублікує інформацію про це призначення у вашому профілі, якщо це буде застосовано.	Стандартні договірні положення, додаток про дані замовників в режимі онлайн та/або додаток щодо обробки даних постачальників і партнерів професійних послуг.
3	Призначте відповідального та підзвітного співробітника (чи групу осіб) в компанії, задля виконання цих Вимог до захисту даних.	Призначте роль відповідальній особі або групі осіб, яким доручено забезпечувати дотримання Вимог до захисту даних постачальником корпорації Майкрософт. Документ з описом повноважень і обов'язків цієї особи або групи, що підтверджує їх роль у системі забезпечення конфіденційності та/або безпеки.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ А. Управління (продовження)	
4	Постачальник має створити, підтримувати й проводити щорічне навчання з питань конфіденційності й безпеки для співробітників, які матимуть доступ до персональних даних, обробку яких здійснює постачальник у зв'язку з виконанням своїх зобов'язань щодо збереження конфіденційності даних корпорації Майкрософт. Якщо ваша компанія не має готових матеріалів, можете скористатися цим загальним сценарієм навчальних заходів і адаптувати його до власних потреб. Примітка: персоналу постачальника може знадобитися проходження додаткового навчання, що проводиться підрозділами корпорації Майкрософт.	Наявність щорічних звітів відвідування навчальних занять. Підрядник має надавати їх корпорації Майкрософт на вимогу. Навчальні матеріали повинні охоплювати опис принципів конфіденційності та безпеки. Документи навчальної підготовки у відповідності Вимогам мають містити дані, що підтверджують проходження навчання щодо вимог до забезпечення конфіденційності; зобов'язань щодо забезпечення безпеки, дотримання вимог чинних договорів і зобов'язань.
5	Постачальник зобов'язується оброблювати персональні дані корпорації Майкрософт лише у відповідності до задокументованих інструкцій корпорації Майкрософт, зокрема сценаріїв передавання персональних даних корпорації Майкрософт до іншої країни або міжнародній організації, за винятком випадків, коли це забороняється законодавчими нормами. В такому випадку обробник або підрядний обробник (постачальник) повинен повідомити контролера (корпорацію Майкрософт) про цю законодавчу вимогу до обробки, якщо закон не забороняє повідомляти таку інформацію за важливих підстав, що становлять суспільний інтерес.	Постачальник має дотримуватися всіх задокументованих інструкцій корпорації Майкрософт (наприклад, угод, технічних завдань або документації до замовлення), зберігати їх в електронному вигляді, і забезпечити вільний доступ до них співробітникам постачальника й підрядникам, залученим до виконання зобов'язань.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ B. Повідомлення	
6	Постачальник зобов'язується застосовувати Декларацію корпорації Майкрософт про конфіденційність під час збору персональних даних від імені корпорації Майкрософт. Повідомлення про конфіденційність має бути зрозумілим і доступним для суб'єктів даних, щоб вони могли прийняти рішення щодо передачі своїх персональних даних постачальнику. Примітка: якщо ваша компанія виступає контролером дій з обробки, ви повинні опублікувати власне повідомлення про забезпечення конфіденційності.	Постачальник використовує найновішу версію Декларації корпорації Майкрософт про конфіденційність, актуальна версія якої опублікована за посиланням fwdlink. Декларація про конфіденційність публікується у будь-якому разі, при зборі персональних даних користувача. В разі необхідності може бути використана версія в режимі офлайн, вона надається перед збором даних. Будь-які заяви про конфіденційність, що використовуються в режимі офлайн, мають бути актуальними опублікованими версіями за чинною датою. Для надання послуг працівниками Майкрософт використовується Microsoft Data Privacy Notice (Повідомлення про захист даних корпорації Майкрософт).
7	Під час збору персональних даних корпорації Майкрософт за допомогою звичайного голосового дзвінка чи з використанням попередньо записаних повідомлень, постачальники мають бути готовими роз'яснити суб'єктам даних методи збору, обробки, використання й зберігання відповідних даних.	Надання розшифровки записаних голосових повідомлень включно з описом способів обробки персональних даних корпорації Майкрософт, зокрема: ▪ збір, ▪ використання, і ▪ зберігання.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ С. Вибір і надання згоди	
8	За можливості постачальник повинен отримати та задокументувати згоду суб'єкта даних на всі дії з обробки (зокрема на будь-які нові та оновлені види дій з обробки), перш ніж збирати його персональні дані. Постачальник повинен відстежувати ефективність обліку переваг для забезпечення термінів реагування на зміни таких переваг, що відповідають більш жорстким вимогам місцевого законодавства.	Постачальник повинен бути в змозі продемонструвати, як суб'єкт даних надає згоду на дії з обробки даних, і що така згода охоплює всі види діяльності з обробки персональних даних суб'єкта. Постачальник повинен бути в змозі продемонструвати, як суб'єкт даних відкликає згоду на процедуру обробки даних. Постачальник має бути в змозі продемонструвати, як перевіряються параметри перед запуском нової дії з обробки. Примітка: доказом можуть виступати знімки з екрану взаємодії з користувачем, експерименти із послугою або технічна документація, яку можна переглянути.
9	Постачальники, які створюють та контролюють веб-сайти та/або програми для корпорації Майкрософт, чи сайти, що мають оформлення бренду Майкрософт; повинні надати суб'єктам даних зрозуміле повідомлення щодо використання файлів cookie, відповідно до зобов'язань, зазначеними в Декларації про конфіденційність Майкрософт і вимогами місцевого законодавства. Постачальники мають використовувати стандартний банер, розроблений 1ES, для відображення можливості вибору для суб'єктів, за винятком випадків, якщо інше не затребувано іншою стороною договору. Ця вимога застосовується, якщо цільові користувачі веб-сайтів знаходяться в Європейському Союзі/Європейській економічній зоні чи в інших регіонах з чинними законами щодо конфіденційності та скрізь, де використовується Декларація про конфіденційність Майкрософт. Примітка: компанії-спонсори Майкрософт повинні зареєструвати веб-сайти Майкрософт на внутрішньому порталі з дотримання вимог щодо роботи в інтернеті (http://aka.ms/wcp) для інвентаризації файлів cookie й керування ними.	Призначення кожного файлу cookie необхідно задокументувати, крім того, потрібно вказати тип, що використовується. ▪ Постійні файли cookie не слід використовувати, якщо достатньо файлів cookie сеансу. ▪ У разі використання постійних файлів cookie термін їх придатності не може перевищувати 13 місяців з моменту останнього відвідування сайту користувачем. Необхідно перевірити відповідність чинним законам ЄС, зокрема: ▪ положення про конфіденційність має бути позначено стандартним підписом «Конфіденційність і файли cookie»; ▪ отримання схвальної згоди користувача перед використанням файлів cookie з «несуттєвою» метою, наприклад для відображення реклами; і ▪ забезпечення терміну дії згоди або повторного запиту на таку згоду не може перевищувати 6 місяців.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ D. Збір	
10	Постачальник зобов'язується відстежувати збір персональних і/або конфіденційних даних корпорації Майкрософт, щоб упевнитися, що збираються лише ті дані, що необхідні для виконання зобов'язань.	Постачальник має надавати документацію для підтвердження того, що зібрані персональні та/або конфіденційні дані корпорації Майкрософт необхідні для виконання зобов'язань. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
11	Перед збором даних від неповнолітніх (згідно чинного законодавства) постачальник має отримати згоду, відповідно до місцевих законів щодо конфіденційності.	Постачальник може надати документацію на підтвердження отримання згоди від батька/матері/опікуна. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
	Розділ E. Зберігання	
12	Забезпечте зберігання персональних і конфіденційних даних корпорації Майкрософт не довше, ніж це необхідно для виконання зобов'язань, за виключенням випадків, коли більший термін зберігання персональних і/або конфіденційних даних корпорації Майкрософт вимагається законом.	Постачальник повинен дотримуватися задокументованих політик зберігання або вимог до зберігання даних, що зазначені корпорацією Майкрософт у договорі (наприклад, у технічному завданні або в замовленні на придбання). Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
13	На власний розсуд корпорації Майкрософт її персональні й конфіденційні дані, що знаходяться у володінні постачальника або під його контролем, повинні бути повернуті в Майкрософт або знищені після виконання зобов'язань чи на вимогу корпорації. У програмах необхідно передбачити процеси, що гарантуватимуть, безпечне знищення даних за командою користувача або автоматично, наприклад через сплив певного часу, видалятимуться без можливості відновлення. Якщо потрібно знищити персональні чи конфіденційні дані корпорації Майкрософт, постачальник має спалити, розтрощити або розрізати на дрібні частки фізичні носії цих даних у такий спосіб, щоб інформацію не можна було прочитати або відновити.	Необхідно документувати утилізацію персональних і конфіденційних даних корпорації Майкрософт (це може передбачати повернення даних корпорації Майкрософт для подальшого знищення). Якщо необхідно знищити дані або корпорація Майкрософт надіслала запит на знищення, слід надавати сертифікат про знищення, підписаний відповідальною особою постачальника.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ F. Суб’єкти даних	
	Суб’єкти даних мають певні законні права, зокрема права доступу до своїх персональних даних, їх видалення, змінення й експорт, обмеження доступу до них і право висувати заперечення щодо їх обробки («**Права суб’єкта даних**»). Для реалізації прав суб’єкта у відповідності до законодавства щодо персональних даних корпорації Майкрософт, постачальник зобов’язаний дати змогу Майкрософт виконати зазначені нижче дії або виконати їх від імені корпорації:	
14	За можливості надавати допомогу корпорації Майкрософт технічними й організаційними засобами при виконанні зобов’язань щодо реагування на запити від суб’єктів даних, які прагнуть реалізувати свої права, без необґрунтованих затримок. Якщо корпорація Майкрософт не надала інших указівок, постачальник зобов’язується направляти всіх суб’єктів даних, які звертаються до нього з питань реалізації своїх прав, безпосередньо до Майкрософт.	Постачальник має зберігати докази щодо документування процесів і процедур з дотримання прав суб’єктів даних. Постачальник має зберігати задокументовані підтвердження тестування. Ці документи мають бути надані на вимогу корпорації Майкрософт.
15	Надаючи відповідь безпосередньо суб’єкту даних або в межах роботи механізму самообслуговування, постачальник має передбачити процеси й процедури ідентифікації суб’єкта даних, який робить запит.	У постачальника повинен бути задокументований метод ідентифікації суб’єктів даних Майкрософт. Постачальник має надавати задокументовані підтвердження на вимогу корпорації Майкрософт.
16	Якщо корпорація Майкрософт просить знайти персональні дані про суб’єкт даних, недоступних через онлайн-механізм самообслуговування, постачальник має докласти розумних зусиль для пошуку потрібних даних, а також зробити й зберігати відповідні записи на підтвердження того, що було здійснено такий пошук.	Постачальник зобов’язується документувати й зберігати підтвердження процедур, щоб підтвердити наявність персональних даних корпорації Майкрософт, надавати ці документи на вимогу корпорації Майкрософт. Постачальник має документувати вжиті заходи на виконання запитів щодо реалізації прав суб’єкта даних, і зберігати ці записи. У цих документах має бути вказано: ▪ дата й час запиту; ▪ дії, виконані у відповідь на запит, запис про інформування корпорації Майкрософт. Постачальник має надати підтвердження ведення таких записів на вимогу корпорації Майкрософт.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ F. Суб’єкти даних (продовження)	
17	Постачальник зобов’язується повідомляти суб’єкта даних про порядок дій, які має виконати особа, щоб отримати доступ до своїх персональних даних корпорації Майкрософт; або реалізувати, пов’язані з такими даними, права в інший спосіб.	Постачальник має зберігати документальні підтвердження комунікацій й виконання процедур доступу до персональних даних корпорації Майкрософт. Постачальник має зберігати задокументовані свідчення й надавати їх на вимогу корпорації Майкрософт.
18	Постачальник повинен реєструвати дату й час запитів на здійснення прав суб’єктів даних, а також дії, що були виконані постачальником у відповідь на ці запити. Якщо постачальник відхилить запит за вказівкою корпорації Майкрософт, він має надати суб’єкту даних письмове пояснення. Постачальник має надавати записи про запити суб’єкта даних на вимогу корпорації Майкрософт.	Постачальник повинен вести облік запитів на отримання доступу/видалення й документувати зміни, що внесені до персональних даних Майкрософт. Постачальник повинен документувати випадки відхилення запитів, а також зберігати докази того, що питання було розглянуто й затверджено корпорацією Майкрософт. Постачальник повинен надавати підтвердження про отримані й відхилені запити на доступ до персональних даних корпорації Майкрософт.
19	Постачальник має надати корпорації Майкрософт або самостійно отримати копії запитаних персональних даних корпорації Майкрософт для суб’єкта даних, який пройшов аутентифікацію, у відповідному друкованому, електронному або усному форматі.	Постачальник має надавати суб’єкту даних персональні дані корпорації Майкрософт у зрозумілому форматі й у формі, зручній для суб’єкта даних і постачальника.
20	Постачальник повинен вжити необхідних заходів безпеки, щоб запобігти використанню персональних даних корпорації Майкрософт, що надаються їй або автентифікованому суб’єкту даних, для ідентифікації іншої особи.	Постачальник має документувати підтвердження процедур, що використовуються як запобіжні заходи, для уникнення ідентифікації особи суб’єкта даних всупереч умовам угоди. Постачальник має надавати документальне підтвердження на вимогу корпорації Майкрософт.
21	Якщо суб’єкт даних вважає, що його персональні дані Майкрософт є неповними або неточними, постачальник зобов’язаний передати це питання на розгляд корпорації Майкрософт, та сприяти усуненню розбіжностей в разі необхідності.	Постачальник повинен документувати випадки розбіжностей й передавати питання на розгляд корпорації Майкрософт. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ G. Субпідрядники	
	Якщо постачальник має намір залучити субпідрядників до обробки персональних або конфіденційних даних корпорації Майкрософт, постачальник повинен:	
22	Постачальник має повідомити корпорацію Майкрософт перш ніж оформити надання послуг субпідрядника або ініціювати будь-які зміни щодо додавання або заміни субпідрядників. Примітка: вкажіть, що згодні з цим зобов'язанням, навіть якщо зараз не залучаєте субпідрядників, але можете зробити це згодом.	Підтвердьте, що персональні дані корпорації Майкрософт оброблюють лише компанії, що відомі корпорації Майкрософт згідно з умовами чинного договору (наприклад, технічного завдання, додатка, замовлення на придбання) або зазначені в базі даних SSPA. Постачальник може опублікувати перелік своїх субпідрядників онлайн і додати посилання в базу даних SSPA.
23	Постачальник зобов'язується документувати характер і обсяг персональних і конфіденційних даних корпорації Майкрософт, які оброблюють субпідрядники, для гарантії того, що збирається лише інформація, необхідна для виконання зобов'язань.	Постачальник повинен вести документацію щодо розкриття або передавання субпідрядникам персональних і конфіденційних даних корпорації Майкрософт. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
24	Якщо корпорація Майкрософт виступає контролером персональних даних, переконайтеся, що субпідрядник використовує персональні дані корпорації Майкрософт відповідно до заявлених контактних параметрів суб'єкта даних.	Постачальник має бути в змозі продемонструвати, як субпідрядники використовують контактні параметри суб'єкта даних. Необхідно надати супровідну документацію (наприклад знімок екрана, угоду про рівень обслуговування (SLA), технічне завдання), де вказано проміжок часу для впровадження змін параметрів субпідрядником.
25	Постачальник зобов'язується обмежити обробку персональних даних корпорації Майкрософт субпідрядником, крім випадків, коли це необхідно для виконання умов договору постачальника з корпорацією Майкрософт.	Постачальник має бути в змозі надати документацію на підтвердження того, що персональні дані корпорації Майкрософт, надані субпідряднику, необхідні для виконання зобов'язань. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ G. Субпідрядники (продовження)	
26	Постачальник повинен розглядати скарги на ознаки будь-якої несанкціонованої або незаконної обробки персональних даних корпорації Майкрософт.	Постачальник має бути в змозі продемонструвати наявність систем і процесів для розгляду скарг, що стосуються несанкціонованого використання або розкриття персональних даних корпорації Майкрософт субпідрядником. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
27	Постачальник повинен негайно повідомляти корпорацію Майкрософт, якщо стає відомо, що субпідрядник оброблює персональні або конфіденційні дані корпорації Майкрософт із будь-якою іншою метою, аніж задля виконання умов договору.	Постачальник має надати субпідряднику інструкцію та засоби для повідомлення про неправомірне використання даних корпорації Майкрософт. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
28	Якщо постачальник збирає персональні дані третіх сторін за дорученням корпорації Майкрософт, постачальник має підтвердити, що політики й методи захисту даних третіх сторін відповідають контракту між постачальником і корпорацією Майкрософт та цим Вимогам.	Постачальник має надавати документацію про належне виконання зобов'язань щодо політик і методів захисту даних третіх сторін. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
29	Постачальник зобов’язаний своєчасно вживати заходів щодо усуненню фактичної або потенційної шкоди, спричиненої несанкціонованою або незаконною обробкою субпідрядником персональних і конфіденційних даних корпорації Майкрософт.	Постачальник має документувати й зберігати підтвердження виконання плану та процедур і надавати їх на вимогу корпорації Майкрософт.
	Розділ H. Якість	
30	Постачальник зобов’язаний підтримувати цілісність усіх персональних даних корпорації Майкрософт, забезпечувати їх точність, повноту й відповідність при обробці в заявлених цілях.	Постачальник має бути в змозі підтвердити виконання процедур з перевірки персональних даних корпорації Майкрософт під час їх збору, створення й оновлення. Постачальник має бути в змозі підтвердити виконання процедур моніторингу та вибірки, щоб перевіряти точність на постійній основі та, за потреби, вносити виправлення. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ I. Моніторинг і примусові дії	
31	Постачальник повинен мати план реагування, що зобов’язує його сповістити корпорацію Майкрософт якомога раніше відповідно до умов договору, без необґрунтованих затримок (залежно від того, що станеться раніше), про випадки порушення безпеки даних, що стали йому відомі. Постачальник повинен на запит або за вказівкою корпорації Майкрософт співпрацювати з нею в будь-якому розслідуванні, щоб пом’якшити або усунути наслідки порушення безпеки даних, зокрема надавати корпорації Майкрософт дані, інформацію, доступ до свого персоналу або обладнання, необхідних для проведення експертної перевірки. Примітка: ознайомтеся з SSPA Program Guide (Керівництво з програми SSPA) для того, щоб дізнатися як сповістити корпорацію Майкрософт про порушення безпеки даних.	У постачальника має бути план реагування на випадки порушення безпеки даних, що передбачає сповіщення клієнтів (корпорації Майкрософт), як описано в цьому розділі. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
32	Постачальник має виконати план усунення наслідків і відстежувати усунення наслідків кожного разу при порушенія безпеки даних для забезпечення своєчасного вжиття належних коригуючих заходів	Постачальник зобов'язаний документувати й зберігати процедури реагування на випадки порушення безпеки даних до їх закриття. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.
33	Постачальник має затвердити офіційну процедуру реагування на всі скарги щодо захисту даних, пов’язаних з персональними даними корпорації Майкрософт, якщо їх контролером виступає корпорація Майкрософт.	Постачальник повинен мати засоби отримання скарг, пов’язаних із персональними даними корпорації Майкрософт, і задокументована процедура реагування на ці скарги. Постачальник має надавати документальні підтвердження на вимогу корпорації Майкрософт.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека	
	Постачальник повинен розробити, впровадити та підтримувати виконання програми інформаційної безпеки, що складається з політик і процедур із захисту та безпечного зберігання персональних і конфіденційних даних корпорації Майкрософт відповідно до належної галузевої практики та вимог чинного законодавства. Програма безпеки постачальника повинна відповідати стандартам, зазначеним нижче у пунктах 34–50.	Розділ J можна замінити чинним сертифікатом ISO 27001. Для цього зверніться до представництва SSPA. Примітка: ви повинні будете надати сертифікат.
34	Постачальник повинен проводити щорічне оцінювання безпеки мережі, яке передбачає: ▪ аналіз суттєвих змін середовища, таких як додавання нового компонента системи, зміна топології мережі чи правил брандмауера, ▪ проведення сканувань на наявність вразливостей, і ▪ ведення журналів змін.	Постачальник повинен документувати оцінювання мережі, журнали змін і результати сканувань. Журнали змін є обов'язковими і в них повинні бути зареєстрованими зміни, інформація щодо їхніх причин; а також ім'я та посада призначеної особи, яка затвердила зміни.
35	Постачальник повинен визначити, повідомити й запровадити політику щодо мобільних пристроїв, що убезпечує та обмежує використання персональних чи конфіденційних даних корпорації Майкрософт або отримання доступу до них на мобільних пристроях.	Постачальник повинен продемонструвати використання відповідної політики дозволених мобільних пристроїв, якщо для обробки персональних або конфіденційних даних корпорації Майкрософт потрібне використання мобільних пристроїв.
36	Постачальник повинен вести облік всіх ресурсів, що використовуються для виконання зобов'язань, а також вказувати ідентифікованого власника цих ресурсів. Постачальник несе відповідальність за інвентаризацію цих інформаційних ресурсів; встановлення прийнятного та дозволеного використання ресурсів; забезпечення належного рівня захисту ресурсів протягом їхнього життєвого циклу.	Постачальник повинен інвентаризувати пристрої, що використовуються для виконання зобов'язань. Інвентарний опис цих ресурсів має містити такі дані: ▪ розташування пристрою; ▪ класифікацію даних на ресурсі; ▪ запис про повернення ресурсу після припинення трудових відносин або завершення дії ділової угоди; і ▪ запис про ліквідацію носія для зберігання даних, якщо він більше не потрібен.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека (продовження)	
37	Постачальник зобов'язується встановити й підтримувати процедури керування правами доступу для перешкоджання несанкціонованому доступу до будь-яких персональних або конфіденційних даних корпорації Майкрософт, що контролюються постачальником.	Постачальник повинен засвідчити впровадження плану керування правами доступу, що містить: ▪ процедури керування доступом, ▪ процедури ідентифікації, ▪ процедури блокування доступу після кількох невдалих спроб отримати його, ▪ впровадження надійних параметрів для вибору облікових даних автентифікації, ▪ деактивацію облікових записів користувачів протягом 48 годин за умови припинення трудових відносин, ▪ ефективні засоби контролю надійності паролів шляхом визначення потрібної довжини, складності й запобігання повторному використанню. Постачальник має засвідчити наявність усталеного процесу нагляду за доступом користувачів до персональних і конфіденційних даних корпорації Майкрософт, забезпечивши виконання принципу найменших повноважень. Цей принцип передбачає наступне: ▪ чітко визначені ролі користувачів; ▪ процедури нагляду за доступом до ролей і обґрунтування схвалення такого доступу; ▪ постачальник повинен переконатися, що користувачі, яким призначено ролі з доступом до даних корпорації Майкрософт, мають документально підтверджені підстави на перебування у відповідній групі або ролі.
38	Постачальник повинен визначити й виконувати процедури керування виправленнями, що передбачають визначення пріоритетів виправлень безпеки для систем, що використовуються для обробки персональних або конфіденційних даних корпорації Майкрософт. Ці процедури містять: ▪ чітко визначений підхід з оцінки ризиків для визначення пріоритетності виправлень, пов'язаних із безпекою, ▪ можливість регулювати та впроваджувати екстрені виправлення, ▪ можливість застосовувати процедури до операційної системи й серверного програмного забезпечення (ПЗ), наприклад сервер програм і ПЗ баз даних,	Постачальник має засвідчити наявність впровадженої процедури керування виправленнями, що відповідає цим Вимогам й охоплює щонайменше зазначені нижче дії: ▪ призначення ступеня важливості для визначення пріоритетності (визначення рівнів важливості повинно бути задокументовано); ▪ документування процедури впровадження екстрених виправлень; ▪ перевірка того, що операційні системи, що більше не підтримуються компаніями-авторами, вилучені з користування; ▪ реєстрація дій по керуванню виправленнями з відстеженням затверджень і винятків.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека (продовження)	
	▪ документування ризиків, які зменшують виправлення, і відстеження будь-яких винятків, ▪ створення вимог щодо припинення використання ПЗ, що більше не підтримує компанія-власник.	
39	Постачальник повинен встановити антивірусне програмне забезпечення і ПЗ для захисту від зловмисних програм на обладнання, що підключене до мережі, використовується для обробки персональних і конфіденційних даних корпорації Майкрософт, зокрема на сервери, робочі і навчальні настільні комп'ютери, для захисту від потенційно шкідливих вірусів і зловмисних програм. Постачальник повинен оновлювати антивірусне програмне забезпечення щоденно або згідно з указівками постачальника ПЗ для захисту від вірусів або зловмисних програм. Примітка: ця вимога стосується всіх операційних систем, зокрема Linux.	Постачальник повинен документувати використання антивірусного ПЗ і ПЗ для захисту від зловмисних програм. Примітка: ця вимога стосується всіх операційних систем.
40	Постачальники, що розробляють ПЗ для корпорації Майкрософт, повинні дотримуватися принципів безпеки за проектом під час створення.	Документи постачальника з технічними характеристиками повинні містити пункти з перевірки безпеки під час циклів розробки.
41	Постачальник має застосовувати програму попередження втраті даних («**DLP**») для запобігання вторгненням, втраті даних або іншій несанкціонованій діяльності. Дані мають бути належним чином класифіковано, позначено й захищено, а постачальник повинен відстежувати інформаційні системи, що використовуються та у яких оброблюються персональні або конфіденційні дані корпорації Майкрософт, на наявність вторгнень, втрати даних або іншої несанкціонованої діяльності. Програма DLP вимагає наявності щонайменше таких процедур: ▪ використання стандартних галузевих серверних, мережевих і хмарних систем виявлення втручання («**IDS**») у разі зберігання персональних або конфіденційних даних корпорації Майкрософт, ▪ упровадження вдосконалених систем захисту від втручання («**IPS**») для відстеження й активного зупинення втрати даних,	Програма DLP повинна бути задокументована з встановленими процедурами щодо запобігання втручанням, втратам та іншим несанкціонованим діям (принаймні з усіма елементами, вказаними в цьому розділі).

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека (продовження)	
	▪ у разі порушення системи захисту вимагається проведення аналізу системи, щоб усунути будь-які вразливі місця, що залишилися, ▪ документування обов'язкових процедур моніторингу роботи інструментів, що виявляють порушення конфіденційності систем, ▪ встановлення процесів реагування на порушення безпеки даних і керування ними, якщо безпеку даних порушено, ▪ інформування (усіх працівників постачальника й підрядників, непов'язаних із виконанням зобов'язань постачальника) про наслідки несанкціонованого завантаження та використання персональних або конфіденційних даних корпорації Майкрософт.	
42	Постачальник повинен невідкладно повідомляти вище керівництво й корпорацію Майкрософт про результати розслідування, проведеного в межах реагування на порушення безпеки даних.	Постачальник повинен впровадити системи й процеси для передавання корпорації Майкрософт результатів розслідування в межах реагування на порушення безпеки даних.
43	Системні адміністратори, працівники, менеджери й треті особи повинні проходити щорічне навчання з вимог безпеки.	Постачальник повинен запровадити навчальну програму з вимог безпеки, зокрема: ▪ щорічне навчання з реагування на порушення безпеки даних; і ▪ імітацію подій і застосування автоматизованих механізмів, що сприяють ефективному реагуванню на критичні ситуації; ▪ постачальник повинен організувати розповсюдження інформації для профілактики порушення безпеки даних, наприклад відомостей про ризики, пов'язані з завантаженням зловмисних програм.
44	Постачальник зобов'язаний переконатися, що процеси планування резервного копіювання захищають персональні й конфіденційні дані корпорації Майкрософт від несанкціонованого використання, доступу, розкриття, змінення та знищення.	Постачальник повинен документально засвідчити оформлені процедури реагування й відновлення з докладним описом, як саме компанія буде діяти у випадку подій, що порушують звичайний порядок роботи, і як будуть підтримуватись заздалегідь визначений рівень інформаційної безпеки відповідно до завдань із забезпечення безперервного захисту інформації, затверджених керівництвом. Постачальник повинен засвідчити наявність визначених і впроваджених процедур періодичного резервного копіювання, безпечного зберігання й ефективного відновлення критично важливих даних.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека (продовження)	
45	Постачальник повинен запровадити та випробувати плани забезпечення безперервних бізнес-процесів і аварійного відновлення.	План аварійного відновлення має передбачати: ▪ чітко визначені ознаки критичної системи для діяльності постачальника; ▪ складений за встановленими ознаками перелік критичних систем, які потрібно відновлювати у випадку аварії; ▪ опис процедур аварійного відновлення для кожної критичної системи, які б гарантували, що спеціаліст, якому незнайома система, зможе відновити роботу програми не довше ніж за 72 години; ▪ постачальник має запровадити щонайменше раз на рік випробовування й перегляд планів аварійного відновлення для перевірки можливості його виконання.
46	Постачальник має встановлювати справжність фізичної особи до надання їй доступу до персональних або конфіденційних даних корпорації Майкрософт і забезпечувати можливість доступу лише з метою виконання покладених на неї зобов'язань.	Постачальник має забезпечити унікальність усіх ідентифікаторів користувачів. Кожен ідентифікатор повинен відповідати стандартному способу автентифікації, наприклад за допомогою Azure Active Directory. Слід передбачити отримання доступу з розширеними правами (адміністративні чи інші типи прав) лише за умови використання двофакторної перевірки, наприклад з використанням смарт-картки або автентифікації за допомогою телефону. Задокументована програма інформаційної безпеки повинна гарантувати, що всі працівники постачальника й субпідрядники отримують доступ до персональних або конфіденційних даних корпорації Майкрософт лише для потреб у межах виконання зобов'язань.
47	Постачальник зобов'язаний забезпечити захист всіх даних, що оброблюються у зв'язку з виконанням ним зобов'язань, під час їх передачі мережами, використовуючи протокол шифрування на основі Transport Layer Security («**TLS**») або Internet Protocol Security («**IPsec**»). Відповідні способи захисту описано в стандартах NIST 800-52 та NIST 800-57. Можна також застосовувати еквівалентні галузеві стандарти. Постачальник повинен відмовляти в наданні будь-яких персональних або конфіденційних даних	Постачальник повинен визначити й забезпечити виконання процесу створення, розгортання та заміни сертифікатів TLS або інших.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека (продовження)	
	корпорації Майкрософт, якщо для цього необхідно використовувати засоби без шифрування.	
48	На всіх пристроях постачальника (наприклад ноутбуки, робочі станції тощо), що мають доступ до персональних або конфіденційних даних корпорації Майкрософт або на яких вони оброблятимуться, необхідно запровадити шифрування даних на рівні дисків.	Дані на всіх пристроях, за допомогою яких оброблюються персональні або конфіденційні дані корпорації Майкрософт, повинні бути зашифровані за допомогою BitLocker або іншого еквівалентного рішення для шифрування дисків, що застосовується в галузі.
49	Необхідно забезпечити використання систем і процедур (які використовують поточні галузеві стандарти, зокрема описані в документі **NIST 800-111**) для шифрування будь-яких персональних і/або конфіденційних даних корпорації Майкрософт, що тимчасово не використовуються (під час зберігання), зокрема: ▪ облікові дані (наприклад, імена користувачів і паролі); ▪ дані платіжних засобів (наприклад номери кредитних карток і банківських рахунків); ▪ персональні дані імміграційних документів; ▪ дані медичних профілів (наприклад, номери медичних карток, біометричні маркери або ідентифікатори, зокрема ДНК, відбитки пальців, візерунки сітківки ока, тембр голосу, дані обличчя й розміри рук, що використовуються для автентифікації); ▪ реєстраційні номери, видані державними органами (наприклад номери соціального страхування або водійських посвідчень); ▪ дані клієнтів Майкрософт (наприклад, дані SharePoint, документи O365, дані користувачів OneDrive); ▪ матеріали, пов'язані з продуктами корпорації Майкрософт, випуск яких ще не оголошено; ▪ дати народження; ▪ інформація з профілів дітей; ▪ географічні дані в реальному часі; ▪ адреси фізичних осіб (не організацій); ▪ номери телефонів фізичних осіб (не організацій); ▪ релігійні переконання; ▪ політичні погляди; ▪ сексуальна орієнтація або сексуальні вподобання; ▪ відповіді на контрольні запитання (наприклад, для двофакторної автентифікації або скидання пароля);	Необхідно переконатися, що персональні й конфіденційні дані корпорації Майкрософт, перелік яких зазначено тут, зберігаються в зашифрованому вигляді.

#	Вимоги до захисту даних для постачальників корпорації Майкрософт	Підтвердження відповідності вимогам
	Розділ J. Безпека (продовження)	
	▪ дівоче прізвище матері.	
50	Постачальник має анонімізувати всі персональні дані корпорації Майкрософт, що використовуються в середовищі розробки або тестування.	Постачальник повинен уникати використання персональних даних корпорації Майкрософт у середовищі розробки або тестування. Якщо такому використанню немає альтернативи, інформацію необхідно належним чином анонімізувати, щоб запобігти встановленню осіб суб'єктів даних і зловживанню персональними даними. Примітка: анонімізовані дані відрізняються від псевдонімізованих. Анонімізовані дані — це дані, що не стосуються певною фізичної особи, яку можна ідентифікувати; якщо суб'єкт персональних даних не можна ідентифікувати або більше неможливо встановити.

Глосарій

Уповноважений представник — це особа, яка має належний рівень повноважень, якій довірено право підпису від імені компанії. Ця особа має достатній рівень обізнаності щодо дотримання конфіденційності й безпеки або проконсультувалася з відповідним експертом, перш ніж відправити відповідь в межах програми SSPA. Крім того, вказуючи своє ім'я в формі SSPA, представник засвідчує, що прочитав й зрозумів ці Вимоги.

EUDPR — Регламент (ЄС) 2018/1725 Європейського Парламенту й Європейської Ради від 23 жовтня 2018 року про захист фізичних осіб у зв'язку з обробкою персональних даних установами, органами, офісами й агенціями Європейського Союзу та вільний рух таких даних; скасовує дію Регламенту (ЄС) №45/2001 і Рішення №1247/2002/ЕС.

Фрилансер — особа, яка виконує завдання або надає послуги за запитом, використовуючи цифрові платформи або інші засоби.

GDPR — Регламент (ЄС) 2016/679 Європейського Парламенту та Європейської Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних; скасовує Директиви 95/46/ЕС (Загальний регламент захисту даних).

Вимоги щодо захисту конфіденційності даних — GDPR, EUDPR, місцеві закони щодо захисту даних ЄС і ЄЕЗ, Закон штату Каліфорнії про захист конфіденційності споживачів, параграф 1798.100 Цивільного Кодексу штату Каліфорнії тощо (далі - «CCPA»), Закон Сполученого Королівства про захист даних 2018 року та всі пов'язані або наступні закони, положення й інші правові вимоги, що застосовуються в Сполученому Королівстві, усі відповідні закони, положення та інші законодавчі вимоги, що стосуються (а) конфіденційності та безпеки даних або (б) використання, збирання, зберігання, безпеки, розголошення, передавання, видалення та іншої обробки будь-яких Персональних даних.

Типові положення ЄС і Стандартні договірні положення означають (і) стандартні положення про захист даних для передачі персональних даних обробникам, які перебувають у третіх країнах і не забезпечують належний рівень захисту

даних, як описано в статті 46 GDPR і затверджено рішенням Європейської Комісії 2021/914 від 4 червня 2021 року; (ii) будь-які наступні стандартні договірні положення, прийняті (a) Європейською Комісією, (b) Європейським наглядовим органом із захисту даних з схваленням Європейською комісією, (c) Великобританією згідно з Загальним федеральним законом про захист даних Великобританії, (d) Швейцарією, згідно з Федеральним законом про захист даних Швейцарії, або (e) урядом юрисдикції, що не відносяться до Швейцарії, Великобританії та ЕС/ЄЕЗ, де положення регулюють міжнародну передачу персональних даних, повинні бути включені й бути юридично обов'язковими для постачальника з дати їх прийняття.

Веб-хостинг — онлайн-сервіс хостингу веб-сайту, що створює та/або підтримує веб-сайти від імені Майкрософт з доменним ім’ям Майкрософт, тобто постачальник надає всі матеріали й послуги, необхідні для створення й підтримання веб-сайту та забезпечення його доступності в інтернеті. Термін «Постачальник сервісу веб-хостингу» або «веб-хост» означає постачальника, який надає інструменти й послуги, необхідні для забезпечення можливостей перегляду веб-сайта або веб-сторінки в інтернеті, такі як файли cookie або веб-маяки для реклами.