ДОГОВІР ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Редакція від 14 серпня 2026 року

Цей Договір про обробку персональних даних (далі також — «Договір») укладається між AJAX SYSTEMS TRADING FZE (далі — «Ajax» або «Оператор») і Контролером, визначеним у розділі 1 цього Договору (далі також — «Контролер»), у зв'язку з використанням Продуктів та Програмного забезпечення Ajax і є обов'язковим для Сторін. Далі кожна з них окремо — «Сторона», а разом — «Сторони».

Користуючись Продуктами та Програмним забезпеченням Ajax, кінцевий користувач приймає умови цього Договору та укладає його. Кінцевий користувач (і, якщо застосовно, особа, яка підписує Договір від його імені) заявляє та гарантує, що кожен із них має необхідну цивільну дієздатність і повноваження для укладення цього Договору та дотримання його умов, а також що кінцевий користувач діятиме відповідно до цього Договору та застосовного законодавства.

ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА МЕТА ДОГОВОРУ

A. У межах цього Договору Оператор, Контролер та відповідні треті особи (тобто Субоператори), визначені в Договорі й погоджені Сторонами, беруть участь у наданні Послуг, для яких необхідна обробка Персональних даних Оператором від імені Контролера. Оператор має право обробляти Персональні дані від імені Контролера на умовах цього Договору та його невіддільних частин, зокрема доповнень, змін до нього тощо.

B. Сторони мають намір виконувати цей Договір відповідно до вимог застосовного законодавства у сфері обробки персональних даних та Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (далі також — «Загальний регламент про захист даних», або «GDPR»).

C. Мета цього Договору — узгодити порядок забезпечення приватності та захисту даних під час надання Послуг (як визначено нижче). Цей Договір та інші пов'язані з ним договірні документи разом становлять договір про обробку персональних даних відповідно до вимог статті 28 GDPR. Сторони мають намір тлумачити цей Договір у спосіб, що відповідає зазначеній меті та їхнім зобов'язанням за GDPR і за іншим застосовним законодавством у сфері захисту даних. Якщо з контексту не випливає інше, терміни, вжиті в цьому Договорі та документах, що додаються до нього, мають те саме значення, що й у GDPR.

1. ВИЗНАЧЕННЯ ТЕРМІНІВ ТА ТЛУМАЧЕННЯ

Якщо в цьому Договорі не визначено інше, терміни та вирази, вжиті з великої літери, мають такі значення:

1.1 «**Договір**» означає цей Договір про обробку персональних даних разом з усіма доповненнями, додатками та додатковою документацією. Під «Угодою з кінцевим користувачем» у цьому Договорі слід розуміти Угоду з кінцевим користувачем Ajax, доступну за адресою https://ajax.systems/end-user-agreement/;

1.2 «**Контролер**» означає власника облікового запису, який як кінцевий користувач зареєстрував його для використання Продуктів та Програмного забезпечення Ajax і визначає цілі та засоби обробки Персональних даних, яку Оператор здійснює від його імені. Контролером може бути фізична або юридична особа;

1.3 «**Законодавство про захист даних**» означає законодавство ЄС у сфері захисту даних (зокрема Загальний регламент про захист даних (GDPR) та законодавство, прийняте на його

виконання або на доповнення до нього), а також законодавство будь-якої іншої країни у сфері захисту даних або приватності, якщо воно застосовується до обробки за цим Договором;

1.4 «**ЄЕЗ**» означає Європейську економічну зону;

1.5 «**Персональні дані**» означає будь-яку інформацію, яку Оператор обробляє від імені Контролера на виконання Угоди з кінцевим користувачем, доступної за адресою https://ajax.systems/end-user-agreement/, чи іншого договору, додатково погодженого Сторонами, або у зв'язку з будь-яким із них і яка стосується ідентифікованої фізичної особи або фізичної особи, яку можна ідентифікувати;

1.6 «**Послуги**» означає послуги, які Оператор надає Контролеру у зв'язку з Продуктами та Програмним забезпеченням Ajax;

1.7 «**Вказівки**» означає будь-які вказівки Контролера Оператору щодо обробки Персональних даних, надані: (a) за допомогою функцій Продуктів та Програмного забезпечення Ajax; (b) у технічних угодах, додатках або іншій документації, погодженій з Оператором; або (c) в інший спосіб, письмово погоджений Сторонами. Щоб уникнути сумнівів, Оператор не зобов'язаний перевіряти правову підставу чи доцільність Вказівок, крім випадків, коли вони суперечать застосовному Законодавству про захист даних;

1.8 «**Субоператор**» означає будь-яку третю особу, залучену Оператором або від його імені для обробки Персональних даних та інших пов'язаних даних від імені Контролера на умовах цього Договору;

1.9 «**Продукти та Програмне забезпечення Ajax**» означає обладнання та пов'язане з ним Програмне забезпечення, які Ajax надає відповідно до Угоди з кінцевим користувачем, доступної за адресою https://ajax.systems/end-user-agreement/.

2. ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Предметом обробки за цим Договором є Персональні дані, що створюються в процесі використання Контролером Продуктів та Програмного забезпечення Ajax або у зв'язку з таким використанням і які Оператор обробляє від імені Контролера для цілей, визначених у цьому розділі.

2.2 Обробка охоплює збирання, зберігання, упорядкування, передавання, пошук і видалення Персональних даних за допомогою хмарної інфраструктури Оператора, а також будь-які інші операції, необхідні для реалізації цілей, визначених у пункті 2.3 цього Договору.

2.3 Оператор обробляє Персональні дані відповідно до задокументованих Вказівок Контролера, як передбачено пунктом 3.1 цього Договору, для таких цілей:

(a) забезпечувати роботу хмарної інфраструктури, яка отримує, обробляє та зберігає події, тривоги й інші дані, створені Продуктами та Програмним забезпеченням Ajax, а також надсилати Контролеру відповідні сповіщення;

(b) забезпечувати Контролеру можливість дистанційного доступу до Продуктів та Програмного забезпечення Ajax і керування ними, зокрема доступ до записів та історії подій, які створюються пристроями;

(c) надавати Контролеру технічну підтримку у зв'язку з використанням Продуктів та Програмного забезпечення Ajax;

(d) забезпечувати Контролеру можливість за допомогою задокументованих Вказівок надавати третім особам, уповноваженим Контролером, доступ до Продуктів та Програмного забезпечення Ajax і пов'язаних із ними Персональних даних, як докладніше описано в пункті 3.3 цього Договору.

2.4 Оператор обробляє Персональні дані протягом строку, визначеного в розділі 9 цього Договору.

2.5 Категорії суб'єктів даних і категорії Персональних даних, що обробляються за цим Договором, наведено в Додатку 1.

3. ЗАГАЛЬНІ ОБОВ'ЯЗКИ ЩОДО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1 **Вказівки.** Оператор обробляє Персональні дані виключно:

(a) для цілей, визначених у розділі 2 цього Договору;

(b) відповідно до задокументованих Вказівок Контролера; та

(c) з дотриманням застосовного Законодавства про захист даних.

Контролер не має права надавати Оператору Вказівки, що передбачають обробку Персональних даних із порушенням застосовного законодавства. Оператор не несе відповідальності за будь-яку шкоду чи збитки, спричинені виконанням Вказівок, які Контролер не мав законного права надавати. Якщо Оператор обґрунтовано вважає, що Вказівка порушує застосовне Законодавство про захист даних, він, якщо це не заборонено законом, невідкладно письмово повідомляє про це Контролера та може призупинити обробку Персональних даних, яких стосується така Вказівка, крім їх зберігання та забезпечення безпеки, до надання Контролером нових Вказівок, які Оператор може виконати. На час такого призупинення Оператор не несе відповідальності за невиконання зобов'язань, виконання яких залежить від призупиненої обробки.

3.2 Оператор дотримується застосовного Законодавства про захист даних і впроваджує належні системи та процедури, щоб Персональні дані, які обробляються за цим Договором, були достатніми, відповідними, не надмірними й точними та не зберігалися довше, ніж це необхідно.

3.3 Контролер може за допомогою задокументованих Вказівок уповноважити Оператора передавати Персональні дані таким категоріям третіх осіб, кожна з яких щодо отриманих Персональних даних є незалежним контролером даних:

(a) компаніям, що надають послуги професійного моніторингу та приймання тривог на пульт централізованого спостереження (ПЦС) і залучені Контролером;

(b) компаніям, що надають послуги безпеки та фізичної охорони й залучені Контролером;

(c) інженерам із монтажу та технічного обслуговування, яким Контролер надав права доступу до PRO-акаунту.

Оператор передає Персональні дані таким третім особам виключно на підставі задокументованих Вказівок Контролера та не несе відповідальності за подальшу обробку таких даних цими третіми особами.

3.4 Оператор уповноважений безпосередньо відповідати на запити суб'єктів даних щодо реалізації їхніх прав за застосовним Законодавством про захист даних у зв'язку з обробкою за цим Договором. Оператор повідомляє Контролера про кожен такий запит і про дії, вжиті за результатами його розгляду, не пізніше ніж через п'ять (5) робочих днів після вжиття таких дій. Обов'язок Оператора надавати допомогу обмежується заходами, які технічно можливо вжити з огляду на характер обробки.

3.5 Крім того, Оператор надає Контролеру допомогу в комерційно обґрунтованому обсязі для виконання передбачених застосовним законодавством про захист даних обов'язків Контролера щодо проведення оцінювання безпеки та оцінювання впливу на захист даних, повідомлення про порушення захисту персональних даних і проведення попередніх

консультацій із компетентним наглядовим органом з урахуванням характеру обробки та інформації, доступної Оператору.

3.6 Зважаючи на сучасний рівень розвитку, витрати на впровадження, характер, обсяг, контекст і цілі обробки, яку Оператор здійснює за цим Договором, а також ризики для прав і свобод фізичних осіб, що різняться за ймовірністю виникнення та тяжкістю, Оператор впроваджує належні технічні та організаційні заходи для захисту Персональних даних від несанкціонованої та незаконної обробки, а також від випадкової втрати, зміни або знищення.

3.7 Такі заходи, якщо вони доцільні й застосовні до конкретної операції з обробки, включають:

i. псевдонімізацію та шифрування Персональних даних;

ii. здатність безперервно забезпечувати конфіденційність, цілісність, доступність і стійкість систем та послуг обробки;

iii. здатність своєчасно відновити доступність Персональних даних і доступ до них у разі фізичного або технічного інциденту;

iv. процедуру регулярного тестування, оцінювання та аналізу ефективності технічних і організаційних заходів для забезпечення безпеки обробки.

3.8 Крім того, Оператор зобов'язаний виконувати наведені нижче обов'язки та забезпечувати їх виконання своїм персоналом:

i. невідкладно надавати Контролеру всю інформацію, яку Контролер може вимагати для виконання своїх обов'язків щодо прав суб'єктів даних, зокрема права на доступ, а також для дотримання вимог, викладених у повідомленнях і запитах будь-яких органів із захисту даних;

ii. забезпечувати, щоб особи, які обробляють Персональні дані, зобов'язалися зберігати конфіденційність або мали відповідний обов'язок щодо конфіденційності, встановлений законом; та

iii. невідкладно повідомляти Контролера про будь-які звернення від суб'єктів даних, омбудсмана з питань захисту даних або будь-якого іншого правоохоронного чи регуляторного органу.

4. ПЕРЕДАВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ЗА МЕЖІ ЄЕЗ

4.1 Персональні дані не можуть передаватися за межі Європейської економічної зони без попередньої письмової згоди Контролера, крім випадків, коли на третю особу поширюється дія Стандартних договірних положень (SCC) або вона погоджується дотримуватися їх, чи коли передавання здійснюється в одному з випадків, передбачених цим Договором, зокрема пунктом 4.2.

4.2 Контролер також поінформований про те, що для виконання умов цього Договору та зобов'язань за ним Оператор може передавати Персональні дані за межі Європейського Союзу або Європейської економічної зони, і надає Оператору дозвіл на таке передавання. У таких випадках Оператор зобов'язується забезпечувати високий рівень захисту Персональних даних, що передаються за межі ЄС/ЄЕЗ, зокрема через включення, за потреби, до відповідних договорів стандартних договірних положень щодо міжнародного передавання даних, передбачених Імплементаційним рішенням Комісії (ЄС) 2021/914, або через застосування іншої належної гарантії відповідно до Законодавства про захист даних.

4.3 Будь-яке положення цього Договору, застосування якого позбавило б стандартні договірні положення, зазначені в пункті 4.2, юридичної дії як належних гарантій відповідно до статті 46 GDPR, не застосовується в частині, у якій воно спричиняє такий наслідок.

5. АУДИТ

5.1 Відповідно до положення 8.9 SCC Сторони погоджують такий порядок реалізації прав на проведення аудиту за цим Договором:

i. для проведення аудиту за цим Договором Сторони залучають виключно незалежних аудиторів, які мають підписати з Оператором угоду про нерозголошення інформації;

ii. аудит не передбачає доступу до приміщень або інформаційних систем Оператора та проводиться виключно як документарна перевірка;

iii. аудит може проводитися не частіше одного разу на рік за умови письмового повідомлення Оператора не пізніше ніж за тридцять (30) календарних днів до запланованої дати початку аудиту;

iv. усі витрати на проведення такого аудиту в повному обсязі несе Контролер; та

v. проведення Контролером будь-якого аудиту жодним чином не обмежує обов'язків і відповідальності Оператора за цим Договором.

5.2 Жодне положення цього розділу не слід тлумачити як таке, що обмежує чи звужує права Контролера за положенням 8.9 SCC. Процедури, визначені в цьому розділі, встановлюють порядок, за яким ці права зазвичай реалізуються на практиці.

6. ПОРУШЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

6.1 Оператор повідомляє Контролера без необґрунтованої затримки, але в будь-якому разі не пізніше ніж через сімдесят дві (72) години з моменту, коли йому стало відомо про будь-яке порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття Персональних даних або доступу до них, які Оператор обробляє від імені Контролера (далі — «Порушення»). Якщо Оператор має обґрунтовані підстави вважати, що таке Порушення сталося, він повідомляє про це Контролера. Оператор повідомляє від імені Контролера наглядовий орган або суб'єкта даних про Порушення лише за відповідною письмовою Вказівкою Контролера або якщо такий обов'язок установлено застосовним законодавством.

6.2 Оператор надає Контролеру всю відповідну інформацію щодо Порушення. Повідомлення Оператора про Порушення має містити щонайменше:

i. опис характеру Порушення та інформації, якої воно стосується;

ii. назву та контактні дані контактного пункту Оператора, де можна отримати додаткову інформацію;

iii. опис заходів, ужитих Оператором для реагування на Порушення, зокрема, за потреби, заходів для зменшення його можливих негативних наслідків.

6.3 Оператор документує всі Порушення, зокрема обставини кожного Порушення, його наслідки та вжиті коригувальні заходи.

7. ЗАЛУЧЕННЯ ТРЕТІХ ОСІБ ДО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

7.1 **Загальний дозвіл.** Контролер надає Оператору загальний дозвіл залучати афілійовані компанії Оператора та інших субпідрядників як Субоператорів для обробки Персональних даних у зв'язку з наданням Послуг (далі — «Субоператори») за умови, що таке залучення не призводить до порушення застосовного законодавства або зобов'язань Оператора за цим Договором. Оператор веде перелік залучених Субоператорів у документі Ajax GDPR White Paper (FAQ), доступному за адресою https://ajax.systems/gdpr-white-paper/. Оператор забезпечує, щоб залучені Субоператори мали належну кваліфікацію, а на них за договором були покладені зобов'язання щодо захисту даних, які забезпечують рівень захисту, не

нижчий за передбачений цим Договором. Такі зобов'язання мають бути закріплені в договорі про обробку персональних даних або іншому юридично обов'язковому договірному документі.

7.2 **Зміна Субоператора.** Відповідно до положення 9 Стандартних договірних положень (SCC), викладених у Доповненні 1, Оператор виконує обов'язок повідомляти Контролера про додавання або заміну Субоператора в такий спосіб: оновлює перелік Субоператорів, опублікований у документі Ajax GDPR White Paper (FAQ) за адресою https://ajax.systems/gdpr-white-paper/, а також надсилає Контролеру повідомлення електронною поштою на адресу, зареєстровану в його обліковому записі, та/або сповіщення через Продукти та Програмне забезпечення Ajax. Таке повідомлення надсилається щонайменше за п'ять (5) робочих днів до початку обробки Персональних даних за цим Договором новим Субоператором або Субоператором, залученим на заміну. Протягом цього строку Контролер може заперечити проти такої зміни, письмово повідомивши про це Оператора. Якщо до закінчення цього строку Оператор не отримає заперечення, зміна вважається погодженою.

8. ВИДАЛЕННЯ ТА ПОВЕРНЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

8.1 У разі припинення або закінчення строку дії Угоди з кінцевим користувачем, закриття облікового запису Контролера або на вимогу Контролера Оператор, за вибором Контролера, видаляє або повертає Контролеру всі Персональні дані, які Оператор обробляє від імені Контролера, та видаляє всі наявні копії таких даних, крім випадків, коли застосовне законодавство вимагає їх подальшого зберігання. Контролер може змінити свій вибір у будь-який час до завершення надання Послуг, письмово повідомивши про це Оператора.

8.2 Якщо Контролер не повідомить про свій вибір, передбачений пунктом 8.1, протягом тридцяти (30) календарних днів із моменту настання відповідної події, Оператор видаляє Персональні дані.

8.3 Персональні дані мають бути видалені з активних систем промислової експлуатації Оператора протягом тридцяти (30) календарних днів із дати відповідного запиту або настання події, зазначеної в пункті 8.1, залежно від обставин.

8.4 Після видалення відповідно до пункту 8.3 Персональні дані можуть залишатися в зашифрованих резервних копіях протягом строку їх зберігання, який не перевищує дванадцяти (12) місяців. Протягом цього строку такі Персональні дані не обробляються для будь-яких інших цілей, доступ до них обмежений, а після закінчення відповідного строку зберігання резервних копій такі Персональні дані остаточно видаляються. У разі відновлення даних із резервної копії Оператор до використання відновлених даних у середовищі промислової експлуатації видаляє Персональні дані тих Контролерів, дані яких було видалено раніше.

8.5 До завершення видалення або повернення Оператор продовжує дотримуватися вимог цього Договору щодо відповідних Персональних даних.

8.6 На вимогу Контролера Оператор письмово підтверджує, що видалення завершено.

8.7 Якщо застосовне законодавство вимагає від Оператора зберігати Персональні дані понад строки, визначені в цьому розділі, Оператор повідомляє Контролера про таку вимогу, якщо таке повідомлення не заборонене законом, та обробляє ці Персональні дані лише в обсязі й протягом строку, яких вимагає застосовне законодавство.

9. СТРОК ДІЇ, ВНЕСЕННЯ ЗМІН ТА ПРИПИНЕННЯ ДІЇ ДОГОВОРУ

9.1 Цей Договір набуває чинності одночасно з Угодою з кінцевим користувачем, доступною за адресою https://ajax.systems/end-user-agreement/, і з дати її прийняття Контролером є її невіддільною частиною. Цей Договір залишається чинним доти, доки Оператор не припинить обробку Персональних даних у зв'язку з наданням Послуг або будь-яким договором між Сторонами та не виконає всі зобов'язання, пов'язані із завершенням обробки, якщо Сторони письмово не погодять інше.

9.2 Припинення або закінчення строку дії цього Договору не звільняє Сторони від зобов'язань щодо конфіденційності чи будь-яких інших обов'язків за цим Договором.

9.3 Ajax може змінювати цей Договір, опублікувавши його оновлену версію на вебсайті Ajax, надіславши повідомлення електронною поштою або сповіщення через Продукти та/або мобільні застосунки. Подальше використання Продуктів або Програмного забезпечення після такого повідомлення означає прийняття Договору зі змінами. Право Ajax змінювати цей Договір не поширюється на Стандартні договірні положення (SCC), викладені в Доповненні 1: їх можна оновлювати лише в межах, передбачених цими SCC.

10. ЗАСТОСОВНЕ ПРАВО ТА ПОРЯДОК ВИРІШЕННЯ СПОРІВ

10.1 До цього Договору, включно з усіма доповненнями, додатками та іншими його невіддільними частинами, застосовується право Республіки Польща, відповідно до якого він тлумачиться.

10.2 Сторони також зобов'язуються дотримуватися Застосовного законодавства про захист даних щодо обробки Персональних даних.

10.3 «Застосовне законодавство про захист даних» означає чинне на відповідний момент законодавство про обробку персональних даних, зокрема Загальний регламент про захист даних (Регламент (ЄС) 2016/679); Закон Великої Британії про захист даних 2018 року (Data Protection Act 2018); Директиву 2002/58/ЄС про опрацювання персональних даних і захист приватності у сфері електронних комунікацій (зі змінами, внесеними Директивою 2009/136/ЄС); Положення про приватність та електронні комунікації 2003 року (Privacy and Electronic Communications Regulations 2003; SI 2003/2426), зі змінами; а також інше законодавство ЄЕЗ щодо персональних даних та будь-яке інше законодавство й нормативні вимоги, чинні на відповідний момент і застосовні до Сторін у зв'язку з використанням Персональних даних, зокрема щодо захисту приватності у сфері електронних комунікацій, залежно від території, на якій надаються Програмне забезпечення та Продукти.

10.4 Будь-який спір, розбіжність чи вимога, що виникають із цього Договору або будь-яким чином пов'язані з ним, зокрема щодо його тлумачення, можливості примусового виконання, виконання, порушення, припинення чи дійсності, підлягають вирішенню судами Республіки Польща у Варшаві, якщо Застосовним законодавством про захист даних не передбачено інше. Мовою судового розгляду є англійська.

10.5 Сторони безвідклично визнають виключну юрисдикцію судів Республіки Польща щодо будь-яких спорів, які виникають із цього Договору або у зв'язку з ним, зокрема щодо його виконання, існування, дійсності, тлумачення, припинення або наслідків такого припинення. Відповідно, будь-які позови чи інші судові провадження, що виникають із цього Договору або у зв'язку з ним, незалежно від того, чи ґрунтуються вони на договірній, чи на позадоговірній відповідальності, мають ініціюватися виключно в судах Республіки Польща. Якщо Контролер є фізичною особою, яка діє як Індивідуальний кінцевий користувач (як визначено в Угоді з кінцевим користувачем), він також може звернутися до суду в країні, у якій має звичайне місце проживання.

ДОПОВНЕННЯ 1. СТАНДАРТНІ ДОГОВІРНІ ПОЛОЖЕННЯ (ДАЛІ ТАКОЖ — «SCC»)

РОЗДІЛ I

Положення 1.

Мета та сфера застосування

(a) Мета цих стандартних договірних положень — забезпечити дотримання вимог Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних) під час передавання персональних даних до третьої країни.

(b) Сторони:

(i) фізичні або юридичні особи, органи публічної влади, агентства чи інші організації (далі — «суб'єкти»), що передають персональні дані та зазначені в Додатку 1 (далі кожен такий суб'єкт — «експортер даних»), та

(ii) суб'єкти в третій країні, що отримують персональні дані від експортера даних безпосередньо або опосередковано через інший суб'єкт, який також є Стороною цих SCC, та зазначені в Додатку 1 (далі кожен такий суб'єкт — «імпортер даних»),

погодилися з цими стандартними договірними положеннями.

(c) Ці SCC застосовуються до передавання персональних даних, описаного в Додатку 1.

(d) Доповнення до цих SCC, що містить згадані в них Додатки, є їх невіддільною частиною.

Положення 2.

Дія та незмінність SCC

(a) Ці SCC встановлюють належні гарантії, зокрема права суб'єктів даних, здійснення яких може бути забезпечене в примусовому порядку, та дієві засоби правового захисту відповідно до статті 46(1) та статті 46(2)(c) Регламенту (ЄС) 2016/679, а щодо передавання даних від контролерів до операторів та/або від операторів до операторів — стандартні договірні положення відповідно до статті 28(7) Регламенту (ЄС) 2016/679, за умови, що до них не вносяться зміни, крім вибору відповідного Модуля чи відповідних Модулів або додавання чи оновлення інформації в Доповненні. Це не перешкоджає Сторонам включати стандартні договірні положення, викладені в цих SCC, до ширшого договору та/або додавати інші положення чи додаткові гарантії за умови, що вони прямо чи опосередковано не суперечать цим SCC і не завдають шкоди фундаментальним правам або свободам суб'єктів даних.

(b) Ці SCC не впливають на обов'язки, покладені на експортера даних Регламентом (ЄС) 2016/679.

Положення 3.

Треті особи-бенефіціари

(a) Суб'єкти даних можуть як треті особи-бенефіціари покликатися на ці SCC і вимагати їх виконання від експортера даних і/або імпортера даних, крім таких положень:

(i) положення 1, положення 2, положення 3, положення 6, положення 7;

(ii) положення 8.1(b), 8.9(a), (c), (d) та (e);

(iii) положення 9(a), (c), (d) та (e);

(iv) положення 12(a), (d) та (f);

(v) положення 13;

(vi) положення 15.1(c), (d) та (e);

(vii) положення 16(e);

(viii) положення 18(a) та (b).

(b) Підпункт (a) не обмежує прав суб'єктів даних, передбачених Регламентом (ЄС) 2016/679.

Положення 4.

Тлумачення

(a) Терміни, що вживаються в цих SCC і визначені в Регламенті (ЄС) 2016/679, мають те саме значення, що й у цьому Регламенті.

(b) Ці SCC слід читати й тлумачити з урахуванням положень Регламенту (ЄС) 2016/679.

(c) Ці SCC не можна тлумачити у спосіб, що суперечить правам і обов'язкам, передбаченим Регламентом (ЄС) 2016/679.

Положення 5.

Переважна сила

У разі суперечності між цими SCC та положеннями пов'язаних договорів між Сторонами, укладених до моменту погодження цих SCC або після цього, переважну силу мають ці SCC.

Положення 6.

Опис передавання даних

Докладні відомості про передавання даних, зокрема категорії персональних даних, що передаються, та цілі такого передавання, наведено в Додатку 1.

Положення 7.

Приєднання до SCC

Необов'язкове положення про приєднання до SCC, передбачене положенням 7, не застосовується.

<u>РОЗДІЛ II</u> — ОБОВ'ЯЗКИ СТОРІН

Положення 8.

Гарантії захисту даних

Експортер даних гарантує, що доклав належних зусиль, аби пересвідчитися, що імпортер даних здатний виконувати свої обов'язки за цими SCC завдяки впровадженню відповідних технічних та організаційних заходів.

8.1 Вказівки

(a) Імпортер даних обробляє персональні дані лише на підставі задокументованих вказівок експортера даних. Експортер даних може надавати такі вказівки протягом усього строку дії договору.

(b) Імпортер даних негайно повідомляє експортера даних, якщо не може виконувати такі вказівки.

8.2 Цільове обмеження

Імпортер даних обробляє персональні дані лише для конкретних цілей передавання, визначених у Додатку 1, якщо експортер даних не надасть інших вказівок.

8.3 Прозорість

На запит експортер даних безоплатно надає суб'єкту даних копію цих SCC разом із Доповненням, заповненим Сторонами. У межах, необхідних для захисту комерційної таємниці або іншої конфіденційної інформації, зокрема інформації про заходи, описані в Додатку 2, а також персональних даних, експортер даних може перед наданням копії приховати в ній частину тексту Доповнення до цих SCC. Однак, якщо без цього суб'єкт даних не зможе зрозуміти зміст SCC або реалізувати свої права, експортер даних має надати змістовний стислий виклад відповідної частини. На запит Сторони повідомляють суб'єкту даних причини такого приховування, наскільки це можливо без розкриття прихованої інформації. Це положення не впливає на обов'язки експортера даних за статтями 13 і 14 Регламенту (ЄС) 2016/679.

8.4 Точність

Якщо імпортеру даних стає відомо, що отримані ним персональні дані є неточними або стали застарілими, він без необґрунтованої затримки повідомляє про це експортера даних. У такому разі імпортер даних співпрацює з експортером даних, щоб стерти або виправити ці дані.

8.5 Строк обробки та стирання або повернення даних

Імпортер даних здійснює обробку лише протягом строку, визначеного в Додатку 1. Після завершення надання послуг з обробки імпортер даних, за вибором експортера даних, видаляє всі персональні дані, які обробляв від імені експортера даних, і засвідчує експортеру даних, що їх видалено, або повертає експортеру даних усі персональні дані, які обробляв від імені експортера даних, та видаляє наявні копії. До видалення або повернення даних імпортер даних продовжує дотримуватися цих SCC.

Якщо місцеве законодавство, що застосовується до імпортера даних, забороняє повернення або видалення персональних даних, імпортер даних гарантує, що й надалі дотримуватиметься цих SCC та оброблятиме такі дані лише в обсязі й протягом строку, яких вимагає таке місцеве законодавство. Це не обмежує застосування положення 14, зокрема передбаченого положенням 14(e) обов'язку імпортера даних протягом усього строку дії договору повідомляти експортера даних, якщо він має підстави вважати, що до нього застосовуються або почали застосовуватися закони чи практики, які не відповідають вимогам положення 14(a).

8.6 Безпека обробки

(a) Імпортер даних вживає відповідних технічних та організаційних заходів для забезпечення безпеки даних; під час передавання таких заходів вживає також експортер даних. Ці заходи мають, зокрема, захищати дані від порушення безпеки, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття таких даних або доступу до них (далі — «порушення захисту персональних даних»).

Визначаючи належний рівень безпеки, Сторони враховують сучасний рівень розвитку, витрати на впровадження, характер, обсяг, контекст і цілі обробки, а також ризики для суб'єктів даних, пов'язані з обробкою. Зокрема, Сторони розглядають можливість застосування шифрування або псевдонімізації, у тому числі під час передавання, якщо мети обробки можна досягти в такий спосіб. У разі псевдонімізації додаткова інформація, що дає змогу пов'язати персональні дані з конкретним суб'єктом даних, за можливості залишається виключно під контролем експортера даних. Виконуючи передбачені цим підпунктом обов'язки, імпортер даних щонайменше впроваджує технічні та організаційні заходи, зазначені в Додатку 2. Імпортер даних регулярно перевіряє, чи й надалі ці заходи забезпечують належний рівень безпеки.

(b) Імпортер даних надає особам зі свого персоналу доступ до персональних даних лише в обсязі, необхідному для виконання й адміністрування договору та контролю за його

виконанням. Імпортер даних забезпечує, щоб особи, уповноважені обробляти персональні дані, взяли на себе обов'язок зберігати конфіденційність або мали відповідний обов'язок щодо конфіденційності, встановлений законом.

(c) У разі порушення захисту персональних даних, які імпортер даних обробляє за цими SCC, імпортер даних вживає відповідних заходів для реагування на порушення, зокрема для зменшення його негативних наслідків. Імпортер даних також без необґрунтованої затримки після того, як йому стало відомо про порушення, повідомляє про нього експортера даних.

Таке повідомлення має містити контактні дані для отримання додаткової інформації; опис характеру порушення, зокрема, за можливості, із зазначенням категорій та приблизної кількості суб'єктів даних, яких воно стосується, а також категорій та приблизної кількості записів персональних даних, яких стосується порушення; його ймовірні наслідки; заходи, вжиті або запропоновані для реагування на порушення, зокрема, за потреби, заходи для зменшення його можливих негативних наслідків. Якщо всю інформацію неможливо надати одночасно, перше повідомлення має містити інформацію, наявну на той момент. Додаткову інформацію імпортер даних надає без необґрунтованої затримки, щойно вона стає доступною.

(d) Імпортер даних співпрацює з експортером даних і допомагає йому виконувати обов'язки за Регламентом (ЄС) 2016/679, зокрема повідомляти компетентний наглядовий орган та суб'єктів даних, яких стосується порушення, з урахуванням характеру обробки та інформації, доступної імпортеру даних.

8.7 Чутливі дані

Якщо передавання охоплює персональні дані, що розкривають расове або етнічне походження, політичні погляди, релігійні чи філософські переконання або членство в професійних спілках, генетичні дані чи біометричні дані з метою однозначної ідентифікації фізичної особи, дані про здоров'я, статеве життя чи сексуальну орієнтацію особи, а також дані про судимості та кримінальні правопорушення (далі — «чутливі дані»), імпортер даних застосовує конкретні обмеження і/або додаткові гарантії, описані в Додатку 1.

8.8 Подальше передавання даних

Імпортер даних розкриває персональні дані третій особі лише на підставі задокументованих вказівок експортера даних. Крім того, імпортер даних може розкривати персональні дані третій особі, яка перебуває за межами Європейського Союзу — у тій самій країні, що й імпортер даних, або в іншій третій країні (далі — «подальше передавання»), — лише якщо на таку третю особу поширюється дія цих SCC або вона погоджується дотримуватися їх за відповідним Модулем, або якщо:

(i) подальше передавання здійснюється до країни, щодо якої відповідно до статті 45 Регламенту (ЄС) 2016/679 ухвалено рішення про відповідність, що охоплює таке передавання;

(ii) третя особа в інший спосіб забезпечує належні гарантії відповідно до статей 46 або 47 Регламенту (ЄС) 2016/679 щодо відповідної обробки;

(iii) подальше передавання необхідне для формування, здійснення або захисту правових претензій у межах конкретного адміністративного, регуляторного чи судового провадження; або

(iv) подальше передавання необхідне для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи.

Під час будь-якого подальшого передавання імпортер даних зобов'язаний дотримуватися всіх інших гарантій, передбачених цими SCC, зокрема принципу цільового обмеження.

8.9 Документування та дотримання вимог

(a) Імпортер даних без зволікання та належним чином розглядає запити експортера даних, що стосуються обробки за цими SCC.

(b) Сторони мають бути спроможні підтвердити дотримання цих SCC. Зокрема, імпортер даних веде належну документацію щодо операцій з обробки, які здійснює від імені експортера даних.

(c) Імпортер даних надає експортеру даних усю інформацію, необхідну для підтвердження виконання обов'язків, передбачених цими SCC, а на запит експортера даних дозволяє проводити аудити операцій з обробки, охоплених цими SCC, та сприяє їх проведенню з обґрунтованою періодичністю або за наявності ознак недотримання цих SCC. Вирішуючи питання про проведення перевірки або аудиту, експортер даних може враховувати відповідні сертифікати, наявні в імпортера даних.

(d) Експортер даних може провести аудит самостійно або доручити його проведення незалежному аудитору. Аудит може передбачати перевірку приміщень або інших фізичних об'єктів імпортера даних і, за потреби, проводиться за умови попереднього повідомлення імпортера даних за розумний строк до проведення аудиту.

(e) На запит компетентного наглядового органу Сторони надають йому інформацію, зазначену в підпунктах (b) і (c), зокрема результати будь-яких аудитів.

Положення 9.

Залучення субоператорів

(a) Імпортер даних має загальний дозвіл експортера даних на залучення субоператорів із погодженого переліку. Імпортер даних окремо письмово повідомляє експортера даних про будь-які заплановані зміни до цього переліку — додавання або заміну субоператорів — щонайменше за п'ять (5) робочих днів до залучення відповідного субоператора, щоб експортер даних мав достатньо часу заперечити проти таких змін. Імпортер даних надає експортеру даних інформацію, необхідну для реалізації права на заперечення.

(b) Якщо імпортер даних залучає субоператора для виконання конкретних операцій з обробки від імені експортера даних, імпортер даних залучає такого субоператора на підставі письмового договору, за яким на субоператора покладаються по суті ті самі обов'язки щодо захисту даних, що й на імпортера даних за цими SCC, зокрема щодо прав суб'єктів даних як третіх осіб-бенефіціарів. Сторони погоджуються, що, виконуючи вимоги цього положення, імпортер даних виконує свої обов'язки за положенням 8.8. Імпортер даних забезпечує виконання субоператором обов'язків, покладених на імпортера даних за цими SCC.

(c) На запит експортера даних імпортер даних надає йому копію такого договору із субоператором та копії всіх подальших змін до нього. У межах, необхідних для захисту комерційної таємниці або іншої конфіденційної інформації, зокрема персональних даних, імпортер даних може перед наданням копії приховати частину тексту договору.

(d) Імпортер даних несе перед експортером даних повну відповідальність за виконання субоператором його обов'язків за договором з імпортером даних. Імпортер даних повідомляє експортера даних про кожен випадок невиконання субоператором обов'язків за цим договором.

(e) Імпортер даних погоджує із субоператором положення на користь третьої особи, яке передбачає, що, якщо імпортер даних фактично перестав існувати, юридично припинив існування або став неплатоспроможним, експортер даних має право розірвати договір із субоператором і надати йому вказівку стерти або повернути персональні дані.

Положення 10.

Права суб'єкта даних

(a) Імпортер даних без зволікання повідомляє експортера даних про будь-який запит, отриманий від суб'єкта даних. Імпортер даних не відповідає на такий запит самостійно, якщо експортер даних не уповноважив його на це.

(b) Імпортер даних допомагає експортеру даних виконувати обов'язки щодо відповіді на запити суб'єктів даних про реалізацію їхніх прав за Регламентом (ЄС) 2016/679. Для цього Сторони, з урахуванням характеру обробки, визначають у Додатку 2 відповідні технічні та організаційні заходи, за допомогою яких надаватиметься така допомога, а також межі та обсяг необхідної допомоги.

(c) Виконуючи обов'язки, передбачені підпунктами (a) і (b), імпортер даних виконує вказівки експортера даних.

Положення 11.

Засоби правового захисту

(a) Імпортер даних у прозорій і легкодоступній формі — в індивідуальному повідомленні або на своєму вебсайті — повідомляє суб'єктам даних про контактний пункт, уповноважений розглядати скарги. Імпортер даних без зволікання розглядає будь-які скарги, отримані від суб'єкта даних.

(b) У разі спору між суб'єктом даних та однією зі Сторін щодо дотримання цих SCC така Сторона докладає всіх можливих зусиль, щоб своєчасно врегулювати спір мирним шляхом. Сторони інформують одна одну про такі спори та, за потреби, співпрацюють для їх урегулювання.

(c) Якщо суб'єкт даних покликається на право третьої особи-бенефіціара відповідно до положення 3, імпортер даних визнає вибір суб'єкта даних:

  (i) подати скаргу до наглядового органу в державі-члені за місцем його звичайного проживання чи роботи або до компетентного наглядового органу відповідно до положення 13;

  (ii) звернутися до компетентних судів, визначених у положенні 18, для вирішення спору.

(d) Сторони визнають, що суб'єкта даних може представляти неприбутковий орган, організація чи асоціація за умов, визначених у статті 80(1) Регламенту (ЄС) 2016/679.

(e) Імпортер даних виконує рішення, обов'язкове відповідно до застосовного права ЄС або держави-члена.

(f) Імпортер даних погоджується, що вибір суб'єкта даних не обмежує його матеріальних і процесуальних прав на використання засобів правового захисту відповідно до застосовного законодавства.

Положення 12.

Відповідальність

(a) Кожна Сторона несе відповідальність перед іншою Стороною чи іншими Сторонами за будь-яку шкоду, яку вона завдала їм унаслідок порушення цих SCC.

(b) Імпортер даних несе відповідальність перед суб'єктом даних, а суб'єкт даних має право на відшкодування будь-якої матеріальної або нематеріальної шкоди, завданої йому імпортером даних або його субоператором унаслідок порушення прав суб'єкта даних як третьої особи-бенефіціара за цими SCC.

(c) Незважаючи на підпункт (b), експортер даних несе відповідальність перед суб'єктом даних, а суб'єкт даних має право на відшкодування будь-якої матеріальної або нематеріальної шкоди, завданої йому експортером даних, імпортером даних або його субоператором унаслідок порушення прав суб'єкта даних як третьої особи-бенефіціара за цими SCC. Це не обмежує відповідальності експортера даних, а якщо експортер даних є оператором, що діє від імені контролера, — також відповідальності контролера за Регламентом (ЄС) 2016/679 або Регламентом (ЄС) 2018/1725, залежно від того, який із них застосовується.

(d) Сторони погоджуються, що, якщо експортера даних відповідно до підпункту (c) визнано відповідальним за шкоду, завдану імпортером даних або його субоператором, експортер даних має право вимагати від імпортера даних тієї частини відшкодування, що відповідає частці відповідальності імпортера даних за цю шкоду.

(e) Якщо за шкоду, завдану суб'єкту даних унаслідок порушення цих SCC, відповідають кілька Сторін, усі такі Сторони несуть солідарну відповідальність, а суб'єкт даних має право звернутися до суду з позовом до будь-якої з них.

(f) Сторони погоджуються, що, якщо одну зі Сторін відповідно до підпункту (e) визнано відповідальною, вона має право вимагати від іншої Сторони чи інших Сторін тієї частини відшкодування, що відповідає частці їхньої відповідальності за шкоду.

(g) Імпортер даних не може покликатися на поведінку оператора або субоператора як на підставу для звільнення від власної відповідальності.

Положення 13.

Нагляд

(a) Наглядовий орган, зазначений у Додатку 1 та відповідальний за забезпечення дотримання експортером даних вимог Регламенту (ЄС) 2016/679 у зв'язку з передаванням даних, є компетентним наглядовим органом.

(b) Імпортер даних визнає юрисдикцію компетентного наглядового органу та співпрацює з ним під час будь-яких процедур, спрямованих на забезпечення дотримання цих SCC. Зокрема, імпортер даних відповідає на запити, допускає проведення аудитів і виконує заходи, застосовані наглядовим органом, зокрема коригувальні й компенсаційні. Імпортер даних письмово підтверджує наглядовому органу, що необхідних заходів ужито.

<u>РОЗДІЛ III</u> — МІСЦЕВЕ ЗАКОНОДАВСТВО ТА ОБОВ'ЯЗКИ У РАЗІ ДОСТУПУ З БОКУ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ

Положення 14.

Місцеве законодавство та практики, що впливають на дотримання SCC

(a) Сторони гарантують, що не мають підстав вважати, що законодавство та практики третьої країни призначення, які застосовуються до обробки персональних даних імпортером даних, зокрема будь-які вимоги щодо розкриття персональних даних або заходи, що дозволяють органам публічної влади отримувати доступ до них, перешкоджають імпортеру даних виконувати свої обов'язки за цими SCC. Така гарантія ґрунтується на розумінні того, що законодавство та практики, які поважають сутність фундаментальних прав і свобод та не виходять за межі того, що є необхідним і пропорційним у демократичному суспільстві для забезпечення однієї з цілей, перелічених у статті 23(1) Регламенту (ЄС) 2016/679, не суперечать цим SCC.

(b) Сторони заявляють, що, надаючи гарантію, передбачену підпунктом (a), вони належним чином урахували, зокрема, такі чинники:

(i) конкретні обставини передавання, зокрема довжину ланцюга обробки, кількість залучених учасників і використані канали передавання; заплановані подальші передавання; тип одержувача; мету обробки; категорії та формат переданих персональних даних; сектор економіки, у якому здійснюється передавання; місце зберігання переданих даних;

(ii) законодавство та практики третьої країни призначення, що мають значення з огляду на конкретні обставини передавання, зокрема ті, що вимагають розкриття даних органам публічної влади або надають таким органам право доступу до них, а також застосовні обмеження та гарантії;[1]

(iii) будь-які відповідні договірні, технічні або організаційні гарантії, запроваджені для доповнення гарантій за цими SCC, зокрема заходи, що застосовуються під час передавання та обробки персональних даних у країні призначення.

(c) Імпортер даних гарантує, що під час оцінювання, передбаченого підпунктом (b), доклав усіх можливих зусиль, щоб надати експортеру даних відповідну інформацію, і погоджується надалі співпрацювати з ним для забезпечення дотримання цих SCC.

(d) Сторони погоджуються документувати оцінювання, передбачене підпунктом (b), та на запит компетентного наглядового органу надавати йому відповідну документацію.

(e) Імпортер даних погоджується без зволікання повідомляти експортера даних, якщо після погодження цих SCC і протягом строку дії договору в нього з'являться підстави вважати, що до нього застосовуються або почали застосовуватися закони чи практики, які не відповідають вимогам підпункту (a). Це стосується, зокрема, випадків зміни законодавства третьої країни або вжиття певного заходу (наприклад, надходження запиту про розкриття даних), що свідчить про застосування такого законодавства на практиці у спосіб, який не відповідає вимогам підпункту (a).

(f) Після отримання повідомлення відповідно до підпункту (e) або якщо з інших причин експортер даних має підстави вважати, що імпортер даних більше не може виконувати свої обов'язки за цими SCC, експортер даних без зволікання визначає відповідні заходи (наприклад, технічні або організаційні заходи для забезпечення безпеки та конфіденційності), яких має вжити експортер даних і/або імпортер даних, щоб відреагувати на ситуацію. Експортер даних тимчасово зупиняє передавання даних, якщо вважає, що належні гарантії такого передавання забезпечити неможливо, або якщо компетентний наглядовий орган надає вказівку це зробити. У такому разі експортер даних має право розірвати договір у частині, що стосується обробки персональних даних за цими SCC. Якщо Сторін договору більше ніж дві, експортер даних може розірвати договір лише щодо тієї Сторони, якої це стосується, якщо Сторони не погодили інше. Якщо договір розірвано відповідно до цього положення, застосовуються підпункти (d) і (e) положення 16.

---

[1] Оцінюючи вплив такого законодавства та практик на дотримання цих SCC, у межах загального оцінювання можна враховувати різні чинники. До них може належати, зокрема, відповідний задокументований практичний досвід попереднього отримання запитів про розкриття даних від органів публічної влади або відсутності таких запитів протягом достатньо репрезентативного періоду. Ідеться, зокрема, про внутрішні записи чи іншу документацію, які постійно ведуть із належною ретельністю та засвідчують на рівні вищого керівництва, за умови, що таку інформацію можна правомірно надавати третім особам. Якщо на підставі такого практичного досвіду роблять висновок, що імпортеру даних ніщо не перешкоджатиме дотримуватися цих SCC, такий досвід має підтверджуватися іншими відповідними об'єктивними чинниками. Сторони мають ретельно оцінити, чи є ці чинники в сукупності достатньо вагомими з погляду їхньої надійності й репрезентативності, щоб підтвердити цей висновок. Зокрема, Сторони мають ураховувати, чи підтверджується їхній практичний досвід і чи не суперечить йому надійна загальнодоступна або доступна в інший спосіб інформація про наявність чи відсутність таких запитів у тому самому секторі та/або про практичне застосування законодавства, наприклад, судова практика та звіти незалежних наглядових органів.

Положення 15.

Обов’язки імпортера даних у разі доступу з боку органів публічної влади

15.1 Повідомлення

(a) Імпортер даних погоджується без зволікання повідомляти експортера даних і, за можливості, суб’єкта даних (за потреби — за допомогою експортера даних), якщо він:

(i) отримує від органу публічної влади, зокрема судового органу, запит про розкриття персональних даних, переданих відповідно до цих SCC, який відповідно до законодавства країни призначення є обов’язковим до виконання. Таке повідомлення має містити інформацію про персональні дані, яких стосується запит, орган, від якого надійшов запит, правову підставу запиту та відповідь, надану на нього; або

(ii) дізнається про будь-який випадок, коли органи публічної влади відповідно до законодавства країни призначення безпосередньо отримали доступ до персональних даних, переданих відповідно до цих SCC. Таке повідомлення має містити всю наявну в імпортера даних інформацію.

(b) Якщо законодавство країни призначення забороняє імпортеру даних повідомляти експортера даних і/або суб’єкта даних, імпортер даних погоджується докласти всіх можливих зусиль, щоб отримати звільнення від дії такої заборони і якнайшвидше надати якомога більше інформації. Імпортер даних погоджується документувати докладені для цього зусилля, щоб на запит експортера даних мати змогу підтвердити їх.

(c) Якщо це дозволено законодавством країни призначення, імпортер даних погоджується регулярно протягом строку дії договору надавати експортеру даних якомога більше інформації, що стосується отриманих запитів (зокрема про кількість запитів, вид даних, яких вони стосуються, органи, від яких надійшли запити, про те, чи оскаржувалися такі запити, та про результати їх оскарження тощо).

(d) Імпортер даних погоджується зберігати інформацію, зазначену в підпунктах (a)–(c), протягом строку дії договору та на запит компетентного наглядового органу надавати йому цю інформацію.

(e) Підпункти (a)–(c) не обмежують обов’язку імпортера даних, передбаченого підпунктом (e) положення 14 та положенням 16, без зволікання повідомляти експортера даних, якщо імпортер даних не може дотримуватися цих SCC.

15.2 Перевірка законності та мінімізація даних

(a) Імпортер даних погоджується перевіряти законність запиту про розкриття даних, зокрема з’ясовувати, чи не виходить такий запит за межі повноважень, наданих органу публічної влади, від якого він надійшов, та оскаржувати його, якщо після ретельного оцінювання дійде висновку, що є обґрунтовані підстави вважати запит неправомірним з огляду на законодавство країни призначення, застосовні міжнародно-правові зобов’язання та принципи міжнародної ввічливості. За тих самих умов імпортер даних використовує можливості подальшого оскарження. Оскаржуючи запит, імпортер даних домагається застосування тимчасових заходів для зупинення дії запиту до того, як компетентний судовий орган вирішить питання по суті. Імпортер даних не розкриває персональні дані, яких стосується запит, доки застосовні процесуальні норми не вимагатимуть такого розкриття. Ці вимоги не обмежують обов’язків імпортера даних за підпунктом (e) положення 14.

(b) Імпортер даних погоджується документувати свою правову оцінку та всі випадки оскарження запиту про розкриття даних і, наскільки це дозволяє законодавство країни призначення, надавати відповідну документацію експортеру даних. На запит компетентного наглядового органу імпортер даних також надає йому цю документацію.

(c) Імпортер даних погоджується надавати у відповіді на запит про розкриття даних мінімальний допустимий обсяг інформації на підставі обґрунтованого тлумачення такого запиту.

<u>РОЗДІЛ IV</u> — ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Положення 16.

Недотримання SCC та розірвання договору

(a) Імпортер даних без зволікання повідомляє експортера даних, якщо з будь-якої причини не може дотримуватися цих SCC.

(b) Якщо імпортер даних порушує ці SCC або не може їх дотримуватися, експортер даних тимчасово зупиняє передавання персональних даних імпортеру даних, доки дотримання цих SCC не буде відновлено або договір не буде розірвано. Це не впливає на застосування підпункту (f) положення 14.

(c) Експортер даних має право розірвати договір у частині, що стосується обробки персональних даних за цими SCC, якщо:

(i) експортер даних відповідно до підпункту (b) тимчасово зупинив передавання персональних даних імпортеру даних, а дотримання цих SCC не відновлено протягом розумного строку, але в будь-якому разі не пізніше ніж через один місяць із моменту такого зупинення;

(ii) імпортер даних допускає істотне або тривале порушення цих SCC; або

(iii) імпортер даних не виконує обов’язкового для нього рішення компетентного суду або наглядового органу щодо його обов’язків за цими SCC.

У таких випадках експортер даних повідомляє компетентний наглядовий орган про таке недотримання SCC. Якщо договір укладено між більш ніж двома Сторонами, експортер даних може розірвати його лише щодо відповідної Сторони, якщо Сторони не погодили інше.

(d) Персональні дані, передані до того, як договір було розірвано відповідно до підпункту (c), за вибором експортера даних негайно повертаються експортеру даних або повністю видаляються. Те саме стосується будь-яких копій цих даних. Імпортер даних засвідчує експортеру даних, що дані видалено. До видалення або повернення даних імпортер даних і надалі забезпечує дотримання цих SCC. Якщо місцеве законодавство, що застосовується до імпортера даних, забороняє повернення або видалення переданих персональних даних, імпортер даних гарантує, що й надалі забезпечуватиме дотримання цих SCC та оброблятиме такі дані лише в обсязі й протягом строку, яких вимагає таке місцеве законодавство.

(e) Будь-яка зі Сторін може відкликати свою згоду на обов’язковість для неї цих SCC, якщо: (i) Європейська Комісія відповідно до статті 45(3) Регламенту (ЄС) 2016/679 ухвалить рішення про відповідність, яке охоплює передавання персональних даних, на яке поширюється дія цих SCC; або (ii) Регламент (ЄС) 2016/679 стане складником правової системи країни, до якої передаються персональні дані. Це не впливає на інші обов’язки щодо такої обробки, встановлені Регламентом (ЄС) 2016/679.

Положення 17.

Застосовне право

До цих SCC застосовується право однієї з держав-членів ЄС за умови, що таке право допускає набуття прав третіми особами-бенефіціарами. Сторони погоджуються, що застосовним є право Польщі.

Положення 18.

Вибір суду та юрисдикція

(a) Будь-який спір, що виникає з цих SCC, вирішується судами однієї з держав-членів ЄС.

(b) Сторони погоджуються, що такими судами є суди Польщі.

(c) Суб’єкт даних також може звернутися до судів держави-члена, у якій він має звичайне місце проживання, з позовом до експортера даних і/або імпортера даних.

(d) Сторони погоджуються підпорядковуватися юрисдикції таких судів.

ДОДАТОК 1. ОПИС ОБРОБКИ ДАНИХ

A. ПЕРЕЛІК СТОРІН

Експортер даних

Роль: Контролер

Ідентифікаційні та контактні дані: Контролер, якого ідентифікують за даними облікового запису, зазначеними ним у Продуктах та Програмному забезпеченні Ajax під час створення облікового запису (ім’я або найменування компанії, адреса та контактна адреса електронної пошти).

Діяльність, пов’язана з даними, що передаються: використання Продуктів та Програмного забезпечення Ajax для охорони приміщень або майна, які контролює Контролер.

Імпортер даних

Роль: Оператор

Найменування: AJAX SYSTEMS TRADING FZE

Адреса: S3B2SR06, Jebel Ali Freezone, Dubai, United Arab Emirates

Контактні дані: privacy@ajax.systems

Діяльність, пов’язана з даними, що передаються: надання Послуг, які дають Контролеру змогу використовувати Продукти та Програмне забезпечення Ajax відповідно до Угоди з кінцевим користувачем.

B. КАТЕГОРІЇ СУБ’ЄКТІВ ДАНИХ

Персональні дані, що передаються за цими SCC, стосуються таких категорій суб’єктів даних:

- Контролера (власника облікового запису) та осіб, яким Контролер надає доступ до облікового запису;
- членів домогосподарства, працівників, відвідувачів та інших фізичних осіб, які перебувають у приміщеннях чи на об’єктах, що охороняються за допомогою Продуктів та Програмного забезпечення Ajax, які використовує Контролер. Залежно від конфігурації, визначеної Контролером, можуть фіксуватися Персональні дані таких осіб, зокрема їхні зображення та відеозаписи.

C. ПЕРІОДИЧНІСТЬ ПЕРЕДАВАННЯ ДАНИХ

Безперервно протягом усього строку використання Контролером Продуктів та Програмного забезпечення Ajax.

D. ПРЕДМЕТ, ХАРАКТЕР І ЦІЛІ ОБРОБКИ

Предмет, характер і цілі обробки визначено в розділі 2 Договору.

E. КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ

Для надання Послуг, визначених у цьому Договорі, Оператор може обробляти:

- унікальні ідентифікатори (ім’я користувача);
- інформацію про використання Продуктів та Програмного забезпечення Ajax (наприклад, запити із застосунку);
- IP-адресу;
- ім’я, прізвище та контактні дані, зазначені під час первинної реєстрації;

- вміст SMS-повідомлень із кодами доступу, що надсилаються кінцевим користувачам під час реєстрації або внесення змін до облікового запису;
- інформацію про мобільні пристрої кінцевих користувачів, зокрема про тип пристрою, операційну систему та мову інтерфейсу;
- зображення, аудіозаписи та відеозаписи, зафіксовані за допомогою Продуктів та Програмного забезпечення Ajax;
- інші дані та інформацію, якщо їх обробка необхідна.

Спеціальні категорії Персональних даних

Оператор не збирає такі дані навмисно. Зображення та відеозаписи, зафіксовані пристроями Контролера, можуть ненавмисно містити біометричні дані (наприклад, зображення облич). До будь-яких таких даних Оператор застосовує додаткові гарантії, описані в Додатку 2. Персональні дані, що належать до спеціальних категорій, можуть оброблятися лише за умови, що така обробка відповідає застосовному Законодавству про захист даних і її ініціює суб'єкт даних або Контролер.

F. СТРОК ОБРОБКИ ТА ЗБЕРІГАННЯ ДАНИХ

Протягом усього строку використання Контролером Продуктів та Програмного забезпечення Ajax. Після припинення такого використання дані мають бути видалені у строк, визначений у розділі 8 Договору.

G. КОМПЕТЕНТНИЙ НАГЛЯДОВИЙ ОРГАН

Якщо застосовується GDPR ЄС, компетентним є наглядовий орган тієї держави-члена ЄС, у якій має осідок Контролер, а якщо Контролер не має осідку в ЄС — наглядовий орган тієї держави-члена, у якій має осідок його представник. Якщо Контролер не має в ЄС ні осідку, ні представника, компетентним наглядовим органом є Комісія із захисту даних Ірландії (Data Protection Commission, DPC).

Якщо застосовується GDPR Великої Британії, компетентним наглядовим органом є Офіс комісара з питань інформації Великої Британії (Information Commissioner's Office, ICO).

ДОДАТОК 2. ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ

Цей Додаток визначає технічні та організаційні заходи (далі також — «ТОМ») і доповнює розділ 3 Договору про обробку персональних даних, укладеного між Оператором і Контролером відповідно до статті 28 GDPR (Регламенту (ЄС) 2016/679).

Інформаційна безпека

Шифрування даних: для шифрування даних під час зберігання застосовується AES-256, а для захисту даних під час передавання — TLS версії 1.2 або новішої.

Псевдонімізація: застосування хешування за алгоритмом SHA-256 до відповідних наборів даних.

Міжмережеві екрани: застосування міжмережевих екранів для вебзастосунків (WAF) та міжмережевих екранів мережевого рівня.

Контроль авторизації: доступ до інформації регулюється чітко визначеними правилами залежно від ролей.

Стійкість: захист від несанкціонованої обробки, втрати або знищення.

Резервне копіювання та відновлення: резервні копії ключових систем створюються у вигляді повних образів, що дає змогу швидко відновлювати системи. Резервні копії шифруються як під час зберігання, так і під час передавання; це стосується також копій, що зберігаються дистанційно або в хмарі. Процедури резервного копіювання та відновлення регулярно тестуються, щоб підтвердити повну працездатність процесу відновлення.

> У разі відновлення з резервної копії раніше видалені Персональні дані видаляються з відновленого набору даних без необґрунтованої затримки, але в будь-якому разі не пізніше ніж через 24 години після відновлення.

Захист від DDoS-атак: застосування спеціалізованих сервісів фільтрації трафіку та автоматизованих засобів протидії, які надає постачальник інфраструктури, для захисту від інфраструктурних атак (рівні 3/4) та атак на рівні застосунків (рівень 7).

Керування оновленнями безпеки: автоматизований моніторинг і встановлення оновлень безпеки для всіх хмарних ресурсів та операційних систем.

1. КОНФІДЕНЦІЙНІСТЬ

1.1 Контроль фізичного доступу

Належні заходи для запобігання доступу неуповноважених осіб до систем обробки даних, у яких обробляють або використовують Персональні дані.

1.2 Технічні заходи

Система сигналізації: використання власних сучасних систем безпеки Ajax (хабів, датчиків руху та сирен) із цілодобовим моніторингом і миттєвим сповіщенням.

Електронний контроль доступу: захищена система доступу до офісу за допомогою RFID-карток і брелоків; журнали доступу ведуться та регулярно перевіряються.

Відеоспостереження: IP-камери високої роздільної здатності для спостереження за входами й виходами та критично важливими зонами всередині приміщень.

Безпека хмарної інфраструктури: AWS керує фізичним доступом до серверів відповідно до підтверджень відповідності AWS вимогам SOC 2 та ISO 27001.

1.3 Організаційні заходи

Політика інформаційної безпеки: комплекс внутрішніх правил щодо фізичної безпеки та захисту активів.

Робочі інструкції з операційної безпеки: задокументовані процедури забезпечення безпеки офісних приміщень і поводження з обладнанням.

Робоча інструкція з контролю доступу: суворі процедури надання, відкликання та аудиту прав фізичного доступу працівників і підрядників.

Політика щодо відвідувачів: вимоги до реєстрації, ідентифікації та супроводу всіх відвідувачів у приміщеннях офісу.

2. КОНТРОЛЬ ЛОГІЧНОГО ДОСТУПУ

Заходи для запобігання несанкціонованому використанню систем обробки даних.

Багатофакторна автентифікація (MFA): обов'язкова під час адміністративного доступу, керування хмарною консоллю та дистанційного входу до систем.

Керування ідентичностями та доступом (IAM): централізоване керування правами користувачів із регулярним переглядом прав доступу.

Доступ через VPN: для будь-якого дистанційного підключення до середовища промислової експлуатації або внутрішніх засобів адміністрування потрібно використовувати зашифровані VPN-тунелі.

3. КОНТРОЛЬ ДОСТУПУ ДО ДАНИХ

Заходи, що забезпечують особам, уповноваженим користуватися системою обробки даних, доступ лише до даних у межах їхніх повноважень.

Керування доступом на основі ролей (RBAC): права доступу надаються виключно відповідно до посадових функцій і в межах службової необхідності.

Ведення журналів аудиту: повне журналювання всіх дій із доступу до даних, їх зміни та видалення в системах, що містять Персональні дані.

4. ЦІЛІСНІСТЬ, ДОСТУПНІСТЬ І СТІЙКІСТЬ

Контроль передавання даних: заходи, що унеможливлюють ознайомлення з Персональними даними, їх копіювання, зміну або видалення без відповідного дозволу під час електронного передавання.

Контроль внесення даних: заходи, що дають змогу перевірити та встановити, чи вносили Персональні дані до систем обробки даних, змінювали або видаляли їх, а також хто саме виконував ці дії.

Контроль доступності: заходи для захисту Персональних даних від випадкового знищення або втрати (наприклад, використання джерел безперебійного живлення (UPS) у центрах обробки даних і резервованих систем зберігання).

Безперервність діяльності та відновлення після аварій: задокументовані плани забезпечення безперервності діяльності та відновлення після аварій підтримуються в актуальному стані, тестуються та перевіряються щонайменше раз на рік.

5. ПРОЦЕДУРИ РЕГУЛЯРНОГО ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ

Керування інцидентами: задокументований процес виявлення інцидентів інформаційної безпеки та потенційних порушень захисту даних, повідомлення про них і реагування на них.

Керування вразливостями: регулярне автоматизоване сканування для виявлення вразливостей і періодичне фахове тестування інфраструктури та застосунків на проникнення.

Обізнаність працівників: регулярне навчання працівників з питань захисту даних, дотримання вимог GDPR та фішингових загроз.

Безпека персоналу: відомості про кандидатів перевіряють відповідно до належних практик найму, а всі працівники та підрядники до отримання доступу до Персональних даних підписують угоди про конфіденційність.

ДОДАТОК 3. ПЕРЕЛІК ПОГОДЖЕНИХ СУБОПЕРАТОРІВ

Оператор веде та оприлюднює актуальний перелік залучених ним субоператорів за адресою:

https://ajax.systems/gdpr-white-paper/

Оператор оновлює цей перелік перед залученням будь-якого нового субоператора відповідно до порядку, визначеного в розділі 7 цього Договору.