Товариство з обмеженою відповідальністю "Підприємство з іноземними інвестиціями "АСБІС-УКРАЇНА"

Політика захисту персональних даних

Версія 2019 року

– Зміст –

ВСТУП

1. Ця Політика обробки та захисту персональних даних (надалі – Політика) визначає порядок обробки та захисту персональних даних у Товаристві з обмеженою відповідальністю "Підприємство з іноземними інвестиціями "АСБІС-УКРАЇНА", юридичній особі, що є належним чином заснована та працює відповідно до законодавства України, код ЄДРПОУ - 25274129; юридична адреса: 03061, Україна, м. Київ, вул. Газова, будинок 30, номер телефону: +380444554410; веб-сайт: www.asbis.ua (надалі – **Компанія** або **Контролер**), та встановлює порядок, спрямований на запобігання та виявлення будь-яких порушень застосовуваних законів про персональні дані.

2. Ця Політика була розроблена відповідно до законодавства України та Європейського Союзу, а саме відповідно до наступних документів:

- Загальний регламент про захист даних (GDPR), прийнятий Європейським парламентом і Радою Європейського Союзу 27 квітня 2016 року;
- Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Рада Європи, Страсбург, 28 січня 1981 року), ратифікована Україною 06 липня 2010 року;
- Закону України «Про захист персональних даних» №2297-17 від 01 червня 2010 р.;
- будь-які інші місцеві закони щодо захисту персональних даних діють на території України.

3. Головні цілі цієї Політики:

- визначення порядку, а також умов обробки персональних даних, зокрема процедур, спрямованих на запобігання порушенню законів та процедур здійснення внутрішнього контролю відповідно до застосовуваного законодавства щодо персональних даних;
- знайомство співробітників Компанії, відповідальних за обробку персональних даних, з Політикою застосовуваного законодавства щодо персональних даних та вимогами Компанії до обробки персональних даних;
- встановлення відповідальності для співробітників, що здійснюють обробку персональних даних, за недотримання вимог застосовуваного законодавства щодо персональних даних;
- дотримання права суб'єктів персональних даних на інформування щодо способів обробки своїх персональних даних Компанією.

4. Політика є обов'язковою для всіх співробітників Компанії.

5. Здійснення захисту персональних даних припиняється, якщо Компанія припиняє свою діяльність, або у випадку знеособлювання відповідних даних, якщо інше не передбачено застосовуваним законодавством.

БАЗОВІ ВИЗНАЧЕННЯ

Для цілей цієї Політики застосовуються наступні визначення:

Уповноважений із захисту даних це людина, відповідальна за контроль над застосуванням Загального регламенту про захист даних (GDPR) та інших застосовуваних законів щодо захисту суб'єктів даних у зв'язку з обробкою персональних даних, та яка здійснює функції, покладені на нього/неї відповідно до цієї Політики та інших застосовуваних законів, а також надає поради керівництву Компанії і здійснює комунікацію між компаніями Групи АСБІС [ASBIS] щодо захисту персональних даних. Уповноважений із захисту даних призначений у

компанії-засновнику АСБІСК ЕНТЕРПРАЙЗІС ПЛС (ASBISC ENTERPRISES PLC) виконує функції Уповноваженого із захисту даних для усіх компаній групи АСБІС.

Персональні дані це будь-яка інформація, що стосується встановленої чи такої, що може бути встановлена, фізичної особи (суб'єкта даних); фізична особа, що може бути встановлена, це така особа, яка може бути ідентифікована, зокрема за ідентифікаційною інформацією, а саме за іменем, ідентифікаційним номером, даними про місцезнаходження, онлайн-ідентифікатором або за одним чи більше факторів, характерних винятково для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної чи соціальної ідентичності цієї фізичної особи.

Обробка це будь-яка операція чи набір операцій, що здійснюються над персональними даними або над групами персональних даних, незалежно від того, автоматично це здійснюється чи ні, зокрема збір, реєстрація, організація, структурування, зберігання, адаптація чи зміна, витягання, обговорення, використання, розкриття шляхом передачі, розповсюдження чи надання будь-яким іншим шляхом, впорядкування чи об’єднання, обмеження на обробку, стирання чи знищення.

Обмеження на обробку це маркування збережених персональних даних з метою обмеження їхньої обробки у майбутньому.

Формування психологічного портрету це будь-яка форма автоматизованої обробки персональних даних, що полягає у застосуванні персональних даних для оцінки особистих характеристик фізичної особи, зокрема для аналізу та прогнозування характеристик, що стосуються продуктивності цієї особи на роботі, її економічного становища, стану здоров'я, надання особистих переваг, інтересів, надійності, поведінки, місцезнаходження чи пересування.

Контролер це фізична чи юридична особа, орган державної влади, відомство чи інший орган, який, самостійно чи у співпраці з іншими, визначає цілі та засоби обробки персональних даних. Для цілей цієї Політики в якості контролера виступає Компанія.

Обробник це фізична чи юридична особа, орган державної влади, відомство чи інший орган, який здійснює обробку персональних даних від імені контролера.

Отримувач це фізична чи юридична особа, орган державної влади, відомство чи інший орган, якому розкриваються персональні дані, незалежно від того це третя сторона чи ні.

Третя сторона це фізична чи юридична особа, орган державної влади, відомство чи інший орган, окрім суб'єкта даних, контролера, обробника та осіб, які від імені контролера чи обробника є уповноваженими на обробку персональних даних.

Згода суб'єкта даних це будь-яке вільно надане, конкретне, усвідомлене та чітке виявлення бажання суб'єкта даних, з допомогою якого він чи вона шляхом висловлення чи чіткої ствердної дії висловлює згоду на обробку персональних даних, що його чи неї стосуються.

Порушення закону про захист персональних даних це порушення захисту, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття чи отримання доступу до персональних даних, що передаються, зберігаються чи якимось іншим чином оброблюються.

Дані про стан здоров'я це персональні дані, що стосуються фізичного чи психічного здоров'я фізичної особи, зокрема дані про надання медичних послуг, що розкривають інформацію про його чи її стан здоров'я.

Міжнародна обробка це одне з двох понять:

- обробка персональних даних, що здійснюється у зв'язку з діяльністю компанії у будь-якій іноземній державі, в якій розташований контролер чи обробник; або

- обробка персональних даних, що здійснюється у зв'язку з діяльністю окремого контролера чи обробника у будь-якій іноземній державі, але яка суттєво впливає чи ймовірно може суттєво впливати на суб'єкти даних у понад одній країні.

СКЛАД ПЕРСОНАЛЬНИХ ДАНИХ

1. До персональних даних, що обробляються у Компанії належать:

- персональні дані теперішніх та колишніх співробітників (ім'я, прізвище, ім'я по батькові, місце і дата народження, адреса, адреса електронної пошти, IP-адреса, номер телефону, національність (громадянство), паспортні дані, ідентифікаційний номер, ІПН, сімейний стан, інформація про дітей та чоловіка/жінку (імена, прізвища, імена по батькові, місця і дати народження, адреси, номера телефонів, паспортні дані, свідоцтва про народження, інформація про стан здоров'я), освіту (зокрема дані про університет, курси підвищення кваліфікації та отримані сертифікати), професію, досвід роботи, знання іноземних мов, фінансовий стан, розмір доходу, майно, зарплатню, обсяг МВО, банківські реквізити, інформація про стан здоров'я, відсутність або наявність судимості, податкова інформація);
- персональні дані членів сімей співробітників (імена, прізвища, імена по батькові, місця і дати народження, адреси, номера телефонів, паспортні дані, свідоцтва про народження, інформація про стан здоров'я);
- персональні дані кандидатів на посади (ім'я, прізвище, ім'я по батькові, місце і дата народження, адреса, адреса електронної пошти, номер телефону, національність (громадянство), категорія кіпрської візи (якщо така є), сімейний стан, інформація про дітей та чоловіка/жінку, освіту (зокрема дані про університет, курси підвищення кваліфікації та отримані сертифікати), професію, досвід роботи, знання іноземних мов, бажану зарплатню та зарплатню на останньому місці роботи);
- персональні дані контактних осіб контрагентів за договорами (про надання послуг, доставку товарів, дистрибуцію, ліцензування тощо), а також осіб, що є сторонами, або представляють юридичні особи, що є сторонами таких договорів (ім'я, прізвище, ім'я по батькові, посада, номер телефону, адреса електронної пошти, паспортні дані, громадянство, адреса проживання, ІПН, банківські реквізити, підпис).

2. Особливі категорії персональних даних:

Компанія не обробляє жодної інформації, що стосується расової чи національної належності, політичних поглядів, релігійних чи філософських переконань, інтимного та особистого життя, окрім наступних випадків:

- суб'єкт персональних даних дав свою письмову згоду на обробку вказаних персональних даних;
- згадані персональні дані є доступними у відкритих джерелах (є чітко оприлюдненими суб'єктом даних), зокрема в соціальних мережах. Обробка персональних даних має негайно зупинитися, якщо для такої обробки немає необхідності.

3. Отримання персональних даних:

- Компанія може отримувати усі персональні дані суб'єкта безпосередньо від самого суб'єкта чи з інших джерел, зокрема від рекрутингової фірми, з відкритих джерел, соціальних мереж, від органів державної влади, з файлів кукі тощо.
- Компанія залишає за собою право перевіряти цілісність та достовірність персональних даних, наданих суб'єктом персональних даних чи кимось ще.

4. Компанія використовує файли кукі (файл кукі це невеликий обсяг даних, до якого зазвичай входить унікальний ідентифікатор, що надсилається на браузер користувацького комп'ютера із серверу, на якому розташований веб-сайт, та зберігається на жорсткому диску користувацького комп'ютера; він дозволяє веб-сайту запам'ятовувати такі речі, як надання переваг і вміст кошика користувача) та схожі технології на своїх сайтах, зокрема на будь-яких сайтах чи мобільних додатках, що керуються Компанією, її дочірніми чи партнерськими компаніями, або від імені цих компаній. Політика компанії групи компаній АСБІС [ASBIS] щодо файлів кукі пояснює, яким чином файли кукі використовуються на веб-сайтах групи компаній АСБІС [ASBIS] в цілому: http://www.asbis.com/cookies-policy.

ЦІЛІ ОБРОБКИ

Правові підстави та цілі обробки персональних даних є наступними:

1. Цілі обробки персональних даних теперішніх співробітників:

- підготовка до укладення, укладення та виконання трудового договору чи договору про надання послуг у відповідності до законодавства України;
- отримання допусків на роботу для іноземних робітників, підготовка для них дозволів на працевлаштування та робочих віз;
- реалізація соціальних програм (зокрема із залучення до плану добровільного медичного страхування) для надання пільг та соціальних гарантій;
- здійснення податкової, юридичної діяльності, діяльності, пов'язаної з людськими ресурсами, фінансового обліку, розрахунок зарплатні та підготовка податкової звітності;
- реалізація спільно з освітніми закладами програм професійної підготовки, навчання та професійної перепідготовки співробітників, зокрема з метою забезпечення їхньої відповідності стандартам професійної кваліфікації;
- підготовка пропусків, що надають доступ на територію Компанії;
- формування внутрішніх джерел персональних даних співробітників, що містять контактну та іншу комерційну інформацію, що підлягає обробці членами Групи компаній АСБІС [ASBIS], зокрема з метою внутрішнього аудиту Компанії для забезпечення відповідності вимогам застосовуваного законодавства;
- забезпечення обміну інформацією, скоординованої роботи та розповсюдження достовірної інформації та інших матеріалів про діяльність Компанії всередині Групи компаній АСБІС [ASBIS], зокрема між спеціалізованими функціональними підрозділами чи групами, члени якої можуть розташовуватися у різних країнах та на різних територіях;
- забезпечення обміну інформацією, скоординованої роботи та розповсюдження достовірної інформації та інших матеріалів про діяльність Компанії між Компанією та її теперішніми і потенційними клієнтами, зокрема під час надання конкретної інформації у пропозиціях про співпрацю та в контрактній документації, а також для планування зобов'язань по відношенню до бізнес-партнерів;
- просування послуг Компанії, незалежно від часу, форми та території;
- ведення політики співробітництва з урядовими органами та місцевими органами влади;
- аналітичне дослідження даних про співробітників Компанії та людей, які працювали в Компанії раніше, з метою підготовки та впровадження програм, спрямованих на

поліпшення умов праці та соціального забезпечення співробітників Компанії;

- забезпечення відповідності вимогам законодавства та інших нормативно-правових актів, допомога у працевлаштуванні, навчанні та кар'єрному зростанні, контроль обсягу та якості виконаної роботи, а також захист майна Компанії;
- співпраця з органами державної влади стосовно вищезгаданих питань;
- інші види діяльності, що не суперечать законодавству України та Європейського Союзу та їхнім вимогам, що стосуються персональних даних.

2. Цілі обробки персональних даних членів сімей співробітників:

- отримання ними гостьових віз (віз для чоловіка/жінки);
- реалізація соціальних програм (залучення до програми добровільного медичного страхування тощо);
- комунікація з членами сімей співробітників при виникненні надзвичайних ситуацій;
- ведення політики співробітництва з урядовими органами та місцевими органами влади;
- інші види діяльності, що не суперечать застосовуваному законодавству та його вимогам, що стосуються персональних даних.

3. Цілі обробки персональних даних кандидатів на посади:

- перевірка правильності, точності та актуальності інформації, що міститься у резюме кандидата, поданого до Компанії або рекрутингової фірми, що співпрацює з Компанією;
- ведення політики співробітництва з урядовими органами та місцевими органами влади;
- аналіз даних кандидатів з метою подальшої роботи з відкритими вакансіями;
- інші види діяльності, що не суперечать застосовуваному законодавству та його вимогам, що стосуються персональних даних.

4. Цілі обробки персональних даних співробітників та контактних осіб контрагентів за договором про надання послуг, а також осіб, що є сторонами або представниками юридичних осіб, що є сторонами договору про надання послуг чи іншого договору:

- укладення та виконання угод, зокрема договорів про надання послуг, доставку товарів, дистрибуцію, ліцензування тощо; взаємодія з членами Групи АСБІС [ASBIS], які можуть працювати у різних країнах та на різних територіях, зокрема з метою внутрішніх перевірок Компанії для забезпечення відповідності міжнародним стандартам та вимогам законодавства;
- ведення політики співробітництва з урядовими органами та місцевими органами влади;
- аналіз даних про колишніх, теперішніх та потенційних клієнтів і постачальників Компанії для підвищення продажів, підвищення ефективності маркетингової діяльності, вдосконалення бізнес-процедур, підвищення якості послуг та підтримки рівня лояльності клієнтів;
- інші види діяльності, що не суперечать застосовуваному законодавству та його вимогам, що стосуються персональних даних.

ДАТА НАБРАННЯ ЧИННОСТІ

Ця Політика набирає чинності з 25 травня 2018 року.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

1. Обробка персональних даних:

- Обробка персональних даних є конфіденційною. Вона має здійснюватися лише особами, що діють від імені Компанії та лише за її вказівками.
- Доступ до персональних даних надається лише тим зі співробітників Компанії, яким такі персональні дані необхідні для виконання своїх обов'язків, пов'язаних з будь-якою з вищезгаданих цілей обробки (зокрема для роботи відділу роботи з персоналом, юридичного відділу, відділу фінансів, відділу інформаційних технологій та адміністрації). Будь-який доступ до персональних даних для інших співробітників Компанії, які не мають прав доступу відповідно до умов цієї Політики, є заборонений.
- Співробітники Компанії, що мають доступ до персональних даних, мають право на обробку лише тих персональних даних, які їм необхідні для виконання своїх конкретних службових обов'язків, пов'язаних з будь-якою з вищезгаданих цілей обробки.
- Документи, що містять персональні дані, зберігаються у структурних відділах Компанії, співробітники яких мають доступ до персональних даних, пов'язаних із виконанням їх службових обов'язків, та несуть відповідальність за взаємодію з відповідним суб'єктом персональних даних.
- Компанія має право доручити третій стороні здійснювати обробку персональних даних за згодою суб'єкта персональних даних, або в інших випадках, передбачених застосовуваним законом, без такої згоди (наприклад, для перевірки правильності, точності та актуальності інформації, що міститься у резюме кандидата на роботу, підготовки дозволів на роботу та робочих віз, оформлення медичного страхування, здійснення податкового, юридичного обліку, обліку, пов'язаного з людськими ресурсами, фінансового обліку, розрахунку зарплатні та підготовки податкової звітності).
- Особа, що обробляє персональні дані від імені Компанії, дотримується принципів та правил обробки персональних даних, встановлених цією Політикою.
- Якщо Компанія доручає іншій особі здійснювати обробку персональних даних, Компанія несе відповідальність перед суб'єктом персональних даних за дії чи упущення такої особи. Особа, що обробляє персональні дані від імені Компанії, несе відповідальність за це перед Компанією.
- Якщо співробітник, що має доступ до персональних даних, є відсторонений від посади, документи та інші матеріали, що містять персональні дані, передаються іншому співробітнику, що має доступ до персональних даних під свій підпис відповідно до наказу керівника структурного підрозділу.
- Зберігання персональних даних, що стосуються особистого життя, зокрема особистого листування, особистих документів та фотографій на персональних робочих комп'ютерах/ноутбуках, персональних робочих мобільних телефонах/смартфонах та/або інших робочих пристроях, є суворо забороненим. Усі робочі пристрої мають використовуватися лише для виконання робочих обов'язків. Компанія має право перевіряти усі персональні робочі пристрої в будь-який момент часу та з будь-яких причин.

2. Система для зберігання персональних даних та авторизації у службах:

- Персональні дані головним чином зберігаються на електронних носіях (на серверах, сховищах, персональних комп'ютерах та інших видах пристроїв зберігання, що застосовуються співробітниками та/або компанією). Електронні бази даних, що містять персональні дані, захищені з допомогою сервера чи механізмів автентифікації, вбудованих в конкретний додаток та/або базу даних.
- Жодні персональні дані не зберігаються на персональних комп'ютерах чи персональних пристроях, окрім тих персональних пристроїв, що є повністю зашифровані з допомогою корпоративних застосунків та дискового шифрування.
- Дозвіл на доступ до персональних даних надається лише уповноваженим особам, що користуються службами автентифікації. Ці особи мають доступ та дозволи лише щодо даних, доступ та дозволи щодо яких є дозволеними.
- Дозвіл на доступ до застосунків, що містять персональні дані та є територіально розосередженими, надається шляхом авторизації за іменем користувача, паролем та токеном, тобто з використанням двофакторної автентифікації для забезпечення найвищого рівня безпеки.
- *Сервер авторизації.* Сервер авторизації здійснює автентифікацію користувачів з допомогою імені користувача та пароля. Коли користувача автентифіковано, до конкретних місць зберігання даних та баз даних застосовуються конкретні дозволи. Сервер автентифікації не зберігає жодні конфіденційні дані на локальних пристроях користувачів, зокрема паролі для входу до системи, а лише переписку між унікальним ідентифікатором користувача та токени, видані цим сервером.
- *Серверне сховище персональних даних (DSI).* Територіально розосереджена група серверів, що зберігають дані користувача у зашифрованому вигляді. Застосовується для AES/GCM/PKCS5Padding-шифрування та має індивідуальний ключ для кожного користувача. При зберігання даних користувача обирається сервер, розташований у країні користувача.
- *Сервер зберігання ключів (DSC).* Сервер, що зберігає відкриті ключі, які застосовуються для шифрування даних користувача. Якщо цей сервер виходить з ладу, дані користувача не можуть бути розшифровані, оскільки необхідна пара з відкритого та закритого ключів.
- *Сервер доступу до даних (API).* Територіально розосереджені сервери для реєстрації та зміни користувацьких даних, а також доступу до користувацьких даних для обробки замовлень з системи управління відносинами з клієнтами та веб-сайту.

3. Заходи із забезпечення безпеки персональних даних:

- Компанія вживає усіх належних організаційних та технічних заходів для забезпечення безпеки персональних даних та їх захисту від випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розповсюдження чи отримання до них доступу, а також від будь-якої іншої форми незаконної обробки, зокрема обмеження цілей, мінімізацію даних та обмежені періоди зберігання (як визначено нижче у розділі «Політика зберігання»).
- Такі заходи забезпечують рівень безпеки, що є належним відповідно до ризиків, пов'язаних з обробкою, та характером даних, що обробляються.
- За відсутності співробітника на його столі не має залишатися жодних документів, що містять персональні дані («Політика чистого столу»).
- Компанія забезпечує належну підготовку із захисту персональних даних для

співробітників, що мають постійний чи регулярний доступ до персональних даних.

4. Міжнародна передача:

Компанія може надавати персональні дані членам групи АСБІС [ASBIS] в інших країнах для наступних цілей:

- формування внутрішніх джерел персональних даних співробітників, що містять контактну та іншу комерційну інформацію, що підлягає обробці членами Групи компаній АСБІС [ASBIS], зокрема з метою внутрішнього аудиту Компанії для забезпечення відповідності вимогам застосовуваного законодавства;
- забезпечення обміну інформацією, скоординованої роботи та розповсюдження достовірної інформації та інших матеріалів про діяльність Компанії всередині Групи компаній АСБІС [ASBIS], зокрема між спеціалізованими функціональними підрозділами чи групами, члени якої можуть розташовуватися у різних країнах та на різних територіях;
- забезпечення обміну інформацією, скоординованої роботи та розповсюдження достовірної інформації та інших матеріалів про діяльність Компанії між Компанією та її теперішніми і потенційними клієнтами, зокрема під час надання конкретної інформації у пропозиціях про співпрацю та в контрактній документації, а також для планування зобов'язань по відношенню до бізнес-партнерів.

У вищезгаданих випадках Компанія та її партнери повинні вжити усіх належних організаційних та технічних заходів для забезпечення безпеки персональних даних та їх захисту від несанкціонованого доступу та розкриття. Компанія та її партнери повинні забезпечити:

- надання доступу до персональних даних лише для тих співробітників, яким такі персональні дані необхідні для виконання своїх обов'язків; заборону будь-якого несанкціонованого доступу;
- збереження суворої конфіденційності документів та інформації, що містить персональні дані, з уникненням несанкціонованого доступу до них та/або їх розкриття;
- розкриття та обробку персональних даних за принципом мінімізації даних (надання та обробка лише тих даних, які є необхідними для цілей обробки);
- зберігання персональних даних не довше, ніж це необхідно для цілей обробки, якщо інший термін не передбачений застосовуваним законодавством та законними інтересами Компанії та її партнерів; максимально можливе обмеження доступу до персональних даних, які неможливо видалити, та/або їх знеособлювання.

Компанія має право передавати персональні дані на території наступних країн:

- Країни Європейського Союзу, а саме: Австрія, Бельгія, Болгарія, Хорватія, Кіпр, Чеська Республіка, Данія, Фінляндія, Франція, Німеччина, Греція, Угорщина, Ірландія, Італія, Латвія, Литва, Люксембург, Мальта, Нідерланди, Польща, Португалія, Румунія, Словаччина, Словенія, Іспанія, Швеція, Велика Британія.
- Країни, що знаходяться поза межами Європейського Союзу, але які Європейська комісія на сьогодні визнала такими, що забезпечують належний рівень захисту, а саме: Андорра, Аргентина, Канада (комерційні організації), Фарерські острови, Гернсі, Ізраїль, Острів Мен, Джерсі, Нова Зеландія, Швейцарія, Уругвай та США (в межах програми із захисту конфіденційності між ЄС та США). Ці рішення про достатність заходів не розповсюджуються на обмін даними у правоохоронній

сфері, який регулюються «Директивою про поліцію» (стаття 36 Директиви (EU) № 2016/680).

- Треті країни, що не забезпечують належного рівня захисту прав суб'єктів даних, якщо така передача даних є вкрай необхідною (наприклад, для укладення чи виконання контракту між суб'єктом даних та Компанією або членом групи АСБІС [ASBIS], чи контракту, укладеного в інтересах суб'єкта даних між Компанією та іншою фізичною чи юридичною особою; або якщо передача даних необхідна для обґрунтування, подання чи захисту правових претензій суб'єкта даних). У випадках міжнародної передачі даних до третіх країн Компанія забезпечує наявність належних заходів з безпеки та ефективних засобів правового захисту для суб'єктів даних.

5. Механізм співробітництва з контролюючим органом:

- Компанія забезпечує перевірку відповідності вимогам цієї Політики, зокрема щоквартальне проведення перевірок захисту персональних даних та застосування методів із забезпечення корегуючих заходів для захисту прав суб'єкта даних. Результати такої перевірки мають бути передані уповноваженому із захисту даних, а доступ до них має здійснюватися за запитом компетентного контролюючого органу.

ПОЛІТИКА ЗБЕРІГАННЯ

1. Компанія зберігає та обробляє персональні дані теперішніх та колишніх співробітників, членів їхніх сімей, кандидатів на роботу, постачальників послуг та контактних осіб контрагентів за наступних умов:

- Персональні дані співробітників та членів їхніх сімей зберігаються та обробляються впродовж терміну дії трудового договору та впродовж 7 (семи) років після його розірвання, якщо інший термін не передбачений застосовуваним законодавством та законними інтересами Компанії (наприклад, для цілей оподаткування та аудиту, звітування перед державними фондами та іншими уповноваженими органами).
- Персональні дані кандидатів на роботу зберігаються та обробляються впродовж 1 (одного) року з моменту першого контакту з кандидатом на роботу, якщо інший термін не передбачений застосовуваним законодавством та законними інтересами Компанії (наприклад, для цілей статистики та формування бази даних кандидатів).
- Персональні дані постачальників послуг зберігаються та обробляються впродовж терміну дії договору про надання послуг (або іншого), якщо інший термін не передбачений застосовуваним законодавством та законними інтересами Компанії (наприклад, для цілей оподаткування та аудиту).
- Персональні дані контактних осіб контрагентів зберігаються та обробляються впродовж терміну ділових відносин, якщо інший термін не передбачений застосовуваним законодавством та законними інтересами Компанії.

2. Компанія вживає усіх належних організаційних та технічних заходів для забезпечення безпеки персональних даних, як це визначено у розділі «Захист персональних даних» вище.

3. Якщо персональні дані видалити неможливо, доступ до цих даних має бути максимально можливо обмеженим, та/або самі персональні дані повинні бути знеособлені.

ПОРЯДОК НАЙМАННЯ ТА ЗВІЛЬНЕННЯ СПІВРОБІТНИКІВ

1. Наймання співробітників.

- Коли на роботу наймається новий співробітник, співробітнику IT-служби має бути повідомлено (словесно чи електронною поштою) завчасно, а саме не пізніше, ніж за 5 (п'ять) робочих днів до дати наймання, відповідним керівником відділу та/або керівником відділу роботи з персоналом про дані нового співробітника (ім'я, прізвище, ідентифікаційний номер, відділ, посада та ресурси, до яких має бути наданий доступ) для створення особистого облікового запису, надання необхідних інформаційних доступів та дозволів тощо.
- В перший робочий день новому співробітнику надається все необхідне обладнання (персональні робочі комп'ютери/ноутбуки, персональні робочі мобільні телефони/смартфони та/або інші робочі пристрої) та доступ до необхідних інформаційних систем. Співробітник IT-служби виконує відповідний запис у спеціальному реєстрі обладнання, а співробітник ставить підпис у згаданому реєстрі, посвідчуючи цим, що він/вона отримав(ла) необхідне робоче обладнання.
- Відділ роботи з персоналом зберігає персональну інформацію про нового співробітника у теці на диску та друковані екземпляри у шафі, що зачиняється. Також деякі персональні дані вносяться в інформаційні системи Компанії, і ці дані є доступними для:

a) керівника відділу (ім'я, прізвище, ідентифікаційний номер, відділ, посада, зарплатня, сімейний стан);

b) відділу роботи з персоналом (усі персональні дані про співробітника);

c) фінансового відділу (ім'я, прізвище, ідентифікаційний номер, відділ, посада, зарплатня);

d) IT-служби (ім'я, прізвище, ідентифікаційний номер, відділ, посада).

2. Звільнення співробітника.

- Коли трудовий договір розривається, незалежно від причини розірвання, про це співробітника IT-служби має бути сповіщено (словесно чи електронною поштою) завчасно, а саме не пізніше, ніж за 5 (п'ять) робочих днів до дати розірвання, відповідним керівником відділу та/або керівником відділу роботи з персоналом. Після цього співробітник IT-служби припиняє роботу усіх інформаційних служб та доступ до даних для відповідного співробітника. Відділ роботи з персоналом вносить оновлені дані до інформаційної системи, і картка співробітника втрачає силу, але всі дані зберігаються в системі (якщо це необхідно, у знеособленому вигляді).
- Співробітник не пізніше, ніж у свій останній робочий день, повертає усі персональні робочі комп'ютери/ноутбуки, персональні робочі мобільні телефони/смартфони та/або інші робочі пристрої. Якщо співробітник йде з компанії з робочим комп'ютером/ноутбуком (за попередньою домовленістю з Компанією), співробітник IT-служби видаляє усі дані з такого ноутбуку та встановлює нову операційну систему.
- Співробітник також подає на підпис робочий обхідний лист усім відповідальним керівникам відділів (IT, відділ роботи з персоналом, фінансовий та юридичний відділ тощо), який засвідчує, що співробітник їм нічого не винний.

УПОВНОВАЖЕНИЙ ІЗ ЗАХИСТУ ДАНИХ

1. Призначення уповноваженого із захисту даних.

- Уповноважений із захисту даних призначається Радою Директорів материнської

компанії ASBISC ENTERPRISES PLC за рекомендацією одного з директорів компанії ASBISC ENTERPRISES PLC з урахуванням його/її професійних якостей та, зокрема, експертних знань про законодавство та практики захисту даних і можливості виконання завдань. Компанія надає контролюючому органу контактні дані призначеного уповноваженого із захисту даних.

- Особа, що бере участь у процесі управління та прийнятті фінансових рішень від імені Компанії, що передбачають вигоду для чи розподіл доходів Компанії, включаючи укладання значних правочинів чи правочинів щодо яких є заінтересованість, не може бути призначена уповноваженим із захисту даних.

2. Обов'язки уповноваженого із захисту даних. Уповноважений із захисту даних виконує наступні завдання:

- інформує та консультує Компанію і співробітників, що здійснюють обробку даних, щодо їхніх обов'язків відповідно до Загального регламенту про захист даних (GDPR) та інших застосовуваних законів;
- контролює забезпечення відповідності цієї Політики та інших документів та процедур Компанії щодо захисту персональних даних вимогам Загального регламенту про захист даних (GDPR) та інших застосовуваних законів;
- визначає зобов'язання, підвищує інформованість та здійснює підготовку персоналу, залученого до процесу обробки даних та пов'язаних з цим перевірок;
- надає консультації на вимогу Компанії щодо оцінки впливу захисту даних та контролює цей процес;
- співпрацює з контролюючим органом та здійснює розгляд скарг;
- виступає, як контактна особа з контролюючим органом з питань, що стосуються обробки даних, зокрема проводить попередню консультацію з контролюючим органом (якщо оцінка впливу захисту даних свідчить про те, що обробка даних призведе до високого ступеня ризику за умови відсутності вжиття заходів Компанією для зниження ступеня цього ризику), та консультує, якщо це необхідно, щодо будь-яких інших питань;
- при виконанні своїх завдань належним чином враховує ризик, пов'язаний з обробкою даних, з урахуванням характеру, обсягу, обставин та цілей обробки;
- контактує з суб'єктами даних щодо усіх питань, пов'язаних із обробкою їхніх персональних даних та здійсненням їхніх прав відповідно до Загального регламенту про захист даних (GDPR);
- зв'язаний зобов'язаннями із дотримання таємності та конфіденційності під час виконання своїх завдань відповідно до закону;
- здійснює комунікацію між компаніями Групи АСБІС [ASBIS] щодо захисту персональних даних;
- здійснює оцінку внутрішніх процедур, документів та процесів для їх відповідності вимогам Загального регламенту про захист даних (GDPR);
- може виконувати інші завдання та обов'язки, за умови що будь-які такі завдання та обов'язки не призводять до конфлікту інтересів.

3. Конфлікти інтересів.

- Уповноважений із захисту даних повинен розуміти та уникати ситуацій, що створюють або можуть створити конфлікт між його/її особистою вигодою, інтересами компанії групи компаній АСБІС [ASBIS] та захисту персональних даних.
- Конфлікт інтересів може відбуватися, коли особиста діяльність, фінансові внески чи об'єднання, до яких входить уповноважений із захисту даних, негативно впливають на його/її судження чи здатність діяти в нагальних інтересах групи

компаній АСБІС [ASBIS] та захисту персональних даних. Щоб зберегти незалежність уповноважений із захисту даних завжди надає інформацію групі компаній АСБІС [ASBIS] про свої відносини, об'єднання, до яких він входить, чи діяльність, що може створити реальні чи потенційні конфлікти інтересів; щоб надати можливість належним чином оцінити та вирішити ситуацію.

- Уповноважений із захисту даних має бути впевнений, що його/її сторонні ділові ініціативи та інша комерційна чи фінансова діяльність не суперечать його/її обов'язкам щодо захисту персональних даних. Уповноважений із захисту даних не може застосовувати обладнання чи ресурси (зокрема конфіденційну інформацію чи об'єкти інтелектуальної власності, або конфіденційну інформацію чи об'єкти інтелектуальної власності клієнтів групи компаній АСБІС [ASBIS] чи інших третіх сторін) для виконання цієї сторонньої діяльності; він також забезпечує, що вони не будуть ставити під загрозу конфіденційність та безпеку персональних даних. Уповноважений із захисту даних не може бути залучений до будь-якої діяльності, що порушує конфіденційність та безпеку персональних даних чи його/її незалежність, чи є незаконною, аморальною або такою, що негативно впливатиме на захист персональних даних.
- Щоб уникати реальних чи потенційних конфліктів інтересів, уповноважений із захисту даних не повинен брати участь у прийманні будь-яких рішень щодо поточних ділових відносин з Компанією, персональних ділових ініціатив чи суб'єктів господарювання, в яких уповноважений із захисту даних має значні фінансові внески чи в яких обіймає керівну посаду. Так само уповноважений із захисту даних повинен утримуватися від використання інформації про ділові можливості та персональні дані, які йому/їй стали відомі через перебування на посаді в групі компаній АСБІС [ASBIS], для своєї власної чи чиєїсь вигоди, окрім випадків, коли це дозволяє закон та застосовувана політика групи компаній АСБІС [ASBIS].

4. Зобов'язання Компанії перед уповноваженим із захисту даних.

Компанія повинна виконувати наступні дії:

- забезпечувати належне та своєчасне залучення уповноваженого із захисту даних у всіх питаннях, що стосуються захисту персональних даних;
- підтримувати уповноваженого із захисту даних у виконанні його/її завдань шляхом надання ресурсів, необхідних для виконання цих завдань, та доступу до персональних даних і процесу обробки даних, а також для збереження його/її експертних знань;
- забезпечувати, щоб уповноважений із захисту даних не отримував жодних вказівок щодо виконання цих завдань; він/вона не має бути відсторонений(на) чи покараний(на) Компанією за виконання своїх завдань; уповноважений із захисту даних безпосередньо звітує перед вищим керівництвом Компанії;
- забезпечувати, щоб будь-які такі завдання та обов'язки уповноваженого із захисту даних не призводили до конфлікту інтересів.

ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Суб'єкт, персональні дані якого обробляються Компанією, має наступні права:

1. **Право на інформування** – отримання від Компанії наступної інформації:
   - ідентифікаційні та контактні дані Компанії, дані її представників та уповноваженого із захисту даних;
   - цілі та правові підстави для обробки персональних даних, законні інтереси

Компанії;

- категорії персональних даних;
- отримувачі персональних даних, зокрема отримувачі у третій країні чи міжнародній організації (якщо такі є), та зазначення належних заходів і засобів безпеки;
- термін, впродовж якого зберігаються персональні дані, чи критерії, що застосовуються для визначення цього терміну, за умови, що Компанія зберігає та обробляє персональні дані впродовж часу, який вимагається застосовуваними законами та нормативно-правовими актами; обробка персональних даних має негайно зупинитися, якщо для такої обробки немає необхідності;
- існування способів автоматизованого прийняття рішень, зокрема формування психологічного портрету, а також важливість та передбачені наслідки такої обробки для суб'єкта даних;
- з якого джерела отримані персональні дані (якщо персональні дані були отримані не від суб'єкта даних);
- чи є надання персональних даних вимогою закону, договору, або вимогою, необхідною для укладення договору; чи зобов'язаний суб'єкт даних надавати персональні дані та які можливі наслідки ненадання таких даних.

2. **Право на доступ до персональних даних** – отримання від Компанії підтвердження обробки/не обробки даних, а також право на отримання копії будь-якого запису, що містить його/її персональні дані.
3. **Право на уточнення** – отримання від Компанії без необґрунтованої затримки можливості виправлення неточних персональних даних про нього/неї, доповнення неповних персональних даних, зокрема шляхом надання додаткової заяви.
4. **Право на стирання («право на можливість забуття»)** – отримання від Компанії можливості стирання персональних даних без необґрунтованої затримки (якщо персональні дані більш не є необхідними для цілей, для яких вони були зібрані, якщо суб'єкт даних відкликає свою згоду, якщо персональні дані оброблялися незаконно тощо).
5. **Право на обмеження** на обробку, якщо персональні дані є неточними; обробка є незаконною, а суб'єкт даних подає запит про обмеження використання даних замість їх видалення; персональні дані більш не є необхідними для цілей обробки, але вони вимагаються суб'єктом для обґрунтування, подання чи захисту правових претензій; суб'єкт даних висловив заперечення проти обробки, щодо якої має бути здійснена перевірка в контексті того, чи переважають законні підстави контролера над законними підставами суб'єкта даних.
6. **Право на перенесення даних** – отримання персональних даних у структурованому, загальноприйнятому та придатному для комп'ютерного читання вигляді, а також право на передачу цих персональних даних до іншого контролера без перешкод з боку Компанії (якщо обробка ґрунтується на згоді чи на договорі і здійснюється з допомогою засобів автоматизованої обробки).
7. **Право на заперечення** в будь-який момент часу проти обробки персональних даних (зокрема проти формування психологічного портрету, що базується на цих положеннях, та випадків, коли персональні дані обробляються для цілей адресного маркетингу).
8. **Право на відкликання згоди** в будь-який момент часу без впливу на законність обробки, яка здійснювалася за згодою, що була надана до її відкликання. Таким

чином, суб'єкт даних розуміє та погоджується з тим, що в разі відкликання цілей обробки персональних даних досягнути не вдасться.

9. **Право на подання скарги до контролюючого органу**, а саме до Уповноваженого Верховної Ради України з прав людини та Секретаріату Уповноваженого із захисту персональних даних, якщо суб'єкт даних вирішить, що його/її права порушені.
10. **Право на дієвий судовий захист** проти контролюючого органу, Компанії чи іншого оброблювача даних.
11. **Право на отримання відшкодування** від Компанії чи іншого оброблювача даних за завдану шкоду.

ВІДПОВІДАЛЬНІСТЬ

1. Особи, винні у порушенні цієї Політики, притягуються до відповідальності та підлягають покаранню, як це встановлено діючим законодавством України та іншими застосовуваними законами.

2. У випадку порушення цієї Політики (розкриття персональних даних неуповноваженим співробітникам та/або іншим третім сторонам, втрата документів чи будь-яких інших матеріалів, що містять персональні дані тощо), Компанія має право застосувати до такого співробітника наступні заходи дисциплінарного покарання: попередження, відсторонення та інші заходи відповідальності, передбачені застосовуваним законодавством.

3. Компанія несе відповідальність за будь-які порушення цієї Політики відповідно до застосовуваного законодавства.

ЗМІНИ ТА ДОПОВНЕННЯ

Компанія може за необхідності змінювати чи вносити доповнення до цієї Політики. Це, наприклад, може відбуватися через зміни у законодавстві, або якщо Компанія змінює профіль діяльності чи практики ведення бізнесу.

Усі зміни будуть доступними за наступним посиланням: asbis.ua; буде також вважатися, що суб'єкти даних погодилися з положеннями Політики одразу після оприлюднення цих змін на веб-сайті.

Компанія закликає суб'єктів персональних даних час від часу ознайомлюватись з Політикою конфіденційності на сайті Компанії.

КОМАНДА, ВІДПОВІДАЛЬНА ЗА ПЕРСОНАЛЬНІ ДАНІ

Олександр Феоклістов
Консультант з правових питань, уповноважений із захисту персональних даних
АСБІСК ЕНТЕРПРАЙЗІС ПЛС [ASBISC ENTERPRISES PLC]
вулиця Колонакіоу, 43, Даймонд Коурт
Агіос Атанасіос, 4103, Лімасол, Кіпр
Телефон: +357 25 857 163
Факс: +357 25 857 288
E-mail: info@asbis.com, a.feoktistov@asbis.com

Юлія Приходько

Директор з кадрових питань
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"ПІДПРИЄМСТВО З ІНОЗЕМНИМИ ІНВЕСТИЦІЯМИ
"АСБІС-УКРАЇНА"
03061, Україна, м. Київ, вул. Газова, 30
Телефон: +380444554411
Факс: +380444554410
E-mail: jp@asbis.ua

Андрій Гордієнко
Адміністратор системи IT4profit
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"ПІДПРИЄМСТВО З ІНОЗЕМНИМИ ІНВЕСТИЦІЯМИ
"АСБІС-УКРАЇНА"
03061, Україна, м. Київ, вул. Газова, 30
Телефон: +380444554411
Факс: +380444554410
E-mail: red@asbis.ua

Віталій Крамар
Адміністратор системи IT4profit
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"ПІДПРИЄМСТВО З ІНОЗЕМНИМИ ІНВЕСТИЦІЯМИ
"АСБІС-УКРАЇНА"
03061, Україна, м. Київ, вул. Газова, 30
Телефон: +380444554411
Факс: +380444554410
E-mail: v.kramar@asbis.ua