Політика захисту персональних даних

DID GLOBAL Ltd.

Ми в DID GLOBAL Ltd. прагнемо забезпечити безпечну обробку персональних даних та поважаємо право на приватність відповідних осіб.

Номер версії та дата останнього оновлення документу:	v. 1.0. [20/04/2022]
Погоджено:	BV, CEO of DID GLOBAL Ltd
Ця політика повинна переглядатися щорічно або щоразу, коли відбуваються зміни у нашій обробці даних.	

1. Сфера застосування та визначення

1.1. Обсяг. Ця **Політика захисту персональних даних** (далі — **«Політика»**) описує внутрішні правила DID GLOBAL Ltd. щодо обробки та захисту персональних даних. Політика застосовується до DID GLOBAL Ltd., включно зі співробітниками та підрядниками DID GLOBAL Ltd. (далі — **«ми», «нас», «наш», «DID GLOBAL»**). Керівництво кожного юридичного утворення несе остаточну відповідальність за впровадження цієї Політики, а також за забезпечення на рівні відповідного утворення наявності адекватних і ефективних процедур для її реалізації та постійного контролю за дотриманням. Для цілей цієї Політики співробітники та підрядники разом надалі іменуються **«співробітники»**.

1.2. Менеджер з конфіденційності. Менеджер з конфіденційності — це співробітник DID GLOBAL Ltd., відповідальний за дотримання вимог щодо захисту персональних даних у DID GLOBAL Ltd. (далі — **«Менеджер з конфіденційності»**). Менеджер з конфіденційності відповідає за виконання обов'язків, передбачених цією Політикою, та за нагляд за іншими співробітниками, на яких поширюється ця Політика, щодо їхнього дотримання Політики. Менеджер з конфіденційності має бути залучений до всіх проєктів на ранньому етапі, щоб врахувати аспекти захисту персональних даних уже на стадії планування.

1.3. Визначення.
1.3.1. Компетентний наглядовий орган означає публічний орган, який відповідає за регулювання та нагляд у сфері захисту персональних даних щодо діяльності DID GLOBAL.
1.3.2. DID GLOBAL означає DID GLOBAL Ltd. — товариство з обмеженою відповідальністю з основним місцем діяльності за адресою: 3RD FLOOR SUITE 207 REGENT STREET, ENGLAND, W1B3HH, UNITED KINGDOM.
1.3.3. Порушення даних означає порушення безпеки та/або конфіденційності, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до Персональних даних, які передавалися, зберігалися або іншим чином оброблялися. Це включає, але не обмежується, електронними листами, надісланими на неправильний або розкритий перелік отримувачів, незаконною публікацією Персональних даних, втратою або крадіжкою фізичних носіїв, а також несанкціонованим доступом до персональної інформації.
1.3.4. Контролер даних означає фізичну або юридичну особу, публічний орган, агентство або інший суб'єкт, який самостійно або спільно з іншими визначає цілі та засоби обробки Персональних даних.
1.3.5. Обробник даних означає фізичну або юридичну особу, публічний орган, агентство або інший суб'єкт, який обробляє Персональні дані від імені контролера даних.
1.3.6. Закони про захист даних означають будь-які закони та правові норми щодо використання та захисту персональних даних, що застосовуються до діяльності DID GLOBAL, включаючи, але не обмежуючись Регламентом (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року щодо захисту фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних і скасування Директиви 95/46/ЕС (Загальний регламент про захист даних, GDPR), а також The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419) Великої Британії.
1.3.7. Запит суб'єкта даних (DSR) означає будь-який запит від Суб'єкта даних, що стосується його персональних даних та/або прав суб'єкта даних.
1.3.8. Суб'єкт даних означає фізичну особу, чиї Персональні дані ми обробляємо. Суб'єкти даних включають, але не обмежуються, користувачами, відвідувачами вебсайту, співробітниками, підрядниками та партнерами DID GLOBAL.
1.3.9. Персональні дані означають будь-яку інформацію, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи; Суб'єкт даних може бути ідентифікований за посиланням на ідентифікатор, такий як ім'я, ідентифікаційний номер, дані про місцезнаходження,

онлайн-ідентифікатор або за одним чи комбінацією факторів, що стосуються фізичної, фізіологічної, генетичної, ментальної, економічної, культурної чи соціальної ідентичності цієї особи.
1.3.10. Обробка означає будь-яку операцію або сукупність операцій, що виконуються DID GLOBAL над Персональними даними, таких як збір, запис, організація, структурування, зберігання, адаптація або зміна, пошук, консультація, використання, розкриття шляхом передачі, поширення або інше надання у доступ, узгодження або поєднання, обмеження, стирання або знищення.
1.3.11. Стандартні договірні положення означають Рішення Європейської Комісії від 5 лютого 2010 року щодо стандартних договірних положень для передачі персональних даних обробникам, що розташовані в третіх країнах, відповідно до Директиви 95/46/ЕС Європейського Парламенту та Ради (2010/87/EU).
1.3.12. Третя сторона - це фізична або юридична особа, яка отримує доступ до Персональних даних для подальшої обробки і не є співробітником, членом або корпоративним афіліатом DID GLOBAL. Це визначення не поширюється на фізичних осіб, які надають послуги DID GLOBAL як підрядники на регулярній основі.
1.3.13. Користувач – це суб'єкт даних, який користується нашими послугами, що надаються на вебсайті DID GLOBAL https://didglobal.biz.

2. Принципи обробки даних

2.1. Діяльність DID GLOBAL з обробки даних має відповідати принципам, викладеним у цьому Розділі. Менеджер з конфіденційності повинен забезпечити, щоб документація щодо відповідності DID GLOBAL, а також фактичні операції з обробки даних відповідали принципам захисту даних.

2.2. Ми повинні обробляти Персональні дані відповідно до таких **принципів**:
2.2.1. Законність, справедливість та прозорість. Ми завжди маємо правову підставу для обробки (описано в Розділі 3 цієї Політики), збираємо обсяг даних, що відповідає меті та правовим підставам, і забезпечуємо поінформованість Суб'єктів даних про обробку.
2.2.2. Обробка для визначених, явних і законних цілей та відсутність подальшої обробки, несумісної з цими цілями (обмеження мети). Ми не повинні обробляти Персональні дані для цілей, не зазначених у нашій документації щодо відповідності, без отримання спеціального погодження Менеджера з конфіденційності.
2.2.3. Адекватність, релевантність та обмеженість тим, що необхідно для цілей обробки (мінімізація даних). Ми завжди стежимо, щоб зібрані дані не були надмірними та обмежувалися суворою необхідністю.
2.2.4. Точність та актуальність. Ми прагнемо видаляти неточні або хибні дані про Суб'єктів даних і забезпечувати оновлення даних. Суб'єкти даних можуть звертатися до нас із запитом на виправлення Персональних даних.
2.2.5. Зберігання даних у формі, що дозволяє ідентифікацію Суб'єктів даних, не довше, ніж це необхідно для цілей обробки (обмеження термінів зберігання). Періоди зберігання мають бути обмежені відповідно до Законів про захист даних та цієї Політики.
2.2.6. Обробка даних таким чином, щоб **забезпечити належний рівень безпеки Персональних даних, включно із захистом** від несанкціонованої або незаконної обробки та випадкової втрати, знищення або пошкодження, із застосуванням відповідних технічних або організаційних заходів (конфіденційність, цілісність і доступність).

2.3. Підзвітність.
2.3.1. Ми повинні мати можливість продемонструвати нашу відповідність Законам про захист даних (принцип підзвітності). Зокрема, ми маємо забезпечити та документувати всі відповідні процедури, дії, внутрішні та зовнішні консультації з питань захисту персональних даних, включно з:

а) фактом призначення особи, відповідальної за відповідність DID GLOBAL у сфері захисту даних;
б) за потреби, записом Оцінки впливу на захист даних (Data Processing Impact Assessment);
в) розробленими та впровадженими повідомленнями, політиками та процедурами, такими як Повідомлення про конфіденційність, ця Політика або процедура реагування на порушення даних;
г) фактом навчання персоналу щодо дотримання Законів про захист даних;
д) оцінкою, впровадженням та тестуванням організаційних і технічних заходів захисту даних.
2.3.2. Менеджер з конфіденційності повинен вести **Реєстр операцій з обробки даних DID GLOBAL**, який є документом підзвітності та описує операції з обробки персональних даних DID GLOBAL, підготовлений відповідно до ст. 30 GDPR (далі — **«Реєстр операцій з обробки»**). Реєстр операцій з обробки має містити, щонайменше, таку інформацію про кожну операцію обробки:
а) контактні дані DID GLOBAL, представника у Великій Британії та, за наявності, відповідальної особи з питань захисту даних;
б) назву операції, її цілі та правову підставу, а також, за наявності, законні інтереси DID GLOBAL;
в) категорії суб'єктів даних та категорії персональних даних, яких це стосується;
г) строки зберігання даних;
д) загальний опис застосовуваних заходів безпеки;
е) отримувачі, включно зі спільними контролерами, обробниками та підрядниками, а також факт міжнародної передачі даних із зазначенням застосованих гарантій;
ж) за наявності, посилання на Оцінку впливу на захист даних;
з) за наявності, посилання на запис про випадок порушення даних, що стосувався персональних даних;
і) якщо DID GLOBAL діє як обробник даних, інформація має включати імена та контактні дані контролерів, ім'я та контактні дані представника контролера (за наявності), категорії обробки (операцій), назви третіх країн або міжнародних організацій, куди передаються персональні дані (за наявності), гарантії для виняткових передач персональних даних до третіх країн або міжнародних організацій (за наявності), та загальний опис технічних і організаційних заходів безпеки.

3. Доступ до персональних даних

3.1. Правові підстави

3.1.1. Кожна операція з обробки має мати одну з правових підстав, зазначених у цьому Розділі, для обробки Персональних даних. Якщо в нас немає жодної з описаних підстав, ми не можемо збирати або надалі обробляти Персональні дані.
3.1.2. Якщо DID GLOBAL планує використовувати персональні дані для цілей, відмінних від зазначених у Реєстрі операцій з обробки, Менеджер з конфіденційності повинен оцінити, визначити та, за потреби, зібрати/задокументувати відповідну правову підставу для такої обробки.
3.1.3. Виконання договору. Якщо між DID GLOBAL і Суб'єктом даних існує договір, наприклад Умови користування сайтом або трудовий договір, і договір вимагає надання Персональних даних від Суб'єкта даних, застосовною правовою підставою буде виконання договору.
3.1.4. Згода. Для обробки персональних даних на підставі згоди ми повинні отримати згоду до початку обробки та зберігати підтвердження згоди разом із записами про Персональні дані Суб'єкта даних. Менеджер з конфіденційності повинен переконатися, що згода, отримана від Суб'єктів даних, відповідає вимогам Законів про захист даних та цієї Політики. Зокрема, Менеджер з конфіденційності має забезпечити, що:
а) Суб'єкт даних має свободу надати або відмовити у наданні згоди;
б) згода надається у формі активної дії Суб'єкта даних, тобто поле для згоди не повинно бути попередньо позначене;
в) запит на згоду чітко формулює цілі обробки, а інша інформація, зазначена в підпункті 6.2, доступна Суб'єкту даних;
г) Суб'єкт даних має право вільно надати згоду або відкликати її.

3.1.5. Законні інтереси. Ми маємо право використовувати персональні дані на підставі наших законних інтересів. Інтереси можуть включати цілі, виправдані характером нашої господарської діяльності, наприклад маркетинговий аналіз персональних даних. Щоб DID GLOBAL могла використовувати законні інтереси як правову підставу для обробки, Менеджер з конфіденційності повинен переконатися, що:

а) законний інтерес в обробці чітко визначено та задокументовано в Реєстрі операцій з обробки;

б) виявлено будь-які передбачувані ризики для прав і інтересів Суб'єктів даних. Приклади ризиків наведені в підпункті 7.2.;

в) Суб'єкти даних мають розумні очікування щодо такої обробки, і вжито додаткових захисних заходів для мінімізації ризиків;

г) за умови положень підпункту 6.7 (Право заперечувати проти обробки), Суб'єкту даних надано можливість відмовитися від обробки для описаних законних інтересів. Якщо хоча б одна з наведених умов не виконується для DID GLOBAL, Менеджер з конфіденційності повинен обрати та запропонувати іншу правову підставу для обробки, наприклад згоду.

3.1.6. Виконання вимог закону та суспільний інтерес. Окрім наведених підстав, ми можемо бути зобов'язані законами Європейського Союзу або законодавством держав-членів ЄС обробляти Персональні дані наших Користувачів. Наприклад, ми можемо бути зобов'язані збирати, аналізувати та контролювати інформацію користувачів для дотримання фінансового або трудового законодавства. У разі наявності такого обов'язку ми повинні переконатися, що:

а) ми обробляємо персональні дані суворо відповідно до відповідних правових вимог;

б) ми не використовуємо та не зберігаємо зібрані Персональні дані для цілей, відмінних від виконання правових вимог;

в) Суб'єкти даних належним чином і своєчасно поінформовані про наші обов'язки, обсяг та умови обробки персональних даних.

Важливо: якщо DID GLOBAL має законодавчі вимоги іншої країни щодо обробки персональних даних, Менеджер з конфіденційності повинен запропонувати використання іншої правової підстави для обробки відповідно до Законів про захист даних, наприклад законних інтересів або згоди.

3.2. Доступ до персональних даних

3.2.1. Співробітники повинні мати доступ до персональних даних на принципі **«потрібно знати»**. Дані можуть бути доступні лише якщо це суворо необхідно для виконання однієї з операцій, зазначених у Реєстрі операцій з обробки. Співробітники та підрядники мають доступ до Персональних даних лише за наявності необхідних повноважень.

3.2.2. Керівники підрозділів DID GLOBAL відповідають за доступ своїх співробітників до персональних даних та їх обробку. Керівники повинні вести перелік співробітників, які мають право доступу та обробки персональних даних. Менеджер з конфіденційності має право переглядати цей перелік і, за потреби, вимагати внесення змін для відповідності вимогам цієї Політики.

3.2.3. Керівники підрозділів DID GLOBAL повинні забезпечити, щоб співробітники під їхнім наглядом знали про Закони про захист даних і дотримувалися правил, встановлених цією Політикою. Щоб гарантувати здатність співробітників виконувати вимоги щодо захисту даних, ми повинні забезпечити їх належним навчанням з питань захисту даних.

3.2.4. Усі співробітники, які мають доступ до персональних даних, повинні суворо зберігати конфіденційність щодо даних, до яких вони мають доступ. Співробітники, що отримують доступ до персональних даних, повинні використовувати лише ті засоби (програмне забезпечення, приміщення тощо) для обробки, які призначені DID GLOBAL. Дані не повинні розголошуватися або іншим чином надаватися поза межами інструкцій керівництва.

3.2.5. Співробітники в межах своєї компетенції повинні сприяти представникам DID GLOBAL, включно з Менеджером з конфіденційності, у будь-яких заходах щодо забезпечення відповідності Законам про захист даних та/або цій Політиці.

3.2.6. Коли співробітник виявляє або вважає, що має місце підозріла діяльність, порушення даних, недотримання Законів про захист даних та/або цієї Політики, або якщо Запит суб'єкта даних (DSR) не

був направлений до компетентного підрозділу DID GLOBAL, співробітник повинен повідомити про таку подію Менеджера з конфіденційності.
3.2.7. Співробітники, які сумніваються, чи мають вони законне право обробляти або розкривати Персональні дані, повинні звернутися за порадою до Менеджера з конфіденційності перед вчиненням будь-яких дій.
3.2.8. Будь-який випадковий доступ до персональних даних для діяльності, не зазначеної в Реєстрі операцій з обробки, заборонено. Якщо існує сувора необхідність у негайному доступі, доступ має бути попередньо погоджений Менеджером з конфіденційності.

4. Треті особи

4.1. До того як передавати персональні дані будь-якій особі поза межами DID GLOBAL, Менеджер з конфіденційності повинен переконатися, що ця **Третя особа** має належний рівень захисту даних і надає достатні гарантії захисту даних відповідно до Законів про захист даних, включно з вимогами щодо обробників (ст. 28 GDPR) та дотриманням правил міжнародних передач (Розділ 5 GDPR). За потреби Менеджер з конфіденційності повинен забезпечити укладення DID GLOBAL відповідного договору про захист даних із третьою особою.

4.2. Співробітник може передавати персональні дані третім особам лише якщо і в тій мірі, в якій це безпосередньо передбачено керівником та зазначено в Реєстрі операцій з обробки.

4.3. Якщо нам необхідно видалити, змінити або припинити обробку Персональних даних, ми повинні забезпечити, щоб Треті особи, яким ми передали Персональні дані, виконали ці зобов'язання відповідно.

4.4. Коли DID GLOBAL залучена як обробник даних від імені іншого суб'єкта, Менеджер з конфіденційності повинен переконатися, що DID GLOBAL дотримується обов'язків обробника. Зокрема, має бути укладено відповідну угоду про обробку даних відповідно до Законів про захист даних. Менеджер з конфіденційності повинен контролювати дотримання інструкцій контролера щодо обробки даних, включно зі сферою обробки, залученням суб-обробників, міжнародними передачами, зберіганням та подальшим розпорядженням обробленими персональними даними. Персональні дані, оброблені в ролі обробника, не повинні оброблятися для інших цілей, ніж ті, що зазначені в відповідних інструкціях, угоді або іншому правовому акті, що регулює відносини з контролером.

5. Міжнародна передача даних

5.1. Якщо у нас є співробітники, підрядники, корпоративні афілійовані особи або Обробники даних за межами ЄЕЗ, і ми передаємо їм Персональні дані для обробки, Менеджер із питань конфіденційності повинен переконатися, що DID GLOBAL вживає всіх необхідних та належних заходів безпеки відповідно до Законів про захист даних.

5.2. Менеджер з конфіденційності повинен оцінити наявні гарантії та запропонувати керівництву DID GLOBAL відповідні заходи захисту для кожної міжнародної передачі. До режимів передачі Персональних даних за межі ЄС належать:
а) якщо Європейська Комісія ухвалює рішення, що країна має адекватний рівень захисту персональних даних, передача не вимагає додаткових гарантій; повний перелік таких юрисдикцій доступний на відповідній сторінці Європейської Комісії;
б) для передачі Персональних даних нашим підрядникам або партнерам (Обробникам або Контролерам) у третіх країнах ми повинні укласти Стандартні договірні положення з цією стороною; проєкт та керівництво доступні на відповідній сторінці Європейської Комісії;

в) якщо у нас є корпоративний афіліат або підрозділ в інших країнах, ми можемо обрати впровадження Обов'язкових корпоративних правил відповідно до ст. 47 GDPR або затвердженого кодексу поведінки відповідно до ст. 40 GDPR;
г) ми також можемо передавати Персональні дані організаціям, які мають затверджену сертифікацію відповідно до ст. 42 GDPR, що підтверджує належний рівень захисту даних компанії.

5.3. В рамках інформаційних зобов'язань DID GLOBAL повинна повідомляти Суб'єктів даних про те, що їхні Персональні дані передаються до інших країн, а також надавати інформацію про гарантії, застосовані для такої передачі. Виконання інформаційного зобов'язання здійснюється відповідно до підпункту 6.2.

5.4. У виняткових випадках («Відступ»), коли ми не можемо застосувати вищезазначені запобіжні заходи та нам потрібно передати Персональні дані, ми повинні отримати чітку згоду (активну заяву) від Суб'єкта даних, або це має бути суворо необхідним для виконання договору між нами та Суб'єктом даних, або застосовуються інші умови відступу відповідно до Законів про захист даних. Менеджер із питань конфіденційності повинен попередньо схвалити будь-які передачі відступу та задокументувати схвалені відступи, а також обґрунтування їх використання.

6. Права суб'єктів персональних даних

6.1. Наші обов'язки.
6.1.1. Менеджер з конфіденційності несе остаточну відповідальність за обробку всіх Запитів суб'єктів даних (DSR), що надходять до DID GLOBAL. У разі отримання незвичних або невирішених DSR співробітник повинен звернутися за порадою до Менеджера з конфіденційності перед вжиттям будь-яких дій.
6.1.2. Відділ підтримки клієнтів DID GLOBAL відповідає за щоденну обробку DSR від користувачів DID GLOBAL. Відділ кадрів (HR) відповідає за обробку DSR від співробітників DID GLOBAL.
6.1.3. Усі DSR від користувачів повинні надсилатися та отримувати відповідь з електронної адреси gdpr@didglobal.biz. DSR від співробітників можуть надсилатися безпосередньо менеджеру з кадрів або на gdpr@didglobal.biz.
6.1.4. Відповідальний співробітник має відповісти на DSR протягом одного (1) місяця з моменту отримання запиту. Якщо виконання DSR потребує більше одного місяця, відповідальний співробітник повинен звернутися до Менеджера з конфіденційності і, за потреби, повідомити Суб'єкта даних про продовження строку відповіді до двох (2) додаткових місяців.
6.1.5. Відповідальний співробітник повинен проаналізувати отриманий DSR за такими критеріями:
а) Ідентифікація Суб'єкта даних. Перед розглядом змісту DSR співробітник має переконатися, що Суб'єкт даних — це та особа, за яку вона себе видає. Для цього має бути встановлено зв'язок між записами персональних даних і Суб'єктом даних. Зазвичай перевіряється електронна адреса Суб'єкта даних — вона має збігатися з тією, що зберігається в базі DID GLOBAL; якщо адреса відрізняється, слід проконсультуватися з Менеджером з конфіденційності, і за його згодою відповідальний співробітник може запросити додаткові дані для ідентифікації (наприклад, дату народження, адресу, електронну адресу). Якщо Суб'єкт даних не пройшов верифікацію, Менеджер з конфіденційності має відмовити у виконанні запиту та повідомити про це Суб'єкта даних без невиправданої затримки, але не пізніше одного (1) місяця з моменту отримання запиту.
б) Персональні дані. Відповідальний співробітник має перевірити, чи має DID GLOBAL доступ до запитуваних персональних даних. Якщо DID GLOBAL не контролює такі дані, співробітник має повідомити Суб'єкта даних і, за можливості, надати інструкції щодо подальших кроків для доступу до відповідних даних.

в) Зміст запиту. Залежно від змісту DSR відповідальний співробітник має визначити тип запиту та перевірити, чи відповідає він умовам, передбаченим цією Політикою та Законами про захист даних. Типи запитів і відповідні умови наведені в підпунктах 6.3–6.9. Якщо запит не відповідає критеріям, співробітник має відмовити у виконанні DSR і повідомити Суб'єкта даних про причини відмови.
г) Безкоштовність. Загалом усі запити Суб'єктів даних та реалізація їх прав є безкоштовними. Якщо відповідальний співробітник вважає, що Суб'єкт даних зловживає правами або діє безпідставно (наприклад, з наміром завдати шкоди або перервати діяльність DID GLOBAL), співробітник має звернутися до Менеджера з конфіденційності, і за його рішенням може або стягнути з Суб'єкта даних розумну плату, або відмовити у виконанні запиту.
д) Документування. Після отримання DSR Менеджер з конфіденційності має забезпечити фіксацію дати й часу, Суб'єкта даних, типу запиту та прийнятого рішення. У разі відмови у виконанні запиту мають бути задокументовані причини відмови.
е) Одержувачі. При розгляді DSR Менеджер з конфіденційності має переконатися, що всі зацікавлені одержувачі були поінформовані про вжиті необхідні заходи.

6.2. Право на отримання інформації
6.2.1. DID GLOBAL має повідомляти кожного Суб'єкта даних про збір та подальшу обробку його Персональних даних.
6.2.2. Інформація, що надається, включає: назву та контактні дані DID GLOBAL; загальні цілі та правову підставу збору й обробки даних; категорії зібраних Персональних даних; одержувачі/категорії одержувачів; строки зберігання; інформацію про права Суб'єкта даних, включно з правом скаржитися до компетентного наглядового органу; наслідки у випадках, коли дані необхідні для виконання договору і Суб'єкт даних не надає потрібні дані; деталі гарантій при передачі даних за межі ЄЕЗ; та будь-яке джерело персональних даних третьої сторони (без деталізації для конкретного випадку, якщо тільки ми не отримали прямий запит від Суб'єкта даних).
6.2.3. Користувачі мають бути поінформовані через Політику конфіденційності, доступну на вебсайті DID GLOBAL і надавану під час реєстрації користувача. Співробітники та підрядники мають отримувати окрему заяву про конфіденційність працівника, яка пояснює деталі, зазначені в п. 6.2.2, у контексті конкретних випадків і цілей.
6.2.4. DID GLOBAL має інформувати Суб'єктів даних про обробку даних, включно з будь-якою новою діяльністю з обробки, у такі строки:
а) якщо персональні дані збираються безпосередньо від Суб'єкта даних — у момент їх збору шляхом надання заяви про конфіденційність;
б) якщо дані збираються з інших джерел: (a) протягом одного місяця з моменту їх збору; (b) якщо дані будуть використані для зв'язку з Суб'єктом даних — не пізніше першого контакту; або (c) якщо передбачається передача даних іншому одержувачу — не пізніше першої такої передачі;
в) за запитом Суб'єкта даних;
г) протягом одного (1) місяця після будь-якої зміни наших практик обробки персональних даних, зміни контролера даних або після суттєвих змін у наших заявах про конфіденційність.

6.3. Право на доступ до інформації
6.3.1. Суб'єкту даних надаються лише ті записи персональних даних, які зазначені в запиті. Якщо Суб'єкт даних запитує доступ до всіх персональних даних, що стосуються його, співробітник має спочатку звернутися до Менеджера з конфіденційності, щоб упевнитися, що всі дані Суб'єкта даних відображені та можуть бути надані.
6.3.2. Суб'єкт даних має право:
а) дізнатися, чи обробляємо ми його Персональні дані;
б) отримати розкриття щодо аспектів обробки, включно з детальною та конкретною інформацією про цілі, категорії Персональних даних, одержувачів/категорії одержувачів, строки зберігання, інформацію про права, деталі відповідних гарантій при передачі даних за межі ЄЕЗ та будь-яке джерело даних третьої сторони;

в) отримати копію Персональних даних, що обробляються, за запитом.

6.4. Право на перевірку інформації та її виправлення
Якщо виявлено, що зібрана інформація є неточною або застарілою (наприклад, містить помилки в даних про громадянство, дату народження, заборгованість чи економічну діяльність), або якщо Суб'єкт даних звертається з відповідним запитом, ми маємо виправити помилки та оновити відповідну інформацію.

6.5. Інформація, яку ми збираємо, може бути або стати неточною чи застарілою (наприклад, містити помилки в даних про громадянство, дату народження, заборгованість чи економічну діяльність). Якщо ми виявимо, що Персональні дані є неточними, або якщо Суб'єкт даних просить нас про це, ми повинні забезпечити виправлення всіх помилок та оновлення відповідної інформації.

6.6. Право на обмеження обробки даних
6.6.1. Обмеження обробки даних дозволяє Суб'єктам даних тимчасово зупинити використання їх даних, щоб запобігти можливій шкоді від такого використання.
6.6.2. Це право застосовується, коли Суб'єкт даних:
а) оспорює точність Персональних даних;
б) вважає, що ми обробляємо Персональні дані незаконно;
в) заперечує проти обробки і бажає, щоб ми не обробляли дані, поки ми розглядаємо запит.
6.6.3. У разі отримання запиту на обмеження ми не повинні обробляти відповідні Персональні дані для жодної іншої мети, окрім зберігання або виконання правових зобов'язань, доки обставини, що зумовили обмеження, не припиняться.

6.7. Право відкликати згоду
Для дій, що вимагають згоди, Суб'єкт даних може відкликати згоду в будь-який час. У разі відкликання ми маємо зафіксувати зміни і не обробляти Персональні дані для цілей, що базувалися на згоді. Відкликання не впливає на законність обробки, здійсненої до відкликання.

6.8. Право заперечувати проти обробки
6.8.1. Якщо ми обробляємо дані на підставі законних інтересів (наприклад, для прямих маркетингових розсилок або маркетингових досліджень), Суб'єкт даних може заперечити проти такої обробки.
6.8.2. Після отримання заперечення ми маємо розглянути запит і, якщо в нас немає переважаючих підстав, припинити обробку для зазначених цілей. Якщо дані мають оброблятися для інших цілей, Менеджер з конфіденційності має забезпечити, щоб у базі було позначено, що дані не можуть бути далі оброблені для оскаржених дій.
6.8.3. Заперечення може бути відхилене лише якщо персональні дані використовуються для наукових/історичних досліджень або статистичних цілей і належним чином захищені (наприклад, анонімізацією або псевдонімізацією).

6.9. Право на видалення
6.9.1. Суб'єкти даних мають право вимагати видалення їх Персональних даних, якщо виконується одна з умов:
а) Персональні дані більше не потрібні для цілей, для яких вони були зібрані;
б) Суб'єкт даних відкликає згоду або заперечує проти обробки (де застосовно) і немає іншої правової підстави для обробки;
в) ми обробляємо Персональні дані незаконно, або їх видалення вимагається чинним законодавством Європейського Союзу або однієї з країн-членів Європейського Союзу.
6.9.2. Ми маємо право відмовити у видаленні, якщо:

а) дані обробляються для наукових/історичних досліджень або статистичних цілей і належним чином захищені (псевдонімізація/анонімізація);
б) дані все ще необхідні для виконання правових зобов'язань (наприклад, фінансове або трудове законодавство).
6.9.3. Видаляються лише ті записи персональних даних, які зазначені в запиті. Якщо Суб'єкт даних просить видалити всі дані, що стосуються його, співробітник має спочатку звернутися до Менеджера з конфіденційності, щоб упевнитися, що всі дані відображені і можуть бути видалені.
6.9.4. Якщо Користувач все ще має обліковий запис і просить видалити інформацію, необхідну для підтримки облікового запису, ми маємо повідомити Користувача, що видалення вплине на користувацький досвід або може призвести до закриття облікового запису.

6.10. Портативність даних
6.10.1. Суб'єкти даних можуть попросити передати всі або частину їх Персональних даних у машинописному форматі третій стороні. Це право застосовується, якщо:
а) персональні дані були зібрані для надання наших послуг (виконання договору); або
б) дані були зібрані на підставі згоди.
6.10.2. Щоб визначити, чи виконуються умови п. 6.9.1, співробітник має звернутися до Менеджера з конфіденційності та перевірити застосовну правову підставу в Реєстрі операцій з обробки. Якщо підстава відсутня, DID GLOBAL може відмовити у запиті, а Менеджер з конфіденційності вирішує, чи виконувати запит добровільно.
6.10.3. Для виконання запиту відповідальний співробітник має зібрати запитувані Персональні дані та надіслати їх у форматі, з яким ми зазвичай працюємо, на адресу організації, вказану Суб'єктом даних. Суб'єкт даних має надати необхідні контактні дані організації.

7. Нові види діяльності з обробки даних

7.1. Повідомлення Менеджеру з конфіденційності
7.1.1. До впровадження будь-якої нової діяльності, що передбачає обробку персональних даних, співробітник, відповідальний за її реалізацію, повинен повідомити Менеджера з конфіденційності.
7.1.2. Після отримання інформації про нову діяльність Менеджер з конфіденційності повинен:
а) визначити, чи необхідна Оцінка впливу на захист даних (DPIA) та/або консультація з Наглядовим органом; у разі позитивної відповіді забезпечити проведення DPIA та/або консультацію з Наглядовим органом відповідно до вимог цього Розділу та Законів про захист даних;
б) визначити правову підставу для обробки та, за потреби, вжити заходів для її фіксації;
в) переконатися, що діяльність з обробки здійснюється відповідно до цієї Політики, інших політик DID GLOBAL та Законів про захист даних;
г) додати операцію з обробки до Реєстру операцій з обробки;
д) за потреби внести зміни до заяв про конфіденційність та повідомити відповідних Суб'єктів даних.

7.2. Оцінка впливу на захист даних (DPIA)
7.2.1. Щоб упевнитися, що наші поточні або плановані операції з обробки не порушують права Суб'єктів даних, DID GLOBAL має, коли це вимагають Закони про захист даних, проводити Оцінку впливу на захист даних (DPIA) — оцінку ризиків обробки з пошуком заходів для їх пом'якшення. Менеджер з конфіденційності має забезпечити проведення DPIA відповідно до цього Розділу.
7.2.2. Менеджер з конфіденційності, за потреби залучаючи компетентних співробітників та/або зовнішніх консультантів, повинен провести DPIA, якщо виконується хоча б одна з наведених умов:
а) обробка передбачає використання нових технологій (наприклад, штучний інтелект, підключені та автономні пристрої) і створює певні правові, економічні або подібні наслідки для Суб'єкта даних;

б) ми систематично оцінюємо та аналізуємо персональні аспекти Суб'єктів даних на основі автоматизованого профілювання, присвоюємо персональні бали/рейтинги і це створює правові або подібні наслідки для Суб'єкта даних;
в) ми обробляємо у великому обсязі чутливі дані (наприклад, дані про кримінальні правопорушення, дані про вразливі категорії, расове чи етнічне походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, генетичні дані, біометричні дані для ідентифікації, дані про здоров'я або сексуальне життя/орієнтацію);
г) ми збираємо або обробляємо персональні дані з публічно доступних джерел у великому обсязі або поєднуємо/зіставляємо різні набори даних;
д) Наглядовий орган у своєму публічному переліку вимагає проведення DPIA для певного типу діяльності, у якій ми задіяні.
7.2.3. Оцінка має містити щонайменше такі відомості:
а) систематичний опис операцій обробки та цілей обробки, включно, за потреби, із зазначенням законного інтересу; опис має охоплювати передбачувані категорії даних і Суб'єктів даних, масштаб обробки (частота, обсяг, очікувана кількість записів тощо), одержувачів, строки зберігання та, за потреби, міжнародні передачі;
б) оцінку необхідності та пропорційності операцій обробки щодо поставлених цілей; DPIA має пояснювати, чи є діяльність необхідною для досягнення мети і чи можна досягти мети менш інвазивними методами;
г) оцінку ризиків для прав і свобод Суб'єктів даних;
д) приклади ризиків: обробка, що може призвести до фізичної, матеріальної або нематеріальної шкоди, зокрема дискримінації, крадіжки особистості, шахрайства, фінансових втрат, шкоди репутації, втрати конфіденційності даних, несанкціонованого відновлення псевдонімізації або інших значних економічних чи соціальних збитків;
е) випадки, коли Суб'єкти даних можуть бути позбавлені прав або контролю над своїми даними; коли обробляються дані, що розкривають расове/етнічне походження, політичні погляди, релігійні/філософські переконання, членство в профспілках, генетичні дані, дані про здоров'я, сексуальне життя або кримінальні правопорушення; коли оцінюються персональні аспекти (наприклад, аналіз або прогнозування продуктивності на роботі, економічного стану, здоров'я, уподобань, надійності, поведінки, місцезнаходження або переміщень) для створення або використання персональних профілів; коли обробляються дані вразливих осіб, зокрема дітей; або коли обробка охоплює велику кількість даних і впливає на велику кількість Суб'єктів даних;
ж) заходи для усунення ризиків, включно із запобіжними заходами, заходами безпеки та механізмами для забезпечення захисту персональних даних і демонстрації відповідності вимогам.
7.2.4. Якщо DPIA не дає ефективного рішення для пом'якшення ризиків, Менеджер з конфіденційності має ініціювати консультацію з компетентним Наглядовим органом для отримання допомоги у пошуку рішення. У такому випадку DID GLOBAL не повинна обробляти персональні дані до отримання схвалення Наглядового органу щодо відповідної діяльності.

8. Зберігання даних

8.1. Загальне правило

8.1.1. Менеджер з конфіденційності повинен переконатися, що DID GLOBAL чітко визначила строки зберігання даних та/або критерії для визначення строків зберігання для кожної операції з обробки. Строки для кожної операції з обробки повинні бути зазначені в Реєстрі операцій з обробки.
8.1.2. Кожен відділ DID GLOBAL повинен дотримуватися строків зберігання даних відповідно до графіка зберігання, наведеного в Реєстрі операцій з обробки. Менеджер з конфіденційності повинен контролювати кожен відділ і забезпечувати дотримання ним цієї вимоги.

8.1.3. Після закінчення терміну зберігання персональні дані повинні бути вилучені з розпорядження відділу, відповідального за обробку, або, у випадках, коли дані не потрібні для жодних інших цілей, повністю знищені, зокрема з резервних копій та інших носіїв.
8.1.4. Щоразу, коли термін зберігання для операції з обробки закінчився, але оброблені персональні дані необхідні для інших цілей обробки, керівник відділу повинен переконатися, що персональні дані не використовуються для припиненої операції з обробки, а відповідальні співробітники не мають до них доступу, якщо це не потрібно для будь-якої іншої діяльності.

8.2. Винятки. Правила, зазначені у підрозділі 8.1, мають такі винятки:
8.2.1. Потреби бізнесу. Терміни зберігання даних можуть бути продовжені, але не більше ніж на 60 днів, у випадку, якщо видалення даних перерве або зашкодить нашій поточній діяльності. Менеджер із питань конфіденційності повинен схвалити будь-яке непередбачене продовження;
8.2.2. Технічна неможливість. Деяку інформацію технічно неможливо або непропорційно складно видалити. Наприклад, видалення інформації може призвести до порушення цілісності системи, або інформацію неможливо видалити з резервних копій. У такому випадку інформація може зберігатися й надалі за умови схвалення Менеджером з конфіденційності та внесення відповідних змін до Реєстру операцій з обробки; та
8.2.3. Анонімізація. Персональні дані можуть оброблятися далі для будь-яких цілей (наприклад, маркетинг), якщо ми повністю анонімізуємо ці дані після закінчення терміну зберігання. Це означає, що всі персональні ідентифікатори та зв'язки з ними будуть видалені з даних. Щоб вважати Персональні дані анонімними, повторна ідентифікація Суб'єкта даних з набору даних має бути неможливою.

.9. Безпека

9.1. Кожен відділ DID GLOBAL повинен вживати всіх належних технічних та організаційних заходів для захисту від несанкціонованого, незаконного та/або випадкового доступу, знищення, зміни, блокування, копіювання, розповсюдження, а також від інших незаконних дій неавторизованих осіб щодо персональних даних, що перебувають під їхньою відповідальністю.

9.2. Працівником, відповідальним за нагляд за безпекою персональних даних у DID GLOBAL, є спеціаліст з інформаційної безпеки. Ця особа впроваджує керівні принципи та інші специфікації щодо захисту даних та інформаційної безпеки у своїй сфері відповідальності. Вона консультує керівництво DID GLOBAL щодо планування та впровадження інформаційної безпеки в DID GLOBAL та повинна бути залучена до всіх проєктів на ранній стадії, щоб враховувати аспекти, пов'язані з безпекою, ще на етапі планування.

10. Процедура реагування на порушення безпеки даних

10.1 Команда реагування
10.1.1. У разі виявлення Порушення даних Генеральний директор DID GLOBAL невідкладно формує **Команду реагування на порушення даних** (далі — Команда реагування), яка опікуватиметься інцидентом, повідомить відповідних осіб та вживатиме заходів для мінімізації ризиків.
10.1.2. Команда реагування має бути мультидисциплінарною групою під керівництвом Генерального директора DID GLOBAL і складатися з Менеджера з конфіденційності, фахівця з питань законодавства про конфіденційність (внутрішнього або зовнішнього) та компетентних

фахівців з інформаційної безпеки DID GLOBAL або залучених зовнішніх спеціалістів за потреби. Команда має забезпечити, щоб усі співробітники та залучені підрядники/обробники дотримувалися цієї Політики та забезпечити оперативну, ефективну й професійну реакцію на будь-яке підозрюване, заявлене або фактичне Порушення даних, що стосується DID GLOBAL.

10.1.3. Потенційні члени Команди реагування повинні бути готові до реагування на Порушення даних. Команда виконує всі обов'язки DID GLOBAL, зазначені в цій Політиці. **Обов'язки Команди реагування включають:**

а) повідомлення про Порушення даних компетентного Наглядового органу;

б) у разі високого ризику для прав і свобод Суб'єктів даних — повідомлення відповідних Суб'єктів даних;

в) якщо DID GLOBAL отримала дані від третьої сторони як обробник і Порушення стосується отриманих даних — інформувати цю третю сторону про Порушення;

г) повідомлення підрядників DID GLOBAL або інших третіх сторін, які обробляють Персональні дані, залучені в Порушенні;

д) вжиття всіх відповідних технічних та організаційних заходів для припинення Порушення та пом'якшення його наслідків;

е) фіксація факту Порушення в Реєстрі операцій з обробки та підготовка внутрішнього звіту про Порушення, що описує подію.

10.1.4. Команда реагування виконує свої обов'язки до повного вжиття всіх необхідних заходів, передбачених цією Політикою.

10.2 Повідомлення Наглядовому органу

10.2.1. DID GLOBAL має повідомити **Компетентний Наглядовий орган** про Порушення даних без невиправданої затримки і, за можливості, не пізніше ніж через **72 години** з моменту, коли стало відомо про Порушення.

10.2.2. Компетентний Наглядовий орган визначається за місцем проживання Суб'єктів даних, чиї дані були задіяні в Порушенні. Якщо Порушення стосується Суб'єктів даних з кількох країн, DID GLOBAL інформує всі відповідні Наглядові органи.

10.2.3. Для підготовки повідомлення до органу Команда реагування повинна використовувати Додаток 1 до цієї Політики, який містить контактні дані органів ЄС. Якщо Порушення стосується Суб'єктів даних з країн, що не входять до ЄС, Команда реагування має звернутися за порадою до компетентного фахівця з питань конфіденційності.

10.2.4. Повідомлення до Наглядового органу має містити щонайменше таку інформацію:

а) характер Порушення даних, включно, де можливо, категорії та приблизну кількість Суб'єктів даних і записів Персональних даних, яких це стосується;

б) ім'я та контактні дані Команди реагування, Менеджера з конфіденційності або, якщо недоцільно, Генерального директора;

в) ймовірні наслідки Порушення даних з точки зору DID GLOBAL, зокрема можливі цілі та подальші ризики (наприклад, крадіжка даних для продажу, шахрайство або шантаж);

г) заходи, вжиті або запропоновані DID GLOBAL для реагування на Порушення, включно з заходами для пом'якшення можливих негативних наслідків.

10.2.5. Для подання повідомлення Команда реагування має використовувати Форму повідомлення про Порушення даних DID GLOBAL для Наглядового органу.

10.3 Повідомлення Суб'єктів даних

10.3.1. Якщо Порушення даних може призвести до **високого ризику** для прав і свобод Суб'єктів даних (наприклад, крадіжка коштів, активів або конфіденційної інформації), ми також повинні повідомити постраждалих Суб'єктів даних без невиправданої затримки. Менеджер з конфіденційності визначає наявність високого ризику, спираючись на фактори ризику, зазначені в підпункті 7.2.3 Політики.

10.3.2. Повідомлення має містити:

а) опис Порушення даних — що сталося і що призвело до інциденту (наприклад, порушення безпеки, недбалість співробітника, помилка системи). Якщо Команда реагування вирішить не розкривати причини, цей пункт не згадується;
б) заходи, вжиті DID GLOBAL щодо Порушення, включно з заходами безпеки, внутрішніми розслідуваннями та повідомленням Наглядовому органу;
в) рекомендації для постраждалих Суб'єктів даних щодо пом'якшення ризиків (наприклад, відновлення доступу до облікового запису, зміна пароля);
г) контактні дані Команди реагування або одного з її членів.
10.3.3. Повідомлення Суб'єктам даних має надсилатися електронною поштою або, якщо це неможливо, іншими доступними засобами зв'язку.
10.3.4. Винятки. Ми не зобов'язані повідомляти Суб'єктів даних, якщо виконується будь-яка з наведених умов:
а) DID GLOBAL застосувала відповідні технічні та організаційні заходи захисту, які зробили Персональні дані недоступними для осіб, що не мають на це повноважень (наприклад, шифрування);
б) DID GLOBAL вжила подальших заходів, які забезпечили, що високий ризик для прав і свобод Суб'єктів даних більше не ймовірний;
в) повідомлення всім зацікавленим Суб'єктам даних вимагало б непропорційних зусиль; у такому випадку має бути здійснено публічне повідомлення або інший подібний захід, що інформує Суб'єктів даних не менш ефективно. У разі застосування одного з винятків ми маємо задокументувати обставини, причини не надсилання повідомлення та вжиті заходи, що підтверджують застосування винятку.

10.4 Комунікація з третіми сторонами
10.4.1. Якщо Порушення даних стосується Персональних даних, які були надані нам або обробляються нами від імені Третьої сторони, ми повинні повідомити цю Третю сторону про інцидент протягом 24 годин. Якщо ми діємо як Обробник даних, повідомлення Третій стороні не звільняє нас від обов'язку пом'якшувати наслідки Порушення, але в такому випадку ми не повідомляємо Наглядовий орган і Суб'єктів даних від імені контролера.
10.4.2. У разі отримання повідомлення про Порушення від Обробника даних або інших третіх сторін, які мають доступ до Персональних даних, Генеральний директор DID GLOBAL має, відповідно до цього Розділу:
- сформувати Команду реагування;
- запросити у Третьої сторони інформацію, зазначену в підпунктах 10.2–10.3;
- за потреби повідомити Компетентні Наглядові органи та Суб'єктів даних;
- виконати інші кроки процедури реагування на Порушення даних.

10.4.3. У разі запиту компетентних органів про надання персональних даних клієнта, залежно від повноважень запиту та наявності порушення закону з боку клієнта, ми не маємо права відмовити у наданні такої інформації компетентним органам. Клієнт зобов'язаний дотримуватися положень законодавства у сфері телекомунікацій при використанні послуг компанії. У такому випадку DID GLOBAL не несе відповідальності за розкриття персональних даних.

11. Міжнародна правова допомога (Mutual Legal Assistance, MLA) та запити правоохоронних органів

11.1. DID GLOBAL Ltd. може отримувати запити про розкриття персональних даних від компетентних іноземних органів через процедури **взаємної правової допомоги (MLA)** або офіційні Листи з проханням (LOR). Усі такі запити мають бути **невідкладно** передані Менеджеру з конфіденційності та Юридичному відділу для розгляду.

11.2. DID GLOBAL Ltd. обробляє такі запити суворо відповідно до застосовного законодавства, включно з **UK GDPR**, **Data Protection Act 2018** та відповідними міжнародними угодами.

11.3. Перед розкриттям будь-яких персональних даних DID GLOBAL Ltd. забезпечує, що:
а) запит подано через офіційні урядові або судові канали і, за потреби, підкріплений дійсним Letter of Request (LOR)**;**
б) запитувальний орган визнано компетентним;
в) запит оцінено з огляду на законність, необхідність і пропорційність;
г) розкривається лише **мінімальна кількість персональних даних**, необхідна для конкретної мети (принцип мінімізації даних);
д) застосовано відповідні гарантії для захисту прав і свобод суб'єктів даних;
е) за наявності правової можливості суб'єктів даних повідомляють про таке розкриття.

11.4. За потреби DID GLOBAL Ltd. може вимагати додаткову інформацію, вимагати завірені переклади англійською мовою або консультуватися з Центральним органом Великої Британії або зовнішніми юридичними радниками. Міжнародні передачі даних, що виникають у зв'язку з MLA-запитами, підлягають відповідним гарантіям. Усі розкриття здійснюються з використанням **безпечних методів передачі**, включно з шифруванням, і повністю документуються. DID GLOBAL Ltd. веде реєстр MLA-запитів і розкриттів відповідно до Реєстру операцій з обробки. DID GLOBAL Ltd. залишає за собою право **відмовити, оскаржити або призупинити** будь-який запит, який не відповідає правовим вимогам або викликає сумніви щодо його обсягу, законності чи пропорційності.

ДОДАТОК 1 ДО ПОЛІТИКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Компетентний наглядовий орган (Competent Supervisory Authority)

Наглядовий орган Сполученого Королівства (United Kingdom Supervisory Authority)
Управління Комісара з питань інформації (Information Commissioner's Office, ICO)

UK Information Commissioner:
John Edwards

Address:
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
United Kingdom

Telephone:
+44 (0)303 123 1113

General Contact Email:
casework@ico.org.uk

International/Data Protection Cooperation:
international.team@ico.org.uk

ДОДАТОК 2 ДО ПОЛІТИКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Контактна інформація з питань міжнародної правової допомоги (Mutual Legal Assistance, MLA)

Центральний орган Великої Британії (UK Central Authority, UKCA)

Department:
Public Safety Group — Home Office

Address:
6th Floor, Fry Building, 2 Marsham Street, London SW1P 4DF
United Kingdom

Official MLA Email:
UKCA-ILOR@homeoffice.gov.uk