

1. Загальні положення

1.1. Ця Політика конфіденційності (надалі - Політика) встановлює комплексний правовий та організаційний режим збору, обробки, зберігання та захисту інформації про ідентифікованих або таких, що можуть бути ідентифіковані, фізичних осіб, залучених до діяльності проєкту ERASMUS+ Jean Monnet Module «European Regulation of the Cryptocurrency Market: Implementation in Ukraine» (далі - ERCM).

1.2. Політику розроблено як гарантію виконання положень Грантової угоди, які вимагають від бенефіціарів суворого дотримання норм Загального регламенту ЄС про захист даних (GDPR - Regulation (EU) 2016/679).

1.3. Проєкт здійснюється на території України Національним юридичним університетом імені Ярослава Мудрого, тому обробка персональних даних також узгоджується з вимогами Закону України «Про захист персональних даних». Специфіка проєкту, що включає проведення модулів сертифікатної програми, організацію міжнародних конференцій, анкетування учасників та активну інформаційну кампанію в цифровому середовищі, зумовлює необхідність обробки значних масивів даних.

1.4. Університет виступає у статусі Контролера даних, самостійно визначаючи цілі та засоби їх обробки в рамках реалізації завдань, делегованих Європейським виконавчим агентством з питань освіти та культури (EACEA).

2. Базові принципи обробки персональних даних

2.1. Принцип законності, справедливості та прозорості передбачає, що збір даних здійснюється виключно на легітимних підставах. Для учасників сертифікатних програм та конференцій такою підставою є надання ними чіткої, свідомої та добровільної згоди шляхом заповнення електронних реєстраційних форм або підписання відповідних документів. Учасникам у доступній формі повідомляється, яка саме інформація збирається та з якою метою.

2.2. Принцип обмеження мети гарантує, що персональні дані збираються виключно для чітко визначених і легітимних цілей: адміністрування навчального процесу, видачі сертифікатів, організації комунікації, оцінки ефективності проєкту та підготовки статистичної звітності. Подальша обробка даних у спосіб, несумісний із цими цілями, не допускається.

2.3. Застосовується принцип мінімізації даних: обробляється лише той обсяг інформації, який є необхідним і релевантним для досягнення визначених цілей. Збір надлишкових даних забороняється.

2.4. Забезпечується точність даних шляхом їх своєчасного оновлення за запитом користувачів, обмеження строків зберігання, а також цілісність і конфіденційність через впровадження належних технічних та організаційних заходів захисту.

3. Категорії даних та цілі обробки

3.1. Для забезпечення прозорості процесів обробки визначено такі категорії суб'єктів персональних даних, обсяг даних та цілі їх використання у проєкті ERCM:

3.1.1. **Слухачі сертифікатної програми / учасники вебінарів:** обробляються прізвище, ім'я, вік, стать (для статистики), електронна пошта, контактний телефон, місце навчання або роботи, результати тестування. Метою є забезпечення доступу до навчальних матеріалів, моніторинг успішності, видача сертифікатів і формування звітності. Обробка здійснюється на підставі згоди.

3.1.2. **Доповідачі конференцій та автори наукових матеріалів:** збираються прізвище, ім'я, науковий ступінь, академічне звання, місце роботи, тема доповіді та контактна інформація.

Дані використовуються для організації заходів, публікації матеріалів і комунікації. Обробка здійснюється на підставі згоди та легітимного інтересу.

3.1.3. Члени робочої групи та запрошені експерти: обробляються паспортні дані, ідентифікаційні коди, банківські реквізити, резюме та інформація про кваліфікацію. Це необхідно для укладення договорів, здійснення виплат і ведення фінансової звітності. Обробка здійснюється на підставі згоди.

3.1.4. Відвідувачі цифрових платформ і вебсайту проекту: обробляються IP-адреси, файли cookie та технічні журнали підключень. Метою є забезпечення кібербезпеки, аналіз ефективності комунікацій та покращення користувацького досвіду. Обробка здійснюється на підставі згоди.

4. Забезпечення прав суб'єктів даних

4.1. Суб'єкти персональних даних у межах проекту ERCM зберігають повний контроль над своєю персональною інформацією. Університет як контролер забезпечує належні умови для вільної та безперешкодної реалізації їхніх прав.

4.2. Кожен учасник має право звернутися до координатора проекту із запитом щодо підтвердження факту обробки його персональних даних, а також отримати копію таких даних.

4.3. У разі виявлення неточностей або неповноти персональних даних, зокрема у реєстраційних формах чи сертифікатах, суб'єкт даних має право вимагати їх негайного виправлення або доповнення.

4.4. Суб'єкт даних має право вимагати видалення своїх персональних даних у разі відсутності необхідності їх подальшої обробки для цілей проекту або у випадку відкликання згоди. Зазначене право може бути обмежене, якщо збереження даних є обов'язковим відповідно до вимог аудиту Європейського Союзу щодо підтвердження цільового використання грантових коштів.

4.5. Суб'єкт даних має право вимагати обмеження обробки його персональних даних, зокрема на період перевірки їх точності, а також заперечити проти обробки, зокрема щодо використання контактних даних для інформаційних розсилок у межах проекту.

4.6. На запит суб'єкта його персональні дані можуть бути надані у структурованому, загальноприйнятому та машинозчитуваному форматі для подальшої передачі іншому контролеру.

4.7. Для реалізації будь-якого з цих прав суб'єкт даних має направити електронний або письмовий запит на ім'я координатора проекту, який підлягає обробці не пізніше одного місяця.

5. Організаційно-технічні заходи захисту та управління інцидентами

5.1. Захист персональних даних є пріоритетом діяльності проекту. Доступ до персональної інформації надається лише уповноваженим особам, функціональні обов'язки яких безпосередньо пов'язані з її обробкою. Такі особи зобов'язані дотримуватися конфіденційності.

5.2. Технічний захист забезпечується використанням сучасних засобів шифрування, захищених сховищ, багатофакторної автентифікації та регулярного резервного копіювання. Дані, що використовуються для аналітики, підлягають знеособленню.

5.3. У разі порушення безпеки персональних даних застосовується процедура реагування, яка передбачає локалізацію інциденту, його документування, проведення розслідування та, за необхідності, повідомлення компетентних органів і суб'єктів даних.

6. Зберігання, архівування та транскордонна передача даних

6.1. У зв'язку з міжнародним характером проєкту може здійснюватися транскордонна передача персональних даних, зокрема для забезпечення взаємодії з іноземними викладачами. Така передача здійснюється лише за умови забезпечення належного рівня захисту даних відповідно до вимог GDPR або на підставі відповідних договірних механізмів.

6.2. Терміни зберігання персональних даних жорстко регламентовані правилами фінансового управління грантами ЄС. Відповідно до статті 20 (Record-keeping) Грантової угоди, усі первинні документи, що підтверджують належну імплементацію проєкту та можуть містити персональні дані (реєстраційні листи, анкети, договори), зберігаються в захищених архівах Університету щонайменше протягом 5 років після здійснення фінального платежу (або 3 років для грантів до 60 000 євро) для забезпечення можливості проведення постпроєктних аудитів інституціями ЄС. Після спливу цього терміну, і якщо відсутні інші юридичні підстави для зберігання, персональні дані підлягають безповоротному знищенню.

ПОЛІТИКА БЕЗПЕКИ

1. Загальні положення