ПОЛІТИКА ЦИФРОВОГО ВРЯДУВАННЯ ТА ЕТИКИ ШТУЧНОГО ІНТЕЛЕКТУ

DIGITAL GOVERNANCE AND AI ETHICS POLICY

Поле	Зміст
Організація	МГЕО «Наш Дім - Манява»
Версія	2.2 FINAL
Попередня версія	2.1
Дата затвердження	13.06.2026
Дата перегляду	Щорічно або раніше у разі змін законодавства, донорських вимог, цифрових ризиків, інструментів, програмної діяльності чи внутрішніх процедур
Відповідальний	Керівник Організації / відповідальна особа з цифрового врядування, даних та етики штучного інтелекту
Пов'язані політики	Політика захисту дітей і вразливих груп; Кодекс етики та поведінки; Політика конфіденційності та захисту персональних даних; Антикорупційна політика; Політика екологічної, кліматичної та громадської відповідальності; Політика фінансового управління та закупівель; Політика моніторингу, оцінки, підзвітності та навчання; Політика управління ризиками
Сайт	https://ourhomemanyava.com

Примітка до версії: v2.2 оновлює політику v2.1 і додає правила щодо строків зберігання та видалення даних, перевірки цифрових і ШІ-постачальників, транскордонної передачі даних, ризиків упередженості ШІ, цифрової доступності та журналу використання ШІ.

Зміст

Додатки

Concise English Reference Summary

Українська версія

1. Мета та сфера застосування

Ця Політика визначає принципи, правила та мінімальні процедури цифрового врядування й етичного використання штучного інтелекту в діяльності МГЕО «Наш Дім - Манява».

Метою Політики є забезпечити, щоб цифрові інструменти, дані, онлайн-комунікація, сайт, карти, фото, відео, форми збору даних і штучний інтелект використовувалися безпечно, етично, прозоро, відповідально та без шкоди для людей, дітей, громад, довкілля, партнерів, донорів і репутації Організації.

Політика застосовується до працівників, членів Організації, волонтерів, консультантів, тренерів, експертів, партнерів та підрядників, які використовують цифрові інструменти або працюють із даними Організації.

- збору, зберігання, аналізу, публікації та архівування цифрових даних;
- використання KoboToolbox, онлайн-форм, таблиць, хмарних папок, електронної пошти, сайту, соціальних мереж, геоінформаційних систем, карт, фото, відео та інструментів штучного інтелекту;
- підготовки донорських звітів, аналітичних матеріалів, новин, презентацій, публікацій, екологічних статей і навчальних матеріалів;
- роботи з персональними даними, даними дітей, чутливими геоданими, відкритими екологічними даними та громадською наукою;
- усіх проєктів і фреймворків Карпатської ініціативи 2026-2028.

2. Основні принципи цифрового врядування

- Безпека: цифрові дані, акаунти, паролі, хмарні папки, форми та сайти мають бути захищені від несанкціонованого доступу.
- Мінімізація даних: збираються лише ті дані, які справді потрібні для діяльності, звітності, моніторингу або безпеки.
- Законність і згода: персональні дані збираються і використовуються на законних підставах, із належною згодою там, де це потрібно.
- Захист дітей: дані дітей, фото, відео, історії, голоси, цитати та будь-які матеріали за участі дітей обробляються з підвищеною обережністю.
- Прозорість: учасники мають розуміти, які дані збираються, для чого вони потрібні та як можуть бути використані.
- Контроль людини: важливі рішення не можуть ухвалюватися автоматично або лише на основі штучного інтелекту.
- Доказовість: цифрові інструменти і штучний інтелект не можуть використовуватися для вигадування фактів, результатів, екологічних даних, цитат, історій або показників.
- Обережність із геоданими: точні координати, маршрути, природні об'єкти, приватні території, місця перебування дітей або чутливі локації не публікуються без оцінки ризику.
- Недопущення цифрових маніпуляцій: Організація не використовує цифрові інструменти для перебільшення результатів або створення неправдивого враження про вплив.

3. Класифікація цифрових даних

Організація класифікує цифрові дані за рівнем доступу та ризику.

Категорія даних	Опис	Приклади	Правило доступу
Публічні дані	Дані, які можуть бути відкрито оприлюднені без ризику	Новини, загальні звіти, публічні фото без персональних ризиків, загальна статистика	Можуть публікуватися після перевірки
Внутрішні дані	Дані для роботи команди, які не призначені для широкого поширення	Робочі таблиці, чернетки звітів, плани заходів, внутрішні нотатки	Доступ лише команді або визначеним особам
Конфіденційні дані	Дані, розкриття яких може зашкодити людям, партнерам, Організації або проєкту	Персональні дані учасників, контакти, форми згоди, фінансові документи, договори	Доступ лише уповноваженим особам
Чутливі дані	Дані з підвищеним ризиком для безпеки, дітей, приватності, природних об'єктів або воєнного контексту	Дані дітей, точні координати, фото з геолокацією, дані вразливих груп, маршрути, інформація про критичну інфраструктуру	Не публікуються без окремої оцінки ризику і дозволу

Перед публікацією будь-яких даних відповідальна особа перевіряє, чи не містять вони персональної, конфіденційної або чутливої інформації.

4. Корпоративні акаунти, доступи та цифрова безпека

Організація використовує корпоративні або офіційно визначені акаунти для роботи з даними Організації, донорськими матеріалами, персональними даними, фінансовими документами, фото, відео, картами та звітами.

- для електронної пошти, хмарних сховищ, банківських, фінансових, донорських і робочих систем використовується двофакторна автентифікація, якщо вона доступна;
- паролі не передаються через незахищені канали;
- однакові паролі не використовуються для різних критичних сервісів;
- доступ до папок і файлів надається за принципом необхідності;
- доступи колишніх працівників, волонтерів, консультантів або партнерів закриваються після завершення співпраці;
- важливі документи резервно копіюються;
- підозрілі листи, посилання, вкладення або запити на зміну банківських реквізитів перевіряються окремим каналом;
- особисті акаунти не використовуються для зберігання персональних даних, донорських документів або чутливих матеріалів Організації;
- правила доступу до банківських, фінансових, бухгалтерських і закупівельних систем визначаються Політикою фінансового управління та закупівель і застосовуються разом із цією Політикою.

5. Захист персональних даних, даних дітей і вразливих груп

Організація обробляє персональні дані відповідно до Політики конфіденційності та захисту персональних даних.

Особлива обережність застосовується до дітей віком до 18 років, ВПО, осіб з інвалідністю, дітей військовослужбовців, малозабезпечених родин та учасників, які можуть бути вразливими через соціальний, безпековий, психологічний або інший контекст.

Заборонено:

- завантажувати персональні дані дітей у відкриті або неперевірені інструменти штучного інтелекту;
- публікувати фото або відео дітей без належної згоди;
- публікувати історії дітей у спосіб, що може створити стигму, жалість, тиск або ризик;
- збирати зайві персональні дані “про всяк випадок”;
- публікувати списки дітей, телефони, адреси, точні місця перебування або інші дані, які можуть створити ризик.

6. KoboToolbox, цифрові форми та збір даних

Організація може використовувати KoboToolbox, онлайн-форми, таблиці та інші цифрові інструменти для моніторингу, оцінки, підзвітності, навчання, реєстрації учасників, збору зворотного зв’язку, громадської науки та екологічних спостережень.

- кожна форма має чітку мету;
- форма не збирає зайвих персональних даних;
- якщо збираються персональні дані, учаснику пояснюється мета збору;
- для дітей застосовуються вимоги Політики захисту дітей і Політики конфіденційності;
- поля з геолокацією використовуються лише за потреби;
- чутливі геодані не публікуються у відкритому доступі;
- доступ до результатів форм мають лише уповноважені особи;
- перед публікацією дані знеособлюються або агрегуються.

7. Геоінформаційні системи, карти, геодані та дрони

Організація може використовувати геоінформаційні системи, карти, GPS-дані, фото з прив’язкою до місця, дрони або безпілотні літальні апарати лише з чіткою освітньою, екологічною, моніторинговою, аналітичною або звітною метою.

Не публікуються без окремої оцінки ризику:

- точні координати місць перебування дітей;
- точні координати приватних територій;
- маршрути польових активностей;
- дані про критичну інфраструктуру;
- матеріали з дронів або безпілотних літальних апаратів;
- точні координати чутливих природних об’єктів;
- дані, які можуть створити ризики для природоохоронних установ, громад, дітей, учасників або безпеки.

Використання дронів або безпілотних літальних апаратів допускається лише за наявності законних підстав, дозволів, безпекової оцінки та відповідальної особи.

8. Сайт, соціальні мережі та цифрова комунікація

Офіційний сайт Організації та соціальні мережі є інструментами публічності, екологічної освіти, доступу до інформації, звітності та комунікації з громадами, партнерами й донорами.

- перед публікацією перевіряються факти, згода на фото/відео/історії, відсутність персональних або чутливих даних;
- екологічні твердження мають бути коректними і не перебільшеними;
- матеріали не мають містити стигматизуючої або маніпулятивної мови;
- матеріали, створені або суттєво відредаговані за допомогою штучного інтелекту, проходять людську перевірку перед публікацією.

9. Етика використання штучного інтелекту

Організація може використовувати інструменти штучного інтелекту як допоміжний інструмент для структурування текстів, редагування, перекладу, підготовки чернеток, узагальнення відкритої інформації, підготовки навчальних матеріалів, аналізу неособистих і нечутливих даних, генерації ідей для комунікації або проєктного планування.

Штучний інтелект не замінює професійне судження, експертну перевірку, рішення керівника, відповідальність команди, донорські вимоги, законодавство або етичні стандарти Організації. Усі матеріали, підготовлені за допомогою штучного інтелекту, розглядаються як чернетки до людської перевірки.

10. Дозволене, обмежене та заборонене використання штучного інтелекту

Категорія	Приклади	Умова
Дозволене використання	Редагування тексту, переклад, структура звіту, підготовка плану, навчальні матеріали, узагальнення відкритих джерел	Потрібна перевірка людиною
Обмежене використання	Аналіз таблиць, робота з чернетками донорських звітів, підготовка чутливих комунікацій, робота з фото або історіями	Не використовувати персональні або чутливі дані без знеособлення
Заборонене використання	Вигадування екологічних даних, результатів водних тестів, цитат, історій учасників, донорських показників, партнерств, фотофактів або доказів	Заборонено завжди
Заборонене використання	Завантаження персональних даних дітей, вразливих груп, приватних адрес, телефонів, форм згоди або чутливих геоданих у неперевірені ШІ-сервіси	Заборонено без окремої правової і безпекової оцінки
Заборонене використання	Автоматичний відбір учасників, волонтерів, партнерів або отримувачів підтримки без рішення людини	Заборонено

Штучний інтелект не може використовуватися для прийняття остаточних рішень щодо фінансування, участі дітей, партнерств, субгрантів, закупівель, оцінки персоналу, реагування на скарги або висновків щодо екологічної шкоди.

11. Перевірка матеріалів, створених за допомогою штучного інтелекту

Перед використанням або публікацією матеріалів, підготовлених за допомогою штучного інтелекту, відповідальна особа перевіряє факти, цифри, назви організацій, посилання на документи, законодавчі твердження, екологічні висновки, відсутність вигаданих джерел, персональних або чутливих даних, дискримінаційної, стигматизуючої або маніпулятивної мови.

Для звичайного редагування, перекладу або мовного покращення окреме публічне маркування не є обов’язковим, якщо донор або законодавство не вимагає іншого.

12. Строки зберігання, архівування, видалення та анонімізація даних

Організація зберігає персональні, проєктні, цифрові, фото-, відео-, географічні та моніторингові дані лише протягом строку, необхідного для досягнення мети їх збору, виконання донорських, юридичних, фінансових, звітних або архівних зобов’язань.

Організація не накопичує персональні або чутливі дані безстроково. Після завершення проєкту, звітного періоду або строку зберігання такі дані мають бути видалені, знеособлені або архівовані з обмеженим доступом.

Тип даних	Орієнтовний строк зберігання	Подальша дія
Форми згоди батьків / законних представників	До 5 років після завершення активності або довше, якщо цього вимагає донор	Архівування або видалення
Фото та відео дітей	До завершення мети використання або строку дії згоди; зазвичай не довше 3-5 років	Видалення або повторна перевірка згоди
Реєстри учасників заходів	До 5 років або відповідно до вимог донора	Видалення або знеособлення
KoboToolbox-записи з персональними даними	До завершення проєкту, аудиту та звітності; зазвичай до 5 років	Експорт у захищений архів, знеособлення або видалення
Донорські звіти та підтвердні документи	До 7 років або довше, якщо цього вимагає донор	Архівування з обмеженим доступом
Знеособлені статистичні або аналітичні дані	Можуть зберігатися довше для навчання, звітності та аналізу тенденцій	Зберігання без персональних даних
Геодані та карти	До завершення проєкту або аналітичної мети	Знеособлення, узагальнення або обмеження доступу
Дані цифрових інцидентів	До 5 років або довше у разі юридичного, донорського чи безпекового ризику	Захищене архівування
Фінансові та закупівельні цифрові документи	Відповідно до Політики фінансового управління та закупівель, зазвичай не менше 7 років	Архівування

Перед видаленням або анонімізацією даних відповідальна особа перевіряє, чи не існує чинної донорської, юридичної, фінансової, аудиторської або safeguarding-потреби у подальшому зберіганні.

Якщо учасник, батьки або законний представник дитини відкликають згоду на використання фото, відео або історії, Організація розглядає таке звернення відповідно до Політики конфіденційності та, за можливості, припиняє подальше використання відповідного матеріалу.

13. Перевірка цифрових, хмарних та ШІ-постачальників

Перед використанням цифрового, хмарного або ШІ-інструменту для роботи з даними Організації відповідальна особа оцінює базові ризики такого інструменту.

- Особлива перевірка потрібна, якщо інструмент може обробляти персональні дані, дані дітей, фото, відео або історії учасників, форми згоди, донорські або фінансові документи, чутливі геодані, внутрішні документи Організації або матеріали, які ще не були публічно оприлюднені.
- Під час перевірки Організація за можливості з'ясовує, чи зберігає сервіс введені дані, чи використовує їх для навчання моделей, чи можна це вимкнути, де розташовані сервери або яка юрисдикція постачальника, чи є умови обробки даних, чи дозволяє сервіс видаляти дані та чи підтримує двофакторну автентифікацію.
- Інструменти штучного інтелекту не повинні використовуватися для обробки персональних даних дітей, форм згоди, приватних адрес, телефонів, медичних або соціально чутливих даних, чутливих геоданих або непублічних донорських документів без окремої оцінки ризику.

Якщо текст або дані потрібно використати в ШІ-інструменті, вони мають бути попередньо знеособлені: імена, контакти, адреси, назви конкретних дітей, приватні деталі, точні координати та інші ідентифікатори мають бути видалені або замінені нейтральними позначками.

14. Упередженість ШІ, цифрова доступність і журнал використання ШІ

Організація визнає, що інструменти штучного інтелекту можуть містити упередження, неточності, помилки, неповні припущення або мовні, соціальні, регіональні чи культурні викривлення.

ШІ не може самостійно визначати, які громади є пріоритетними для проєкту, які діти, школи, партнери або групи мають бути залучені, хто має отримати підтримку, які екологічні проблеми є доведеними або які рішення слід приймати щодо фінансування, субгрантів, закупівель чи партнерств.

Будь-які висновки, підготовлені за допомогою ШІ, мають перевірятися людиною з урахуванням місцевого контексту, доступних доказів, консультацій із громадами, донорських вимог і принципу недискримінації.

Організація також прагне забезпечувати цифрову доступність своїх інструментів і матеріалів. Форми, анкети, публікації, сайти й цифрові матеріали мають бути, за можливості, написані простою мовою, придатні для використання з мобільного телефону, не надмірно довгі або складні, доступні офлайн або в паперовій альтернативі, якщо учасники не мають стабільного інтернету, та адаптовані для дітей, молоді, людей з інвалідністю або інших груп, якщо це потрібно для участі.

15. Реєстр цифрових інструментів і програмного забезпечення

Організація веде внутрішній Реєстр цифрових інструментів і програмного забезпечення, які використовуються для роботи.

Інструмент	Мета використання	Тип даних	Персональні дані	Дані дітей	Юрисдикція / сервери, якщо відомо	Використання даних для навчання ШІ	Рішення
Microsoft 365	Документи, пошта, хмарні файли	Внутрішні, конфіденційні	Можливо	Ні / за потреби	Потребує перевірки умов сервісу	Ні	Дозволено
Google Workspace	Пошта, форми, таблиці, диск	Внутрішні, персональні за потреби	Можливо	Ні / за потреби	Потребує перевірки умов сервісу	Ні	Дозволено
KoboToolbox	Форми, опитування, моніторинг	Учасники, анкети, геодані за потреби	Можливо	Можливо	Потребує перевірки умов сервісу	Ні	Дозволено з обмеженнями
Canva	Дизайн, публікації, інфографіка	Медіаматеріали	Можливо	Можливо	Потребує перевірки умов сервісу	Можливо, залежно від налаштувань	Дозволено з обмеженнями
WordPress / сайт	Публікації, сторінки, новини	Публічні матеріали	Ні / мінімально	Ні / за згодою	Україна / інше залежно від хостингу	Ні	Дозволено
Інструменти штучного інтелекту	Редагування, переклад, структура текстів	Лише знеособлені або нечутливі дані	Ні	Ні	Потребує перевірки умов сервісу	Залежить від сервісу	Дозволено з обмеженнями

Рішення щодо інструменту може бути: дозволено; дозволено з обмеженнями; лише для знеособлених даних; лише для публічних матеріалів; не використовувати.

16. Реагування на цифрові інциденти

Цифровий інцидент - це подія, яка може створити ризик для даних, акаунтів, систем, репутації, донорської звітності, дітей, учасників або безпеки Організації.

- злам електронної пошти або акаунту;
- втрата доступу до хмарної папки;
- випадкове надсилання персональних даних не тій особі;
- публікація фото або даних без згоди;
- витік даних дітей;
- публікація чутливих геоданих;
- фішинг;
- підозрілий запит на зміну банківських реквізитів;
- втрата пристрою з робочими даними;
- використання штучного інтелекту для створення неправдивих або неперевірених матеріалів.

Крок	Дія	Відповідальний	Орієнтовний строк	Документування
1	Виявити та зафіксувати інцидент	будь-який член команди	негайно	повідомлення відповідальній особі
2	Обмежити ризик: змінити пароль, зупинити доступ, видалити публікацію, заблокувати посилання	відповідальна особа / керівник	до 24 годин	журнал інцидентів
3	Оцінити масштаб: які дані, кого стосується, який ризик	керівник / відповідальна особа	24-48 годин	коротка оцінка інциденту
4	Повідомити постраждалих, донора, партнера або компетентний орган, якщо це потрібно	керівник Організації	залежно від вимог і ризику	лист / повідомлення
5	Усунути причину і відновити контроль	відповідальна особа / команда	до 10 робочих днів або швидше	коригувальні дії
6	Зафіксувати уроки	команда	після закриття інциденту	журнал уроків

Якщо інцидент стосується персональних даних, Організація діє відповідно до Політики конфіденційності. Якщо інцидент стосується дітей або вразливих груп, застосовується Політика захисту дітей і вразливих груп. Якщо інцидент стосується фінансових акаунтів або банківських реквізитів, застосовується Політика фінансового управління та закупівель.

17. Ролі та відповідальність

Роль	Відповідальність
Керівник Організації	Загальний нагляд за цифровим врядуванням, затвердження політики, рішення щодо суттєвих цифрових ризиків, інцидентів і використання штучного інтелекту
Відповідальна особа з цифрового врядування / даних	Реєстр цифрових інструментів, контроль доступів, оцінка цифрових ризиків, реагування на інциденти
Відповідальна особа з моніторингу, оцінки, підзвітності та навчання	Якість даних, цифрові форми, KoboToolbox, індикатори, знеособлення даних, журнал уроків
Комунікаційна особа	Перевірка публікацій, сайту, соціальних мереж, фото, відео, ШІ-матеріалів і дотримання правил відповідальної комунікації
Фінансова відповідальна особа / бухгалтер	Захист фінансових даних, банківських доступів, донорських документів і фінансових файлів
Відповідальні за заходи	Збір згод, фото, списків участі, цифрових форм, захист даних учасників і дітей
Партнери та підрядники	Дотримання правил захисту даних, цифрової безпеки, етичного використання ШІ та конфіденційності відповідно до угод

18. Навчання команди та волонтерів

Організація прагне щорічно проводити базове ознайомлення команди та волонтерів із правилами цифрового врядування і етики штучного інтелекту.

- безпечне використання електронної пошти;
- розпізнавання фішингу;
- двофакторну автентифікацію;
- захист персональних даних;
- правила фото і відео дітей;
- роботу з KoboToolbox;
- очищення даних перед публікацією;
- роботу з чутливими геоданими;
- етичне використання штучного інтелекту;
- заборону вигадування даних і результатів;
- реагування на цифрові інциденти.

Факт ознайомлення може фіксуватися підписом, електронним підтвердженням, протоколом навчання або іншим простим способом.

19. Перегляд політики

Політика переглядається щорічно або раніше у разі змін законодавства, нових донорських вимог, появи нових цифрових інструментів, цифрового інциденту, зміни структури Організації, зміни програмної діяльності, оновлення пов'язаних політик, змін у практиках використання штучного інтелекту або появи нових ризиків для даних, дітей, геоданих чи цифрової безпеки.

Оновлення Політики документується із зазначенням версії, дати та суті змін.

Затверджено: Керівник Організації _____ / Микола Скиданюк /

Дата: 13.06.2026

Додатки

Додаток 1. Чеклист перед використанням штучного інтелекту

- Чи містить текст персональні дані?
- Чи містить текст дані дітей?
- Чи містить текст приватні адреси, телефони, фото, історії або чутливі геодані?
- Чи можна знеособити текст перед використанням?
- Чи не просимо ШІ вигадати факти, цифри, цитати або результати?
- Чи буде матеріал перевірений людиною?
- Чи не містить результат неперевірених джерел?
- Чи не перебільшує результат вплив Організації?
- Чи не створює текст екологічну маніпуляцію?
- Чи відповідає текст політикам Організації?

Додаток 2. Журнал цифрових інцидентів

Дата	Тип інциденту	Опис	Дані / система	Ризик	Негайні дії	Відповідальний	Статус	Уроки

Додаток 3. Матриця доступу до цифрових даних

Тип даних	Хто має доступ	Чи можна публікувати	Умови
Публічні матеріали	команда / комунікаційна особа	так	після перевірки
Внутрішні робочі документи	команда	ні або частково	за потреби
Персональні дані учасників	уповноважені особи	ні	лише для проєктної мети
Дані дітей	мінімально необхідні особи	ні	лише за згодою і з підвищеним захистом
Геодані	відповідальні особи	лише агреговано або після оцінки ризику	без чутливих координат
Фінансові документи	керівник / фінансова особа / бухгалтер	ні	відповідно до фінансової політики

Додаток 4. Чеклист публікації цифрового матеріалу

- Чи перевірено факти?
- Чи є згода на фото/відео/історію?
- Чи немає персональних даних дітей?
- Чи немає чутливих геоданих?
- Чи не перебільшено результат?
- Чи не видаються освітні спостереження за офіційні висновки?
- Чи не створює матеріал ризик для громади, дитини, партнера або природного об'єкта?
- Чи перевірено текст, якщо він створений або відредагований ШІ?
- Чи відповідає матеріал Кодексу етики та поведінки?
- Чи відповідає матеріал Політиці конфіденційності?

Додаток 5. Журнал використання ШІ

Дата	Матеріал / завдання	Інструмент	Мета використання	Чи були персональні дані	Чи знеособлено дані	Хто перевірив	Рішення

Concise English Reference Summary

The Ukrainian version of this Policy is the primary and official working version approved by the Organization. This English summary is provided for donor review and communication with international partners.

Youth Public Environmental Organization “Our Home - Manyava” applies digital governance and artificial intelligence ethics rules to ensure safe, transparent and responsible use of digital tools, cloud systems, websites, online forms, KoboToolbox, GIS, maps, photos, videos, open environmental data and AI-assisted content.

The Policy prohibits the use of AI to fabricate environmental data, water testing results, quotes, participant stories, donor indicators, partnerships or evidence. Personal data of children, vulnerable groups, private addresses, sensitive geodata and consent forms must not be uploaded to unverified AI tools.

The Organization applies human review, data minimization, access control, two-factor authentication where available, retention and deletion rules, vendor risk checks, incident logging, safe publication checks and responsible communication standards. The Policy is linked to the Organization’s Safeguarding Policy, Privacy Policy, MEAL Policy, Risk Management Policy, Financial Management and Procurement Policy, Environmental, Climate and Community Resilience Policy and Code of Conduct.

Approved by: Head of the Organization _____ / Mykola Skydaniuk /

Date: 13.06.2026