ГРОМАДСЬКА ОРГАНІЗАЦІЯ «ГЛОБАЛЬНА БЕЗПЕКА»

ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Статус документа	Внутрішня політика та публічне повідомлення про обробку персональних даних
Затверджено	Рішенням Правління від 12.06.2026, протокол № 2
Дата набрання чинності	12.06.2026
Володілець персональних даних	ГО «Глобальна безпека»
Відповідальна особа	Голова Правління, Коржевський І.І.
Контакт з питань приватності	info@go-global-security.org
Перегляд	Не рідше одного разу на три роки або після істотних змін у діяльності чи законодавстві

Київ, 2026

ГРОМАДСЬКА ОРГАНІЗАЦІЯ «ГЛОБАЛЬНА БЕЗПЕКА»

1. Мета, сфера дії та нормативна основа

1.1. Ця Політика визначає порядок збирання, використання, зберігання, передачі, захисту та видалення персональних даних Громадською організацією «Глобальна безпека» (далі – Організація).

1.2. Політика поширюється на фактичні напрями діяльності Організації: аналітичні дослідження у сферах громадської, інформаційної та гуманітарної безпеки; безпековий, інформаційний, аналітичний і проєктний консалтинг; створення вебресурсів, баз даних, інформаційних систем та інших цифрових рішень; незалежне оцінювання і сертифікацію професійних компетентностей; реалізацію спільних проєктів і суспільних ініціатив.

1.3. Політика застосовується до персональних даних членів Організації, працівників, волонтерів, експертів, консультантів, партнерів, підрядників, клієнтів, респондентів, учасників заходів, школярів та їхніх законних представників у межах дослідницьких і просвітницьких ініціатив, кандидатів на сертифікацію, членів кваліфікаційних та апеляційних комісій, а також користувачів вебсайту і цифрових продуктів.

1.4. Організація може діяти як володілець персональних даних, як розпорядник за договором із партнером або замовником, а у спільних проєктах – як спільний володілець із письмово розподіленими обов’язками.

1.5. Політика розроблена відповідно до Конституції України, законів України «Про захист персональних даних», «Про інформацію», «Про громадські об’єднання» та з урахуванням принципів GDPR, якщо вони застосовуються за умовами міжнародного проєкту або договору.

1.6. Захист приватності є складовою принципів прозорості, поваги до прав людини, добровільності, незалежності оцінювання та відповідального використання даних і технологій.

2. Основні терміни та відповідальні ролі

Термін	Визначення
Персональні дані	відомості про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Обробка	будь-яка дія з персональними даними, зокрема збирання, запис, зберігання, використання, передача, знеособлення та видалення.
Володілець персональних даних	особа, яка визначає мету, склад даних і порядок їх обробки.
Розпорядник персональних даних	особа, яка обробляє дані від імені володільця за договором та його інструкціями.
Суб’єкт персональних даних	фізична особа, якої стосуються персональні дані.
Згода	добровільне, конкретне, поінформоване та однозначне волевиявлення особи щодо обробки її даних.
Псевдонімізація	відокремлення ідентифікаторів від основного набору даних із зберіганням ключа відповідності окремо.
Знеособлення	перетворення даних так, щоб особу неможливо було ідентифікувати розумними засобами.
Порушення безпеки	втрата, знищення, зміна, несанкціоноване розкриття або доступ до персональних даних.

2.1. Відповідальність

- Правління затверджує Політику, визначає відповідальну особу та забезпечує необхідні ресурси.
- Голова Правління організовує виконання Політики та приймає рішення щодо істотних інцидентів.
- Відповідальна особа веде реєстр операцій обробки, опрацьовує запити суб'єктів, координує оцінювання ризиків та реагування на порушення.
- Керівник проєкту визначає мету, склад даних, правила інформування учасників, доступ, передачу та строки зберігання.
- Керівник сертифікаційного процесу забезпечує захист заяв, документів, тестових матеріалів, результатів і апеляцій.
- Кожна особа з доступом до даних зобов'язана дотримуватися конфіденційності та негайно повідомляти про можливий інцидент.

3. Принципи та правові підстави обробки

Законність і прозорість. дані обробляються на належній підставі, а особа отримує зрозумілу інформацію про таку обробку.
Обмеження мети. дані використовуються лише для заздалегідь визначеної та сумісної мети.
Мінімізація. збирається лише інформація, необхідна для конкретної діяльності.
Точність. неточні або застарілі дані виправляються чи видаляються.
Обмеження зберігання. дані зберігаються не довше, ніж цього потребують мета, закон, договір або захист прав.
Безпека. застосовуються організаційні та технічні заходи проти втрати й несанкціонованого доступу.
Підзвітність. мета, підстава, доступ, передачі, строки та заходи захисту документуються.
Privacy by design. захист даних враховується під час створення анкет, баз даних, цифрових систем і процедур сертифікації.
Не нашкодь. обробка не повинна створювати непропорційний фізичний, цифровий, соціальний або репутаційний ризик.
3.2. Правовою підставою можуть бути згода, виконання договору, законодавчий обов'язок, статутна суспільно корисна діяльність за належної підстави, законний інтерес після оцінки балансу прав або інша підстава, визначена законом.
3.3. Згода не використовується формально там, де особа не має вільного вибору. Відкликати згоду має бути так само легко, як її надати.

4. Категорії даних та цілі обробки

Категорія	Приклади	Основна мета
Контактні та ідентифікаційні	ПІБ, посада, організація, email, телефон, адреса для листування	комунікація, партнерство, участь у заходах і проєктах
Професійні	освіта, досвід, компетентності, кваліфікація, сертифікати	добір експертів, консалтинг і сертифікація
Членські та договірні	заяви, протокольні відомості, договори, реквізити для виплат	управління Організацією, виконання договорів і звітність
Дослідницькі	анкети, відповіді до і після інформаційних занять, інтерв'ю, записи, транскрипти	аналітичні дослідження і підготовка рекомендацій
Сертифікаційні	заяви, документи про освіту і досвід, відповіді, результати, записи прокторингу, апеляції	допуск, оцінювання, видача та перевірка сертифікатів
Клієнтські	контактні дані, матеріали запиту, інформація про процеси, ризики і цифрові системи	безпековий, інформаційний, аналітичний і проєктний консалтинг
Технічні	IP-адреса, журнали входу, cookie, параметри пристрою	робота вебсайту, цифрових продуктів і кібербезпека
Фото, відео і голос	матеріали заходів, інтерв'ю та дистанційного оцінювання	документування, комунікація або контроль доброчесності за належної підстави

5. Аналітичні дослідження та робота зі школярами

5.1. До початку дослідження визначаються мета, склад даних, правова підстава, строки, доступ, правила передачі та публікації.

5.2. Учасникам або їхнім законним представникам надається зрозуміла інформація про добровільність, мету, використання результатів і контакт для звернення.

5.3. Під час оцінювання обізнаності школярів щодо мінної безпеки збираються лише ті відомості, які необхідні для визначення рівня знань до і після інформаційних занять. ПІБ учнів не включаються до аналітичних звітів.

5.4. Дані неповнолітніх обробляються з мінімізацією ідентифікаторів, належною згодою законного представника, обмеженим доступом і забороною публікації персоналізованих результатів.

5.5. Результати оприлюднюються переважно в агрегованій формі. Для малих груп окремо оцінюється ризик повторної ідентифікації.

5.6. Фото, відео, прямі цитати або персональні історії дітей використовуються лише за окремою належною згодою та після оцінки можливого ризику.

5.7. Відмова від участі у дослідженні не може впливати на доступ до інформаційного заняття або інших заходів Організації.

6. Консалтинг та цифрові рішення

6.1. Обсяг доступу до даних клієнта визначається договором і принципом необхідності знати.

6.2. Дані одного клієнта не використовуються в інтересах іншого клієнта або в публічній аналітиці без окремої правової підстави.

6.3. Під час оцінювання безпекових ризиків Організація не оприлюднює точні відомості про вразливості, інфраструктуру, облікові записи або інші деталі, здатні створити додаткову загрозу.
6.4. Під час створення вебресурсів, баз даних та інформаційних систем застосовуються рольовий доступ, безпечні налаштування за замовчуванням, резервне копіювання та журналювання критичних дій.
6.5. У договорі щодо цифрового продукту визначаються ролі сторін, право власності на дані, коло користувачів, строки зберігання, порядок видалення, підтримка та реагування на інциденти.
6.6. Після завершення консалтингового завдання матеріали повертаються, видаляються або зберігаються відповідно до договору.

7. Незалежне оцінювання і сертифікація

7.1. Дані кандидата використовуються лише для реєстрації, перевірки документів, допуску, ідентифікації, проведення іспиту, прийняття рішення, видачі та перевірки сертифіката, а також розгляду апеляції.
7.2. Документи про освіту, досвід та професійні досягнення доступні лише уповноваженим особам.
7.3. Тестові завдання, практичні кейси, відповіді, записи дистанційного прокторингу та протоколи захищаються від несанкціонованого доступу.
7.4. Автоматизована система може використовуватися для тестування і технічної перевірки, але не є єдиною підставою остаточного рішення. Практичні завдання оцінюються уповноваженими експертами.
7.5. Результати не передаються роботодавцю, навчальному провайдеру або іншій особі без правової підстави й належного інформування кандидата.
7.6. Відкритий реєстр сертифікатів містить лише мінімальні відомості, необхідні для перевірки чинності документа.
7.7. Апеляційні матеріали доступні лише незалежній апеляційній комісії та відповідальним адміністративним особам.

8. Вебсайт, форми звернення та cookies

8.1. Контактні форми на сайті можуть збирати ім’я, організацію, електронну адресу, телефон, тему та короткий опис запиту для опрацювання звернення.
8.2. Обов’язковими мають бути лише поля, необхідні для відповіді. Надані відомості не використовуються для іншої мети без окремої підстави.
8.3. Необхідні cookies можуть використовуватися для роботи сайту та безпеки. Необов’язкові cookies для аналітики активуються відповідно до вимог щодо згоди.
8.4. Інформаційні розсилки містять спосіб відмови. Службові повідомлення щодо проєкту, консультації або сертифікації відрізняються від рекламних.

9. Передача даних і залучені постачальники

9.1. Дані можуть передаватися провайдерам хостингу, електронної пошти, відеоконференцій, прокторингу, платіжних, бухгалтерських, юридичних та IT-послуг лише в необхідному обсязі.
9.2. Договори з розпорядниками визначають мету, конфіденційність, заходи безпеки, субпідрядників, строки і порядок видалення даних.

9.3. У спільних та міжнародних проєктах дані можуть передаватися партнерам, координаторам або аудиторам відповідно до договору та інформації, наданої учасникам.
9.4. Донори та партнери не отримують необмеженого доступу до ідентифікованих дослідницьких або сертифікаційних даних лише через фінансування чи співпрацю.
9.5. Організація не продає персональні дані.
9.6. Передача за межі України або Європейської економічної зони здійснюється лише за наявності належної підстави, договору та відповідних гарантій.

10. Використання штучного інтелекту

10.1. ШІ може використовуватися для перекладу, редагування, пошуку, класифікації та аналітичної підтримки.
10.2. До несанкціонованих зовнішніх сервісів заборонено завантажувати непублічні дані респондентів, документи кандидатів, тестові матеріали, клієнтські матеріали, паролі, платіжні або інші чутливі дані.
10.3. Фактичні твердження, джерела, ідентифікація осіб і результати, отримані за допомогою ШІ, перевіряються людиною.
10.4. Рішення щодо допуску, сертифікації, апеляції або іншого істотного наслідку для особи не ухвалюється виключно автоматизованою системою без людського перегляду.

11. Безпека і реагування на інциденти

- рольовий доступ і принцип найменших привілеїв;
- унікальні облікові записи, надійні паролі й багатофакторна автентифікація для критичних систем;
- шифрування передавання та, де доцільно, зберігання;
- резервне копіювання і перевірка відновлення;
- журналювання критичних дій та оновлення програмного забезпечення;
- угоди про конфіденційність і навчання осіб, які працюють із даними;
- безпечне видалення електронних і паперових носіїв.

11.2. Доступ переглядається після зміни ролі, завершення проєкту або співпраці. Спільні паролі та неконтрольовані копії даних не допускаються.
11.3. У разі інциденту необхідно негайно повідомити відповідальну особу, обмежити подальший доступ, зберегти докази, визначити склад і обсяг даних, оцінити можливу шкоду та задокументувати вжиті заходи.
11.4. Якщо це вимагається законом або необхідно для зменшення шкоди, Організація повідомляє компетентний орган, партнера або постраждалих осіб.

12. Права суб’єктів персональних даних

- отримувати інформацію про мету, склад, джерела, одержувачів і строки обробки;
- мати доступ до своїх даних;
- вимагати виправлення неточних або неповних відомостей;
- вимагати видалення даних за відсутності законної підстави для подальшого зберігання;
- відкликати згоду, якщо обробка ґрунтується на згоді;
- заперечувати проти обробки на підставі законного інтересу;
- вимагати людського перегляду істотного автоматизованого рішення;
- подати скаргу до Організації, Уповноваженого Верховної Ради України з прав людини або суду.

12.2. Організація може запросити інформацію для підтвердження особи. Обмеження запиту допускається лише з підстав, передбачених законом, необхідності захисту прав інших осіб, конфіденційності іспитових матеріалів або збереження доказів, і має бути пояснене.

13. Строки зберігання

Категорія	Строк або правило
Звернення через сайт	до 3 років після завершення комунікації, якщо звернення не стало частиною договору чи спору
Членські, договірні та бухгалтерські документи	відповідно до законодавства, Статуту та внутрішньої номенклатури
Дані кандидатів, яких не залучено	до 1 року або довше за окремою згодою
Дослідницькі дані	за планом дослідження, інформацією для учасників і вимогами партнера або донора
Сертифікаційні документи і результати	протягом строку чинності сертифіката та строку, необхідного для перевірки й апеляцій
Записи дистанційного оцінювання	до завершення строку апеляції та перевірки доброчесності, якщо довше зберігання не обґрунтоване
Клієнтські матеріали	за договором і розумним строком для захисту прав сторін
Технічні журнали	від кількох місяців до 2 років залежно від безпекової потреби
Скарги, апеляції та інциденти	протягом строку, необхідного для розгляду, захисту прав і підзвітності

13.2. Після завершення строку дані безпечно видаляються, знищуються або безповоротно знеособлюються.

14. Реєстр обробок, оцінювання ризиків і навчання

14.1. Організація веде реєстр основних операцій обробки із зазначенням мети, підстави, категорій даних, систем, одержувачів, строків та заходів безпеки.

14.2. До запуску обробки даних дітей, масштабного дослідження, дистанційного прокторингу, нової бази даних або іншого процесу підвищеного ризику проводиться оцінювання впливу на приватність.

14.3. Нові цифрові платформи, постачальники і партнери проходять перевірку приватності та безпеки.

14.4. Працівники, волонтери, експерти, дослідники, оцінювачі та адміністратори проходять навчання відповідно до своїх ролей.

15. Порушення Політики, оновлення та контакти

15.1. Несанкціонований доступ, копіювання, передавання, публікація, використання даних для особистої вигоди або приховування інциденту є порушенням цієї Політики.

15.2. Можливі заходи включають обмеження доступу, навчання, попередження, зміну ролі, припинення договору або співпраці та звернення до компетентних органів.

15.3. Добросовісне повідомлення про інцидент захищається від помсти.

15.4. Чинна версія Політики публікується на офіційному вебсайті Організації.

15.5. Запити, відкликання згоди, скарги або повідомлення про можливе порушення надсилаються на info@go-global-security.org із темою «Захист персональних даних».

15.6. Політика набирає чинності з дати затвердження Правлінням.

Додаток 1. Мінімальна форма Реєстру операцій обробки

Процес	Мета і підстава	Категорії даних / осіб	Система та доступ	Одержувачі	Строк	Заходи захисту

Додаток 2. Privacy by Design Checklist

- Чи визначена конкретна мета?
- Чи можна зменшити обсяг даних?
- Чи визначена правова підстава?
- Чи надано зрозумілу інформацію?
- Чи потрібні дані дітей або інші чутливі дані?
- Чи обмежено доступ?
- Чи перевірено постачальників і передачі?
- Чи встановлено строк видалення?
- Чи оцінено ризик повторної ідентифікації?
- Чи є план реагування на інцидент?
- Чи забезпечено людський контроль автоматизованих рішень?

Додаток 3. Форма повідомлення про порушення безпеки

Поле	Інформація
Дата і час виявлення	
Особа, яка повідомляє	
Система / проєкт / процес	
Опис події	
Категорії та приблизний обсяг даних	
Кількість і категорії постраждалих осіб	
Чи стосуються дані дітей або сертифікації	
Уже вжиті заходи	
Можливі наслідки	
Необхідна термінова допомога	

Додаток 4. Основні нормативні та інформаційні джерела

1. Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, у чинній редакції.
2. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII, у чинній редакції.
3. Закон України «Про громадські об’єднання» від 22 березня 2012 року № 4572-VI, у чинній редакції.
4. Регламент (ЄС) 2016/679 (General Data Protection Regulation, GDPR).
5. Privacy and Personal Data Protection Policy of the Scientific Center of Innovative Research, 2026, використана як структурний зразок.