ЗАТВЕРДЖЕНО
наказом Президентки організації
від 27 червня 2024р. № 27/06
_____ Бєлова А.А.

Політика конфіденційності та захисту персональних даних Громадської організації «Об'єднання ромських жінок «Голос Ромні»

I. МЕТА І ЗАВДАННЯ

1.1. Ця політика встановлює вимоги та процедури збору, обробки та захисту персональних даних бенефіціарів, а також збереження інформації, захисту інформації на публічних ресурсах Громадської організації «Об'єднання ромських жінок «Голос Ромні» (надалі - "Організація").

1.2. Метою політики є:
1.2.1 забезпечити відповідності діяльності Організації законодавству України та вимогам Загального регламенту про захист персональних даних (GDPR) щодо збору, обробки та зберігання персональних даних бенефіціарів та членів Команди Організації.
1.2.2. забезпечити механізми та процедури захисту та конфіденційності збору, обробки та зберігання персональних даних та інформації про бенефіціарів та членів Команди Організації, а також підвищення рівня свідомості та відповідальності членів Команди Організації у сфері інформаційної безпеки.
1.3 Вимоги цього положення стосуються як членів Команди Організації, так і представників влади або установ, які здійснюють перевірку діяльності Організації.

II. ОСНОВНІ ПОНЯТТЯ

2.1. Персональні дані - будь-яка інформація, що стосується ідентифікованої фізичної особи ("бенефіціар", "Член Команди Організації").
2.2. Команда Організації - особи, залучені до реалізації проектів та програм Організації, в тому числі працівники, тимчасово залучені особи, виконавці за цивільно-правовими договорами тощо.
2.3. Бенефіціар - це особа, яка безпосередньо отримує товари або послуги в межах програм Організації. До осіб, визначених цим терміном, відносяться вразливі та постраждалі групи населення, особливо діти, включаючи біженців, внутрішньо переміщених осіб та інших вразливих осіб, а також членів громад, які їх приймають.
2.4. Обробка персональних даних - будь-яка операція або сукупність операцій, здійснених з персональними даними, включаючи збір, запис, організацію, збереження,

адаптацію, зміну, витяг, консультування, використання, передачу, поширення, об'єднання, блокування, видалення або знищення, тощо.
2.3. База персональних даних - організована структура, що містить персональні дані бенефіціарів та забезпечує їх систематизацію та доступ до них.
2.4. Власник бази персональних даних - Організація, яка володіє та керує базою персональних даних бенефіціарів та членів Команди Організації визначеною у цьому положенні.
2.5. Суб'єкт персональних даних - фізична особа, до якої належать персональні дані та яка ідентифікована або може бути ідентифікована за допомогою таких даних.
2.6. Згода суб'єкта персональних даних - будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки;
2.7. Знеособлення персональних даних - вилучення відомостей, які дають змогу ідентифікувати особу.
2.8. Зберігання інформації - забезпечення належного стану інформації та її матеріальних носіїв
2.9. Конфіденційність інформації - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

III. ВІДПОВІДАЛЬНІ ОСОБИ ТА СФЕРА ЗАСТОСУВАННЯ

3.1 Дана політика поширюється на всю Команду Організації, включаючи осіб з повною трудовою зайнятістю, неповною зайнятістю або тимчасових працівників, всіх підрядників, замовників, партнерських організацій, що співпрацюють з Організацією в процесі реалізації проектів чи організаційної діяльності, усіх, хто надає послуги за договором та опосередковано на бенефіціарів та інші сторони, які є учасниками фінансових чи інших відносин із Організацією, кожен з котрих мають право на захист.
3.2. Президентка Організації приймає стратегічне рішення щодо збору, обробки, зберігання та передачі персональних даних, конфіденційності та захисту інформаційної безпеки.
3.3. Керівник відділу інформаційних систем та технології відповідає за забезпечення виконання цієї політики щодо безпечного та правильного збирання, зберігання, обробку та передачу персональних даних, конфіденційності та інформаційної безпеки, відповіді на запити, включаючи розробку та впровадження політик та процедур інформаційної безпеки.
3.4. Керівник відділу інформаційних систем та технології може призначати членів команди свого відділу відповідальними за зберігання, обробку та передачу персональних даних, конфіденційності та інформаційної безпеки оформивши відповідний наказ.
3.5. Керівник відділу інформаційних систем та технології відповідає за ознайомлення членів Команди з цією політикою, а також вживатиме заходів з підвищення обізнаності Команди Організації щодо знань захисту та безпеки в обробці та зберіганні персональних даних, конфіденційності та інфомаційної безпеки.
3.6. Президент Організації, Правління, керівники напрямів, координатори програм, проєктні менеджери, керівники функціональних відділів, керівники регіональних офісів Організації та Менеджер з персоналу зобов'язуються вживати ефективних заходів щодо збирання, обробки та зберігання персональних даних, конфіденційності та не можуть без письмового дозволу керівника відділу інформаційних систем та технологій та Президента Організації передавати персональні дані інших сторонам за їх запитом.

3.7. Встановлення програмного забезпечення, антивірусних програм, оновлення операційних систем на всіх мережевих пристроях у Організації виконує виключно системний адміністратор за погодження керівника відділу інформаційних систем та технологій.
3.8. Системний адміністратор не пізніше ніж 1 раз на квартал має проводити перевірку оновлення операційних систем, програмного забезпечення для забезпечення максимального рівня безпеки Організації, а також забезпечувати захист мережевого з'єднання шляхом використання зашифрованих протоколів, фаєрволів та інших технологій захисту.
3.9. Правління Організації забезпечує нагляд та робочий контроль обробки персональних даних Організації, конфіденційності та інформаційної безпеки.

IV. КОНФІДЕНЦІЙНІСТЬ, ЗБЕРЕЖЕННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ ОРГАНІЗАЦІЇ.

4.1. Членам Команди на початку своєї роботи у Організації створюється робоча пошта Організації в Google Workspace системним адміністратором.
4.2. Запит на створення робочої пошти для нового співробітника робить фахівець відділу по роботі з персоналом, системному адміністратору Організації.
4.3. Член Команди Організації отримує відповідні інструкції та доступ до робочої пошти у перший робочий день. Після отримання корпоративної пошти працівник матиме доступ до хмарних технологій Організації таких як гугл-диск Організації та інші, де використовується принцип найменшого можливого доступу (Least Privilege), де кожному користувачеві надаються тільки ті привілеї та рівень доступу, які необхідні для виконання його обов'язків.
4.4. Члени команди використовують адресу робочої електронної пошти лише для комунікації в рамках виконання своїх обов'язків, пов'язаних з діяльністю Організації.
4.5. Забороняється використання корпоративної пошти у власних цілях.
4.6. Для запобігання несанкціонованого доступу к Google Workspace використовується двофакторна авторизація (MFA). При необхідності передачі конфіденційної інформації електронною поштою, слід використовувати дворівневе шифрування для забезпечення безпеки передачі даних згідно налаштувань в електронної пошти.
4.7. Члени Команди з моменту отримання робочої електронної пошти Організації повинні дотримуватись вимог до конфіденційності інформації, розповсюдження якої виконується через цей канал. Вони не повинні розголошувати конфіденційну інформацію третім особам без належних дозволів керівника відділу інформаційних систем та Президента Організації.
4.8. Після припинення співпраці з членом Команди, обліковий запис блокується в день припинення співпраці з членом команди Організації на запит фахівця відділу по роботі з персоналом, системним адміністратором Організації та через два тижні архівується системним адміністратором.
4.9. Члени команди Організації при отриманні робочого комп'ютера (ноутбука, планшета тощо) мають звернутись до системного адміністратора для налаштування комп'ютера механізмами авторизації та аутентифікації для доступу до мережі Організації та встановлення захисту.
4.10. Для забезпечення конфіденційності інформації на комп'ютері проводиться шифрування носія за допомогою BitLocker. Резервний ключ зберігається у особистому акаунті Microsoft.
4.11. Регулярне резервне копіювання інформації проводиться для запобігання втраті даних. Резервні копії зберігаються в безпечному місці, віддаленому від основного місця

зберігання. Один раз на добу робиться бекап даних серверів 1С, IDP та Codejig, раз в квартал Google disc.
4.12. При публікації будь-якої інформації на публічних ресурсах, необхідно дбати про збереження конфіденційності персональних даних та конфіденційної інформації Організації. За це відповідає керівник відділу публічної інформації. Це стосується сторінок Організації в соціальних мережах (фейсбук, телеграм-каналів тощо) та корпоративного сайту.
4.13. Доступ до публічних ресурсів, де розміщується інформація Організації, обмежений і доступний лише відповідальним особам, які мають на це повноваження. Керівник відділу публічної інформації періодично перевіряє список користувачів-адмінів соціальних сторінок та інших спільних ресурсів (групи, канали тощо).
4.14. Будь-яка інформація, яка стала відома членам команди Організації, у зв'язку з виконанням обов'язків за договором із Організацією, і розголошення якої може нанести шкоду другій Стороні, є комерційною таємницею і не підлягає розголошенню третім особам або опублікуванню без попередньої згоди на це іншої сторони. За розголошення вказаної інформації винна сторона несе відповідальність, передбачену діючим законодавством України.
4.15. Конфіденційною вважається у тому числі інформація, яка складає дійсну або потенційну комерційну цінність для Організації та є невідомою третім особам, і по відношенню до якої Організація вживає заходи щодо охорони її конфіденційності, а також інша інформація, яка не є комерційною таємницею, але відносно якої Організацією було заявлено, що вона є конфіденційною.
4.16. Члени колективу зобов'язуються протягом строку дії договору із Організацією та протягом двох років після його припинення не розголошувати та не розкривати третім особам конфіденційну інформацію, надану їм Організацією, та не використовувати її з будь-якою іншою метою, окрім тієї, для якої така інформація була надана Організацією, без отримання попередньої письмової згоди Організації. Організація залишає за собою право у разі необхідності контролювати використання членами команди конфіденційної інформації та її збереження.
4.17. Члени колективу та Організація зобов'язуються дотримуватися конфіденційності переговорів, листування та інших дій, пов'язаних з договірними умовами, та не розголошувати таку інформацію третім особам без письмової згоди іншої сторони.

V. БАЗИ ПЕРСОНАЛЬНИХ ДАНИХ ВЛАСНИКОМ, ЯКИХ Є ОРГАНІЗАЦІЯ

4.1. Обробка персональних даних Організацією здійснюється для реалізації програм та проектів Організації, захисту бенефіціарів та членів Команди Організації та інших цілей визначеними законодавством України і вимогам Загального регламенту про захист персональних даних (GDPR)
4.2. Підставами виникнення права на використання персональних даних є:
● згода суб'єкта персональних даних на обробку його персональних даних письмово чи за допомогою електронних засобів (Додаток 1);
● дозвіл на обробку персональних даних, наданий Організації відповідно до законодавства України та вимогам Загального регламенту про захист персональних даних (GDPR) виключно для здійснення його повноважень.
4.3. Організація володіє та обробляє наступні бази персональних даних:
4.3.1. База даних бенефіціарів, яка містить основну інформацію про бенефіціарів Організації, включаючи ім'я, прізвище, контактні дані, інформацію про отримувану підтримку тощо.
4.3.2. Метою оброблення бази персональних даних бенефіціарів є виконання вимог законодавства, реалізації прав, наданих Організації законодавством та забезпечення

реалізації податкових відносин та відносин у сферах бухгалтерського обліку, аудиту, тощо.
4.3.3. База персональних даних членів команди Організації. В базі персональних даних членів команди Організації міститься інформація про Прізвище, Ім'я, по-батькові, дату та місце народження, домашній та мобільний телефон, електронну адресу, місце реєстрації, паспортні дані, реєстраційний номер облікової картки платника податків, освіту, сімейний стан, дітей, громадянство, наявність закордонного паспорту, наявність та категорію водійських прав, наявність судимості, дані про досвід роботи, та інші дані за потребою.
4.3.4. Метою оброблення бази персональних даних членів команди Організації є ведення кадрового діловодства, підготовка відповідно до вимог законодавства та внутрішніх стандартів та політик Організації, статистичної, адміністративної та іншої інформації з питань персоналу, а також внутрішніх документів Організації з питань реалізації визначених законодавством і колективним договором прав та обов'язків у сфері трудових правовідносин і соціального захисту тощо.
4.4. Володіючи базою персональних даних бенефіціарів та членів команди Організації, Організація зобов'язується використовувати ці дані тільки для визначених цілей, зазначених у статуті або інших правових документах Організації, і згідно з принципами законності, справедливості та прозорості.
4.5. Організація не буде передавати персональні дані бенефіціарів та членів команди Організації третім особам без належних правових підстав, таких як згода бенефіціарів або законні вимоги відповідних органів.
4.6. Передачі персональних даних третім особам Організація робить виключно за наказом Президента Організації та письмовою згодою Керівника відділу інформаційних систем та технології.
4.7. Підставою передачає персональних даних має бути уклада угода або письмово зафіксовані інші механізми, що гарантують адекватний рівень захисту цих даних та забезпечують дотримання вимог законодавства про захист персональних даних України та вимогам Загального регламенту про захист персональних даних (GDPR).

VI. ОБМЕЖЕНИЙ ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ

5.1. Організація забезпечує обмежений доступ до персональних даних бенефіціарів та членів команди Організації тільки співробітникам та іншим особам, які мають необхідний письмовий дозволений доступ до таких даних від Президентки Організації та керівника відділу інформаційних систем та технології.
5.2. Доступ до персональних даних надається лише в межах, необхідних для виконання визначених завдань та обов'язків в реалізації проєктів та програм Організації.
5.3. Керівник відділу інформаційних систем та технології розробляє та оновлює навчання та інструктаж щодо використання та обробки персональних даних
5.4. Організація забезпечує регулярне навчання та інструктаж свого персоналу щодо використання та обробки персональних даних відповідно до вимог законодавства та політик Організації не рідше ніж 1 раз на півроку. Відповідальний за постійне навчання та підвищення кваліфікації членів команди Організації є керівник відділу інформаційних систем та технології.
5.5. Персонал Організації, який має доступ до персональних даних бенефіціарів та членів команди Організації, зобов'язується дотримуватися конфіденційності та виконувати всі необхідні заходи безпеки для захисту цих даних згідно цієї Політики українського законодавства та Загального регламенту про захист персональних даних (GDPR).
5.6. Права суб'єктів персональних даних:

5.6.1. Суб'єкти персональних даних мають право на захист своїх персональних даних та використання їх відповідно до законодавства та цього положення.

5.6.2. Суб'єкти персональних даних мають наступні права:
а) Право на інформацію: Суб'єкти персональних даних мають право бути інформованими про те, що їхні персональні дані збираються та обробляються, цілі обробки, категорії отримувачів даних та правову підставу для обробки згідно Додатку 1.
б) Право на доступ: Суб'єкти персональних даних мають право отримувати доступ до своїх персональних даних, які зберігаються в базі персональних даних Організації, і отримувати копії цих даних подавши відповідний письмовий запит на керівника відділу інформаційних систем та технології.
в) Право на виправлення: Суб'єкти персональних даних мають право вимагати виправлення неправдивих або недостовірних персональних даних, які стосуються їх.
г) Право на вилучення: Суб'єкти персональних даних мають право вимагати видалення своїх персональних даних з бази персональних даних Організації у разі, коли ці дані більше не потрібні для визначених цілей або якщо обробка їх незаконна.
д) Право на обмеження обробки: Суб'єкти персональних даних мають право обмежити обробку своїх персональних даних у певних ситуаціях, зокрема, якщо обробка є незаконною або суб'єкт персональних даних заперечує проти обробки.
е) Право на перенесення даних: Суб'єкти персональних даних мають право отримати свої персональні дані, які вони надали Організації, у структурованому, звичайно використовуваному та машинночитаному форматі, а також передати ці дані, які вони надали Організації, у структурованому, звичайно використовуваному та машинночитаному форматі, а також передати ці дані іншому володарю персональних даних без перешкоди з боку Організації, якщо обробка ґрунтується на згоді або укладеному договорі та здійснюється автоматизованим способом.
ж) Право на відкликання згоди: У разі, коли обробка персональних даних здійснюється на підставі згоди суб'єкта даних, суб'єкт має право в будь-який час відкликати свою згоду. Відкликання згоди не впливає на законність обробки, здійсненої до відкликання згоди.
з) Право на подання скарги: Суб'єкти персональних даних мають право подавати скарги до відповідних контролюючих органів, якщо вони вважають, що їхні права в сфері захисту персональних даних порушені.
і) Інші права: Суб'єкти персональних даних також мають інші права, передбачені законодавством про захист персональних даних.
5.6. Застосування прав суб'єктів персональних даних здійснюється шляхом звернення до Організації згідно Статті 16 Закону України "Про захист персональних даних". Організація зобов'язаний забезпечити можливість здійснення цих прав та відповідно реагувати на запити суб'єктів персональних даних у межах вимог законодавства.

VII. ПОРЯДОК ОБРОБЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

6.1. Оброблення персональних даних здійснюється відповідно до вимог законодавства, принципів конфіденційності та безпеки персональних даних, а також вимог Загального регламенту про захист персональних даних (GDPR).
6.2. Персональні дані збираються та обробляються згідно дозволу встановленої форми (Додаток 1).

6.3. Оброблення персональних даних може здійснюватися з використанням автоматизованих засобів, які використовує Організація (CRM-системи тощо), а також без автоматизованих засобів (зберігання письмових дозволів в офісі тощо).
6.4. Організація забезпечує виконання належних заходів для захисту персональних даних від несанкціонованого доступу, випадкового втрати або пошкодження, знищення, зміни, поширення або незаконної обробки постійно оновлюючи безпеку автоматизованих засобів зберігання персональних даних та безпечне і захищене місце в офісі, архіві Організації для не автоматизованих засобів, засобів зберігання персональних даних.
6.5. Здійснення обробки персональних даних може здійснюватися Організацією або за його дорученням третіми особами на підставі укладених угод або на підставі законних підстав, визначених законодавством.
6.6. Організація забезпечує зберігання персональних даних (автоматизованих так і не автоматизованих) протягом періоду, необхідного для досягнення цілей обробки згідно умов договору реалізації проєкту, якщо інше не передбачено законодавством або угодою з суб'єктом персональних даних.
6.7. Припинення оброблення персональних даних може здійснюватися за ініціативою суб'єкта персональних даних, за письмовим запитом контролюючих органів або у разі виконання законних вимог, визначених законодавством.
6.8. Передача персональних даних третім особам може здійснюватися лише у випадках, передбачених законодавством, договором реалізації проєкту та відповідно до вимог забезпечення конфіденційності та безпеки персональних даних.
6.9. Організація зобов'язана здійснювати реєстрацію процесів оброблення персональних даних, зокрема ведення реєстру обробки персональних даних та інших необхідних документів, відповідно до вимог законодавства.
6.10. У разі порушення безпеки персональних даних, що може призвести до несанкціонованого доступу, втрати, зміни або пошкодження таких даних, Організація зобов'язаний повідомити відповідний контролюючий орган та суб'єктів персональних даних відповідно до вимог законодавства.
6.11. Організація забезпечує належні умови для здійснення прав суб'єктів персональних даних, зокрема прав на доступ до персональних даних, виправлення неправдивих або недостовірних даних, вилучення даних тощо.

Додаток 1

ЗГОДА на обробку персональних даних (може бути інтегрована в інші документи Організації, де бенефіціар ставить свій підпис та поінформований про збір даних)

Підписуючи цей документ, Я _____ надаю свою згоду на:

- збір, реєстрацію, зберігання, використання та інші форми обробки моїх персональних даних, у тому числі з використанням інформаційних систем,
- моніторинг, а також на проведення фотофіксації будь-яких необхідних особистих документів, що надані мною у паперовому вигляді або у форматі фотокопії.

Згода надається у повному обсязі, без додаткового письмового повідомлення для оформлення, надання та проведення моніторингу якості отриманої допомоги та інших цілей, пов'язаних із отриманою допомогою.

Я також надаю згоду на передання та обробку усіх без винятку персональних даних третіми особами для проведення перевірки та оцінки якості отриманої допомоги.

Своїм підписом я підтверджую, що мене повідомлено про мої права як суб'єкта персональних даних, які визначені в ст. 8 Закону України «Про захист персональних даних», а також про мету збору цих даних та осіб, яким ці дані передаються.

Дата:_____ Підпис:_____