

ЗАТВЕРДЖЕНО

Протокол Загальних зборів

ГО «Центр сталих ініціатив»

№ 4 від «05» лютого 2024р.



Положення про порядок обробки та захисту персональних даних співробітників, членів організації та учасників проєктів

Розділ 1. Загальні вимоги та мета

- 1.1. Цим Положенням про обробку та захист персональних даних співробітників, членів організації та учасників проєктів (далі - Положення) регулюються відносини, пов'язані із захистом персональних даних під час їх обробки в рамках діяльності Громадської організації «Центр сталих ініціатив» (далі – Організація).
- 1.2. Положення дає визначення основним поняттям, що стосуються персональних даних (далі - ПД); містить мету обробки ПД; процедуру обробки ПД; права суб'єктів ПД; порядок захисту ПД; інші вимоги законодавства України із захисту ПД.
- 1.3. Вимоги цього Положення стосуються як співробітників так і членів організації та учасників проєктів Організації та представників органів влади, що здійснюють перевірку діяльності Організації (в т. ч. її філій та підрозділів).
- 1.4. Державна реєстрація баз персональних даних (далі - БПД) здійснюється відповідно до статті 9 Закону України «Про захист персональних даних».

Розділ 2. Визначення термінів

- 2.1. У цьому Положенні нижченаведені терміни вживаються в такому значенні:

база персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

відповідальна особа – визначена особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці, відповідно до законодавства України про захист ПД;

володілець бази персональних даних - фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

Державний реєстр баз персональних даних - єдина державна інформаційна система збору, накопичення та обробки відомостей про зареєстровані бази персональних даних;

загальнодоступні джерела персональних даних – довідники, адресні книги, реєстри, списки, каталоги, інші систематизовані збірники відкритої інформації, які містять персональні дані, розміщені та опубліковані з відома суб'єкта персональних даних. Не вважаються загальнодоступними джерелами персональних даних соціальні мережі та інтернет-ресурси, в яких суб'єкт персональних даних залишають свої персональні дані (окрім випадків, коли суб'єктом персональних даних прямо зазначено, що персональні дані розміщені з метою їх вільного поширення та використання);

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;

знеособлення персональних даних - вилучення відомостей, які дають змогу ідентифікувати особу;

обробка персональних даних - будь-яка дія або сукупність дій, здійснених повністю або частково в інформаційній (автоматизованій) системі та/або в картотеках персональних даних, які пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням відомостей про фізичну особу;

персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

розпорядник бази персональних даних - фізична чи юридична особа, якій володільцем бази персональних даних або законом надано право обробляти ці дані;

суб'єкт персональних даних - фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних;

третя особа - будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону;

особливі категорії даних - персональні дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя.

Розділ 3. Бази персональних даних, володільцем та розпорядником яких є Організація

3.1. Організація є володільцем бази персональних даних:

- Працівники організації;
- Члени організації;
- Учасники проєктів організації

3.2. База/бази Організації знаходяться за адресою: с. Здовбиця Рівненська обл. Рівненський р-н. вул. Четверта, будинок 105

Розділ 4. Мета обробки персональних даних

4.1. Метою обробки ПД є забезпечення реалізації відносин між Організацією та:

- Співробітниками: трудових, адміністративно – правових, податкових та відносин у сфері бухгалтерського обліку; у сфері управління людськими ресурсами, зокрема кадровим потенціалом відповідно до Кодексу законів про працю України, Податкового кодексу України, Закону України «Про бухгалтерський облік та фінансову звітність в Україні», Закону України «Про зайнятість населення»).
- Членами організації: ведення обліку членів організації, управління людськими ресурсами;
- Учасниками проєктів: цивільно-правових відносин; надання комплексної допомоги бенефіціарам організації;

4.2. Категорія ПД, які обробляються:

- Співробітники: прізвище, ім'я, по батькові, паспортні дані; реєстраційний номер облікової картки платника податків; номер телефону, особисті відомості (вік, стать, родинний стан, склад сім'ї); місце проживання фактичне та за державною реєстрацією тощо).
- Членів організації: прізвище, ім'я, по батькові, паспортні дані; реєстраційний номер облікової картки платника податків; статус родин, у складі якого підрозділу служив або служить член вашої родини; місце проживання; номер телефону.
- Учасники проєктів: прізвище, ім'я, по батькові, номер телефону; соціальний статус родин, місце проживання;

Розділ 5. Порядок обробки персональних даних

5.1. Згода суб'єкта персональних даних у випадках оформлення трудових відносин, оформлення цивільно-правової угоди, має бути документальним добровільним волевиявленням фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки.

5.2. Згода суб'єкта персональних даних має бути надана шляхом підписання суб'єктом персональних даних затвердженого наказом Голови правління Організації тексту згоди-повідомлення.

- 5.3.Згода-повідомлення складається у двох примірниках, один з яких після підписання суб'єктом персональних даних залишається у нього, а інший зберігається в Організації протягом всього часу обробки персональних даних вказаного суб'єкта персональних даних.
- 5.4.Згода суб'єкта персональних даних у випадках прийняття до складу членів (асоційованих членів) Організації або включення до складу учасників проектів може бути надана в письмовій або усній формі.
- 5.5.Повідомлення суб'єкта персональних даних про включення його персональних даних до бази персональних даних, права, визначені Законом України «Про захист персональних даних», мету збору даних та осіб, яким передаються його персональні дані здійснюється під час *оформлення трудових відносин відповідно до законодавства про працю, оформлення цивільно-правової угоди, заповнення анкети на вступ до членів (асоційованих членів) Організації або під час включення до складу учасників проектів.*
- 5.6.Обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя (особливі категорії даних) забороняється.

Розділ 6. Умови розкриття інформації про персональні дані третім особам

- 6.1.Порядок доступу до ПД третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних на обробку цих даних, або відповідно до вимог закону.
- 6.2.Доступ до ПД третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону України «Про захист персональних даних» або неспроможна їх забезпечити.
- 6.3.Суб'єкт відносин, пов'язаних з ПД, подає запит щодо доступу (далі - запит) до персональних даних володільцю бази персональних даних.
- 6.4.У запиті зазначається:
- прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи - заявника);
 - найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи - заявника);
 - прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
 - відомості про БПД, стосовно якої подається запит, чи відомості про володільця чи розпорядника цієї бази;
 - перелік ПД, що запитують;
 - мета запиту.
- 6.5.Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження. Протягом цього строку володілець БПД доводить до відома особи, яка подає запит, що запит буде задоволене або відповідні ПД не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті. Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.
- 6.6.Усіх співробітників, бенефіціарів та учасників проектів Організації зобов'язані дотримуватися вимог конфіденційності щодо ПД та інформації щодо рахунків у цінних паперах та обігу цінних паперів.
- 6.7.Відстрочення доступу до ПД третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати 45 (сорока п'яти) календарних днів.
- 6.8.Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

6.9. У повідомленні про відстрочення зазначаються:

- прізвище, ім'я та по батькові посадової особи;
- дата відправлення повідомлення;
- причини відстрочення;
- строк, протягом якого буде задоволено запит.

6.10. Відмова у доступі до ПД допускається, якщо доступ до них заборонено згідно із законом.

6.11. У повідомленні про відмову зазначаються:

- прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;
- дата відправлення повідомлення;
- причина відмови.

Розділ 7. Захист персональних даних

7.1. Організацію обладнано системними і програмно-технічними засобами та засобами зв'язку, які запобігають втратам, крадіжкам, несанкціонованому знищенню, викривленню, підробленню, копіюванню інформації і відповідають вимогам міжнародних та національних стандартів.

7.2. Відповідальна особа організовує роботу, пов'язану із захистом ПД при їх обробці, відповідно до закону. Відповідальна особа визначається наказом Голови правління Організації. Обов'язки відповідальної особи щодо організації роботи, пов'язаної із захистом ПД при їх обробці зазначаються у посадовій інструкції.

7.3. Відповідальна особа зобов'язана:

- знати законодавство України в сфері захисту ПД;
- розробити процедури доступу до ПД співробітників відповідно до їхніх професійних чи службових або трудових обов'язків; бенефіціарів та учасників проєктів.
- забезпечити виконання співробітниками, бенефіціарами та учасниками проєктів вимог законодавства України в сфері захисту ПД та внутрішніх документів, що регулюють діяльність Організації щодо обробки і захисту ПД у БПД;
- розробити порядок (процедуру) внутрішнього контролю за дотриманням вимог законодавства України в сфері захисту ПД та внутрішніх документів, що регулюють діяльність Організації щодо обробки і захисту персональних даних у БПД, який, зокрема, повинен містити норми щодо періодичності здійснення такого контролю;
- повідомляти керівництво Організації про факти порушень співробітниками, бенефіціарами та учасниками проєктів вимог законодавства України в сфері захисту персональних даних та внутрішніх документів, що регулюють діяльність Організації щодо обробки і захисту ПД у БПД у термін не пізніше одного робочого дня з моменту виявлення таких порушень;
- забезпечити зберігання документів, що підтверджують надання суб'єктом ПД згоди на обробку своїх ПД та повідомлення вказаного суб'єкта про його права.

7.4. З метою виконання своїх обов'язків відповідальна особа має право:

- отримувати від співробітників, бенефіціарів та учасників проєктів Організації необхідні документи, у тому числі накази й інші розпорядчі документи, видані Головою правління Організації, пов'язані із обробкою персональних даних;
- робити копії з отриманих документів, у тому числі копії файлів, будь-яких записів, що зберігаються в локальних обчислювальних мережах і автономних комп'ютерних системах;
- доступу до всіх приміщень, документів Організації;
- брати участь в обговоренні виконуваних ним обов'язків організації роботи, пов'язаної із захистом ПД при їх обробці;
- вносити на розгляд Голові правління пропозиції щодо покращення діяльності Організації та вдосконалення методів роботи, подавати зауваження щодо діяльності Організації та варіанти усунення виявлених недоліків у процесі обробки ПД;
- здійснювати взаємодію з іншими співробітниками, бенефіціарами та учасниками проєктів Організації при виконанні своїх обов'язків з організації роботи, пов'язаної із захистом ПД при їх обробці;

- 7.6. Працівники, що мають доступ до ПД, у тому числі, здійснюють їх обробку зобов'язані не допускати розголошення у будь-який спосіб ПД, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з ПД, крім випадків, установлених законом.
- 7.7. Особи, що мають доступ до ПД, у тому числі, здійснюють їх обробку у разі порушення ними вимог Закону України «Про захист персональних даних» несуть відповідальність згідно законодавства України.
- 7.8. Персональні дані не повинні зберігатися довше, ніж це необхідно для мети, для якої такі дані зберігаються, але у будь-якому разі не довше строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних та/або про працю.
- 7.9. Строк зберігання ПД, що містяться у системі обліку, документах, що подаються до Організації, засвідчених в установленому законодавством порядку, складає 10 років

Розділ 8. Права суб'єкта персональних даних

8.1. Суб'єкт персональних даних має право:

- знати про місцезнаходження БПД, яка містить його персональні дані, її призначення та найменування, місцезнаходження та / або місце проживання (перебування) володільця чи розпорядника цієї бази або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
- отримувати інформацію про умови надання доступу до ПД, зокрема інформацію про третіх осіб, яким передаються його ПД, що містяться у відповідній БПД;
- на доступ до своїх ПД, що містяться у відповідній БПД;
- отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його ПД у відповідній БПД, а також отримувати зміст його ПД, які зберігаються;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх ПД органами державної влади, органами місцевого самоврядування при здійсненні їхніх повноважень, передбачених законом;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх ПД будь-яким володільцем та розпорядником цієї бази, якщо ці дані обробляються незаконно чи є недостовірними;
- на захист своїх ПД від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- звертатися з питань захисту своїх прав щодо ПД до органів державної влади, органів місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних;

Розділ 9. Порядок роботи з запитами суб'єкта персональних даних

- 9.1. Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з ПД, без зазначення мети запиту, крім випадків, установлених законом.
- 9.2. Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно.
- 9.3. Суб'єкт персональних даних подає запит щодо доступу (далі - запит) до персональних даних володільцю бази персональних даних.
- У запиті зазначаються:
- прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує особу суб'єкта персональних даних;
 - інші відомості, що дають змогу ідентифікувати особу суб'єкта персональних даних;
 - відомості про БПД, стосовно якої подається запит, чи відомості про володільця чи розпорядника цієї бази;
 - перелік ПД, що запитуються.
- 9.4. Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження. Протягом цього строку володільць БПД доводить до відома суб'єкта персональних даних, що запит буде задоволене або відповідні ПД не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті. Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

Голова Правління



О.О. Чижевський

ПРОЦЕДУРА ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ співробітників, членів організації та учасників проєктів

Громадської організації «Центр сталих ініціатив» (далі — Організація) приділяє значну увагу захисту персональних даних співробітників, членів організації та учасників проєктів. Процедура доступу до персональних даних (далі — Процедура) розроблено у відповідності до вимог Закону України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI (далі — Закон 2297) та Генерального регламенту про захист даних ЄС 2016/679 (EU General Data Protection Regulation, далі — GDPR). Визначення термінів у цій Процедурі вживається у значенні, передбаченому Законом 2297, додаткові визначення наведені у 1 розділі.

1. ОСНОВНІ ВИЗНАЧЕННЯ

1.1. Персональні дані (ПД) - будь-які дані, що дозволяють ідентифікувати співробітників, членів організації та учасників проєктів:

- Співробітники: прізвище, ім'я, по батькові, паспортні дані; реєстраційний номер облікової картки платника податків; номер телефону, особисті відомості (вік, стать, родинний стан, склад сім'ї); місце проживання фактичне та за державною реєстрацією; тощо).
- Членів організації: прізвище, ім'я, по батькові, паспортні дані; реєстраційний номер облікової картки платника податків; статус родин, у складі якого підрозділу служив або служить член вашої родини; місце проживання; номер телефону.
- Учасники проєктів: прізвище, ім'я, по батькові, номер телефону; соціальний статус родин, місце проживання;

1.2. Принципами обробки ПД є:

- принцип законності, персональні дані повинні оброблятися лише на законних підставах;
- принцип сумісності, персональні дані повинні бути отримані із конкретними законними цілями та оброблятися відповідно до них;
- принцип адекватності і не надлишковості, персональні дані повинні бути адекватними, не надлишковими, відповідати цілям обробки;
- принцип точності, персональні дані повинні бути точними та акуратними;
- принцип строкості зберігання, персональні дані не повинні зберігатися довше, ніж це визначено відповідними нормативно - правовими актами;
- принцип дотримання прав фізичної особи, персональні дані повинні оброблятися з дотриманням прав суб'єкта персональних даних, включаючи право на доступ до них.

1.4. Відповідальна особа - співробітник Організації залучений до процесу обробки ПД та/або супроводження питань, пов'язаних з цією обробкою.

1.5. Обробка ПД - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем, що здійснюється у суворій відповідності з визначеними процедурами, з обов'язковим дотриманням:

- певних умов їх зберігання;
- обмеження режиму доступу до них;
- повноти та цілісності персональних даних.

1.6. Процедура обробки ПД — деталізований опис дій, що виконують Відповідальні особи

Організації під час Обробки ПД, в якому зазначаються:

- мета обробки;
- перелік Відповідальних осіб;
- порядок обміну даними;
- заходи захисту;
- терміни зберігання та порядок знищення;
- порядок контролю відповідності.

2. ВИДИ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Внутрішні персональні дані (ВПД) -співробітників, членів організації та учасників проєктів Організації обробляються у базах ВПД з метою ведення кадрового діловодства, підготовки статистичної, управлінської та іншої звітної інформації з питань персоналу.

Паперові копії первинних документів зберігаються в особистих справах співробітників.

ВПД зберігаються в Компанії протягом дії трудових відносин між співробітником та Компанією, а також 2 (два) роки після їх припинення. Наприкінці визначеного терміну зазначені ВПД мають передаватись в архів для постійного зберігання протягом 75 років.

2.2. Зовнішні ПД (ЗПД)— персональні дані, отримані від Замовників послуг Організації, обробка яких здійснюється на підставі та в межах виконання укладених угод/договорів про надання відповідних послуг. Замовник послуг забезпечує дотримання вимог законодавства щодо захисту ПД перед передачею їх Організації, а Організація в свою чергу — під час обробки.

ЗПД оброблюються згідно з Процедурою обробки ПД, яка є невід'ємною частиною угоди про надання відповідних послуг.

ЗПД зберігаються у терміни визначені у Процедурі обробки ПД але більше термінів дії відповідних угод з Замовником послуг Організації.

Голова Правління



О.О. Чижевський



ЗАТВЕРДЖЕНО

Протокол Загальних зборів
ГГО «Центр сталих ініціатив»
№ 4 від «05» лютого 2024р.

**Порядок (процедуру) внутрішнього контролю
за дотриманням вимог законодавства України в сфері захисту ПД та внутрішніх
документів, що регулюють діяльність Організації щодо обробки і захисту персональних
даних у БПД, який, зокрема, повинен містити норми щодо періодичності здійснення
такого контролю**

1. Обробка персональних даних в програмно-технічних комплексах Організації здійснюється із застосуванням засобів мережевого захисту від несанкціонованого доступу.
2. Доступ в програмно-технічні комплекси Організації здійснюється у суворій відповідності з діючими процедурами щодо керування доступом.
3. Відповідальні особи Організації допускаються до обробки персональних даних лише після їх авторизації. Доступ осіб, які не пройшли процедуру ідентифікації та/або автентифікації, блокується. В інформаційній (автоматизованій) системі, де обробляються персональні дані, здійснюється реєстрація, зокрема:
 - результатів ідентифікації та/або автентифікації Відповідальних осіб;
 - дій з обробки персональних даних;
 - результатів перевірки цілісності засобів захисту персональних даних.
4. Відповідальний Організації проводить аналіз реєстраційних даних. Реєстраційні дані захищаються від модифікації та знищення.
5. Організація забезпечує антивірусний захист в інформаційній (автоматизованій) системі.
6. Ступінь доступу до обробки ПД (внесення змін, формування звітів та аналітичної інформації, перегляд або інше за потреби) визначається посадою Відповідальної особи.
7. Кожний співробітник Організації складає та власноручно підписує зобов'язання про збереження інформації з обмеженим доступом.
8. Оформлені належним чином зобов'язання щодо збереження інформації з обмеженим доступом зберігаються в особистих справах Відповідальних осіб.
9. Відповідальна особа здійснює постійний контроль за дотриманням співробітниками Процедури обробки персональних даних, а також за законністю обробки персональних даних, захистом персональних даних при їх обробці.
10. Про всі виявлені факти несанкціонованого поширення ПД Організація повідомляє суб'єктів ПД та Голову правління у термін, що не перевищує 72 (сімдесят дві) години.
11. Персональні дані, зібрані з порушенням вимог Закону 2297 підлягають видаленню або знищенню в базах персональних даних у встановленому законодавством порядку.

Голова Правління



О.О. Чижевський