*ЗАТВЕРДЖЕНО*

 *Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПОСАДОВИХ ОСІБ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика захисту персональних даних посадових осіб виконавчого комітету Криворізької міської ради (надалі – Політика захисту РІІ посадових осіб) є документом, що встановлює основні принципи, за якими обробляються персональні дані (надалі – PII) посадових осіб виконкому міської ради в межах області дії СУІБ.

1.2. Політика захисту РІІ посадових осіб поширюється на обробку персональних даних посадових осіб будь-яким відділом, управлінням, іншим виконавчим органом міської ради або особою в усіх країнах і регіонах.

1.3. Політика захисту РІІ посадових осіб регулює управління РІІ, що стосуються посадових осіб і містить правила та процедури, що застосовуються до всіх відділів, управлінь, інших виконавчих органів міської ради і окремих осіб виконкому міської ради, що спрямовані на забезпечення захисту РІІ належним чином під час їх обробки в усіх країнах та регіонах.

1.4. Політика захисту РІІ посадових осіб розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки», ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови» (надалі – ДСТУ ISO/IEC 27701), Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄC (Загального регламенту про захист даних) (надалі – GDPR), політик, процедур і технічних заходів: D4.1-СУІБ «Політика інформаційної безпеки», D4.2-СУІБ «Політика захисту персональних даних».

#### *2. Терміни, визначення та скорочення*

2.1. Заявник – це суб’єкт PII, який за допомогою сервісів підсистеми «WebПортал» подає запит (електронне звернення) до повноважних органів виконкому міської ради з метою отримання адміністративних, інших публічних послуг, у тому числі з дозвільних питань, видачі документів дозвільного характеру, голосування за електронні петиції та подання скарг

2.2. Суб’єкт PII – фізична особа, персональні дані якої обробляються в межах її згоди, та якої стосується ідентифікаційна інформація в межах визначеної мети обробки персональних даних, що встановлює склад цих персональних даних та процедури їх обробки, якщо інше не визначено законом.\*

2.3. Інформаційно комунікаційна система (надалі – ІКС) – інформаційно комунікаційна система виконкому міської ради, компоненти якої виконують функції для забезпечення інформаційної діяльності.

2.4. Актив – активом є все, що має цінність для виконкому міської ради й потребує захисту [інформаційний актив, апаратне забезпечення, програмне забезпечення, інфраструктура, мережа розповсюдження інформації, посадові особи, сервіси, технології та ресурси (фінансові, технічні, адміністративні, організаційні) для забезпечення інформаційної діяльності, нематеріальні активи (імідж, довіра, сертифікати відповідності, ліцензії тощо)].

2.5. Власник активу – відповідальна посадова особа або відділи, управління інші виконавчі органи міської ради, у розпорядженні та/або користуванні, та/або розробці, та/або підтримці яких перебуває актив, що може впливати на інформаційну безпеку (надалі − ІБ) та кібербезпеку.\*\*

2.6. Інформаційний актив (надалі − ІА) – це сукупність відомостей (інформації у фізичній або електронній формі), що представляє цінність для виконкому міської ради, а також будь-яка інформаційна система обробки, обміну чи фізичного місця зберігання інформації.

2.7. Єдина інформаційна система міста Кривий Ріг (надалі – ЄІС) – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб’єктів, інформаційну підтримку та супроводження їх діяльності й становить сукупність взаємопов’язаних функціональних підсистем, програмно-інформаційних комплексів, комп’ютерних програм, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку й захист інформації, внутрішню та зовнішню інформаційну взаємодію.

2.8. Chief Executive Officer ( надалі – CEO) – власник і розпорядник СУІБ.

2.9. Chief Security Officer (надалі – CSO) – відповідальний за ІБ, який відповідає за керування процесом організації безпеки у виконкомі міської ради, включаючи фізичну безпеку, ІБ, кібербезпеку та інші види безпеки в межах сфери застосування СУІБ.

2.10. Chief Information Security Officer (надалі − CISO) − відповідальний за розробку та впровадження політик і процедур ІБ, управління ризиками, забезпечення кібербезпеки, реагування на інциденти, підвищення обізнаності працівників та контроль за дотриманням законодавства у сфері захисту інформаційних систем і даних.

2.11. Data Protection Officer (надалі − DPO) − відповідальний за захист персональних даних у виконкомі міської ради, відповідає за організацію роботи, пов’язаної із захистом персональних даних у процесі інформаційної діяльності виконкому в межах області дії СУІБ.

2.12. PII – персональні дані.

2.13. Зацікавлені сторони – це фізичні або юридичні особи, які можуть впливати або на яких може вплинути інформаційна діяльність виконкому міської ради. Зацікавленими сторонами вважаються:

2.13.1 органи державної влади України та за кордоном, у тому числі регуляторний орган, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

2.13.2 органи місцевого самоврядування;

2.13.3 суспільство, громадські організації, міжнародні організації, міжнародні фінансові інституції, медіа, ділові, експертні та галузеві об’єднання, компанії енергетичного чи суміжних секторів економіки, дипломатичні кола тощо;

2.13.4 банки, інвестори, рейтингові агентства;

2.13.5 суб’єкти PII, процесори PII, підпроцесори PII, співконтролери PII, акціонери/власники бізнесу;

2.13.6 інші учасники інформаційного обміну, постачальники послуг/сервісів (у тому числі хмарних), провайдери та партнери, постачальники баз даних.

2.14. Третя сторона – це фізична або юридична особа, що може вплинути на ІБ та безперервність робочих процесів. У контексті СУІБ третя сторона може не мати створений та зареєстрований акаунт у межах області дії СУІБ. Це можуть бути члени сімей посадових осіб, суб’єктів PII, процесорів PII, підпроцесорів PII, співконтролерів PII, екстрені служби, консультанти (включаючи юристів, податкових консультантів, консультантів з питань праці тощо), які можуть мати вплив на ІБ в межах області дії СУІБ.

2.15. Контролер PII – фізична або юридична особа, державний орган, агентство або будь–який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки PII.

2.16. Chief Human Resources Officer (надалі – CHRO) – відповідальна особа за кадрову політику.

2.17. Chief Legal Officer (надалі – CLO) – керівник юридичного підрозділу.

#### *3. Загальні принципи обробки персональних даних*

3.1. PII посадових осіб обробляються законно, справедливо та прозоро по відношенню до особи.

3.2. PII посадових осіб збираються для конкретних, явних і законних цілей і не обробляються в подальшому способом, несумісним з цими цілями.

3.3. PII посадових осіб мають бути адекватними, відповідними та обмеженими тим, що необхідно для цілей, для яких вони обробляються. CISO з DPO застосовують анонімізацію або псевдонімізацію PII посадових осіб, де це можливо для зменшення ризиків відповідних осіб. DPO здійснює контроль, щоб контролер РІІ забезпечив дотримання Політики PII щодо анонімізації та псевдонімізації.

3.4. PII посадової особи мають бути точними та, у разі необхідності, підтримуватися в актуальному стані, вживати відповідні заходи для забезпечення своєчасного видалення або виправлення PII посадової особи, які є неточними з огляду на цілі, для яких вони обробляються.

3.5. Відповідно до Політики захисту PII посадових осіб PII зберігаються не довше, ніж це необхідно для цілей, для яких вони обробляються.

3.6. Беручи до уваги стан технологій і доступні заходи безпеки, вартість реалізації, а також ймовірність і серйозність ризиків конфіденційності, вживаються відповідні технічні і організаційні заходт для забезпечення відповідної безпеки РІІ, включаючи захист від випадкового або незаконного знищення, втрати, зміни, несанкціонованого доступу або розголошення.

3.7. Виконком міської ради, як контролер PII посадових осіб, несе відповідальність та дотримується принципів, викладених у розділі 4 Політики захисту PII посадових осіб.

#### *4. Законні цілі обробки персональних даних*

Відділи, управління, інші виконавчі органи міської ради, або окремі особи, можуть обробляти PII посадової особи у законних цілях, що включають, але не обмежуються:

4.1. Управління кадрами: мета включає заходи з управління кадровою політикою, що здійснюються під час найму або виконання трудового договору, такі як: співбесіди, прийом на посаду, припинення роботи, відвідування, управління продуктивністю, компенсації та пільги, навчання, послуги посадовим особам, здоров’я та безпека праці, а також інша діяльність з метою управління кадрами або захисту життєво важливих інтересів посадової особи.

4.2. Опрацювання PII вважається законним у разі його необхідності для укладення трудового договору або наміру щодо вкладення трудового договору.

4.3. Інші операції: мета включає таку інформаційну діяльність, як управління відрядженнями та витратами, активами виконкому міської ради, надання ІТ-послуг, ІБ, проведення внутрішніх аудитів та службових розслідувань, виконання зобов’язань, юридичні консультації, підготовка до судових процесів тощо.

4.4. Дотримання закону: обробка РІІ посадової особи з метою виконання юридичного зобов’язання, наприклад: розкриття PII особи податковому органу з метою дотримання чинного законодавства у сфері податкових відносин.

#### *5. Вимоги до обробки персональних даних*

Будь-яка обробка PII посадової особи відділами, управліннями, іншими виконавчими органами міської ради та окремими особами виконкому міської ради має здійснюватися із законною метою та відповідати таким вимогам:

5.1. Повідомлення посадових осіб: з метою прозорості обробки персональних даних, коли відділ, управління, іншиий виконавчий орган міської ради або фізична особа збирає PII посадової особи, така особа має бути повідомленою про типи даних, які збираються, мету та види обробки, права посадової особи й заходи безпеки, ужиті для захисту PII. Повідомлення може приймати форму публікації або оновлення заяв про захист PII посадових осіб, наприклад: включення умов щодо захисту PII у трудові договори, унесення заяви про PII до відповідних ІТ-систем, процесів та управління ІТ.

5.2. Вибір і згода посадової особи: виконком міської ради може обробляти PII посадової особи із законною метою як роботодавець і, як правило, може робити це без отримання згоди особи, щоб підвищити ефективність внутрішньої роботи. Діяльність з кадрової політики, така як: співбесіди, прийом на посаду, звільнення, відвідування, компенсації та пільги, послуги посадовим особам, охорона здоров’я та безпека праці, можуть включати обробку PII.

5.3. Збір даних: виконком міської ради та окремі особи збирають PII посадових осіб для законних цілей і дотримуються принципу мінімізації даних. Якщо PII кандидата на посаду або посадової особи збираються від третьої сторони (наприклад, кадрових агентств або агентств з перевірки даних), виконком міської ради докладає зусиль, щоб третя сторона отримала PII законними засобами.

5.4. Жоден відділ, управління, інший виконавчий орган міської ради або окрема особа виконкому міської ради не має права збирати PII кандидатів на роботу чи посадової особи в спосіб, який суперечить закону чи діловій етиці.

5.5. Виконком міської ради вживає заходи щодо інформування посадових осіб про дотримання конфіденційності, нерозголошення службової інформації під час виконання посадових обов’язків.

5.6. Використання, зберігання та утилізація: виконком міської ради та окремі особи використовують, зберігають та розпоряджаються персональними даними посадових осіб у спосіб, який узгоджується з повідомленням особи, а також забезпечує точність, цілісність і актуальність. Уживаються належні заходи безпеки, щоб захистити PII посадової особи від випадкового або незаконного знищення, втрати, зміни, несанкціонованого доступу або розголошення відповідно до Політики інформаційної безпеки та інших документів, що передбачають безпеку PII.

5.7. Виконком міської ради та окремі особи не повинні незаконно знищувати або змінювати персональні дані посадових осіб. Вони не повинні отримувати доступ, продавати або надавати PII будь-якій третій стороні незаконно або без дозволу.

5.8. У ході робочих операцій DPO вирішує, чи будуть персональні дані посадової особи оброблятися такими способами, щоб мінімізувати ризик захисту даних: PII можуть бути анонімними з метою незворотної деідентифікації; дані можуть бути зведені в статистичні результати чи результати опитування (принципи обробки персональних даних не застосовуються до анонімних даних і сукупних даних, оскільки вони не є РІІ.).

5.9. Розкриття інформації третій стороні: коли виконкому міської ради та окремим особам необхідно розкрити персональні дані посадових осіб постачальнику чи іншій третій стороні, вони мають переконатися, що постачальник чи інша третя сторона забезпечать відповідні заходи безпеки для захисту PII від пов’язаних ризиків. Вони також повинні вимагати від третьої сторони забезпечити такий самий рівень захисту даних за договором або іншою домовленістю.

5.10. Для забезпечення відповідного рівня захисту персональних даних посадових осіб, виконком міської ради включає в тексти договорів з підрядниками, третіми сторонами інформацію щодо дотримання відповідних вимог законодавчих актів із захисту РІІ та розподілу відповідальності за їх порушення.

5.11. Розкриття РІІ у відповідь на запит правоохоронного або судового органу включає, перш за все, повідомлення про це CLO та DPO, який є уповноваженим для вжиття скоординованих заходів для обробки запиту.

5.12. Транскордонна передача персональних даних посадових осіб: якщо виконком міської ради передає персональні дані посадових осіб за межі України та або обробляє PII за межами України, слід ураховувати таке:

5.12.1 різні країни висувають різні вимоги до транскордонної передачі РІІ (наприклад, відсутність обмежень, умовне обмеження або заборона на передачу певних типів РІІ за межі країни);

5.12.2 перед передачею PII за межі країни виконком міської ради та окремі особи повинні проконсультуватися з DPO та CLO, щоб визначити, чи є транскордонна передача необхідною та законною.

5.13. Під час передачі персональних даних з Європейської економічної зони особа, яка передає, і особа, якій передаються, підписують угоду про передачу даних відповідно до норм Європейського Союзу і політики транскордонної передачі даних. Одержувач повинен забезпечити належний захист переданих даних відповідно до угоди про передачу даних.

5.14. Доступ посадових осіб: виконком міської ради надає посадовим особам розумні засоби для доступу до PII, що зберігаються про них, і дозволяє оновлювати, виправляти, видаляти або передавати свої PII, якщо це доречно або вимагається в межах чинного законодавства стосовно обробки PII.

#### *6. Обов'язки посадових осіб щодо РІІ*

6.1. CEO, DPO, CSO, CHRO, CISO, керівники відділів, управлінь, інших виконавчих органів міської ради у межах повноважень відповідають за своєчасне виконання заходів з оцінки та обробки ризиків, а також за оцінку впливу на захист PII.

6.2. Посадові особи відділів, управлінь, інших виконавчих органів міської ради повинні звертатися до Політики захисту PII посадових осіб під час обробки PII інших осіб.

#### *7. Реагування у разі невідповідності*

Будь-яка особа, якій відомо про витік PII посадових осіб, повинна повідомити про це відповідальним особам – CSO та DPO. Якщо необхідно повідомити про порушення даних за межі виконкому міської ради, слід дотримуватися процедури реагування на порушення даних. Однак, якщо цього вимагає місцеве законодавство країни, де відбулося порушення PII, особа, визначена в процедурі порушення PII, повинна повідомити про інцидент регулюючий орган та/або зацікавлених сторін протягом звітного періоду, визначеного законом.

*\*Залежно від юрисдикції та конкретного законодавства про захист персональних даних і конфіденційності фрази: «суб’єкт даних» або «суб’єкт PII» або «власник ідентифікаційної інформації» є синонімом фрази «суб’єкт PII».*

*\*\*Термін «Власник» ідентифікує посадових осіб, відділи, управління, інші виконавчі органи міської ради, для яких установлено відповідальність щодо здійснення контролю за створенням, розвитком, підтримкою, використанням безпеки активів та ресурсів СУІБ. Термін «Власник» не означає, що особа дійсно має право власності на активи/ресурс/ризик СУІБ.*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***