*ЗАТВЕРДЖЕНО*

*Рішення виконкому міської ради*

*25.07.2025 №938*

***ПОЛІТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ***

***ВИКОНАВЧОГО КОМІТЕТУ КРИВОРІЗЬКОЇ МІСЬКОЇ РАДИ***

#### *1. Загальні положення*

1.1. Політика захисту персональних даних виконавчого комітету Криворізької міської ради (надалі – Політика захисту РІІ) є документом, що встановлює основні принципи, за якими виконком міської ради здійснює обробку персональних даних (надалі – PII) суб’єктів РІІ (фізичних осіб, посадових осіб, працівників постачальників послуг та сервісів, ділових партнерів і працівників третіх та зацікавлених сторін, заявників).

1.2. Політика захисту PII визначає відповідальність посадових осіб виконкому міської ради в межах області дії системи управління інформаційною безпекою (надалі – СУІБ) з питань обробки та захисту PII.

1.3. Політика захисту РІІ поширюється на виконком міської ради, треті та зацікавлені сторони, що безпосередньо чи опосередковано контролюються контролером РІІ, чи уповноваженими органами в зв’язку з обробкою РІІ суб’єктів РІІ при здійсненні інформаційної діяльності в Європейській економічній зоні (надалі – ЄЕЗ) та обробці РІІ суб’єктів РІІ у ЄЕЗ під контролем контролера РІІ.

1.4. Політика захисту PII застосовується до всієї області дії СУІБ:

1.4.1 усіх робочих процесів і обробки PII, що обробляються в Єдиній інформаційній системі міста Кривий Ріг (надалі – ЄІС): «Підсистема документообігу», «Підсистема кадрового забезпечення» та «WebПортал»;

1.4.2 усіх мереж, пристроїв та засобів обробки інформації, якими володіють або користуються користувачі ЄІС, підрядники, консультанти, постачальники, партнери та інші користувачі, пов’язані з інформаційною діяльністю виконкому міської ради або іншими особами, які використовують чи отримують доступ до ЄІС щодо обробки PII у межах області дії СУІБ.

1.5. Політика захисту РІІ стосується:

1.5.1 усіх посадових осіб виконкому міської ради, що мають певну роль у межах області дії СУІБ, постійних, тимчасових та всі інших сторін, пов’язаних з обробкою PII в області дії СУІБ;

1.5.2 працівників зацікавлених та третіх сторін, дотичних до інформаційної діяльності виконкому міської ради та обробки РІІ у межах області дії СУІБ (у тому числі обслуговування компонентів ЄІС);

1.5.3 суб'єктів PII, які подають письмові звернення до виконкому міської ради або через ЄІС за допомогою підсистеми «WebПортал» до таких ресурсів як «Подати електронне звернення» та «Подати електронну петицію».

1.6. Політика захисту РІІ розроблена відповідно до вимог чинного законодавства України, міжнародних стандартів та нормативно-правових актів, що регламентують сферу інформаційної безпеки, а саме: Закону України «Про захист персональних даних», 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», розпорядження міського голови від 31.05.2011 №122-р «Про захист персональних даних», рішень виконкому міської ради від 14.05.2014 №141 «Про затвердження порядку обробки персональних даних, володільцем яких є Криворізька міська рада, її виконком», зі змінами, 21.07.2021 №377 «Про затвердження Регламенту виконавчого комітету Криворізької міської ради в новій редакції», зі змінами, Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням PII і про вільний рух таких PII, 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» D5.1-СУІБ «Повідомлення про конфіденційність» (додаток до Політики конфіденційності), D6.1-СУІБ «Уповноважена особа із захисту даних», D12-СУІБ «Положення про застосовність (SoA)», D14.19-СУІБ «Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю», D15.3-СУІБ «Угода про обробку персональних даних» (зразок на випадок, якщо є дозвіл процесору PII від контролера PII на обробку PII), D15.4-СУІБ «Угода про обробку персональних даних» (зразок на випадок, якщо є заборона процесору PII від контролера PII на обробку PII), D15.7-СУІБ «Заява про конфіденційність», D16.1-СУІБ «Процедура реагування на порушення даних і сповіщення».

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

2.1. Заявники – 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, PII якої обробляються в межах її згоди та якої стосується ідентифікаційна інформація в межах визначеної мети обробки PII, що встановлює склад цих персональних даних і процедури їх обробки, якщо інше не визначено законом.\*

2.3. Суб’єкти ЄІС – Криворізька міська рада, її виконавчі органи, підприємства, установи, організації, заклади комунальної власності міста, районні в місті ради, що користуються підсистемами ЄІС та обробляють інформацію для реалізації наданих повноважень.

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

2.5. 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)].

2.6. 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.\*\*

2.7. 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.

2.8. 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.

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

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

2.11. 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.

2.12. 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.

2.13. Інформаційно-комунікаційна система (надалі – ІКС) – до складу якої належить комплекс апаратних, програмних, апаратно–програмних (фізичних та/або віртуальних) телекомунікаційних засобів, призначених для маршрутизації, комутації, зберігання, приймання, передавання інформації між кінцевим обладнанням ІКС у межах виконання цілей виконкому міської ради.

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

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

2.14.2 органи місцевого самоврядування;

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

2.14.4 банки, інвестори, рейтингові агентства;

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

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

2.15. Третя сторона – це фізична або юридична особа, що може вплинути на ІБ та безперервність процесів. У контексті СУІБ третя сторона може не мати створений та зареєстрований акаунт у межах області дії СУІБ. Це можуть бути сім’ї 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.

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

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

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

2.19. «Footer» – HTML тег, що задає нижній колонтитул документу або розділу, у ньому можуть міститися: ім'я автора, дата документа, контактна й правова інформація.

#### *3. Основні принципи обробки РІІ*

3.1. Принципи захисту PII окреслюють основні обов’язки виконкому міської ради щодо захисту РІІ під час обробки в межах області дії СУІБ. РІІ за своєю специфікою є особливо чутливими до фундаментальних прав і свобод, потребують особливого захисту, оскільки контекст їх опрацювання може створити істотні ризики для суб’єктів РІІ.

3.2. PII мають оброблятися в законний правомірний та прозорий спосіб щодо суб’єкта PII. Суб’єкт РІІ надав згоду на опрацювання своїх РІІ для однієї або декількох відповідних цілей. Виконком міської ради повинен вжити необхідних заходів для надання будь-якої інформації щодо обробки РІІ суб’єкту РІІ у стислій прозорій доступній для розуміння формі, з використання чітких і простих формулювань.

3.3. PII повинні збиратися для визначених, явних і законних цілей і в подальшому не оброблятися іншим способом, несумісним із цими цілями.

3.4. PII мають бути адекватними відповідними та обмеженими тим, що необхідно для цілей, для яких вони обробляються, та в подальшому не опрацьовуватися в спосіб, що є несумісним з такими цілями. Виконком міської ради повинен застосовувати анонімізацію або псевдонімізацію PII, якщо це можливо, щоб зменшити ризики для відповідних суб’єктів PII.

3.5. PII мають бути точними та, у разі необхідності, оновлюватися. Уживаються відповідні кроки, щоб забезпечити своєчасне видалення або виправлення без затримки PII, які є неточними з огляду на цілі, для яких вони обробляються.

3.6. PII, у формі, що дозволяє ідентифікацію суб'єктів РІІ, повинні зберігатися не довше, ніж це необхідно для цілей, для яких вони обробляються.

3.7. Беручи до уваги стан технологій та інші доступні заходи безпеки, вартість реалізації, а також імовірність і суттєвість ризиків для PII, виконком міської ради повинен використовувати відповідні технічні чи організаційні заходи для обробки PII у спосіб, який гарантує відповідну безпеку опрацювання PII, включаючи захист від випадкового чи незаконного опрацювання, знищення, втрати, зміни, несанкціонованого доступу або розголошення.

#### *4. Побудова захисту РІІ у господарській діяльності*

4.1. Виконком міської ради вживає усіх заходів із захисту PII відповідно до нормативно-правових національних та міжнародних актів.

4.2. Для виконання вимог прозорості виконком міської ради на офіційному вебсайті Криворізької міської ради та її виконавчого комітету (надалі – вебсайт виконкому міської ради) розміщує дані про:

4.2.1 володільця та розпорядника РІІ;

4.2.2 контролера РІІ та процесора РІІ;

4.2.3 місцезнаходження РІІ;

4.2.4 склад РІІ;

4.2.5 мета обробки РІІ;

4.2.6 зацікавлені та треті особи, яким передаються РІІ, що обробляються;

4.2.7 права суб’єктів даних;

4.2.8 нормативно-правові документи, які регламентують інформаційну діяльність з обробки PII.

4.3. Окрім вказаної вище інформації, на вебсайті виконкому міської ради <https://kr.gov.ua/> для загального доступу розміщується «Політика конфіденційності офіційного вебсайта Криворізької міської ради та її виконавчого комітету».

4.4. Також на сторінках вебсайту виконкому міської ради <https://kr.gov.ua/>, де суб’єкт РІІ уносить свої РІІ для подачі запиту, електронного звернення або електронної петиції, додано технологію «checkbox», за допомогою яких суб’єкт РІІ має можливість підтвердити добровільну згоду (поставивши відмітку) на обробку РІІ та ознайомлення з нормативно-правовими документами щодо обробки РІІ.

4.5. Виконком міської ради повинен збирати PII тільки в межах передбачених чинним законодавством. Якщо PII збираються від третьої чи зацікавленої сторони, DPO має переконатися, що PII збираються законно.

4.6. Зберігання РІІ передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

4.7. Цілі, правові підстави для обробки, перелік РІІ, які виконком міської ради збирає, передача третім та зацікавленим сторонам, зберігання та видалення PII мають відповідати інформації, що міститься в D5.1-СУІБ «Повідомлення про конфіденційність». Виконком міської ради в інформаційній діяльності цілеспрямовано й послідовно підтримує точність, цілісність, конфіденційність і актуальність PII відповідно до мети обробки, використовує адекватні механізми безпеки, призначені для захисту PII, для запобігання несанкціонованому доступу, крадіжці, неправомірному використанню чи зловживанню PII, знищенню, а також запобіганню витоку PII.

4.8. DPO відповідає за забезпечення дотримання вимог, наведених у цьому розділі.

4.9. Кожного разу, коли виконком міської ради використовує стороннього постачальника або ділового партнера для обробки PII від свого імені в ролі процесора РІІ, DPO має переконатися, що цей процесор PII створить заходи безпеки для захисту PII, які відповідають пов’язаним ризикам (зловживання PII, роз-криття PII, порушення обробки PII тощо). Для цього використовується анкета відповідності процесора PII (зразок наведений у D15.2-СУІБ «Анкета відповідності процесора персональних даних»). Виконком міської ради за договором вимагає від постачальника або ділового партнера забезпечити такий рівень захисту PII. Постачальник або діловий партнер має обробляти PII лише для виконання своїх договірних зобов’язань перед виконкомом міської ради або за його вказівками, а не для будь-яких інших цілей. Коли виконком міської ради обробляє PII спільно з незалежною третьою або зацікавленою стороною, то повинен чітко вказати відповідні обов’язки третьої або зацікавленої сторони у відповідному контракті чи будь-якому іншому юридично обов’язковому документі, такому як D15.3-СУІБ «Угода про обробку персональних даних» (зразок на випадок, якщо є дозвіл процесору РІІ від контролера РІІ на обробку РІІ) або D15.4-СУІБ «Угода про обробку персональних даних» (зразок на випадок, якщо є заборона процесору РІІ від контролера РІІ на обробку РІІ).

4.10. DPO розробляє та погоджує відповідні частини контракту (договору), що стосуються обробки РІІ.

4.11. Виконком міської ради своєчасно інформує суб’єкта РІІ про підстави для транскордонної передачі PII, умови договорів (у частині, що стосується суб’єкта PII), створених відповідно до вимог D15.7-СУІБ «Заява про конфіденційність» та/або про будь-які заплановані зміни в цьому відношенні, щоб суб’єкт РІІ мав можливість заперечити проти таких змін або розірвати договір.

4.12. Перед передачею PII за межі ЄЕЗ необхідно вжити відповідних заходів безпеки, включаючи підписання Угоди про передачу даних, як того вимагає Європейський Союз, і, якщо потрібно, необхідно отримати дозвіл від відповідного органу із захисту даних. Суб’єкт PII, який отримує PII, зобов’язаний дотримуватися принципів обробки PII, викладених у Процедурі транскордонної передачі даних. Для забезпечення необхідного рівня захисту РІІ виконком міської ради

використовує угоду про передачу даних з одержувачем третьої або зацікавленої сторони на основі контрактів з наведенням усіх вимог з питань забезпечення конфіденційності PII у межах області дії СУІБ та в межах цілей, що визначені в згоді суб’єкта PII про обробку PII. Суб’єкт PII може запросити додаткову інформацію щодо цього обміну та отримати від DPO інформацію стосовно проведених заходів захисту PII, скориставшись своїми правами, як указано у розділі 7 Політики захисту PII.\*\*\*

4.13. Суб'єкт РІІ повинен мати право на отримання від контролера РІІ під-твердження факту опрацювання його РІІ і, якщо це так, – доступу до РІІ та інформації про:

4.13.1 категорії відповідних РІІ;

4.13.2 одержувача та категорії одержувача, якому РІІ були або будуть роз-криті, зокрема одержувачі в третіх країнах або міжнародні організації;

4.13.3 період, протягом якого передбачається, що РІІ будуть зберігати, або, якщо це неможливо, критерії визначення такого періоду;

4.13.4 право подавати скаргу до наглядового органу;

4.13.5 будь-яку інформацію щодо джерела (якщо РІІ не збирають від суб'єкта РІІ);

4.13.6 наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу і, принаймні в таких випадках, достовірної інформації про логіку, значимість та передбачувані наслідки такого опрацювання для суб'єкта РІІ;

4.13.7 право запросити обмеження обробки PII.

4.14. Якщо суб’єкт PII вважає, що будь-яка інформація, яку виконком міської ради має про нього, є неправильною або неповною, суб’єкт РІІ має право пред’являти вмотивовану вимогу відділу, управлінню, іншому виконавчому органу міської ради щодо заборони обробки РІІ (їх частини) та/або зміни їх складу/змісту. Така вимога розглядається DPO упродовж десяти днів з моменту отримання.

4.15. Якщо за результатами розгляду такої вимоги виявлено, що РІІ суб’єкта РІІ (їх частина):

4.15.1 обробляються незаконно, відділ, управління, інший виконавчий орган міської ради, у якому відбувалася ця обробка PII, припиняє їх обробку та DPO інформує про це суб’єкта РІІ;

4.15.2 є недостовірними, відділ, управління, інший виконавчий орган міської ради, у якому відбувалася ця обробка PII, припиняє їх обробку та/або змінює їх склад/зміст і DPO інформує про це суб’єкта РІІ. У разі, якщо вимога не підлягає задоволенню, DPO надає суб’єкту РІІ мотивовану відповідь щодо відсутності підстав для її задоволення.

4.15.3 Суб’єкт РІІ має право відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для їх обробки є його згода. З моменту відкликання згоди відділ, управління, інший виконавчий орган міської ради зобов’язаний припинити обробку РІІ.

4.16. Якщо РІІ суб'єкта РІІ виконком міської ради передає до третьої країни або до міжнародної організації, суб'єкт РІІ повинен мати право бути повідомленим про належні гарантії щодо передавання РІІ.

4.17. Для забезпечення доступу та PII, у підсистемі «WebПортал» мають бути впроваджені такі технології:

4.17.1 аутентифікація – вебсайт має вимагати обов'язкову аутентифікацію суб’єкта РІІ (користувач ЄІС, заявник) перед створенням петиції або зверненням із використанням двофакторної або багатофакторної автентифікації суб’єкта РІІ для підвищення рівня безпеки;

4.17.2 шифрування даних – усі PII, що передаються між користувачем та сайтом, повинні бути зашифровані за допомогою протоколу HTTPS. Це забезпечить захист від перехоплення даних у процесі передачі.

4.18. Суб’єкти PII мають право отримати за запитом копію PII, які вони надали виконкому міської ради в структурованому форматі, і безкоштовно передавати ці дані іншому контролеру PII. DPO надає консультації контролеру РІІ, щоб такі запити оброблялися протягом одного місяця, не були надмірними та не впливали на права суб’єкта PII та на PII інших осіб

4.19. За запитом суб’єкти РІІ мають право вимагати від виконкому міської ради видалення своїх РІІ. Коли виконком міської ради діє як контролер РІІ, DPO надає консультації контролеру РІІ, що він повинен вжити відповідних заходів, у тому числі технічних, для інформування інших контролерів РІІ/процесорів PII, які опрацьовують РІІ, що суб’єкт РІІ направив запит на стирання такими контролерами РІІ/ процесорами PII будь-яких посилань на такі РІІ, їх копії чи відтворення.

4.20. Порядок розкриття РІІ третім особам зобов’язує виконком міської ради реєструвати розкриття, які РІІ були розкриті, кому й коли. Порядок розкриття РІІ та умови для відхилення таких запитів повинні відповідати інформації, що міститься в D5.1-СУІБ «Повідомлення про конфіденційність».

#### *5. Правила справедливої обробки РІІ*

5.1. РІІ повинні оброблятися лише за наявності явно наданої згоди на обробку РІІ від суб’єктів PII.

5.2. Згідно з вимогами статті 11 Закону України «Про захист персональних даних» обробка персональних даних, яка потребує згоди суб'єкта персональних даних, має базуватися на інформованій, добровільній і чітко вираженій згоді користувача, що досягається за допомогою використання такої технології:

5.2.1 у підсистемах «Підсистема документообігу», «Підсистема кадрового забезпечення» – згода суб'єкта даних (форма зафіксована у документі D9.1-СУІБ «Форма згоди суб'єкта даних»), D14.19-СУІБ «Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю»;

5.2.2 у підсистемі «WebПортал» – згода суб’єкта РІІ на обробку РІІ має бути чіткою, добровільною, усвідомленою і однозначною. Вебсайт виконкому міської ради, який збирає РІІ, отримує однозначну згоду від користувачів на обробку PII цього користувача (наприклад, через застосування технології «checkbox» – елемент інтерфейсу, який дозволяє суб’єкту РІІ вибирати або скасовувати вибір, відзначаючи позначкою певний пункт, що не заповнений за замовчуванням, та надають можливість суб’єкту РІІ особисто поставити позначку про згоду або відмовитися). Також суб’єкту РІІ вебсайт виконкому міської ради має надати можливість відкликати згоду. Користувачам надається можливість легко відкликати свою згоду на обробку РІІ у будь-який момент. Крім того суб’єкт РІІ має можливість підтвердити, що він ознайомлений з нормативно-правовою базою СУІБ у частині обробки PII та відповідальністю за надання правдивої інформації (приклад: Я згоден на використання моїх персональних даних. Я ознайомлений з нормативно правовою базою за переліком, розміщеним на вебсайті виконкому міської ради);

5.2.3 підсистема «WebПортал» забезпечує право суб’єкта РІІ на відкликання згоди в будь-який момент. Оскільки згода надається суб’єктом РІІ через вебсайт виконкому міської ради, на сайті розміщується онлайн-форма на відкликання згоди. Посилання на онлайн-форму відкликання розміщується на кожній сторінці вебсайта у «Footer».

5.3. Політикою захисту РІІ виконком міської ради гарантує, що збір персональних даних відбувається лише в цілях надання відповідних послуг, сервісів та виконання чинного законодавства України [PII заявників збираються тільки ті, що потрібні для створення петиції, електронного звернення подання скарги тощо: ім'я, прізвище, по батькові, стать, місце народження, адреса електронної пошти, фізична адреса (юридична адреса), ідентифікаційний номер, номер телефону та зміст звернення)].

5.4. Під час збору або перед збором PII для будь-якої діяльності з обробки PII, DPO несе відповідальність за належне інформування контролером РІІ суб’єктів PII про їх такі права:

5.4.1 знати про джерела збирання, місцезнаходження своїх РІІ, мету їх обробки, місцезнаходження або місце перебування контролера PII та процесора PII, або дати відповідне доручення щодо отримання цієї інформації уповноваженим суб’єктом РІІ особам, крім випадків, установлених законом;

5.4.2 отримувати інформацію про умови надання доступу до РІІ, зокрема інформацію про третіх осіб, яким передаються РІІ;

5.4.3 право на доступ до власних РІІ;

5.4.4 отримувати не пізніше ніж за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються РІІ суб’єкта РІІ, а також отримувати зміст таких РІІ;

5.4.5 пред'являти вмотивовану вимогу контролеру PII та/або процесору PII із запереченням проти обробки РІІ;

5.4.6 пред'являти вмотивовану вимогу про зміну або знищення РІІ будь-яким контролером PII та/або процесором PII, якщо ці дані обробляються незаконно чи є недостовірними;

5.4.7 на захист РІІ від:

5.4.7.1 незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням або несвоєчасним їх наданням;

5.4.7.2 на захист від надання відомостей, що є недостовірними або ганьблять честь, гідність та ділову репутацію суб’єкта РІІ;

5.4.8 звертатися зі скаргами на обробку РІІ до Уповноваженого Верховної Ради України з прав людини або до суду;

5.4.9 застосовувати засоби правового захисту в разі порушення законодавства про захист РІІ;

5.4.10 уносити застереження стосовно обмеження права на обробку своїх РІІ під час надання згоди;

5.4.11 відкликати згоду на обробку РІІ;

5.4.12 знати механізм автоматичної обробки РІІ;

5.4.13 на захист від автоматизованого рішення, що має для нього правові наслідки.

5.5. У разі наявності кількох видів діяльності з обробки PII, виконком міської ради розробляє різні повідомлення, що відрізнятимуться залежно від діяльності з обробки та категорій зібраних PII. Якщо РІІ передаються третім особам, DPO має переконатися, що суб’єкти PII були повідомлені про це.

5.6. Якщо обробка PII ґрунтується на згоді суб’єкта PII або на інших законних підставах, DPO контролює, щоб контролер РІІ був спроможним довести те, що суб'єкт РІІ надав явну згоду на опрацювання своїх РІІ. DPO контролює, щоб контролер РІІ надав суб’єктам PII варіанти надання згоди й має повідомити та гарантувати, що їх згоду (щоразу, коли згода використовується як законна підстава для обробки) можна відкликати в будь-який час. Для відповідних функціональних підсистем ЄІС це будуть такі дії щодо підтвердження надання згоди суб’єктом РІІ:

5.6.1 у підсистемах «Підсистема документообігу», «Підсистема кадрового забезпечення» – підписання суб’єктом РІІ згоди суб'єкта даних (згідно з формою документа D9.1-СУІБ «Форма згоди суб'єкта даних») та підписання суб’єктом РІІ заяви про ознайомлення та прийняття документів СУІБ та конфіденційністю (згідно з формою документа D14.19-СУІБ «Заява про ознайомлення та прийняття документів системи управління інформаційною безпекою та конфіденційністю»);

5.6.2 у підсистемі «WebПортал» – забезпечення на вебсайті надання згоди суб’єктом РІІ на обробку РІІ, та її фіксація, через проставлення позначки про згоду в «checkbox», або відмову від надання такої згоди. Якщо збір PII стосується особи віком до 16 років, має бути додана позначка про згоду батьків із доданням цієї згоди, щоб переконатися, що контролеру РІІ батьківська згода була надана перед збиранням за допомогою форми згоди батьків (форма додається до довідкових матеріалів, доступних на вебсайті виконкому міської ради).

5.7. На вебсайті виконкому міської ради суб’єкту РІІ надається можливість легко відкликати свою згоду на обробку РІІ у будь-який момент. Для доступу до своїх PII на вебсайті впроваджуються відповідні технічні й організаційні заходи

для гарантування безпеки РІІ, такі як: шифрування даних, захист від несанкціонованого доступу, резервне копіювання та інші заходи безпеки.

5.8. Окрім можливості надання та відкликання згоди, Суб’єкт РІІ має можливість підтвердити, що він ознайомлений з нормативно-правовою базою СУІБ у частині обробки PII та відповідальністю за надання правдивої інформації через поставлення позначки про ознайомлення у «checkbox» (приклад: Я згоден на використання моїх персональних даних, Я ознайомлений з нормативно правовою базою за переліком, розміщеним на вебсайті виконкому міської ради).

5.9. Під час реєстрації електронних звернень або електронних петицій суб’єкт РІІ повинен особисто підтвердити (поставити відповідну позначку в «checkbox») у відповідних розділах вебсайта виконкому міської ради за посиланням <https://kr.gov.ua/> про те, що він згоден з обробкою РІІ та ознайомлений з нормативно-правовою базою.

5.10. Якщо збір PII стосується особи віком до 16 років, DPO має переконатися, що контролеру РІІ батьківська згода була надана перед збиранням за допомогою форми згоди батьків. У разі надходження запитів на виправлення, зміну або знищення записів PII, DPO має забезпечити обробку контролером РІІ цих запитів протягом розумного періоду часу. DPO реєструє запити та веде журнал.\*\*\*\*

5.11. PII обробляються лише з метою, для якої вони були спочатку зібрані. У випадку, якщо виконком міської ради хоче обробляти зібрані PII для іншої мети, він повинен отримати згоду від суб’єктів PII у чіткій та лаконічній письмовій формі. Будь-який такий запит містить початкову мету, для якої збиралися дані, а також нову або додаткову мету (або цілі). Запит також має містити причину зміни мети (цілей). DPO несе відповідальність за контроль дотримання правил цього пункту.

5.12. DPO гарантує, що методи збору відповідають чинному законодавству, передовій практиці та галузевим стандартам. DPO відповідає за створення та ведення Реєстру порушень даних (зразок форми викладений у D16.2-СУІБ «Реєстр порушень даних»).

#### *6. Організаційна структура та обов'язки відповідальних осіб у сфері СУІБ*

6.1. Відповідальність за забезпечення належної обробки PII лежить на кожному, хто має доступ до PII, які обробляються виконкомом міської ради в межах області дії СУІБ.

6.2. Основні сфери відповідальності за обробку PII покладаються на такі організаційні ролі:

6.2.1 CEO приймає рішення та затверджує загальні стратегії виконкому міської ради щодо захисту PII, обирає для призначення DPO.

6.2.2 DPO відповідає за управління програмою захисту PII і розробку та просування наскрізних політик захисту PII, як це визначено в його посадовій інструкції. DPO відповідає за:

6.2.2.1 інформування та надання рекомендацій контролеру РІІ або процесору РІІ і посадовим особам, які здійснюють опрацювання, щодо їх обов'язків відносно захисту РІІ під час обробки;

6.2.2.2 надання на запит рекомендації щодо оцінювання впливу на захист даних (DPIA) та здійснення моніторингу його проведення;

6.2.2.3 співпрацю з наглядовими органами у сфері захисту РІІ;

6.2.2.4 діяльність як координаційного центру для наглядових органів з питань, що стосуються опрацювання, у тому числі попередньої консультації з питань DPIA і надання консультації за необхідності, щодо будь-якого іншого питання;

6.2.2.5 затвердження будь-яких заяв про захист PII, що додаються до таких повідомлень, як електронні листи та друковані листи;

6.2.2.6 розгляд будь-яких запитів щодо захисту PII від медіа;

6.2.2.7 за передачу обов’язків щодо захисту PII постачальникам і підвищення рівня обізнаності постачальників щодо захисту PII, а також за передачу вимог щодо PII будь-якій третій стороні – постачальнику, якого вона використовуює. DPO зобов’язаний переконатися, що виконком міської ради залишає за собою право перевіряти постачальників;

6.2.2.8 своєчасність і повноту впровадження заходів з оцінки, обробки, планування та моніторингу ризиків, які виникають у процесі інформаційної діяльності виконкому міської ради;

6.2.2.9 ведення реєстру порушень даних, якісну та плідну співпрацю з уповноваженими органами із захисту PII;

6.2.2.10 звітність щодо PII та своєчасніть/оперативність доповіді CEO стосовно виявлених або потенційно існуючих подій, що можуть призвести до інцидентів;

6.2.2.11 вирішення питань, що виникають під час діяльності з управління ризиками та інцидентами. DPO згідно з вимогами статі 24 пункту 2 Закону України «Про захист персональних даних» зобов’язаний підготувати повідомлення та організувати доведення інформації про призначення DPO Уповноваженому Верховної Ради України з прав людини з метою оприлюднення факту призначення DPO та контактних даних для зв’язку.

6.2.3. CSO відповідає за забезпечення відповідності всіх систем, послуг, сервісів та обладнання виконкому міської ради, що використовуються для зберігання PII, прийнятним стандартам безпеки.

6.2.4 CISO відповідає за виконання регулярних перевірок і сканування ЄІС, щоб переконатися, що обладнання та програмне забезпечення безпеки функціонують належним чином.

6.2.5 CHRO разом з CLO відповідають за:

6.2.5.1 підвищення обізнаності посадових осіб, які працюють з PII;

6.2.5.2 наскрізний захист PII посадових осіб виконкому міської ради, який гарантує, що РІІ посадових осіб обробляються відповідно до законних цілей у межах визначених повноважень з урахуванням діючих обмежень.

6.2.6 CSO, CISO, CHRO, CLO разом із DPO відстежують і аналізують закони про PII та зміни до нормативних актів, розробляють вимоги їх дотримання і допомагають досягати цілей щодо PII в процесі інформаційної діяльності виконкому міської ради.

#### *7. Інструкції щодо створення головного наглядового органу*

7.1. Визначення головного наглядового органу має значення лише в тому випадку, якщо виконком міської ради здійснює транскордонну обробку PII.

7.2. Транскордонна обробка PII здійснюється, якщо:

7.2.1 обробка PII здійснюється відділами, управліннями, іншими виконавчими органами міської ради, розташованими в інших державах-членах (постійно чи тимчасово);

7.2.2 обробка PII, що відбувається із застосуванням активів виконкому міської ради в межах області дії СУІБ в Європейському Союзі (надалі – ЄС), але яка суттєво впливає або може суттєво вплинути на суб’єктів PII у більш ніж одній державі-члені ЄС.

7.3. Якщо виконком міської ради здійснює інформаційну діяльність стосовно обробки PII лише в одній державі-члені ЄС та його діяльність з обробки впливає лише на суб’єктів PII у цій державі-члені, тоді немає необхідності створювати головний наглядовий орган. Єдиним компетентним органом буде наглядовий орган країни, де виконком міської ради здійснює інформаційну діяльність на законних підставах.

#### *8. Реагування на випадки порушення персональних даних*

У разі наявної інформації про ймовірне або фактичне порушення PII, CSO із DPO зобов’язані доповісти СЕО, провести службове розслідування та своєчасно вжити відповідних заходів щодо виправлення порушень відповідно до політик щодо порушення PII згідно з інформацією, що міститься в D5.1-СУІБ «Повідомлення про конфіденційність». Якщо існує будь-який ризик для прав і свобод суб’єктів PII, виконком міської ради має повідомити відповідні органи захисту PII. Виконком міської ради повідомляє відповідного представника органу захисту PII протягом 72 годин.

#### *9. Конфлікт щодо виконання правових вимог*

9.1. Політика захисту PII призначена для дотримання законів і правил у місці заснування та країнах, у яких виконком міської ради здійснює інформаційну діяльність. У разі суперечності між Політикою захисту PII та відповідними законами й нормативними актами, останні мають переважну силу.

9.2. Політика захисту персональних даних поширюється на всіх посадових осіб виконкому міської ради, працівників третіх та зацікавлених сторін, відряджених, консультантів і підрядників, незалежно від місця їх розташування, посади чи статусу.

*\*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.*

*\*\*\*Цей пункт буде застосовуватися кожного разу, якщо в процесі інформаційної діяльності виникає така необхідність (наприклад, під час виконання обов’язків посадовими особами виконкому міської ради у ЄЕЗ необхідно здійснити транскордонну передачу PII у межах області застосування СУІБ).*

*\*\*\*\*Стаття 8(2) GDPR зазначає, що «Контролер PII зобов’язаний докладати розумних зусиль, щоб перевірити в таких випадках, що згода надана або схвалена носієм батьківської відповідальності за дитину, беручи до уваги доступні технології».*

***Керуюча справами виконкому Олена ШОВГЕЛЯ***