



ВИКОНАВЧИЙ ОРГАН КИЇВСЬКОЇ МІСЬКОЇ РАДИ
(КИЇВСЬКА МІСЬКА ДЕРЖАВНА АДМІНІСТРАЦІЯ)

**ДЕПАРТАМЕНТ З ПИТАНЬ ЗАПОБІГАННЯ
ТА ВИЯВЛЕННЯ КОРУПЦІЇ**

НАКАЗ

15 листопада 2025 року

№ 62-02

Про затвердження Порядку обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Відповідно до статей 6, 24 Закону України «Про захист персональних даних», пункту 1.2 розділу 1 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року № 1/02-14, та з метою подальшого вдосконалення роботи із забезпечення дотримання вимог до обробки та захисту персональних даних у Департаменті з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)

НАКАЗУЮ:

1. Затвердити Порядок обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації), що додається.

2. Головному спеціалісту-юрисконсульту Департаменту з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації) забезпечити в установленому порядку подання цього наказу на державну реєстрацію до Центрального міжрегіонального управління Міністерства юстиції (м. Київ).

3. Цей наказ набирає чинності з дня його оприлюднення.

4. Контроль за виконанням цього наказу залишаю за собою.

Директор

Олег ТИМОШЕНКО

**Згідно
з оригіналом**

ЗАТВЕРДЖЕНО

Наказ Департаменту з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)

« 15 » жовтня 2025 року № 62-0Д

Порядок

обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)

I. Загальні положення

1. Порядок обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації) (далі – Порядок), встановлює загальні вимоги до організаційних і технічних заходів обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації) (далі – Департамент), під час їх обробки в інформаційних системах Департаменту та на паперових носіях.

2. Терміни у цьому Порядку вживаються у значеннях, наведених в Законах України «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах».

3. До персональних даних належать будь-які відомості чи сукупність відомостей про особу, за якими вона ідентифікується чи може бути конкретно ідентифікованою.

4. Персональні дані, що обробляються, є інформацією з обмеженим доступом, крім випадків, передбачених статтею 5 Закону України «Про захист персональних даних» (далі – Закон).

5. Персональні дані в інформаційних системах Департаменту обробляються автоматизовано в електронній формі за допомогою програмних засобів та у паперовій формі (зберігання звернень, запитів на інформацію, які надійшли у паперовій формі; документів, що містять персональні дані працівників Департаменту або кандидатів на зайняття вакантних посад, призначення на які здійснюється Департаментом, тощо).

6. Володільцем персональних даних є Департамент.

7. Обробка персональних даних, щодо яких встановлені особливі вимоги, та/або яка становить особливий ризик для прав і свобод суб'єктів персональних даних, здійснюється відповідно до статей 7 та 9 Закону.

8. Цей Порядок є обов'язковим до виконання працівниками Департаменту, яким надано доступ до інформації, що містить персональні дані, у межах виконання ними своїх повноважень.

9. Організацію роботи, пов'язаної із захистом персональних даних, обробку яких здійснює Департамент, забезпечує відповідальна особа з питань захисту персональних даних (далі – відповідальна особа), яка визначається наказом Департаменту. У випадках, передбачених Законом, володілець також визначає обов'язки та права осіб, відповідальних за організацію роботи, пов'язаної із захистом персональних даних під час їх обробки.

II. Мета та підстави обробки персональних даних

1. Обробка персональних даних, володільцем яких є Департамент, здійснюється з метою:

- реалізації завдань і функцій Департаменту, що належать до його компетенції, кадрової політики у Департаменті з питань добору персоналу, документального оформлення прийняття на роботу та звільнення;

- забезпечення реалізації вимог законодавства про звернення громадян, про доступ до публічної інформації;

- забезпечення проходження державної служби та реалізації трудових відносин, управління персоналом, ведення військового та податкового обліків;

- ведення діловодства з питань управління персоналом, адміністративно-правових відносин та відносин з питань бухгалтерського обліку та/або підготовки відповідно до вимог законодавства статистичної, управлінської та іншої інформації з питань, що належать до компетенції Департаменту;

- забезпечення реалізації вимог законодавства в сфері оплати праці щодо виплати заробітної плати працівникам Департаменту через установи банків; щодо матеріальної відповідальності працівників за шкоду, заподіяну Департаменту внаслідок порушення покладених на них трудових обов'язків; щодо відшкодування витрат та одержання інших компенсацій у зв'язку з службовими відрядженнями працівників; щодо відомостей про оплату праці працівника та захисту інтересів суб'єктів персональних даних або інших осіб.

2. Департамент здійснює обробку персональних даних на підставах, визначених статтею 11 Закону.

Обробка персональних даних фізичних осіб, які надають Департаменту послуги за цивільно-правовими договорами, здійснюється на підставі правочину, стороною якого є суб'єкт персональних даних, або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних.

III. Категорії суб'єктів та склад персональних даних

1. Департамент здійснює обробку персональних даних таких категорій суб'єктів:

- працівників Департаменту та кандидатів на зайняття вакантних посад, призначення на які, здійснюється Департаментом;

- осіб, які звертаються до Департаменту в порядку, визначеному Законами України «Про звернення громадян», «Про доступ до публічної інформації», «Про адвокатуру та адвокатську діяльність»;

- осіб, які надають Департаменту послуги за цивільно-правовими договорами.

2. Склад персональних даних, які обробляються Департаментом, залежить від категорії суб'єкта персональних даних.

3. Департаментом обробляються персональні дані:

1) працівників Департаменту:

- прізвище, власне ім'я, по батькові (за наявності);

- дата й місце народження;

- реквізити паспорта громадянина України (назва документа, серія (за наявності), номер, дата видачі та уповноважений суб'єкт, що видав документ);

- реєстраційний номер облікової картки платника податків або серія (за наявності) або номер паспорта (для осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті);

- відомості про освіту;

- відомості про трудову діяльність;

- військово-облікові дані;

- відомості про сімейний стан;

- відомості про адресу задекларованого/зареєстрованого місця проживання (перебування);

- відомості про засоби зв'язку;

- інші персональні дані, необхідність обробки яких визначена законодавством;

2) кандидатів на зайняття вакантних посад Департаменту:

- прізвище, власне ім'я, по батькові (за наявності);

- дата й місце народження;

- реквізити паспорта громадянина України (назва документа, серія (за наявності), номер, дата видачі та уповноважений суб'єкт, що видав документ);

- реєстраційний номер облікової картки платника податків або серія (за наявності) або номер паспорта (для осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті);

- відомості про освіту;

- відомості про трудову діяльність;

- військово-облікові дані;

- відомості про сімейний стан;

- відомості про адресу задекларованого/зареєстрованого місця проживання (перебування);

- відомості про засоби зв'язку;

- інші персональні дані, необхідність обробки яких визначена законодавством;

3) осіб, які звертаються в порядку, визначеному Законами України «Про звернення громадян», «Про доступ до публічної інформації», «Про адвокатуру та адвокатську діяльність»:

- прізвище, власне ім'я, по батькові (за наявності);

- відомості про адресу задекларованого/зареєстрованого місця проживання (перебування);

- наявність пільг, які є підставою для першочергового розгляду звернення;

- відомості про засоби зв'язку;

- інші дані, які особа добровільно, за власним бажанням, надає про себе;

4) осіб, які надають Департаменту послуги за цивільно-правовими договорами:

- прізвище, власне ім'я, по батькові (за наявності);

- відомості про засоби зв'язку;

- відомості про адресу задекларованого/зареєстрованого місця проживання (перебування);

- інші персональні дані, необхідність обробки яких визначена законодавством.

IV. Порядок обробки персональних даних

1. Спосіб збирання, накопичення персональних даних

1. Збирання персональних даних працівників Департаменту здійснюється шляхом надання ними відповідних документів, визначених законодавством, зокрема, про державну службу, працю.

Накопичення таких персональних даних здійснюється згідно з вимогами законодавства про державну службу, працю.

Накопичення персональних даних працівників здійснюється за допомогою уніфікованої автоматизованої системи бухгалтерського обліку та звітності і в особових справах працівників.

Збирання персональних даних кандидатів на зайняття вакантних посад, призначення на які здійснюється Департаментом, здійснюється шляхом надання ними відповідних документів, визначених законодавством, зокрема про державну службу, працю.

Персональні дані кандидатів на зайняття вакантних посад Департаменту накопичуються в паперовій та електронній формах.

2. Персональні дані осіб, які звертаються до Департаменту в порядку, визначеному Законами України «Про звернення громадян», «Про доступ до публічної інформації», «Про адвокатуру та адвокатську діяльність», збираються шляхом використання відомостей про таких осіб, зазначених ними у заявах, зверненнях та запитах на інформацію, адвокатських запитах.

Накопичення персональних даних зазначеної категорії суб'єктів здійснюється за допомогою системи електронного документообігу.

3. Персональні дані осіб, які надають Департаменту послуги за цивільно-правовими договорами, збираються під час укладання цивільно-правового договору відповідно до вимог Цивільного кодексу України.

2. Строки та умови зберігання персональних даних

1. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством.

2. Персональні дані працівників Департаменту та кандидатів на зайняття вакантних посад, призначення на які здійснюється Департаментом, зберігаються у строк, визначений законодавством, зокрема Кодексом законів про працю України, Законом України «Про державну службу».

3. Персональні дані осіб, які звертаються до Департаменту в порядку, визначеному Законами України «Про звернення громадян», «Про доступ до публічної інформації», зберігаються протягом п'яти років з дати звернення.

4. Персональні дані осіб, які надають Департаменту послуги за цивільно-правовими договорами, зберігаються в уніфікованій автоматизованій системі бухгалтерського обліку та звітності протягом строку, визначеного законодавством.

5. Забезпечення збереженості та цілісності персональних даних здійснюється відповідно до вимог розділу V цього Порядку.

3. Внесення змін, видалення або знищення персональних даних

1. Працівники структурних підрозділів Департаменту, які здійснюють обробку персональних даних в обсягах, визначених їх посадовими інструкціями, переглядають персональні дані на предмет їх актуальності та достовірності відповідно до законодавства.

2. Зміни до персональних даних вносяться на підставі:

- 1) вмотивованої письмової вимоги суб'єкта персональних даних;
- 2) припису Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб Секретаріату Уповноваженого Верховної Ради України з прав людини;
- 3) рішення суду, що набрало законної сили;
- 4) звернення інших суб'єктів відносин, пов'язаних із персональними даними, якщо на це є згода суб'єкта персональних даних.

3. Персональні дані видаляються або знищуються у спосіб, що виключає подальшу можливість поновлення таких персональних даних.

4. Персональні дані підлягають видаленню або знищенню у разі:

- 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;
- 2) припинення правовідносин між суб'єктом персональних даних та Департаментом, якщо інше не передбачено законом;
- 3) видання відповідного припису Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб Секретаріату Уповноваженого Верховної Ради України з прав людини;

4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

5. Персональні дані, зібрані з порушенням вимог Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

6. Суб'єкт персональних даних має право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними.

7. Якщо за результатами розгляду такої вимоги виявлено, що персональні дані суб'єкта обробляються незаконно або є недостовірними, Департамент припиняє обробку персональних даних суб'єкта та інформує про це суб'єкта персональних даних.

4. Доступ до персональних даних

1. Працівники, які обробляють персональні дані, мають бути ознайомлені з вимогами Закону та інших нормативно-правових актів у сфері захисту персональних даних.

2. Працівники, які обробляють персональні дані, зобов'язані:

1) запобігати втраті персональних даних та їх неправомірному використанню;

2) не розголошувати персональні дані, які їм було довірено або які стали відомі у зв'язку з виконанням посадових обов'язків (таке зобов'язання залишається чинним після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених Законом).

Керівники структурних підрозділів Департаменту, у межах своїх повноважень, забезпечують контроль за виконанням встановлених законодавством вимог із забезпечення захисту персональних даних.

Загальна організація та координація діяльності, пов'язаної з обробкою та захистом персональних даних у Департаменті, покладається на відповідальну особу, визначену наказом директора Департаменту.

3. Відповідальна особа веде облік працівників, які мають доступ до персональних даних, обробку яких здійснює Департамент. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частин) суб'єктів, які необхідні у зв'язку з виконанням ними своїх професійних чи службових або трудових обов'язків. Такі працівники надають письмове Зобов'язання про нерозголошення персональних даних (далі - Зобов'язання), за формою згідно з додатком 1.

4. Відомості про працівників Департаменту, які надали письмове Зобов'язання заносяться до Журналу реєстрації зобов'язань про нерозголошення персональних даних, за формою згідно з додатком 2, в електронній формі (за наявності технічної можливості).

5. Датою надання права доступу до персональних даних вважається дата надання Зобов'язання відповідним працівником.

6. Датою позбавлення права доступу до персональних даних вважається дата звільнення працівника, дата переведення на посаду, виконання обов'язків

на якій не пов'язане з обробкою персональних даних або передбачає доступ до іншого переліку персональних даних.

7. Суб'єкт персональних даних має право на одержання від Департаменту будь-яких відомостей про себе без зазначення мети запиту, крім випадків, визначених законодавством.

8. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законодавством.

5. Умови передачі персональних даних третім особам

1. Доступ до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних на обробку цих даних, наданої володільцю персональних даних, або відповідно до вимог Закону.

Доступ до персональних даних третіх осіб здійснюється відповідно до вимог законодавства.

2. Про передачу персональних даних третій особі володільць персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди, якщо інше не передбачено Законом.

Повідомлення, зазначені вище, не здійснюються у разі:

передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законодавством;

здійснення обробки персональних даних в історичних, статистичних чи наукових цілях;

повідомлення суб'єкта персональних даних відповідно до вимог частини другої статті 12 Закону.

V. Заходи забезпечення захисту персональних даних

1. Обробка персональних даних в структурних підрозділах Департаменту здійснюється відповідно до законодавства.

2. Обробка персональних даних здійснюється у спосіб, що унеможливило доступ до них сторонніх осіб.

Працівники, які відповідно до посадових обов'язків здійснюють обробку персональних даних, допускаються до обробки лише після їх авторизації у відповідних системах.

3. Обробка персональних даних в інформаційних системах здійснюється відповідно до законодавства у сфері захисту інформації в інформаційно-комунікаційних системах.

З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо унеможливлення несанкціонованого доступу до персональних даних та технічного й програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

У випадку несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайної ситуації, працівники Департаменту вживають заходи, визначені Планом дій працівників Департаменту з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації) на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайної ситуації (додаток 3).

4. Факти порушень процесу обробки та захисту персональних даних підлягають документальній фіксації відповідальною особою.

Така документальна фіксація, а також опис дій працівників на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, надзвичайної ситуації здійснюється Департаментом відповідно до законодавства.

Головний спеціаліст-юрисконсульт

Володимир БОНДАР

Додаток 1

до Порядку обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)
(пункт 3 глави 4 розділу IV)

**Зобов'язання
про нерозголошення персональних даних**

Я,

(прізвище, власне ім'я, по батькові (за наявності))

(структурний підрозділ, посада)

відповідно до статті 10 Закону України «Про захист персональних даних» зобов'язуюсь не розголошувати у будь-який спосіб персональні дані інших осіб, що стали відомі мені у зв'язку з виконанням посадових обов'язків.

Підтверджую, що зобов'язання буде чинним після припинення мною діяльності, пов'язаної з обробкою персональних даних, крім випадків, встановлених законодавством.

(дата)

(підпис)

Додаток 2

до Порядку обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)
(пункт 4 глави 4 розділу IV)

Журнал реєстрації зобов'язань про нерозголошення персональних даних

№ з/п	Посада, структурний підрозділ	Прізвище, власне ім'я, по батькові (за наявності)	Дата надання зобов'язання про нерозголошення персональних даних	Дата позбавлення права доступу до персональних даних та їх обробки	Причина позбавлення права доступу до персональних даних та їх обробки (звільнення, переведення на посаду, виконання обов'язків на якій не пов'язане з обробкою персональних даних)
1	2	3	4	5	6

Додаток 3

до Порядку обробки та захисту персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації)
(пункт 3 розділу V)

План

дій працівників Департаменту з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації) на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайної ситуації

1. При виявленні ознак несанкціонованого доступу до персональних даних, володільцем яких є Департамент з питань запобігання та виявлення корупції виконавчого органу Київської міської ради (Київської міської державної адміністрації) (далі – Департамент), таких як: несанкціоноване отримання логінів і паролів, підбір паролів та ключів, працівник, який виявив дані ознаки, зобов'язаний негайно:

- припинити обробку персональних даних;
- повідомити безпосереднього керівника або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їхній обробці у Департаменті (далі – відповідальна особа);
- звернутися письмово до адміністратора системи з метою блокування доступу до облікового запису.

2. При виявленні зараження програмного забезпечення та носіїв інформації комп'ютерними вірусами працівник зобов'язаний:

- негайно припинити обробку персональних даних;
- вимкнути комп'ютерну техніку від електроживлення;
- повідомити безпосереднього керівника або відповідальну особу.

3. При вчиненні випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних тощо, необхідно:

- припинити обробку персональних даних;
- повідомити безпосереднього керівника, відповідальну особу та адміністратора системи;

4. При відмові та/або збої програмного забезпечення, за допомогою якого здійснюється обробка персональних даних у Департаменті, працівник зобов'язаний:

припинити обробку персональних даних;
повідомити безпосереднього керівника, відповідальну особу та адміністратора системи.

5. При виявленні пошкодження, втрати, викрадення документа або іншого носія персональних даних невідкладно повідомити безпосереднього керівника або відповідальну особу.

6. У разі виникнення надзвичайної ситуації (пожежа, повінь, стихійне лихо тощо) працівник має:

вжити невідкладних заходів щодо оповіщення відповідних служб реагування;

забезпечити збереження носіїв персональних даних осіб від втрати та пошкодження (за наявної можливості та у спосіб, що не загрожує життю та здоров'ю працівників);

повідомити безпосереднього керівника або відповідальну особу.

7. Про всі випадки, передбачені пунктами 1-6 цього Плану, та/або інші випадки, що призвели до пошкодження, псування, несанкціонованого доступу, знищення, поширення тощо персональних даних, працівник, який виявив даний факт, та безпосередній керівник невідкладно письмово повідомляють відповідальну особу.

8. Після отримання повідомлення відповідальна особа складає Акт про факт порушення процесу обробки та захисту персональних даних у Департаменті (далі - Акт).

Акт підписується відповідальною особою та працівником, яким виявлено (вчинено) дане порушення. Відмова від підпису працівника фіксується відповідно до вимог законодавства.

Підписаний Акт надається директору Департаменту або особі, яка виконує його обов'язки, для прийняття рішення про проведення службового розслідування або здійснення дисциплінарного провадження, повідомлення правоохоронних органів про несанкціонований доступ до персональних даних та вжиття відповідних заходів реагування.