МЕТОДИЧНІ РЕКОМЕНДАЦІЇ З ПОСИЛЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2021

ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

АСОЦІАЦІЯ МІСТ УКРАЇНИ
СПІЛЬНИМИ ЗУСИЛЛЯМИ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ З ПОСИЛЕННЯ ІНСТИТУЦІЙНОЇ СПРОМОЖНОСТІ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Посібник “Методичні рекомендації з посилення інституційної спроможності органів місцевого самоврядування щодо захисту персональних даних” написано та розповсюджується ВАОМС “Асоціація міст України” в рамках реалізації проєкту “Посилення інституційної спроможності органів місцевого самоврядування щодо захисту персональних даних”

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного Фонду «Відродження» в рамках спільної ініціативи «EU4USociety». Матеріал відображає позицію авторів і не обов’язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу.

ЗМІСТ

ПЕРЕДМОВА

Початок XXI століття ознаменувався новим витком розвитку інформаційних технологій, які стають невід'ємною частиною нашого повсякденного життя. Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а самі персональні дані знаходять все ширше використання в найрізноманітніших сферах від бізнесу до політики. Їх використання стає багатоаспектнішим і, окрім допомоги в роботі та побуті, вони можуть слугувати для декого інструментом порушення прав та свобод людини, зокрема права на приватність.

У зв'язку з цим, розвиток системи захисту персональних даних є одним із найбільш актуальних завдань, які стоять перед українським суспільством на сучасному етапі. Захист персональних даних та його вдосконалення є не просто обов'язком держави і предметом державно-правового регулювання, але повинні нерозривно розглядатися в поєднанні зі захистом прав та свобод людини, в тому числі захистом права на повагу до приватного життя.

Крім того, створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України, в тому числі пов'язаних із європейською інтеграцією нашої держави.

Конфіденційність особистих даних завжди була важливою. Тому люди здавна вішали замки на шафи для документів і придумали градацію «рівнів доступу». Але, оскільки все більше наших даних оцифровується, конфіденційність даних теж набуває все більшого значення.

В наш час, одна компанія може володіти особистою інформацією мільйонів клієнтів – даними, які їй потрібно зберігати та обробляти максимально конфіденційно, щоб персональні дані клієнтів залишалися максимально захищеними, а репутація компанії залишалася незаплямованою. Але конфіденційність даних – це не лише турбота бізнесу.

Ви, як посадова особа місцевого самоврядування, багато ставите на карту, коли йдеться про конфіденційність персональних даних. Чим більше ви знаєте про це, тим краще ви зможете захистити себе та ввірені вам дані від великої кількості ризиків.

Конфіденційність персональних даних стосується того, як слід поводитися з інформацією – або з даними – виходячи з її відносної важливості. Наприклад, ви, швидше за все, не будете проти поділитися своїм ім'ям з незнайомою вам людиною у процесі представлення/знайомства, але є й інша інформація, якою ви б не поділилися, принаймні, поки не познайомитеся з цією людиною ближче. Однак, зверніться до ЦНАПу, за довідкою, і вас, ймовірно, попросять поділитися величезною кількістю особистої інформації, яка явно виходить за межі вашого імені.

НОРМАТИВНО-ПРАВОВІ АКТИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1. Конвенція про захист осіб у зв'язку із автоматизованою обробкою персональних даних від 28.01.1981 (модернізована)

2. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27.04.2016

3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI зі змінами

4. Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних»:

Типовий порядок обробки персональних даних;

Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних;

Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів

ТЕРМІНИ, АБРЕВІАТУРИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

ВРУ – Верховна Рада України

ЄСПЛ – Європейський суд з прав людини

КМ РЄ – Комітет міністрів Ради Європи

Конвенція 108+ – Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних

ООН – Організація Об'єднаних Націй

Закон № 2297 – Закон України «Про захист персональних даних»

Закон № 2657 – Закон України «Про інформацію»

ККУ – Кримінальний кодекс України

КУпАП – Кодекс України про адміністративні правопорушення

ОМС – органи місцевого самоврядування

Уповноважений – Уповноважений Верховної Ради України з прав людини

Порядок – Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14

Типовий порядок – Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14

Порядок повідомлення Уповноваженого – Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів, затверджений Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14

ЦНАП – центра надання адміністративних послуг

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована[1]. Відповідно до Закону України «Про інформацію»[2] «інформація про фізичну особу» та «персональні дані» є тотожними поняттями. Згідно з ч. 2 цієї ж статті не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини.

[1] абз. 8 ст. 2 Закону України від 01.06.2010 № 2297-VI «Про захист персональних даних» (далі по тексту – Закон № 2297)
[2] ст. 11 Закону України від 02.10.1992 № 2657-XII «Про інформацію» (далі по тексту – Закон № 2657)

Обробка персональних даних – 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.

Конфіденційна інформація про фізичну особу – сюди належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

База персональних даних — іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних

Суб'єктом персональних даних є фізична особа, персональні дані якої обробляються.

Контрагент — одна із сторін договору у цивільно-правових відносинах.

Володілець персональних даних — фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Розпорядник персональних даних — фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця (як приклад вашої ролі як розпорядника — робота з Державним реєстром речових прав на нерухоме майно).

Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

Європейський Союз складається з 28 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів, до реалізації яких долучилися понад 60 тисяч активістів та організацій України на суму понад 200 мільйонів доларів США.
Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

ПРОБЛЕМАТИКА

Персональні дані стають все більш цінними. Крім того, навички та можливості для отримання різних типів персональних даних розвиваються надзвичайно швидко. Несанкціонована, необережна або неосвічена обробка персональних даних може завдати великої шкоди.

По-перше, слід розуміти, що метою захисту персональних даних є не просто захист даних певної особи, а захист основних прав та свобод людей, які мають відношення до цих даних. Захищаючи особисті дані, можна гарантувати, що права та свободи людей не будуть порушені.

> **Наприклад**, неправильна обробка персональних даних може спричинити ситуацію, коли людину не вірно обліковують на роботі, що в подальшому може призвести до проблем з нарахуванням загального трудового стажу та/або пенсійного забезпечення тощо, або, що ще гірше, вона може втратити поточну роботу.

По-друге, недотримання правил захисту персональних даних може призвести до ще більш жорстких ситуацій, коли можливо спричинити загрозу для життя, маніпулюючи інформацією про стан здоров'я.

По-третє, правила щодо захисту даних необхідні для забезпечення справедливої та зручної для споживачів процедури надання послуг. Дотримання правил захисту персональних даних унеможливлюють ситуацію вільного продажу персональних даних, а це означає, що люди мають більший контроль над тим, хто та які товари та/або послуги їм пропонує.

Якщо особисті дані втрачаються розпорядником та/або володільцем персональних даних, це може завдати значної шкоди репутації, а також призвести до штрафів, тому важливо дотримуватись правил захисту персональних даних.

Для забезпечення безпеки персональних даних важливо знати, які дані обробляються, чому вони обробляються і на яких підставах. Крім того, важливо визначити, які заходи безпеки застосовуються.

Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

Вперше право особи на захист від втручання інших у приватне життя, зокрема, з боку держави, закріплено у статті 12 (повага до приватного та сімейного життя) такого міжнародно-правового документу, як Загальна декларація прав людини Організації Об'єднаних Націй 1948 року.

В Україні питання врегулювання правовідносин, пов'язаних з обробкою даних та гарантування права на повагу до приватного і сімейного життя унормовано Законом України «Про захист персональних даних».

Посадові особи органів місцевого самоврядування постійно працюють із персональними даними у різних сферах суспільних відносин: у сфері соціально-економічного і культурного розвитку, в галузі житлово-комунального господарства, побутового,

торговельного обслуговування, громадського харчування, транспорту і зв'язку, у сферах освіти, охорони здоров'я, культури, молодіжної політики, фізкультури і спорту, соціального захисту населення, у сфері регулювання земельних відносин та інших.

З огляду на те, що в органах місцевого самоврядування ведуться різноманітні журнали (звернень громадян, прийому громадян, наданих послуг тощо), створюються та/або оновлюються різноманітні реєстри, наприклад, територіальної громади, ІАС «Діти», ПК «ІС «Соціальна громада» та інші, в рамках Закону № 2297 орган місцевого самоврядування виступає в тій чи іншій конкретній ситуації або володільцем, або розпорядником персональних даних.

Наприклад, Інформація про найманих працівників є базою персональних даних, оскільки особові справи, трудові книжки, копії паспортів, документів про освіту зберігаються та обробляються роботодавцем.

Згідно з визначенням, наведеним у Законі №2297, **володілець** персональних даних – це фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Тому володільцем може бути:

- той, хто визначає мету обробки, склад даних і процедури обробки;
- суб'єкт, визначений законом.

Дещо інша ситуація, коли йдеться про обробку персональних даних, державними органами влади, ОМС. У таких випадках мета обробки, склад даних, порядок їх обробки, як і те, хто володілець, часто визначено законами та/або підзаконними нормативно-правовими актами.

Наприклад, Стаття 37-1 Закону України «Про місцеве самоврядування в Україні» передбачає, що до відання виконавчих органів сільських, селищних, міських рад належать такі делеговані повноваження щодо повноважень у сфері реєстрації місця проживання фізичних осіб, як формування та ведення реєстру територіальної громади відповідно до закону. Здійснюючи свої повноваження, органи реєстрації здійснюють обробку персональних даних осіб, які зареєстровані та/або зняті з місця реєстрації на території відповідної адміністративно-територіальної одиниці, на яку поширюються повноваження відповідної сільської, селищної або міської ради.

Розпорядник персональних даних – це фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

Наприклад, Підприємства, що надають житлово-комунальні послуги, укладають договори з приватними компаніями, на підставі яких останні ведуть облік щодо кількості та якості послуг, наданих підприємством споживачам, та облік виконання споживачами оплати за вказані послуги. У вказаному договорі підприємства визначають мету обробки, склад даних, повноваження компаній щодо обробки персональних даних споживачів, зобов'язання щодо їх захисту та відповідальність за порушення договору.

Отже, компанії обробляють персональні дані споживачів за вказівкою підприємства та у визначених ним межах. Тому такі компанії є розпорядниками персональних даних.

Також варто мати на увазі, якщо згідно з законом володілець персональних даних є орган державної влади чи орган місцевого самоврядування, то розпорядником може бути підприємство державної або комунальної форми власності, що належить до сфери управління цього органу.

Одержувач персональних даних – це фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа.

Третя особа – це будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого ВРУ з прав людини, якій володілець чи розпорядник персональних даних передає персональні дані.

ВАЖЛИВО: ОМС, їх виконавчі органи здійснюють обробку персональних даних таких категорій суб'єктів персональних даних:

- Працівників
- Заявників
- Контрагентів.

Обробка персональних даних здійснюється у паперовому вигляді, за допомогою засобів Microsoft Office (Exel/word/..) та в інформаційних системах/реєстрах.

Процедури обробки, строк обробки та склад персональних даних повинні бути пропорційними меті обробки. А мета обробки персональних даних повинна бути чіткою і законною, більше того — має бути визначена до початку їх збору.

Статтею 11 Закону № 2297 визначений перелік підстав для обробки персональних даних.

ВАЖЛИВО: За загальним правилом обробка персональних даних в ОМС здійснюється на підставі закону. Проте, підставою обробки персональних даних контрагентів виступає договір, адже укладення договору резюмує надання згоди на обробку даних, необхідних для його виконання сторонами. В окремих випадках обробка персональних даних може здійснюватися і на підставі згоди суб'єкта персональних даних.

Також слід зазначити, що використання державними органами, ОМС згоди як підстави для обробки персональних даних повинно бути зведене до мінімуму. При її використанні слід враховувати, що суб'єкт має право в будь-який час відкликати свою згоду, після чого обробка повинна бути негайно припинена.

Згода суб'єкта на обробку його персональних даних повинна бути добровільною та інформованою. Згода може надаватися суб'єктом у письмовій або електронній формі, що надає змогу зробити висновок про її надання. Документи (інформація), що підтверджують надання суб'єктом згоди на обробку його персональних даних, зберігаються володільцем впродовж часу обробки таких даних.

Разом із тим із наведеного вище випливає, що не завжди від особи — суб'єкта персональних даних слід отримувати згоду на обробку його персональних даних.

ВАЖЛИВО: У випадках, визначених законом, та з метою виконання обов'язків, які покладені на вас у зв'язку із службою в ОМС, **згода від суб'єкта не потрібна**. Не потрібно відбирати згоду особи на обробку її персональних даних у зв'язку із працевлаштуванням (з метою ведення кадрового діловодства та забезпечення реалізації трудових відносин).

Тому безпідставне вимагання від особи підписати згоду на обробку її персональних даних фактично є перешкодою цій особі у реалізації її прав та свобод та захисту її інтересів.

Відповідно до частини другої статті 24 Закону № 2297, в органах державної влади, органах місцевого самоврядування, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Основне завдання такої посадової особи полягає в тому, щоб налагодити належним чином роботу з персональними даними, що обробляє володілець/розпорядник, чи вжити всіх можливих заходів з метою налагодження такої роботи (бо останнє слово все ж залишається за керівництвом володільця-розпорядника).

Компетенцію та повноваження такої особи чи підрозділу зазвичай самостійно визначає володілець у своїх внутрішніх документах. Законодавство надає лише їх мінімальний перелік.

Нижче подано примірний перелік типових функцій та повноважень структурного підрозділу/відповідальної особи, які повинні забезпечити належне виконання покладених на них завдань, які передбачають необхідність:

1) Оцінювати ризики від обробки персональних даних володільцем і надавати з урахуванням проведеного оцінення консультації володільцеві щодо належної організації процесу обробки персональних даних (і документувати цю діяльність). З цією метою відповідальна особа/підрозділ насамперед повинна, виходячи з того, яка мета обробки персональних даних володільцем, склад персональних даних, категорії суб'єктів персональних даних та операції з обробки, які проводить (планує) володілець, оцінити потенційні ризики від таких операцій. Зокрема, чи істотною буде шкода, завдана суб'єктові, від втрати (видалення) таких даних, їх незаконного чи випадкового поширення, а також чи сильна мотивація у працівників володільця, третіх осіб намагатися отримати ці дані чи незаконно комусь передати.

Виходячи з проведеного оцінення, відповідальна особа чи структурний підрозділ розробляє пропозиції щодо порядку захисту персональних даних, роботи із запитами суб'єктів і третіх осіб, визначення оптимального складу даних, що підлягатиме обробці, порядку збору персональних даних і повідомлення про це суб'єкта, порядку та рівнів доступу працівників до персональних даних, порядку документування процесів, пов'язаних з обробкою персональних даних тощо.

З цією метою в державних органах така відповідальна особа повинна бути залучена до всіх процесів, пов'язаних з розробкою нормативно правових актів, що регламентуватимуть порядок обробки персональних даних володільцем.

2) Консультувати в разі необхідності інші підрозділи володільця щодо розгляду запитів суб'єктів і третіх осіб про отримання доступу до персональних даних.

3) Проводити моніторинг процесів обробки персональних даних на предмет їх

відповідності до законодавства та Закону. Відповідальна особа чи структурний підрозділ може проводити аудит дотримання володільцем чи розпорядником законодавства про захист персональних даних. У разі виявлення порушень, а саме недотримання законодавства чи недоліків у самому законодавстві, доводити результати роботи до відома керівництва з рекомендаціями щодо усунення вказаних проблем.

4) У разі виявлення порушення прав суб'єктів персональних даних одразу доводити це до відома керівництва та Уповноваженого, надавати рекомендації керівництву щодо вжиття першочергових заходів, спрямованих на мінімізацію потенційних негативних наслідків, ініціювання розслідування інциденту, повідомлення суб'єкта/ів персональних даних, чиї права порушено.

5) Ознайомлювати керівництво та працівників володільця з вимогами чинного законодавства про захист персональних даних, змінами до законодавства, актуальними питаннями обробки персональних даних у сфері діяльності володільця, організовувати відповідні навчання для працівників.

6) Взаємодіяти з Уповноваженим, що може проявлятися в таких основних напрямках, як консультації з приводу доцільності та порядку обробки персональних даних володільцем, отримання з цього приводу роз'яснень Уповноваженого; направлення Уповноваженому для погодження розроблених проєктів нормативно-правових актів, що стосуються питань обробки персональних даних); співпраця в ході проведення Уповноваженим перевірки володільця; забезпечення вчасного та повного виконання приписів Уповноваженого.

У випадках роботи з персональними даними, які становлять особливий ризик правам людини (чутливі персональні дані[3]), володілець також визначає обов'язки та права осіб, відповідальних за організацію роботи, пов'язаної із захистом персональних даних під час їх обробки.

З метою виконання таких функцій відповідальна особа/підрозділ повинна володіти відповідними повноваженнями, а саме:

1) щодо безперешкодного доступу до приміщень, де проводиться обробка персональних даних;

2) щодо доступу до всієї інформації та документів, що стосуються обробки персональних даних, яку проводить володілець чи розпорядник, зокрема персональних даних, що містяться в базах даних володільця, журналу реєстрації обліку операцій, пов'язаних з обробкою персональних даних тощо;

3) завчасно отримувати повну інформацію щодо будь-яких операцій, пов'язаних з обробкою персональних даних, що планує володілець/розпорядник;

4) правом безпосереднього звітування керівництву володільця чи розпорядника.

ВАЖЛИВО: Для виконання вказаних вище завдань і функцій відповідальна особа чи працівники відповідного підрозділу повинні володіти відповідними навичками та досвідом, зокрема відповідною кваліфікацією у сфері захисту персональних даних і безпеки інформації. Для цього рекомендується наявність у неї відповідної освіти чи проходження такою особою відповідного спеціалізованого навчання.

[3] – Стаття 7 Закону № 2297. Особливі вимоги до обробки персональних даних

Вимога щодо підготування таких уповноважених осіб насправді достатньо значуща. У разі витоку персональних даних чи іншого порушення порядку у відповідальних осіб і представників структурних підрозділів володільця та розпорядника буде одним із факторів для встановлення ступеня вини.

Законодавство, внутрішньовідомчі документи та посадова інструкція таких відповідальних осіб або ж положення про структурний підрозділ повинні гарантувати їхню незалежність і безсторонність. Для цього рекомендується, щоб обов'язки щодо організації процедури захисту персональних даних були покладені на особу, що належить до керівного складу володільця (чи підпорядковується безпосередньо керівництву).

Якщо на відповідальну особу покладено також інші обов'язки, вони не повинні конфліктувати з її обов'язками щодо організації роботи, пов'язаної із захистом персональних даних. Крім цього, така особа має бути забезпечена всіма необхідними (зокрема фінансовими та людськими) ресурсами для ефективного виконання нею своїх обов'язків. Керівники володільця не мають права примушувати відповідальних осіб до надання тих чи інших рекомендацій чи виконання певним чином їхніх обов'язків у сфері захисту персональних даних.

ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Володілець/розпорядник персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки.

Орієнтовний перелік організаційних заходів:

1. визначення структурного підрозділу або відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці. Інформація про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, повідомляється Уповноваженому.

> **ВАЖЛИВО:** відповідно до частини другої статті 24 Закону обов'язок створення (визначення) структурного підрозділу або відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці покладено лише на органи державної влади, органи місцевого самоврядування, а також у володільців чи розпорядників персональних даних, що здійснюють обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних та підлягає повідомленню відповідно до цього Закону.

2. прийняття внутрішнього документа, який регламентує порядок та особливості обробки персональних даних в ОМС;

3. визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;

4. ведення обліку працівників, які мають доступ до персональних даних суб'єктів та визначення рівня доступу працівників до персональних даних суб'єктів.

Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків.

Усі інші працівники володільця/розпорядника мають право на повну інформацію лише стосовно власних персональних даних.

ВАЖЛИВО: Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником. 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. У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику..

5. розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

6. визначення строку зберігання персональних даних, обробка яких ведеться у паперовому вигляді та за допомогою засобів Microsoft office/IC.

В будь-якому разі персональні дані обробляються/зберігаються не довше, ніж це передбачено законодавством у сфері архівної справи та діловодства;

7. визначення процедури знищення персональних даних, строк зберігання яких закінчився;

8. регулярне навчання співробітників, які працюють із персональними даними.

Варто зазначити, що Закон України «Про захист персональних даних» – це рамковий документ. Його положення регулюють правові відносини, пов'язані із захистом та обробкою персональних даних у всіх сферах суспільних відносин. З цих же причин Закон № 2297 не може детально визначати порядок та процедуру обробки персональних даних у всіх вказаних сферах. У зв'язку з цим, кожна галузь права і сфера діяльності містить (і повинна містити) свої положення, які регламентують особливості обробки персональних даних у відповідній сфері суспільного життя.

Тобто, органи місцевого самоврядування, як володільці/розпорядники персональних даних самостійно визначають порядок обробки персональних даних, ураховуючи специфіку обробки персональних даних у різних сферах своєї діяльності, відповідно до вимог, визначених чинним законодавством.

Такий внутрішній документ органу місцевого самоврядування (Положення, Порядок) повинен врегульовувати ті питання, що не охоплюються нормативно-правовими актами, а також деталізувати їх положення та пристосовувати до реалій роботи відповідного державного органу, органу місцевого самоврядування.

Виходячи із Закону та Типового порядку, внутрішні документи органів місцевого самоврядування, що регламентують обробку персональних даних, повинні містити та якомога чіткіше визначати:

1) інформацію про володільця персональних даних. Якщо їх декілька – інформацію про кожного, а також співвідношення їхніх повноважень;

2) інформацію про розпорядника персональних даних (у разі наявності);

3) мету обробки персональних даних;

4) категорії суб'єктів, чиї персональні дані обробляють;

5) склад персональних даних, що їх обробляють;

6) порядок і спосіб збору персональних даних;

7) порядок верифікації та видалення персональних даних;

8) строк зберігання персональних даних;

9) гарантії дотримання прав суб'єктів персональних даних:

– порядок реалізації права суб'єкта на доступ до своїх персональних даних;

– порядок надання інформації щодо порядку обробки персональних даних;

– порядок надання інформації щодо того, яким третім особам передавали дані;

– порядок розгляду звернень щодо видалення чи зміни персональних даних;

– порядок розгляду заперечень проти обробки персональних даних;

– порядок розгляду скарг на незаконність обробки персональних даних;

10) третіх осіб, яким передають / яким надають доступ до персональних даних;

11) проведення транскордонної передачі даних (у разі наявності): підстави, порядок та отримувачів;

12) технічні та організаційні засоби захисту персональних даних (нижче наведено приблизний перелік):

– розмежування рівнів доступу працівників володільця до персональних даних та їхніх повноважень щодо обробки;

– порядок та умови отримання працівниками доступу до персональних даних;

– ведення обліку операцій обробки персональних даних (фіксація в журналі відомостей щодо особи, яка проводить операцію, характер дій щодо персональних даних (перегляд, копіювання, друк, передача тощо), щодо яких персональних даних, час таких дій тощо);

– тестування та оновлення системи технічного захисту;

– інше.

13) алгоритм дій на випадок випадкової втрати чи зміни персональних даних, їх незаконної обробки.

Відповідно до статті 9 Закону № 2297 володілець персональних даних має повідомити Уповноваженого про обробку персональних даних, **яка становить особливий ризик** для прав і свобод суб'єктів персональних даних (це дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних), упродовж тридцяти робочих днів з дня початку такої обробки.

Згідно з Порядком повідомлення Уповноваженого обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів, — це будь-яка дія або

сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, яка здійснюється відносно таких «чутливих» персональних даних.

Наприклад, В період запровадження у 2020 році карантинних обмежень у зв'язку з пандемією Covid-2019 голова територіальної громади на одній з нарад доручив керуючому справами щодня до 10.00 год. надавати список працівників, які захворіли на коронавірусну хворобу та які контактували з хворими для забезпечення їх самоізоляції. Збір та обробка даної інформації саме у такій формі є грубим порушенням законодавства у сфері захисту персональних даних. Крім цього, збиралась та оброблялась інформація про стан здоров'я працівників, яка становить особливий ризик правам людини. У цьому випадку, керівництву ОМС необхідно було додержуватися процедури обробки «чутливих» персональних даних, яка визначена Законом № 2297 та Порядком повідомлення Уповноваженого.

Згідно ст. 8 Закону № 2297, суб'єкт персональних даних має право:

– знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані

– на доступ до своїх персональних даних

– отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних

– пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних

– пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними

– на захист своїх персональних даних 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 із скаргами на обробку своїх персональних даних до Уповноваженого або до суду

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних

– вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди

– відкликати згоду на обробку персональних даних

– знати механізм автоматичної обробки персональних даних

– на захист від автоматизованого рішення, яке має для нього правові наслідки. Суб'єкт персональних даних має право пред'являти вмотивовану вимогу володільцю персональних даних щодо заборони обробки своїх персональних даних (їх частини) та/або зміни їх складу/змісту. Така вимога розглядається володільцем впродовж 10 днів з моменту отримання.

ВАЖЛИВО: Суб'єкт персональних даних повідомляється (письмово) про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані (ст. 12 Закону № 2297).

ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ

Порядок доступу до персональних даних третіх осіб передбачений ст. 16 Закону № 2297 та визначається умовами згоди суб'єкта персональних даних, наданої володільцю персональних даних на обробку цих даних, або відповідно до вимог закону.

Порядок доступу третіх осіб до персональних даних, які знаходяться у володінні розпорядника публічної інформації, визначається Законом України від 13.01.2011 № 2939-VI «Про доступ до публічної інформації», крім даних, які отримує Міністерство фінансів України від інших органів під час здійснення повноважень з контролю за дотриманням бюджетного законодавства в частині моніторингу пенсій, допомог, пільг, субсидій, інших соціальних виплат.

Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу до персональних даних володільцю персональних даних. У запиті зазначаються:

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 базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

перелік персональних даних, що запитуються;

мета та/або правові підстави для запиту.

Строк вивчення запиту на предмет його задоволення не може перевищувати 10-ти робочих днів з дня його надходження. (протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акт). Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Відповідно до ч. 1 ст. 24 Закону № 2297, володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у т. ч. незаконного знищення чи доступу до них.

Відповідно до ст. 22 Закону № 2297, контроль за дотриманням законодавства про захист персональних даних здійснюють уповноважений Верховної Ради України з прав людини у сфері захисту персональних даних (далі — Уповноважений) та/або суди.

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ

Громадяни, посадові особи, громадяни – суб'єкти підприємницької діяльності притягуються до адміністративної відповідальності[4] за вчинення таких правопорушень:

– неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються;

– неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних;

– ухилення від державної реєстрації бази персональних даних;

– недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них;

– невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних щодо усунення порушень законодавства про захист персональних даних.

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ

За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності[5].

[4] – стаття 188-39 Кодексу України про адміністративні правопорушення
[5] – стаття 182 Кримінального кодексу України

ЗРАЗКИ ДОКУМЕНТІВ

Орієнтовний перелік нормативно-правових та розпорядчих актів виконавчих органів територіальної громади, які допоможуть унормувати питання роботи із захистом персональними даними:

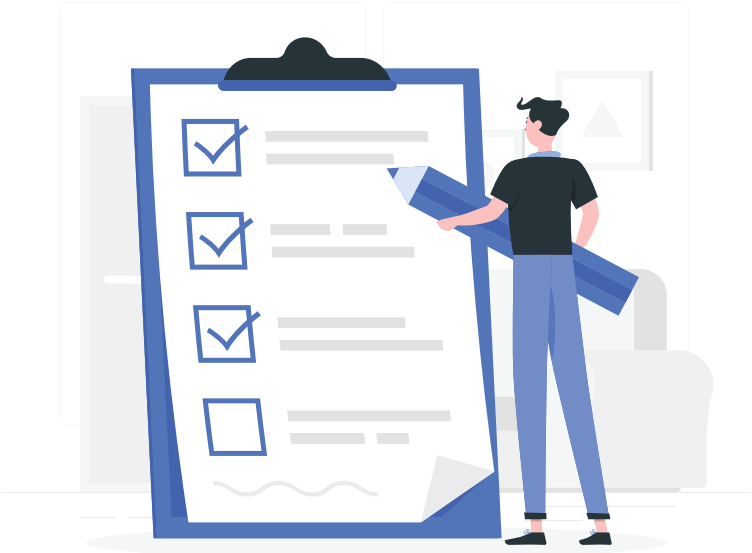
1. рішення виконавчого комітету громади або розпорядження сільського, селищного, міського голови щодо:

   – затвердження Порядку/Положення про обробку персональних даних у виконавчому комітеті та/або апараті ради та/або виконавчих органах;

   – призначення відповідальної особи за організацію роботи, пов'язаної із захистом персональних даних

2. Журнал обліку працівників, які мають доступ до персональних даних
3. Зобов'язання про нерозголошення персональних даних
4. Повідомлення про обробку персональних даних
5. Журналу обліку запитів на доступ до персональних даних
6. Положення про порядок обробки і захисту персональних даних

Отже, у додатках наводимо проєкти документів з переліку. Слід врахувати, при впровадженні, організаційну структуру саме вашої громади, наявність виконавчих органів, комунальних підприємств тощо.



РОЗ'ЯСНЕННЯ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ[6]:

– Рекомендації Уповноваженого Верховної Ради України з прав людини щодо захисту персональних даних під час дистанційного надання освітніх послуг

– Уповноважений наголошує на тому, що ненадання особою згоди на обробку персональних даних не може бути перешкодою для реалізації права на працю

– Рекомендації Уповноваженого Верховної Ради України з прав людини щодо дотримання права на приватність під час встановлення і використання систем відеоспостереження у громадських місцях

– Роз'яснення щодо надання копій пенсійних справ померлих родичів

– Рекомендації органам місцевого самоврядування щодо здійснення відеоспостереження в громадських місцях

– Роз'яснення щодо порядку доступу до персональних даних за запитами державних органів

– Роз'яснення щодо доступу до персональних даних за адвокатськими запитами

– Кроки для захисту персональних даних

– Права суб'єкта персональних даних

– типові порушення законодавства про захист персональних актів та рекомендації щодо їх усунення

– Рекомендації щодо застосування законодавства про захист персональних даних для органів реєстрації (виконавчих органів сільської, селищної або міської ради, центрів надання адміністративних послуг)

– Роз'яснення щодо деяких питань обробки персональних даних при дистанційному укладенні правочинів в інформаційно-телекомунікаційних мережах

ВАЖЛИВО: За посиланням https://study.ed-era.com/ru/courses/course/#!372 рекомендуємо переглянути онлайн-курс «Захист персональних даних», розроблений Уповноваженим Верховної Ради України з прав людини та Офісом Ради Європи у співпраці зі студією онлайн-освіти EdEra, який включає поглиблену версію курсу для держслужбовців та людей, які працюють із персональними даними. Слухачі курсу матимуть змогу отримати відповідний сертифікат про підвищення кваліфікації.

[6] https://ombudsman.gov.ua/ua/page/zpd/zakonodavstvo/normativno-pravovi-akti/

ПРОЄКТ РІШЕННЯ ВИКОНАВЧОГО КОМІТЕТУ АБО РОЗПОРЯДЖЕННЯ/ НАКАЗУ СІЛЬСЬКОГО, СЕЛИЩНОГО, МІСЬКОГО ГОЛОВИ

ВИКОНАВЧИЙ КОМІТЕТ

РІШЕННЯ

від __.__.202_ № __

_____

Про затвердження Порядку обробки персональних

даних у виконавчому комітеті _____ ради

Відповідно до ст.. Закону України «Про місцеве самоврядування в Україні», статті 24 Закону України “Про захист персональних даних” та Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року N 1/02-14,

ВИРІШИВ:

1. Затвердити Порядок (Положення) обробки персональних даних у виконавчому комітеті _____ ради, що додається.

2. Визначити відповідальним за організацію роботи, пов’язану із захистом персональних даних при їх обробці _____ (посада ПІП).

3. Особам, відповідальним за організацію роботи з питань захисту персональних даних в виконавчому комітеті, забезпечити дотримання Порядку обробки персональних даних у виконавчому комітеті _____ ради, затвердженого цим розпорядженням.

4. Відповідальній особі (посада ПІП) забезпечити/вжити заходів щодо:

-

-

5. Контроль за виконанням цього розпорядження покласти на _____

_____ (підпис) _____

ПРОЄКТ ЖУРНАЛУ ОБЛІКУ ПРАЦІВНИКІВ, ЯКІ МАЮТЬ ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ

Журнал обліку працівників,

які мають доступ до персональних даних

№№	П. І. Б. співробітника,	Посада	Дата надання права роботи з персональними даними, № наказу	Дата звільнення/ переведення на іншу посаду, № наказу
1	2	3	4	5
1	Ісаков Ігор Вікторович	Інспектор з кадрів	12.11.2020, №119-дн	20.10.2021, №18-дн
…	…	…	…	…

ПРОЄКТ ЗОБОВ'ЯЗАННЯ ПРО НЕРОЗГОЛОШУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

КОМУ (посада, виконавчий орган, ПІБ)

КОГО (посада, виконавчий орган, ПІБ)

Зобов'язання

про нерозголошення персональних даних

Відповідно до статті 10 Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI зобов'язуюсь не допускати розголошення у будь-який спосіб персональних даних, які мені було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення мною діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

«____» _____ 201___ р. _____

(підпис)

ПРОЄКТ ПОВІДОМЛЕННЯ ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

ПОВІДОМЛЕННЯПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ _____ *(стосується працівників)*

Відповідно до вимог Закону від 01.06.10 р. № 2297-VI «Про захист персональних даних» повідомляємо, що в цілях реалізації трудових правовідносин та з метою ведення кадрового діловодства та забезпечення реалізації трудових відносин _____ (володілець персональних даних із зазначенням адреси та реквізитів) проводить обробку персональних даних працівників за правилами чинного законодавства.

Виконується обробка таких персональних даних співробітників:

1. Паспортні дані, ідентифікаційний код.
2. Дані про освіту.
3. Дані про трудову діяльність.
4. Дані про військовий облік (за наявності).
5. Дані про стан здоров'я (відповідно до ст. 24 КЗпП).
6. Дані про сімейний стан, а також про склад сім'ї.
7. Адреса реєстрації, а також адреса фактичного проживання, номер телефону.
8. Відомості про співробітника, які підтверджують його право на отримання пільг і компенсацій (інвалідність, статус матері-одиначки тощо).

Персональні дані обробляються у інформаційних системах: _____

Зазначені персональні дані знаходяться за адресою:_____

Передаються вказані персональні дані в установленому законодавством порядку до органів фіскальної служби, Пенсійного фонду, служби зайнятості, а також до інших органів державної влади і місцевого самоврядування відповідно до законодавства.

_____ вживає заходи із захисту персональних даних працівників від несанкціонованої обробки. У зв'язку із цим обробка персональних даних здійснюється виключно працівниками, які підписали Зобов'язання про нерозголошення персональних даних, що стали їм відомі в результаті виконання своїх посадових обов'язків.

Згідно зі ст. 8 Закону № 2297-VI «Про захист персональних даних» кожний працівник/ця має право: знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом; отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані; на доступ до своїх персональних даних отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних; пред'являти вмотивовану

вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними; на захист своїх персональних даних 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 із скаргами на обробку своїх персональних даних до Уповноваженого або до суду; застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних; вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди; відкликати згоду на обробку персональних даних; знати механізм автоматичної обробки персональних даних; на захист від автоматизованого рішення, яке має для нього правові наслідки.

_____ (підпис) _____

ПРОЄКТ ЖУРНАЛУ ОБЛІКУ ЗАПИТІВ НА ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ

ЖУРНАЛ

обліку запитів на доступ до персональних даних

№ з/п	ПІБ (найменування) особи, що звернулася із запитом	Дата звернення	База персональних даних, стосовно якої подається запит	Перелік персональних даних, що запитуються	Мета та/ або правові підстави для запиту	Результати розгляду запиту (дата та номер відповіді, задоволено/
1	2	3	4	5	6	7

ПРОЄКТ ПОЛОЖЕННЯ ПРО ПОРЯДОК ОБРОБКИ І ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

ПОЛОЖЕННЯ ПРО ПОРЯДОК ОБРОБКИ І ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1. Поняття, терміни і склад персональних даних

1.1. Терміни у цьому Порядку вживаються у значенні, наведеному в Законі України «Про захист персональних даних» і Типовому порядку обробки персональних даних, затвердженому наказом Уповноваженого Верховної Ради України від 08.01.2017 року №1/02-14:

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

– 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;

– 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;

– 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;

– 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.

1.2. Складові які утворюють персональні дані:

– прізвище, ім'я, по-батькові;

– дата народження;

– місце народження;

– ідентифікаційний податковий номер;

– адреса місця проживання (за паспортом або фактичне) та дата реєстрації за місцем проживання або за місцем перебування;

– домашній та/або мобільний номер телефону;

– фотографія;

– тощо, що не суперечать законодавству України.

1.3. Документи, які можуть зберігати персональні дані:

– паспорт громадянина;

– трудовий договір;

– відомості про трудовий та/або загальний стаж;

– декларація про доходи;

– особові справи та трудові книжки співробітників;

– оригінали та/або копії наказів щодо особового складу;

– особові справи, які містять матеріали з підвищення кваліфікації та перепідготовки співробітників, їх атестації, службових розслідувань;

– відомості щодо заробітної плати, доходів та винагород працівників;

– відомості щодо наявності адміністративних правопорушень;

– відомості про майно суб'єкта персональних даних (майнове становище, включаючи транспорт, нерухомість, кредити та/або позики);

– відомості про номер і серію страхового свідоцтва державного пенсійного страхування;

– відомості про соціальні пільги;

– відомості про освіту;

– відомості про склад сім'ї;

– відомості про сімейний стан;

– відомості про військовий облік;

– відомості про спеціальність;

– довідка про наявність судимостей;

– відомості щодо заборгованості за комунальні послуги;

– відомості щодо заборгованості за оренду землі або комунальної власності;

– відомості щодо опіки; піклування та усиновлення дітей;

– інші, що не суперечать законодавству України.

2. Загальні положення

2.1. Цей Порядок встановлює загальні вимоги до організаційних та технічних заходів захисту персональних даних під час їх обробки у базах персональних даних володільцем та розпорядником персональних даних, яких є виконавчі органи територіальної громади (далі – володілець/розпорядник).

2.2 Обробка персональних даних, володільцем/розпорядником яких є територіальна громада, здійснюється з метою:

– забезпечення реалізації конституційного права громадян на звернення, вирішення питань, порушених в заявах, пропозиціях або скаргах громадян, адміністративно-

правових відносин, підготовки статистичної, адміністративної та іншої інформації відповідно до Конституції України, Законів України “Про Уповноваженого Верховної Ради України з прав людини”, “Про звернення громадян”, “Про доступ до публічної інформації”, постанови Кабінету Міністрів України від 14.04.97 N 348 “Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об’єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форми власності, в засобах масової інформації”;

– забезпечення проходження служби в органах місцевого самоврядування та трудових відносин, управління персоналом, військового та податкового обліків;

– проведення моніторингу та оцінки якості послуг.

2.3. Підставами для обробки персональних даних є:

– згода суб’єкта персональних даних на обробку його персональних даних (ДОДАТОК);

– дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

– укладення та виконання 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;

– захист життєво важливих інтересів суб’єкта персональних даних;

– необхідність виконання обов’язку володільця персональних даних, який передбачений законом.

2.4. Обробка персональних даних здійснюється на підставі відповідних положень Конституції України, Законів України «Про захист персональних даних», «Про адміністративні послуги», «Про електронні довірчі послуги» та інших законів України з метою здійснення повноважень володільця/розпорядника.

2.5. Режим безпечної обробки персональних даних знімається у випадках знеособлювання або після закінчення 75-річного терміну зберігання документів, якщо інше не визначено законом.

2.6. Посадові особи, в обов’язок яких входить ведення баз персональних даних, зобов’язані забезпечити кожному суб’єкту персональних даних можливість ознайомлення з документами і матеріалами, що безпосередньо зачіпають його права і свободи, якщо інше не передбачено законом.

2.7. Персональні дані не можуть бути використані з метою заподіяння майнової та моральної шкоди суб’єктам персональних даних. Обмеження прав суб’єктів персональних даних на основі використання інформації про їх соціальне походження, про расову, національну, мовну, релігійну та партійну приналежності заборонено і карається відповідно до законодавства.

2.8. Посадові особи володільця/розпорядника, які відповідно до своїх повноважень, володіють інформацією про суб’єктів персональних даних, отримують і використовують її, несуть відповідальність відповідно до законодавства України за порушення режиму захисту, обробки та порядку використання цієї інформації.

2.9. Це положення є обов’язковим для виконання всіма співробітниками виконавчих органів громади, які мають доступ до персональних даних суб’єкта персональних даних.

2.10. Володільцем баз персональних даних, які пов'язані с діяльністю органів місцевого самоврядування, є виконавчі органи територіальної громади.

2.11. Кожне управління або окремий структурний підрозділ виконкому, які підпорядковуються голові, заступникам голови або керуючому справами виконкому, комунальні підприємства ради визначають посадову особу, відповідальну за організацію роботи з базами персональних даних.

2.12. Забороняється створення будь-яких баз персональних даних без погодження з відповідальним за ведення баз персональних даних.

2.13. Питання захисту персональних даних, не врегульовані даним Положенням, вирішуються згідно з нормами чинного законодавства України.

3. Обов'язки володільця/розпорядника

3.1. З метою забезпечення прав і свобод людини і громадянина відповідальний працівник володільця/розпорядника при обробці персональних даних зобов'язана/ний дотримуватися наступних загальних вимог:

– обробка персональних даних може здійснюватися виключно з метою забезпечення дотримання законів та інших нормативних правових актів;

– при визначенні обсягу і змісту оброблюваних персональних даних необхідно керуватися Конституцією України, Кодексом законів про працю та іншими законами України;

– усі персональні дані слід отримувати у суб'єкта персональних даних. Якщо персональні дані можливо одержати тільки в третьої сторони, то суб'єкт повинен бути повідомлений про це заздалегідь і від нього має бути отримано письмову згоду на це;

– володілець/розпорядник не має права отримувати та обробляти персональні дані суб'єкта про його расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також дані, що стосуються здоров'я чи статевого життя;

– захист персональних даних суб'єкта від їхнього неправомірного використання або втрати забезпечується володільцем/розпорядником за рахунок місцевого бюджету.

4. Права суб'єкта персональних даних

4.1. Знати мету обробки персональних даних.

4.2. Вимагати виключення або виправлення невірних або неповних персональних даних.

4.3. Вільний безкоштовний доступ до своїх персональних даних, включаючи право на отримання копій будь-якого запису, який містить її/його персональні дані.

4.4. Знати про місцезнаходження бази персональних даних, яка містить її/його персональні дані, її призначення та найменування, місцезнаходження та/або місце проживання (перебування) володільця/розпорядника цієї бази.

4.5. Отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються її/його персональні дані у відповідній базі персональних даних.

4.6. Отримувати не пізніш як за тридцять календарних днів з дня надходження запиту,

крім випадків, передбачених законом, відповідь про те, чи зберігаються її/його персональні дані у відповідній базі персональних даних, а також отримувати зміст її/його персональних даних, які зберігаються.

4.7. Відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для обробки є згода суб'єкта персональних даних.

4.8. Застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.

5. Збір, обробка та зберігання персональних даних

5.1. До збору, обробки, передачі та зберігання персональних даних суб'єкта можуть мати доступ відповідальні співробітники виконавчих органів територіальної громади, визначені окремим розпорядчим документом.

5.2. При передачі персональних даних суб'єкта володілець/розпорядник повинен дотримуватися наступних вимог:

– не повідомляти персональні дані суб'єкта третій стороні без письмової згоди суб'єкта, за винятком випадків, коли це необхідно з метою попередження загрози життю та здоров'ю суб'єкта або в інтересах національної безпеки, економічного добробуту та прав людини;

– не повідомляти персональні дані суб'єкта в комерційних цілях без її/його письмової згоди;

– дозволяти доступ до персональних даних суб'єктів тільки спеціально уповноваженим особам, при цьому зазначені особи повинні мати право отримувати тільки ті персональні дані суб'єкта, які необхідні для виконання конкретних функцій.

5.3. Усі заходи конфіденційності при зборі, обробці та зберіганні персональних даних суб'єкта поширюються як на паперові, так і на електронні (автоматизовані) носії інформації.

5.4. Забороняється відповідати на запити пов'язані з передачею персональних даних телефоном та/або факсом та/або іншими засобами голосового зв'язку.

6. Доступ до персональних даних

6.1. Право доступу до персональних даних мають відповідальні співробітники виконавчих органів територіальної громади, визначені окремим розпорядчим документом.

6.2. Доступ до персональних даних третім особам не надається, якщо вони відмовляються письмово взяти на себе зобов'язання щодо виконання вимог Закону України «Про захист персональних даних».

6.3. Наглядово-контролюючі органи та/або правоохоронні органи мають доступ до інформації тільки у сфері та межах своєї компетенції.

7. Захист персональних даних

7.1. Володілець/розпорядник вживає заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

7.2. Окремим розпорядчим документом визначає перелік і склад заходів, спрямованих

на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки.

7.3. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадковій втраті або знищенню, незаконній обробці чи доступу до персональних даних.

7.4. Володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів. Володілець/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб'єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків. Такий рівень доступу визначається, зокрема, змістом посадової інструкції.

7.5. Усі інші працівники володільця/розпорядника мають право на повну інформацію лише стосовно власних персональних даних.

7.6. Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних (ДОДАТОК), які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

7.8. Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником.

7.9. 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.

7.10. У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику.

7.11. Володілець веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем/розпорядником зберігається інформація про:

– дату, час та джерело збирання персональних даних суб'єкта,

– зміну персональних даних,

– перегляд персональних даних,

– будь-яку передачу (копіювання) персональних даних суб'єкта,

– дату та час видалення або знищення персональних даних.

Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

7.12 Вимоги щодо обліку та збереження інформації про перегляд персональних даних не поширюється на володільця, який здійснює обробку персональних даних в реєстрі, який є відкритим для населення в цілому.

7.13. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

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

7.15. Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані.

7.16. Взаємодія з Уповноваженим Верховної Ради України з прав людини здійснюється в порядку, визначеному Законом України «Про Уповноваженого Верховної Ради України з прав людини».

8. Відповідальність за розголошення персональних даних

8.1. Керуючий справами володільця/розпорядника несе відповідальність за нерозголошення персональної інформації, яка зберігається в базах персональних даних.

8.2. Керівник, який дозволяє доступ співробітника до конфіденційного документа, несе персональну відповідальність за даний дозвіл.

8.3. Кожен співробітник організації, який отримує для роботи конфіденційний документ, несе одноосібну відповідальність за збереження носія і конфіденційність інформації. При прийомі на роботу відділ кадрів отримує згоду у кожного співробітника на збір та обробку його персональних даних (ДОДАТОК).

8.4. Особи, винні в порушенні встановленого законом порядку збирання, зберігання, використання або поширення інформації про суб'єктів персональних даних, несуть дисциплінарну, адміністративну або кримінальну відповідальність згідно з законами України.

8.5. Усі особи зазначені в п. 6.1. цього Положення, пов'язані з отриманням, обробкою та захистом персональних даних, зобов'язані укласти «Угоду про нерозголошення персональних даних» (ДОДАТОК) та до їх посадових інструкцій повинно бути додано пункт про відповідальність.

КОЛЕКТИВ АВТОРІВ

Олександр Лашко, координатор проєктів Асоціації міст України

Людмила Непийвода, Регіональний представник Уповноваженого Верховної Ради України з прав людини в Івано-Франківській області (підготовка матеріалів та редагування на громадських засадах)

Юрій Стефанчук, виконавчий директор Івано-Франківського регіонального відділення Асоціації міст України

ВИКОРИСТАНІ ДЖЕРЕЛА:

– Рада Європи, 2021. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА ПРАКТИЧНІ АСПЕКТИ, Науково-практичний посібник Маркіян Бем, Іван Городиський

– https://i.factor.ua/ukr/journals/ms/2018/april/issue-4/article-35777.html «І знов про персональні дані», МІСЦЕВЕ САМОВРЯДУВАННЯ, КВІТЕНЬ, 2018/№ 4

– Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2019 рік: https://ombudsman.gov.ua/ua/page/secretariat/docs/presentations/&page=4

– Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2020 рік: https://ombudsman.gov.ua/ua/page/secretariat/docs/presentations/&page=5