



УЖГОРОДСЬКА МІСЬКА РАДА

ВИКОНАВЧИЙ КОМІТЕТ

Р І Ш Е Н Н Я

17.09.2021

Ужгород

№ 410

Про порядок обробки та захисту персональних даних в Ужгородській міській раді

Керуючись статтею 52, частиною шостою статті 59 Закону України «Про місцеве самоврядування в Україні», законами України «Про захист персональних даних», «Про інформацію», «Про звернення громадян», «Про доступ до публічної інформації», наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних», беручи до уваги розпорядження міського голови 30.07.2021 № 145-р «Про відповідальну особу з організації роботи із захисту персональних даних при їх обробці», з метою реалізації державної політики в сфері захисту персональних даних, врегулювання відносин, пов'язаних із їхнім захистом під час обробки, виконком міської ради **ВИРІШИВ:**

1. Затвердити Положення про порядок обробки та захисту персональних даних в Ужгородській міській раді, що додається.
2. Затвердити Примірний план дій працівників структурних підрозділів виконавчих органів міської ради на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій згідно з додатком.
3. Керівникам виконавчих органів міської ради з метою забезпечення захисту персональних даних у відповідних базах персональних даних вживати комплекс організаційних заходів, викладених у Положенні.
4. Контроль за виконанням рішення покласти на керуючого справами виконкому І. Фартушка.

Міський голова

Богдан АНДРІЙВ

Положення про порядок обробки та захисту персональних даних в Ужгородській міській раді

1. Загальні відомості

1.1. Положення про порядок обробки та захисту персональних даних в Ужгородській міській раді (далі – Положення) визначає комплекс організаційних та технічних заходів для забезпечення захисту персональних даних від несанкціонованого доступу, витоку інформації, неправомірного використання або втрати даних під час обробки.

1.2. Положення розроблено на підставі законів України «Про захист персональних даних», «Про інформацію», «Про звернення громадян», «Про доступ до публічної інформації», наказу Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних».

1.3. Положення є обов'язковим для виконання працівниками структурних підрозділів виконавчих органів міської ради, які мають доступ до персональних даних та обробляють персональні дані суб'єктів звернень.

1.4. Усі терміни у цьому Положенні визначаються відповідно до закону та порядку.

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

1.6. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

2. Мета обробки персональних даних

2.1. Обробка персональних даних у виконавчих органах міської ради проводиться з метою забезпечення реалізації конституційного права громадян на звернення, трудових, адміністративно-правових та інших відносин, вирішення питань, порушених у заявах, пропозиціях або скаргах громадян, інших випадках, передбачених законодавством.

2.2. Обробка персональних даних здійснюється відкрито і прозоро, із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

2.3. У разі зміни визначеної мети обробки персональних даних на нову мету, яка є не сумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом.

3. Склад персональних даних

3.1. Склад персональних даних визначається відповідно до вимог чинного законодавства, що регулює діяльність Ужгородської міської ради та її виконавчих органів щодо правового, організаційного, матеріально-технічного та іншого забезпечення діяльності, підготовки аналітичних, інформаційних та інших матеріалів, звернення громадян тощо, та інші дані, які особи добровільно, за власним бажанням, надають про себе.

3.2. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їхньої обробки.

3.3. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

4. Підстави для обробки персональних даних

4.1. Підставами для обробки персональних даних є:

- згода суб'єкта персональних даних на обробку його персональних даних;
- 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;
 - необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

4.2. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

4.3. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

4.4. Збирання персональних даних є складовою процесу їхньої обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

4.5. Суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

- в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;
- в інших випадках протягом тридцяти робочих днів із дня збору персональних даних.

5. Обов'язки працівників структурних підрозділів виконавчих органів міської ради, які обробляють персональні дані суб'єктів звернень

5.1. Працівники структурних підрозділів виконавчих органів міської ради, які обробляють персональні дані суб'єктів звернень мають бути обізнані з вимогами закону та інших нормативно-правових актів у сфері захисту персональних даних.

5.2. Працівники зобов'язані:

- використовувати персональні дані лише відповідно до посадових чи службових обов'язків, запобігати втраті персональних даних або їхньому неправомірному використанню;

- не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням посадових чи службових обов'язків (крім випадків, передбачених законом) при цьому таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом;

- терміново повідомляти безпосереднього керівника та відповідальну особу, що організує роботу, пов'язану із захистом персональних даних при їх обробці, у разі:

 - втрати або неумисного знищення носіїв інформації з персональними даними;

 - втрати ними ключів від приміщень, сейфів, шаф, де зберігаються персональні дані;

 - якщо ідентифікаційні дані для входу в Автоматизовану систему стали відомі іншим особам, за винятком працівників управління програмного та комп'ютерного забезпечення Ужгородської міської ради;

 - виявлення спроби несанкціонованого доступу до персональних даних;

 - в інших випадках, що загрожують або призвели до пошкодження, псування, несанкціонованого доступу, знищення, поширення тощо персональних даних;

 - при звільненні з роботи або переведенні на іншу посаду своєчасно передати керівнику структурного підрозділу, носії інформації, що містять відомості про персональні дані, які були отримані або створені особисто чи спільно з іншими працівниками під час виконання посадових обов'язків.

5.3. Працівники структурних підрозділів виконавчих органів міської ради, які мають доступ до баз персональних даних відповідно до своїх посадових обов'язків, надають письмове зобов'язання про нерозголошення персональних даних, які їм були довірені або стали відомі у зв'язку з виконанням службових обов'язків за формою, згідно з додатком 1 до цього Положення.

5.4. Зобов'язання про нерозголошення персональних даних реєструються

у Журналі реєстрації зобов'язань про нерозголошення персональних даних за формою, згідно з додатком 2 до цього Положення.

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

5.6. 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.

6. Порядок та документальне забезпечення обробки персональних даних суб'єктів звернень у виконавчих органах міської ради

6.1. Обробка персональних даних здійснюється:

- у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк не більше, ніж це необхідно відповідно до мети їхньої обробки, не довше, ніж це передбачено законодавством у сфері архівної справи та діловодства;

- у разі виявлення відомостей про особу, які не відповідають дійсності, такі відомості мають бути невідкладно змінені або знищені.

6.2. Використання персональних даних працівниками структурних підрозділів виконавчих органів міської ради при розгляді звернень громадян передбачає будь-які дії працівників щодо обробки цих даних, дії щодо їхнього захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

Використання персональних даних працівниками здійснюється у разі створення ними умов для захисту цих даних. Забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних із такими даними.

Використання персональних даних працівниками, суб'єктів відносин, пов'язаних із персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків.

Доступ до персональних даних осіб – суб'єктів звернень, внесених до Автоматизованої системи та картотек персональних даних, мають міський голова, його заступники, керуючий справами виконкому, відповідальна особа, інші працівники структурних підрозділів виконавчих органів міської ради, відповідно до своїх посадових обов'язків в обсязі, необхідному для виконання таких обов'язків.

6.3. Доступ до персональних даних суб'єкта персональних даних та третіх осіб.

Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю персональних даних на обробку цих даних, або відповідно до вимог закону.

Поширення персональних даних суб'єктів звернень третім особам допускається в мінімально необхідних обсягах і лише з метою виконання завдань, які відповідають об'єктивній причині поширення відповідних даних.

Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог закону або не спроможна їх забезпечити.

7. Знищення персональних даних

7.1. Персональні дані видаляються або знищуються у порядку, встановленому відповідно до вимог закону.

7.2. Видалення та знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних.

7.3. Персональні дані підлягають видаленню або знищенню у разі:

- закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;
- припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;
- видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;
- набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

7.4. Персональні дані, зібрані з порушенням вимог Закону, підлягають видаленню або знищенню в установленому законодавством порядку.

7.5. Відповідальність за дотримання закону при знищенні або видаленні персональних даних покладається на керівників виконавчих органів міської ради.

8. Захист персональних даних суб'єктів звернень при їх обробці в Автоматизованій системі

8.1. Право доступу до Автоматизованої системи надається працівникам структурних підрозділів виконавчих органів міської ради, які відповідно надали письмове зобов'язання щодо нерозголошення персональних даних.

8.2. Автоматизована система в обов'язковому порядку забезпечується антивірусним захистом та засобами безперебійного живлення елементів системи. Відповідні заходи забезпечує управління програмного та комп'ютерного забезпечення Ужгородської міської ради.

**Примірний план
дій працівників структурних підрозділів виконавчих органів міської ради
на випадок несанкціонованого доступу до персональних даних,
пошкодження технічного обладнання, виникнення надзвичайних ситуацій**

1. При виявленні ознак несанкціонованого доступу до персональних даних суб'єктів звернень до виконавчих органів міської ради, таких як: несанкціоноване отримання логінів і паролів, підбір паролів та ключів, працівник, який виявив дані ознаки, зобов'язаний негайно:

- припинити обробку персональних даних;
- звернутися до адміністратора системи з метою блокування доступу до облікового запису;
- повідомити безпосереднього керівника та відповідальну особу, що організує роботу, пов'язану із захистом персональних даних при їхній обробці (далі – відповідальна особа);
- змінити паролі доступу (за наявності технічної можливості).

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 адміністратора системи;
- повідомити безпосереднього керівника та 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;
- про всі події та факти повідомити безпосереднього керівника та відповідальну особу.

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

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

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

6. У разі виникнення надзвичайних ситуацій (пожежа, повінь, стихійні лиха тощо):

- 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 та відповідальну особу.

7. Про всі випадки несанкціонованого доступу до персональних даних, 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 керівник виконавчого органу невідкладно письмово повідомляють про подію відповідальну особу.

Повідомлення реєструється відповідно до вимог діловодства у виконавчих органах міської ради.

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

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

Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.

9. Підписаний Акт надається міському голові або, в разі його відсутності, – посадовій особі, на яку покладено виконання його повноважень для прийняття рішення про проведення службового розслідування, повідомлення правоохоронних органів про несанкціонований доступ до персональних даних та вжиття відповідних заходів реагування.

Керуючий справами виконкому

Ігор ФАРТУШОК

Додаток 1
до Положення

Зобов'язання про нерозголошення персональних даних

(прізвище, ім'я, по батькові)

(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 мені відомі у зв'язку з виконанням посадових обов'язків або повноважень.

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

_____ 20__ року

(підпис)

Додаток 2
до Положення

Журнал
реєстрації зобов'язань про нерозголошення персональних даних

№ з/п	Прізвище, ім'я, по батькові	Структурний підрозділ, посада	Дата надання зобов'язання про нерозголошення персональних даних	Дата надання права на доступ до персональних даних	Дата позбавлення права доступу до персональних даних та їх обробки
1.	2.	3.	4.	5.	6.