ДЕСНЯНСЬКА РАЙОННА В МІСТІ КИЄВІ ДЕРЖАВНА АДМІНІСТРАЦІЯ

РОЗПОРЯДЖЕННЯ

13.06.2018 № 327

Про затвердження Порядку обробки та захисту персональних даних у структурних підрозділах апарату Деснянської районної в місті Києві державної адміністрації

Відповідно до статей 6, 13, 39 Закону України «Про місцеві державні адміністрації», Закону України «Про захист персональних даних», Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних», з метою встановлення загальних вимог до організаційних і технічних заходів захисту персональних даних під час їх обробки у структурних підрозділах апарату Деснянської районної в місті Києві державної адміністрації:

1. Затвердити Порядок обробки та захисту персональних даних у структурних підрозділах апарату Деснянської районної в місті Києві державної адміністрації (далі - Порядок), що додається.

2. Працівникам/співробітникам апарату Деснянської районної в місті Києві державної адміністрації забезпечити неухильне дотримання вимог Порядку.

3. Покласти на керівників структурних підрозділів апарату Деснянської районної в місті Києві державної адміністрації персональну відповідальність за невиконання чи неналежне виконання вимог Закону України «Про захист персональних даних» та Порядку.

4. Керівникам структурних підрозділів Деснянської районної в місті Києві державної адміністрації зі статусом юридичної особи публічного права забезпечити розроблення та затвердження в установленому порядку документів

про обробку та захист персональних даних, вжиття необхідних заходів щодо обробки та захисту персональних даних.

5. Затвердити План дій працівників апарату Деснянської районної в місті Києві державної адміністрації на випадок несанкціонованого доступу до персональних даних та виникнення надзвичайних ситуацій.

6. Відділу з питань внутрішньої політики, зв'язків з громадськістю та засобами масової інформації апарату Деснянської районної в місті Києві державної адміністрації забезпечити висвітлення цього розпорядження на офіційному веб-сайті Деснянської районної в місті Києві державної адміністрації.

7. Контроль за виконанням цього розпорядження покласти на керівника апарату Деснянської районної в місті Києві державної адміністрації.

Голова Г. Заболотний

ЗАТВЕРДЖЕНО
Розпорядження Деснянської районної
в місті Києві державної адміністрації
13 червня 2018 № 327

Порядок
обробки та захисту персональних даних у структурних підрозділах апарату Деснянської районної в місті Києві державної адміністрації

1. Загальні положення

1.1. Цим Порядком обробки та захисту персональних даних у структурних підрозділах апарату Деснянської районної в місті Києві державної адміністрації (далі - Порядок) визначено загальні вимоги до обробки та захисту персональних даних суб'єктів персональних даних, що обробляються повністю чи частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

1.2. Порядок розроблено відповідно до Закону України «Про захист персональних даних» (далі — Закон), Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних».

1.3. У Порядку терміни вживаються у значеннях, наведених у Законі.

2. Вимоги до обробки персональних даних

2.1. Володілець визначає:

1) мету та підстави обробки персональних даних;
2) категорії суб'єктів персональних даних;
3) склад персональних даних;
4) порядок обробки персональних даних, а саме:

- спосіб збору, накопичення персональних даних;
- строк та умови зберігання персональних даних;
- умови та процедуру зміни, видалення або знищення персональних даних;
- умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані;
- порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних;
- заходи забезпечення захисту персональних даних; процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них.

2.2. 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.

2.3. Процедури обробки, строк обробки та склад персональних даних повинні бути пропорційними меті обробки.

2.4. Мета обробки персональних даних повинна бути чіткою і законною.

2.5. Мета обробки персональних даних повинна бути визначена до початку їх збору.

2.6. У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних, окрім випадків, визначених законодавством, повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до нової мети.

2.7. Обробка персональних даних здійснюється володільцем персональних даних лише за згодою (повідомлення) про обробку персональних даних суб'єкта персональних даних (додається), за винятком тих випадків, коли така згода не вимагається Законом.

2.8. Згода суб'єкта на обробку його персональних даних повинна бути добровільною та інформованою. Згода може надаватися суб'єктом у письмовій або електронній формі, що дає 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.

2.9. Володілець персональних даних, крім випадків, передбачених законодавством України, повідомляє суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних та третіх 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 з дня збору персональних даних.

Володілець зберігає інформацію (документи), яка підтверджує надання заявнику вищезазначеної інформації протягом усього періоду обробки персональних даних.

2.10. 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. В будь-якому разі вони обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це передбачено законодавством у сфері архівної справи та діловодства.

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

2.12. 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.

2.13. Якщо за результатами розгляду такої вимоги виявлено, що персональні дані суб'єкта (їх частина) обробляються незаконно, володілець припиняє обробку персональних даних суб'єкта (їх частини) та інформує про це

суб'єкта персональних даних.

2.14. У разі якщо вимога не підлягає задоволенню, суб'єкту надається мотивована відповідь щодо відсутності підстав для її задоволення.

2.15. Суб'єкт персональних даних має право відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для обробки є згода суб'єкта персональних даних. З моменту відкликання згоди володілець зобов'язаний припинити обробку персональних даних.

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

2.17. Порядок доступу до персональних даних суб'єкта персональних даних та третіх осіб визначається статтями 16-17 Закону.

2.18. Володілець повідомляє суб'єкта персональних даних про дії з його персональними даними на умовах, визначених статтею 21 Закону.

3. Захист персональних даних

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

3.2. 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.

3.3. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадковим втратам або знищенню, незаконній обробці, у тому числі незаконному знищенню чи доступу до персональних даних.

3.4. Організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників володільця/розпорядника;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

3.5. 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.

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

3.7. 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.

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

3.9. 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.

3.10. 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.

3.11. Володілець/розпорядник 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;
- працівника, який здійснив одну із указаних операцій;
- мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них. У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

3.12. Вимоги щодо обліку та збереження інформації про перегляд персональних даних не поширюються на володільців/розпорядників, які здійснюють обробку персональних даних в реєстрі, який є відкритим для населення в цілому.

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

3.14. 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 роботи технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

3.15. В апараті Деснянської районної в місті Києві державної адміністрації розпорядженням Деснянської районної в місті Києві державної адміністрації визначається відповідальна особа за організацію роботи, пов'язаної із захистом персональних даних при їх обробці (далі - відповідальна особа).

3.16. Інформація про відповідальну особу повідомляється Уповноваженому ерховної Ради України з прав людини відповідно до Закону.

3.17. Відповідальна особа виконує такі завдання:

- інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;
- взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його Секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

3.18. З метою виконання вказаних завдань відповідальна особа:

- забезпечує реалізацію прав суб'єктів персональних даних;
- користується доступом до будь-яких даних, які обробляються володільцем/розпорядником, та до всіх приміщень володільця/розпорядника, де здійснюється така обробка;
- у разі виявлення порушень законодавства про захист персональних даних та/або цього Порядку повідомляє про це керівника володільця/розпорядника з метою вжиття необхідних заходів;
- аналізує загрози безпеці персональних даних.

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

3.20. Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані відповідальною особою.

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

3.22. Організація роботи, пов'язаної із захистом персональних даних при їх обробці, тих володільців/розпорядників, на яких не поширюються вимоги частини другої статті 24 Закону, покладається безпосередньо на тих осіб, які здійснюють обробку персональних даних, або, у разі необхідності, — на окремі структурні підрозділи чи посадових осіб.

Керівник апарату О. Машківська

ДОДАТОК
до Порядку обробки та захисту персональних даних у структурних підрозділах апарату Деснянської районної в місті Києві державної адміністрації

Згода (повідомлення) про обробку персональних даних

Я _____
що мешкає за адресою _____

документ що посвідчує особу_____
даю згоду на обробку персональних даних (назва володільця персональних даних)_____
на таких умовах:

1. Персональні дані оброблятимуться з метою *надання адміністративних послуг*

2. Володільцем оброблятимуться такі персональні дані: *ПІБ, адреса реєстрації місця проживання ,реєстраційний номер облікової картки платника податків, телефон, паспортні дані, для фізичних осіб - підприємців та юридичних осіб - найменування, код ЄДРПОУ. адреса реєстрації та / або місце знаходження для юридичної особи*
3. Розпорядником персональних даних є (назва та адреса розпорядника персональних
даних): територіальні підрозділи ЦОВВ місцевого самоврядування, органи виконавчої влади уповноважені відповідно до запиту надавати-адміністративні послуги

4. Володілець/розпорядник здійснюватиме з персональними даними такі дії: ***обробляє персональні дані в межах чинного законодавства***

5. Персональні дані передаватимуться (назва та адреса третьої особи) ***з метою оформлення адміністративної послуги***

Згода дається на термін, необхідний для досягнення мети, зазначеної в п.1, і може бути відкликана за заявою, направленою володільцю персональних даних.

Підпис Дата

ЗАТВЕРДЖЕНО
Розпорядження Деснянської районної
в місті Києві державної адміністрації
13 червня 2018 року № 327

ПЛАН ДІЙ
працівників апарату Деснянської районної в місті Києві державної адміністрації на випадок несанкціонованого доступу до персональних даних та виникнення надзвичайних ситуацій

№ п/п	Подія	Дії працівників	Відповідальні
1	Вихід з робочого стану технічного обладнання (пошкодження в результаті механічних, температурних та інших впливів)	Повідомити підрозділ або осіб, що проводять налагодження та ремонт технічного обладнання відповідно до повноважень та прав доступу	Керівники структурних підрозділів Деснянської районної в місті Києві державної адміністрації(далі - керівники підрозділів, відділів); відділ інформаційних технологій Деснянської районної в місті Києві державної адміністрації
2	Некоректна робота (збій, зависання, відмова запуску) програмного забезпечення	Припинити роботу, повідомити підрозділ або осіб, що проводять налагодження програмного забезпечення відповідно до повноважень та прав доступу	Керівники підрозділів; відділ інформаційних технологій Деснянської районної в місті Києві державної адміністрації
3	Ураження автоматизованої системи(далі - АС) вірусами	Закрити всі програми, пов'язані із обробкою персональних даних, за можливості запустити сканування АС антивірусною програмою, повідомити підрозділ або осіб, які відповідають за інформаційну безпеку	Керівники підрозділів; відділ інформаційних технологій Деснянської районної в місті Києві державної адміністрації
4	Отримання сторонніми особами логінів та паролів	Знеструмити технічне обладнання, відключити мережу Інтернет,	Керівники підрозділів; відділ інформаційних технологій Деснянської

	доступу до баз даних	повідомити про це осіб, відповідальних за інформаційну безпеку, вжити відповідних заходів щодо зміни або блокування паролів та логінів	районної в місті Києві державної адміністрації; головний спеціаліст відділу запобігання і виявлення корупції та взаємодії із правоохоронними органами Деснянської районної в місті Києві державної адміністрації
5	Спроба отримання несанкціонованого доступу до персональних даних	Закрити всі програми, пов'язані із обробкою персональних даних, створити умови неможливості доступу сторонніх осіб до програмних та апаратних засобів, повідомити всіх осіб відповідальних за безпеку	Керівники підрозділів; відділ інформаційних технологій Деснянської районної в місті Києві державної адміністрації; головний спеціаліст відділу запобігання і виявлення корупції та взаємодії із правоохоронними органами Деснянської районної в місті Києві державної адміністрації
6	Виникнення пожежі	Діяти згідно з Інструкцією про дотримання вимог протипожежної безпеки, затвердженої відповідно до вимог чинного законодавства	Керівники підрозділів; відділ адміністративно - господарського забезпечення Деснянської районної в місті Києві державної адміністрації; Управління з питань надзвичайних ситуацій Деснянської районної в місті Києві державної адміністрації; оперативний черговий
7	Виникнення надзвичайних ситуацій	Повідомити відповідний державний орган (служба надзвичайних ситуацій, поліція і т.д.), за можливості вжити заходів для збереження апаратних	Керівники підрозділів; відділ адміністративно - господарського забезпечення Деснянської районної в місті Києві державної

		засобів доступу до баз даних(флешнакопичувачі, компакт - диски, інші ключі доступу)	адміністрації; Управління з питань надзвичайних ситуацій Деснянської районної в місті Києві державної адміністрації; оперативний черговий

Керівник апарату О. Машківська