

Рекомендації Уповноваженого Верховної Ради України з прав людини щодо деяких питань обробки персональних даних внутрішньо переміщених осіб органами державної влади та органами місцевого самоврядування

За оцінками ООН у зв'язку з військовою агресією проти України мільйони людей покинули свої домівки. Підтримка осіб, які стали вимушеними переселенцями та постраждали від військової агресії, є одним із пріоритетів держави.

Водночас під час парламентського контролю за додержанням законодавства про захист персональних даних виявлено факти збору органами державної влади та органами місцевого самоврядування персональних даних внутрішньо переміщених осіб в мережі Інтернет з використанням Google форм.

За допомогою зазначених Google форм здійснюється збір таких персональних даних, як: прізвище, ім'я, по батькові, дата народження, серія і номер паспорту, реєстраційний номер облікової картки платника податків, адреса електронної пошти, номер телефону, адреса проживання до евакуації, поточна адреса проживання, соціальний статус, інформація про виплати, матеріальний стан, номер довідки ВПО, наявність інвалідності, відомості про потреби (ліки, продукти, одяг, психологічна підтримка), відомості про членів сім'ї тощо.

Використання Google форм або інших подібних приватних сервісів для обробки персональних даних внутрішньо переміщених осіб та/або інших категорій суб'єктів персональних даних не відповідає вимогам законодавства у сфері захисту персональних даних, зокрема положенням статті 4 Закону України «Про захист персональних даних» (далі – Закон), згідно із якою розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності.

Також зазначені Google форми не містять належного повідомлення суб'єкта персональних даних про володільця та розпорядника персональних даних, склад та зміст зібраних персональних даних, їх місцезнаходження, свої права, мету збору персональних даних та осіб, яким будуть передаватись персональні дані, що не відповідає вимогам статей 8 та 12 Закону.

Крім того, необхідно зауважити, що обробка персональних даних органами державної влади і органами місцевого самоврядування має здійснюватись на підставі пунктів 2 та 5 частини першої статті 11 Закону, а саме дозволу на обробку персональних даних, який наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень, а також у зв'язку з необхідністю виконання обов'язку володільця персональних даних, який передбачений законом.

Тобто обробка персональних даних органами державної влади і органами місцевого самоврядування не потребує отримання згоди на обробку персональних даних.

Варто наголосити, що не можна обумовлювати реалізацію законодавчо встановлених прав особи наданням нею згоди на обробку її персональних даних.

Отже, використання органами державної влади та органами місцевого самоврядування Google форм або інших подібних приватних сервісів становить загрозу для права на приватність осіб, які заповнюють такі форми.

У зв'язку з цим органам державної влади та органам місцевого самоврядування як володільцям персональних даних рекомендується здійснювати збір персональних даних засобами власних офіційних веб-сайтів. Якщо є потреба залучити розпорядника персональних даних, то врахувати, що розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності.

Водночас для дотримання вимог законодавства про захист персональних даних необхідно здійснити такі кроки:

1. Визначити мету обробки персональних даних. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних. Склад та зміст персональних даних, які будуть збиратись, мають бути відповідними, адекватними та ненадмірними щодо визначеної мети їх обробки.

2. Визначити підстави для обробки персональних даних. Обробка персональних даних органами державної влади і органами місцевого самоврядування має здійснюватись на підставі пунктів 2 та 5 частини першої статті 11 Закону.

3. Розробити та передбачити належні інформаційні повідомлення для громадян на офіційних веб-сайтах органів державної влади та органів місцевого самоврядування. Перед початком збору персональних даних необхідно надати особі вичерпну інформацію про те, хто буде обробляти її персональні дані (зазначити відомості про володільця, розпорядника персональних даних, третіх осіб), повідомити про правові підстави, мету обробки, склад і зміст персональних даних, права особи, які визначені статтею 8 Закону. Така інформація має бути доступною для особи та розміщуватися перед заповненням форм, що передбачають збір персональних даних.

4. Визначити порядок обробки персональних даних, враховуючи специфіку обробки персональних даних у різних сферах, відповідно до вимог Закону та 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», зокрема:

- 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.

5. Визначити перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки. Передбачити заходи, спрямовані на запобігання випадкових втрати або знищення персональних даних, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. Вжити 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.

6. Визначити такі організаційні заходи:

- порядок ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- навчання працівників, які працюють з персональними даними.

7. Отримати від працівників, які мають доступ до персональних даних, 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.

8. Визначити структурний підрозділ або відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці.

9. Визначити, чи передбачається обробка персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, а також чи є для цього правові підстави та мета. Обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів – це будь-яка дія або сукупність дій, яка здійснюється відносно персональних даних про:

- расове, етнічне та національне походження;
- політичні, релігійні або світоглядні переконання;

- членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;

- стан здоров'я;

- статеве життя;

- біометричні дані;

- генетичні дані;

- притягнення до адміністративної чи кримінальної відповідальності;

- застосування щодо особи заходів у рамках досудового розслідування;

- вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»;

- вчинення щодо особи тих чи інших видів насильства;

- місцеперебування та/або шляхи пересування особи.

10. Повідомити Уповноваженого про структурний підрозділ або відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних, а також про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних за формою, яка визначена в наказі Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних».

Звертаю увагу, що статтею 188-39 Кодексу України про адміністративні правопорушення встановлено адміністративну відповідальність за порушення законодавства у сфері захисту персональних даних.

Уповноважений

Дмитро ЛУБІНЕЦЬ