

## **Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних**

1. Згідно з порядком повідомлення володільці розпорядники, що здійснюють обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, повідомляють Уповноваженого про такі види обробки. Основним критерієм при визначенні того, чи становить певна обробка такий ризик є те, які категорії персональних даних обробляються.

2. В сенсі цього Порядку до таких категорій персональних даних слід відносити відомості 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, місцеперебування та або шляхи пересування особи, факт притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування та заходів, передбачених Законом України «Про оперативно-розшукову діяльність», вчинення щодо особи тих чи інших видів насильства.

3. При цьому, обробка вважатиметься чутливою в разі якщо **1)** склад персональних даних про особу, які обробляються володільцем, включає відомості вказаного в п. 2 змісту або **2)** коли володільцем розпорядником обробляються персональні дані певної категорії суб'єктів, яку можна виділити за вказаним в п. 2 критерієм.

4. Приклад першого випадку: володільцем обробляються такі дані: ім'я, прізвище, по батькові, місце проживання, паспортні дані, відомості про притягнення до кримінальної відповідальності. Остання група відомостей робить обробку такою, що несе ризик для прав і свобод суб'єкта і поширює на володільця розпорядника вимогу повідомлення.

5. Приклад другого випадку: володільцем обробляється звичайний склад даних: ім'я, прізвище, по батькові, місце проживання, паспортні дані, однак всі ці дані належать особам, що притягувалися до кримінальної відповідальності. Відтак, можна сказати, що володільцем обробляються персональні дані осіб, що притягувалися до кримінальної відповідальності. Фактично обробляються відомості щодо притягнення особи до кримінальної відповідальності. Відтак, на такого володільця поширюватиметься вимога щодо повідомлення.

6. Щодо змісту даних, вказаних в п. 2 вище слід зазначити про таке:

- світоглядні переконання особи – сукупність поглядів, оцінок та життєвих принципів особи, що визначають загальне розуміння та сприйняття світу та місце кожного у ньому. Мова у даному пункті йдеться саме про загальноприйнятні світоглядні переконання. Наприклад: пацифізм, фемінізм, вегетаріанство тощо;

- стан здоров'я особи – тобто медична інформація про особу, що містить не лише свідчення про стан здоров'я, а й про історію її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я (виняток становить медичні довідки, листи працездатності і т.д., які обробляються володільцем при реалізації трудових відносин);

- статеве життя – будь-яка інформація про особу, що стосується її вибору та поведінки у статевих відносинах (включається інформація про сексуальну орієнтацію особи);

- біометричні дані - сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (наприклад відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук, відцифрований малюнок сітківки ока тощо);

- генетичні дані – інформація, що стосується всіх даних стосовно спадкових властивостей особи або стосовно способу успадкування характеристик в межах відповідної групи людей, також це стосується всіх даних про утримання будь-якої генетичної інформації (генів), що відноситься до будь-яких аспектів здоров'я або захворювання;

- вчинення щодо особи тих чи інших видів насильства – інформація про те, що особа піддавалась різноманітним видам насилля, катувань, мордування, нелюдського чи такого, що принижує гідність поводження. Наприклад, інформація вказаного характеру з матеріалів кримінального провадження з матеріалів кримінального провадження;

- місцеперебування та або шляхи пересування особи – це інформація, що дає можливість визначити місцеперебування конкретної особи у певному часовому просторі. Наприклад: зняття готівкових коштів в банкоматах, використання платіжної чи будь-якої іншої іменної картки при розрахунках за товари та послуги, білінгові системи мобільних операторів, геолокаційні послуги мобільних операторів, використання іменних квитків. В дану категорію не потрапляє інформація про місце проживання, місце реєстрації, службові та інші відрядження та поїздки.

**Щодо процедури повідомлення.**

7. Володільці персональних даних, на яких поширюється вимога повідомлення Уповноваженого про обробку, повідомляють Уповноваженого у будь-який доступний їм спосіб. А саме: надсилання інформації листом на адресу Секретаріату Уповноваженого, електронною поштою, факсом, а також подання заяви особисто через спеціально встановлену скриньку для вхідної кореспонденції, розміщену в приміщенні Секретаріату Уповноваженого.

8. До розгляду приймаються заяви, що заповнені за формою, визначеною у додатках до Порядку, без виправлень. Всі розділи заяви повинні бути заповнені. Дані, вказані у заяві, повинні бути вірними та підтверджуватись підписом і печаткою (у разі наявності) на кожній сторінці заяви.

### **Щодо відомостей, які підлягають повідомленню.**

9. Володільць у заяві, форма якої затверджена Порядком повідомлення, вказує лише інформацію щодо обробки тих категорій персональних даних, які вказані в п. 1.2 Порядку повідомлення, незважаючи на кількість і різноманітність наявних в його розпорядженні баз персональних даних і їх місцезнаходження. Так, якщо володільць веде декілька баз даних і лише в одній він обробляє персональні дані, які можна віднести до однієї із вказаних в п. 1.2 категорій, у заяві вказується лише інформація про обробку вказаних в п. 1.2 даних.

10. Далі надається короткий виклад того, яка інформація та в якому обсязі повинна повідомлятися Уповноваженому. Так, відповідно до Порядку повідомлення та форми затвердженої Порядком заяви Уповноваженому повинна повідомлятися інформація про:

- володільця розпорядника персональних даних.

Відомості про розпорядників зазначаються для кожного окремо. У випадку якщо кількість розпорядників надто велика, а їх місцезнаходження є загальнодоступною інформацією вказується загальна характеристика таких розпорядників. Наприклад, якщо це філії представництва головної компанії тощо;

- склад персональних даних.

Тут вказуються тільки ті категорії даних, які визначені пунктом 2 вище. Наприклад: володільцем ведеться обробка персональних даних у декількох базах. У одній із баз обробляються дані такого змісту: ім'я, прізвище, по батькові, місце проживання, номер телефону, електронна адреса, проведені медичні обстеження, поставлені діагнози та призначене лікування. Останні три позиції відносяться до інформації про стан здоров'я. Відтак, у заяві необхідно відмітити лише інформацію про стан здоров'я;

- мету обробки персональних даних. Мета обробки повинна визначатися в положеннях нормативно-правових актів, що безпосередньо уповноважують володільця на обробку персональних даних, або в положеннях установчих чи інших документів, що визначають вид діяльності володільця, яка обумовлює необхідність обробки персональних даних. Відповідно в цій частині заяви володільцем чітко та стисло формується мета обробки та положення вказаних документів, які підтверджують її існування;

- категорію чи категорії суб'єктів персональних даних, чиї персональні дані обробляються. В цій частині зазначаються загальні відомості про категорію суб'єктів, наприклад: постійні клієнти, власники платіжних карток, контрагенти, пацієнти тощо. При цьому, слід повторно наголосити, що якщо володільцем ведеться обробка персональних даних у декількох базах, де обробляються дані декількох категорій суб'єктів, у заяві слід вказувати лише ту категорію суб'єктів (чи категорії), щодо якої ведеться обробка вказаних в п. 2 даних;

- третіх осіб, яким передаються персональні дані суб'єктів. Перш за все володільцю слід вказати, чи здійснюється ним поширення вказаних в п. 2 персональних даних загалом. Якщо такі операції здійснюються слід вказати, кому персональні можуть передаватися.

**Не потрібно вказувати на те, кому можуть передаватися персональні дані відповідно до закону.** Наприклад: не потрібно вказувати про те, що персональні дані можуть передаватися на запити державних органів, до чийої компетенції належить право отримувати таку інформацію (в ході перевірки, розслідування тощо). Така інформація є відкритою, оскільки безпосередньо передбачена законодавством.

Натомість володільцям слід вказати лише інформацію про можливу передачу вказаних в п. 2 персональних даних з інших підстав (згода особи, укладення договору та інші).

Слід вказати найменування та адресу всіх суб'єктів, кому можуть передаватися вказані в п. 2 персональні дані.

У випадку якщо персональні дані можуть передаватися групі однотипних третіх осіб, вказується їх загальна характеристика. Наприклад: володілець має представництва філії, яким передаються персональні дані (лише ті, що належать до категорій, вказаних в п. 2 вище) після їх збору. В такому випадку не потрібно давати інформацію про кожну філію представництво. Достатньо вказати, що персональні дані передаються іншим структурним підрозділам володільця;

- транскордонну передачу персональних даних. Вказуються країни та іноземні суб'єкти, яким можуть передаватися дані, мета передачі (мета, як правило, повинна відповідати меті обробки), а також підстави обробки;
- місце (фактична адреса) обробки персональних даних, зазначаються адреси, де містяться картотеки чи магнітні носії (сервери), де здійснюється обробка вказаних в п. 2 вище даних;
- загальний опис технічних та організаційних заходів, що вживаються володільцем з метою забезпечення захисту персональних даних, які належать до вказаних в п. 2 вище категорій.

Сюди відноситься, наприклад, інформація про те:

- чи було прийнято окремий порядок обробки (і в тому числі захисту) персональних даних;
- чи призначено (створено) відповідальну особу структурний підрозділ, який організовує роботу, пов'язану із захистом персональних даних;
- який порядок доступу до приміщень, де стоять комп'ютери картотеки, в яких здійснюється обробка персональних даних. Наприклад: приміщення, де здійснюється обробка персональних даних, замикаються не замикаються. Доступ до таких приміщень мають всі працівники володільця визначене коло працівників. Доступ здійснюється за допомогою ключа ідентифікаційної чи мікропроцесорної карти. Приміщення обладнані не обладнані сигналізацією;
- який порядок доступу до персональних даних, які містяться на комп'ютерах в картотеках. Наприклад: такі комп'ютери захищені кодом доступу паролем. Кожен із працівників має свій особистий код доступу;
- чи ведеться, як це вимагається Типовим порядком обробки персональних даних, облік операцій, пов'язаних з обробкою персональних даних суб'єкта, та доступом до них;
- чи приєднані комп'ютери, на яких здійснюється обробка персональних даних, до мережі та чи встановлено антивірусне та інше програмне забезпечення;
- інші заходи.

Вказаний перелік не є вичерпним і наводиться як приклад. Володільць самостійно визначає, які заходи безпеки запроваджувати з метою адекватного захисту персональних даних, які ним обробляються. Запроваджені ним заходи вказуються у заяві.

Слід наголосити, що виклад зазначеної інформації у заяві довільний і володільцю слід надати лише **загальні** відомості.

Приклад викладу вказаної інформації:

Володільцем прийнято внутрішній порядок обробки персональних даних та визначену відповідальну особу. Приміщення, де стоять комп'ютери, на яких здійснюється обробка персональних даних, замикаються. Для отримання ключа необхідно поставити відмітку в журналі. Визначено коло працівників, що мають доступ до персональних даних, а також рівні доступу таких працівників. Комп'ютери, де містяться персональні дані, захищені паролем. Кожен працівник має особистий пароль. Всі операції, пов'язані з обробкою персональних даних, автоматично фіксуються за допомогою спеціалізованого програмного забезпечення.