

**«Європейський Союз та Рада Європи працюють разом
зادля посилення операційної спроможності Омбудсмана у захисті прав людини»**

Фінансується
Європейським Союзом
та Радою Європи



COUNCIL OF EUROPE



Впроваджується
Радою Європи

Рекомендацій

**щодо усунення центральними органами виконавчої влади
типових порушень законодавства про захист персональних даних у процесі підготовки та
прийняття нормативно-правових актів**

Підготовлені:

Олегом Заярним, національним консультантом Ради Європи

I. Вступ

Необхідність розробки рекомендацій щодо усунення центральними органами виконавчої влади України типових порушень законодавства про захист персональних даних при розробці нових, внесенні змін та доповнень до чинних нормативно-правових актів, пояснюється швидким розвитком сфери захисту персональних даних та появою нових специфічних викликів у цій сфері.

Для України як держави-члена Ради Європи одним з пріоритетних завдань у внутрішній та зовнішній політиці є утвердження і забезпечення високих стандартів прав людини, визнаних в діяльності Ради Європи. Ключове місце в системі інструментів Ради Європи щодо правового захисту персональних даних займає Конвенція Ради Європи №108 «Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних» (далі - Конвенція Ради Європи №108). Окрім того Додатковим протоколом від 08 листопада 2001 року до Конвенції Ради Європи № 108 було визначено умови формування та вимоги до діяльності наглядових органів у державах-членах Ради Європи у сфері захисту персональних даних.

Ратифікація Україною 06 липня 2010 року Конвенції №108, а згодом Додаткового протоколу до неї засвідчила взяття Україною безпосередніх зобов'язань щодо імплементації у норми національного законодавства стандартів вироблених Радою Європи та вимог до діяльності наглядового органу у сфері обробки і захисту персональних даних.

Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 03.07.2013 року № 383-VII, який набрав чинності 01.01.2014 року правовим статусом наглядового органу у сфері захисту персональних даних було наділено Уповноваженого Верховної Ради України з прав людини.

Реалізація повноважень щодо парламентського контролю за дотриманням прав і свобод людини та наглядового органу у сфері захисту персональних, даних Уповноваженому Верховної Ради України з прав людини, перед усім спрямована на усунення типових порушень законодавства про захист персональних даних, належне нормативне забезпечення обробки персональних даних у різних сферах суспільного життя.

Дані рекомендації базуються на аналізі типових порушень законодавства про захист персональних даних, які мають місце в діяльності ЦОВВ при розробці нових та внесенні змін до вже чинних нормативно-правових актів у системному зв'язку з вимогами Конвенції Ради Європи № 108, та Закону України «Про захист персональних даних», практикою Європейського Суду з прав людини (далі – ЄСПЛ). Під типовим порушенням, для цілей цих рекомендацій, розуміється недотримання, обмеження чи скасування прав учасників відносин у сфері обробки

та захисту персональних даних у сфері виконавчої влади, порушення принципів, процедур, мети або підстав обробки персональних даних, обумовлені розробкою, прийняттям, виконанням, чи не прийняттям ЦОВВ нормативно-правових актів, що характеризуються глибокою схожістю за змістом, наслідками, а також причинами виникнення.

Надані рекомендації можуть бути застосовані при підготовці нових, а також внесенні змін і доповнень до чинних нормативно-правових актів ЦОВВ, які виступають володільцями або розпорядниками публічних реєстрів або інформаційно-телекомунікаційних систем, в яких здійснюється обробка персональних даних та/або виконують функції володільця персональних даних за законодавством України.

II. Загальні рекомендації щодо недопущення ЦОВВ типових порушень законодавства про захист персональних даних при підготовці нових або внесенні змін до чинних нормативно-правових актів з питань обробки та захисту персональних даних.

1) При прийнятті центральними органами виконавчої влади (далі – ЦОВВ) нормативно-правових актів у сфері обробки та захисту персональних даних необхідно керуватися нормами Конституції України, Конвенції Ради Європи «Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 року № 108 (далі - Конвенції Ради Європи № 108), Закону України «Про захист персональних даних» від 01.06.2010 року № 2297-VI, вимогами Типового порядку обробки персональних даних (далі - Типовий порядок), Типового повідомлення про обробку персональних даних, затверджених Наказом Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) від 08.01.2014 року № 1/02-14, інших актів законодавства про захист персональних даних практики Європейського Суду з прав людини (далі – ЄСПЛ) з відповідних питань, потреби забезпечення правомірної обробки персональних даних, дотримання прав суб'єктів персональних даних у відносинах з ЦОВВ, підприємствами, установами та організаціями, які перебувають у їхньому підпорядкуванні.

2) При прийнятті нормативно-правових актів з питань обробки та захисту персональних даних необхідно виходити перед усім зі змісту компетенції конкретного ЦОВВ, визначеної положенням, іншим правовстановчим актом про цей державний орган, іншими актами національного законодавства.

3) Проекти нормативно-правових актів ЦОВВ, які містять положення, спрямовані на врегулювання суспільних відносин у сфері обробки або захисту персональних даних,

зачіпають права суб'єктів персональних даних, підлягають обов'язковому попередньому погодженню Уповноваженим у встановленому законодавством України порядку.

4) У процесі розробки нормативно-правових актів слід дотримуватися правил законодавчої техніки, що застосовуються для підготовки нормативно-правових актів в практиці діяльності ЦОВВ, уникати використання неоднозначних суджень, неконкретизованих понять, а також встановлення дискретних повноважень щодо ЦОВВ, як володільців або розпорядників персональних даних, чи розпорядників публічних реєстрів, баз даних, інформаційно-телекомунікаційних систем.

5) Передусім, при формулюванні понятійного апарату проєктів нормативно-правових актів, ЦОВВ необхідно застосовувати визначення понять, наведені в нормах Конвенції Ради Європи № 108, Законі України «Про захист персональних даних», інших законах України та міжнародних договорах, згоду на обов'язковість яких надано Верховною Радою України. З метою уникнення випадків дублювання вже сформульованих в нормах законодавства України визначень понять, не допущення їх розширеного або звуженого тлумачення, при підготовці проєктів нормативно-правових актів ЦОВВ рекомендується робити прямі вказівки на статті, а за необхідності частини та пункти, підпункти статей Законів, інших підзаконних нормативно-правових актів, де раніше були сформульовані відповідні визначення.

6) До проєктів нормативно-правових актів можуть включатися норми з питань, що потребують врегулювання в діяльності ЦОВВ, як володільця або розпорядника персональних даних, чи розпорядника публічного реєстру, бази даних, інформаційно-телекомунікаційної системи, призначеної для обробки персональних даних та щодо яких суб'єкт нормотворчої діяльності здійснює функції володільця від імені держави.

7) Якщо проєкт нормативно-правового акту передбачає порядок обробки персональних даних в одній або декількох сферах суспільних відносин, такий нормативно-правовий акт повинен включати складові частини, визначені у Типовому порядку обробки персональних даних.

8) Приписи до проєкту з питань, які вимагають оперативного рішення структурними підрозділами з питань обробки персональних даних або забезпечення ведення реєстрів, інформаційно-телекомунікаційних систем, в яких обробляються персональні дані, не рекомендується, крім випадків, коли слід дати вказівку вирішити визначене питання або переглянути раніше прийнятий нормативно-правовий акт.

9) Якщо при підготовці проєкту нормативно-правового акту передбачається внесення істотних змін у чинні нормативно-правові акти з питань обробки та захисту персональних даних або коли з одного й того ж питання є декілька нормативно-правових актів, доцільно підготувати новий нормативно-правовий акт. До проєкту такого акту

включаються нові, а також раніше прийняті нормативні приписи, які повинні зберегти свою чинність.

10) Проект нового нормативно-правового акту розробляється також, коли є потреба внесення змін до багатьох пунктів чинного нормативно-правового акту або змінити пункти, до яких раніше було внесено багато змін, або нормативно-правовий акт, до якого повинні вноситись зміни, застарів і багато його частин визнано такими, що втратили чинність.

11) Нові приписи з окремих питань обробки і захисту персональних даних, які вирішені у раніше виданих актах, що пройшли державну реєстрацію, готуються, як правило, у формі змін та доповнень тексту цих нормативно-правових актів.

III. Типові порушення законодавства про захист персональних даних у процесі розробки ЦОВВ нормативно-правових актів та рекомендації щодо їх недопущення (усунення).

Типове порушення 1. Не врахування ЦОВВ при розробці проєктів нормативно-правових актів підстав для обробки персональних даних, передбачених у статті 11 Закону України про захист персональних даних в діяльності суб'єктів владних повноважень.

1.1. Нормативні вимоги.

Вичерпний перелік підстав для обробки персональних даних передбачено статтею 11 Закону.

За своєю сутністю підстави обробки персональних даних зазначені у пунктах 1, 3 частини першої статті 11 Закону України «Про захист персональних даних» ґрунтуються на вільному, поінформованому волевиявленні суб'єкта персональних даних. Натомість, підстави для обробки персональних даних, зазначені у пунктах 2, 4 – 6 частини першої статті 11 Закону України «Про захист персональних даних» не передбачають необхідності одержання дозволу суб'єкта персональних даних на обробку інформації про нього.

Згода суб'єкта персональних даних є лише однією з шести підстав для обробки персональних даних, передбачених статтею 11 Закону. За наявності підстав, визначених пунктами 2-6 частини першої статті 11 Закону України «Про захист персональних даних», обробка персональних даних здійснюється без згоди суб'єкта персональних даних.

Однією з таких підстав є «дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень» (пункт 2 частини першої статті 11 Закону).

У статті 8 Конвенції про захист прав людини і основоположних свобод від 04.11.1950 (ратифікованої Україною 17.07.1997) (далі – Європейська Конвенція) гарантовано право на повагу до приватного і сімейного життя: кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Конституція України в розвиток зазначених положень Конвенції «Про захист прав людини і основоположних свобод» у частині другій статті 32 закріпила норму, згідно з якою, не допускається 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 прав людини.

Зазначене кореспондується з підпунктом 2.7. пункту 2 Типового порядку обробки персональних даних, обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли така згода не вимагається Законом.

Особливості дозволу на обробку персональних даних, наданого володільцю персональних даних відповідно до закону як підстави для обробки персональних даних полягають у наступному:

- надається переважно суб'єктам владних повноважень;
- діє не довше, ніж це необхідно суб'єкту владних повноважень для виконання покладених на нього обов'язків;
- стосується лише чітко визначених наборів персональних даних;
- має строковий характер;
- надається лише в межах компетенції суб'єкта владних повноважень.

Відповідно, за загальним правилом обробка персональних даних ЦОВВ, їх територіальними органами або підрозділами ґрунтується на підставі дозволу, наданому законом для такої обробки, хоча законодавство України допускає випадки, в яких обробка персональних даних ЦОВВ передбачає обов'язковість одержання згоди на таку обробку, або укладення з ним правочину. Прикладом відносин, у яких підставою для обробки персональних даних виступає згода суб'єкта персональних даних або укладений з ним правочин є з суб'єктом персональних даних є трудові відносини з суб'єктом персональних даних – працівником ЦОВВ, укладення договору про надання фізичною особою-підприємцем ЦОВВ господарських послуг, тощо.

Відповідно до статті 2 Закону, згода суб'єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

Наведене визначення містить дві суттєві ознаки згоди на обробку персональних даних:

- добровільність (означає відсутність прямого або опосередкованого примусу при її наданні);
- поінформованість (означає, що перед наданням згоди суб'єкт повинен отримати достовірну інформацію про те, ким, з якою метою будуть оброблятися його персональні дані, кому будуть передаватися, які саме дані, а також про права, визначені Законом).

Суб'єкт персональних даних також має право відмовитись від надання згоди на обробку персональних даних, відкликати згоду на обробку персональних даних, яка була надана такою особою раніше, вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди, 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, заперечувати проти обробки своїх персональних даних.

Таким чином, проєкт нормативно-правового акту може передбачати необхідність одержання згоди суб'єкта персональних даних, або укладення з ним правочину, як підстави для обробки персональних даних державним органом або органом місцевого самоврядування лише у випадках, коли такий орган вступає у приватно-правові відносини із суб'єктом персональних даних і не наділений в них владними повноваженнями.

1.2. Правові позиції судової практики, на яких ґрунтується роз'яснення щодо запобігання викладеного типового порушення:

– «Amann v. Switzerland» (заява № 27798/95, рішення від 16.02.2000) - Прослуховування телефонних розмов. Законодавча невизначеність повноважень щодо зберігання інформації про особу;

– «Rotaru v. Romania» (заява № 28341/95, рішення від 04.05.2000) Законність ведення службою безпеки таємного реєстру. Відсутність законодавчих гарантій;

– «K.H. and Others v. Slovakia» (заява № 32881/04, рішення від 06.11.2009) – Ненадання лікарнею заявникам копій їх медичної документації;

– «L.H. v. Latvia» (заява № 52019/07, рішення від 29.04.2014) - Збір інформації контролюючим органом із метою оцінки якості наданої пацієнту медичної допомоги лікарнею.

Відсутність легітимної мети збору персональних даних. Надмірний об'єм зібраної інформації.
Неврахування інтересів пацієнта;

– «Zaichenko v. Ukraine» (№ 2) (заява №45797/09, рішення від 26/02/2015) – Відсутність визначеної законодавством процедури збору інформації під час проведення експертизи стану психіатричного здоров'я особи (в чийх діях вбачаються ознаки адміністративного правопорушення) в рамках провадження у справі про адміністративне правопорушення;

– «Friedl v. Austria» (заява № 15225/89, рішення від 31/01/1995) - Законність здійснення відеофіксації силового розпуску мирного зібрання;

– «Avilkina and Others v. Russia» (заява № 1585/09, рішення від 06.06.2013) – Збір медичної інформації прокуратурою. Законодавча невизначеність повноважень щодо збору інформації про особу. Надмірний об'єм інформації, що збирається.

– Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/20122, Абзаци третій, четвертий пункту 5 мотивувальної частини, положення частини другої статті 32 Основного Закону України передбачають вичерпні підстави можливого правомірного втручання в особисте та сімейне життя особи (в тому числі й тієї, яка займає посаду, пов'язану з функціями держави або органів місцевого самоврядування, та членів її сім'ї). Такими підставами є: згода особи на збирання, зберігання, використання та поширення конфіденційної інформації стосовно неї, а також, у разі відсутності такої згоди, випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Даючи офіційне тлумачення положень частин першої, другої статті 32 Конституції України у системному зв'язку з частиною другою статті 34 цієї Конституції, Конституційний Суд України дійшов висновку, що збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини.

1.3. Рекомендовано:

- При підготовці проєкту нормативно-правового акту, яким визначається порядок обробки персональних даних або правовий режим функціонування публічного реєстру (бази даних), інформаційно-телекомунікаційної системи, призначеної для відповідних дій з

персональними даними, ЦОВВ обов'язково повинен зазначати, що обробка даних здійснюється з дотриманням вимог Закону України «Про захист персональних даних».

- Якщо проектом нормативно-правового акту передбачається врегулювання відносин В – суб'єкту нормотворчої діяльності у проекті відповідного акту обов'язково з посиланням на конкретні пункти частини першої статті 11 Закону України «Про захист персональних даних» необхідно вказати вичерпний перелік підстав для обробки персональних даних.

Типове порушення 2. Ігнорування правових підстав або недостатність правових підстав для прийняття ЦОВВ нормативно-правового акту з питань обробки та/або захисту персональних даних.

2.1. Нормативні вимоги:

Будь-який нормативно-правовий акт, який розробляється ЦОВВ у сфері обробки і захисту персональних даних повинен мати необхідну правову основу для його ухвалення. Такою правовою основою перед усім є норми Конституції України, зокрема, закріплені у статті 32, Конвенції Ради Європи «Про захист прав людини і основоположних свобод», Конвенції Ради Європи № 108, інших міжнародних договорів, згоду на обов'язковість яких надано Верховною Радою України, Закону України «Про захист персональних даних», інших Законів України з питань обробки та захисту персональних даних, Укази Президента України, Постанови Кабінету Міністрів України, тощо.

Як слідує з положень частини другої статті 19 Конституції України, органи державної влади та органи місцевого самоврядування, їх посадові та службові особи зобов'язані діяти на підставі, в межах повноважень і у спосіб, передбачений Конституцією і законами України.

З наведеної норми слідує, що одним з критеріїв, що характеризує правомірність діяльності органу державної влади, зокрема ЦОВВ, як суб'єкта нормотворчої діяльності є наявність законних підстав для його діяльності.

Відповідно до частини другої статті 8 Основного Закону, Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй.

Міністерство у межах своїх повноважень, на основі і на виконання Конституції та законів України, актів Президента України та постанов Верховної Ради України, прийнятих відповідно до Конституції та законів України, актів Кабінету Міністрів України видає накази, які підписує міністр, частина перша статті 15 Закону України «Про центральні органи виконавчої влади» від 17.03.2011 року № 1166-VI з наступними змінами та доповненнями.

При цьому, згідно з частиною другою статті 15 вказаного Закону України, накази міністерства, видані в межах його повноважень, є обов'язковими для виконання центральними органами виконавчої влади, їх територіальними органами, місцевими державними адміністраціями, органами влади Автономної Республіки Крим, органами місцевого самоврядування, підприємствами, установами і організаціями всіх форм власності та громадянами.

Відповідно до пункту 1.2. Типового Порядку, володільці, розпорядники персональних даних самостійно визначають порядок обробки персональних даних, враховуючи специфіку обробки персональних даних у різних сферах, відповідно до вимог, визначених Законом України «Про захист персональних даних» та цим Порядком.

Відповідно до частини першої статті 1 Закону України «Про захист персональних даних», цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Частиною другою статті 1 вказаного Закону також передбачено, що цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Слід підкреслити, частиною першою статті 27 Закону України «Про захист персональних даних» закріплено важливу нормативну вимогу, відповідно до якої: «Положення щодо захисту персональних даних, викладені в цьому Законі, можуть доповнюватися чи уточнюватися іншими законами, за умови, що вони встановлюють вимоги щодо захисту персональних даних, що не суперечать вимогам цього Закону».

Таким чином, при прийнятті ЦОВВ нормативно-правових актів, які спрямовані на врегулювання відносин щодо обробки та/або захисту персональних даних допускається лише уточнення конкретних положень Закону України «Про захист персональних даних» лише за умови, якщо таке уточнення не має наслідком зміну або скасування правових гарантій. Слід звернути увагу, згідно з абзацом другим частини шостої статті 15 Закону України «Про центральні органи виконавчої влади», проекти наказів міністерства, які мають нормативно-правовий характер, оприлюднюються на офіційному веб-сайті міністерства відповідно до Закону України "Про доступ до публічної інформації", крім випадків виникнення надзвичайних ситуацій та інших невідкладних випадків, передбачених законом, коли такі проекти актів оприлюднюються негайно після їх підготовки, визначених відповідним Законом.

Необхідно звернути увагу, якщо проектом нормативно-правового акту передбачається врегулювання відносин щодо обробки та захисту персональних даних громадян держав-членів Європейського Союзу, такий проєкт повинен обов'язково містити посилання на положення прийнятого 27 квітня 2016 року Європейським Парламентом Регламенту 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, (далі - Регламент 2016/679)

Відповідно до статті 3 GDPR, територіальна сфера дії охоплює:

- опрацювання персональних даних в контексті діяльності осідку контролера або оператора в Європейському Союзі, незалежно від того, чи відбувається власне опрацювання в межах Європейського Союзу чи ні;
- опрацювання персональних даних суб'єктів даних, які перебувають у Європейському Союзі, контролером або оператором, який має осідок поза межами Європейського Союзу;
- якщо опрацювання даних пов'язано з:(а) постачанням товарів чи наданням послуг таким суб'єктам даних у Європейському Союзі, незалежно від того, чи вимагають оплату від таких суб'єктів даних; або (b) моніторингом поведінки суб'єктів даних, якщо така поведінка має місце у межах Європейського Союзу;
- опрацювання персональних даних контролером, що має осідок поза межами Європейського Союзу, але в місці, де застосовується законодавство держави-члена в силу публічного міжнародного права.

Таким чином, за наявності у проєкті нормативно-правового акту положень спрямованих на врегулювання однієї з груп вказаних суспільних відносин, посилання на конкретний пункт статті 3 GDPR є обов'язковим.

2.2. Правові позиції судової практики, на яких ґрунтується роз'яснення щодо запобігання викладеного типового порушення:

- «С. і Марпер проти Сполученого Королівства» («S. and Marper v. United Kingdom»; заяви № 30562/04 та № 30566/04; рішення від 04.12.2008 р.) - захист персональних даних відіграє фундаментальне значення для реалізації права людини на повагу до приватного і сімейного життя, гарантованого ст. 8 Конвенції. Внутрішнє законодавство повинно забезпечувати відповідні гарантії для запобігання будь-якого використання персональних даних, яке може бути несумісним із гарантіями, передбаченими цією статтею.

- Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої

статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012, абзац другий пункту 3 мотивувальної частини, лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці.

2.3. Рекомендовано:

- ЦОВВ у тексті нормативно-правового акту, який стосується обробки персональних даних, повинен зазначати, що обробка даних здійснюється з дотриманням вимог Конституції України, Конвенції Ради Європи № 108, Закону України «Про захист персональних даних», а також вказувати на повні назви інших Законів України та нормативно-правових актів, зокрема, Укази Президента України, Постанови Кабінету Міністрів України, що складають правову основу для прийняття нормативно-правового акту.

- Якщо нормативно-правовий акт передбачає обробку персональних даних у різних сферах суспільних відносин, на яку поширюються норми спеціального закону, ЦОВВ повинен зазначити, що норми спеціального закону діють у частині, в якій вони не суперечать Закону України «Про захист персональних даних».

- Якщо проєкт нормативно-правового акту спрямований на врегулювання окремих аспектів транскордонної обробки персональних даних, обов'язково необхідно вказати на міжнародно-правові акти (конвенції, міжнародні договори), на підставі яких передбачається транскордонна обробка персональних даних.

– Якщо до проєкту нормативно-правового акту включено положення щодо обробки персональних даних громадян держав-членів Європейського Союзу, такий проєкт повинен містити обов'язкову вказівку на норми GDPR, як правову основу ухвалення відповідно-нормативно-правового акту, а також визначати сферу застосування положень GDPR, що підлягають застосуванню до суспільних відносин, на врегулювання яких спрямований проєкт нормативно-правового акту.

Типове порушення 3. ЦОВВ у проєктах нормативно-правових актів не завжди визначають мету обробки персональних даних або формулюють відповідну мету з порушенням вимог Конвенції № 108 та Закону України «Про захист персональних даних».

3.1. Нормативні вимоги:

Згідно з положеннями статті 5 Конвенції № 108, персональні дані, що піддаються автоматизованій обробці, повинні:

- отримуватися та оброблятися сумлінно та законно;
- зберігатися для визначених і законних цілей та не використовуватися у спосіб, не сумісний із цими цілями;
- бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються;
- бути точними та в разі необхідності оновлюватися;
- зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються.

Закон України «Про захист персональних даних» у частині першій статті 6 передбачає, що 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.

Підпунктом 1 пункту 2.1. Типового порядку встановлено, що володільць визначає мету та підстави обробки персональних даних. Згідно з пунктом 2.3. Типового порядку, процедури обробки, строк обробки та склад персональних даних повинні бути пропорційними меті обробки. Пунктом 2.4. Типового Порядку безпосередньо встановлено, що мета обробки персональних даних повинна бути чіткою і законною, а також, відповідно до пункту 2.5. згаданого Порядку, мета обробки персональних даних повинна бути визначена до початку їх збору.

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

Таким чином, мета обробки персональних даних – це ті цілі, для досягнення яких володільцем здійснюється обробка персональних даних, включаючи безпосередню ідентифікацію самого суб'єкта персональних даних.

Мета обробки персональних даних визначається володільцем, або його статутом (положенням) або безпосередньо нормами законодавства України.

3.2. Правові позиції судової практики, на яких ґрунтується роз'яснення щодо запобігання викладеного типового порушення:

- «S. and Marper v. The United Kingdom» (заяви № 30562/04 30566/04, рішення від 04.12.2008) – Законність збору та зберігання працівниками поліції відбитків пальців, профілів та зразків ДНК затриманих, підозрюваних тощо. Відсутність достатньо чіткої мети збору інформації, відсутність необхідності у зборі такого великого об'єму даних у порівнянні з отримуваними перевагами, неврахування індивідуальних обставин осіб, чиї дані зберігалися;

- «Ciubotaru v. Moldova» (заява № 27138/04, рішення від 27/04/2010) – Відмова державних органів змінити в державному реєстрі інформацію про національність особи. Покладення законодавством на особу непропорційного тягара доведення;

- «Авілкіна та інші проти Російської Федерації» («Avilkina and Others v. Russia»; заява № 1585/09; рішення від 06.06.2013)) - формулювання «згідно із законом» наказує, що оскаржувана міра повинна мати певні підстави в національному законодавстві та відповідати принципу верховенства права;

- «Пантелесенко проти України» («Panteleyenکو v. Ukraine»; заява № 11901/02; рішення від 29.06.2006) - вираз «відповідно до закону» у пункті 2 ст. 8 Конвенції значною мірою покладає на національне законодавство і державу обов'язок дотримання матеріальних і процесуальних норм (з відповідними виправленнями).

3.3. Рекомендовано:

- При підготовці проєктів нормативно-правових актів, які встановлюють порядок обробки персональних даних або визначають правовий режим функціонування публічних реєстрів (баз даних), інформаційно-телекомунікаційних систем, призначених для обробки персональних даних, ЦОВВ – суб'єкт нормотворчої діяльності повинен обов'язково визначити мету обробки персональних даних у відносинах, що підлягають врегулюванню.

- У проєктах нормативно-правових актів мета обробки персональних даних повинна визначатися ЦОВВ з урахуванням міжнародних стандартів і національного законодавства і бути сформульованою з дотриманням критеріїв чіткості, законності та пропорційності, а також бути сформульованою до початку обробки персональних даних.

- Якщо проєкт нормативно-правового акту одночасно визначає порядок обробки персональних даних та правовий режим публічного реєстру (бази даних), інформаційно-телекомунікаційної системи, де передбачається відповідна обробка, мета повинна визначатися окремо по кожному з цих аспектів правового регулювання. При цьому, мета функціонування публічного реєстру (бази даних), інформаційно-телекомунікаційної системи повинна враховувати мету обробки персональних даних, для виконання якої і утворюється відповідний інформаційний ресурс.

Типове порушення 4. Недотримання ЦОВВ у процесі розробки проєктів нормативно-правових актів принципів відповідності, адекватності та ненадмірності обробки персональних даних.

4.1. Нормативні вимоги:

Згідно з пунктом «с» статті 5 Конвенції Ради Європи № 108, персональні дані, що піддаються автоматизованій обробці, повинні бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються.

Частиною другою статті 32 Конституції України встановлено, що не допускається 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 прав людини.

Згідно з частиною третьою статті 6 Закону України «Про захист персональних даних», склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки.

Відповідно до пункту 2.3. Порядку, процедури обробки, строк обробки та склад персональних даних повинні бути пропорційними меті обробки.

Слід звернути увагу, стаття 2 Закону України «Про захист персональних даних» визначає обробку персональних даних, як будь-яку дію 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.

4.2. Правові позиції судової практики, на яких ґрунтується роз'яснення щодо запобігання викладеного типового порушення:

– «M.K. v. France» (заява № 19522/09, рішення від 18042013) – ведення реєстру відбитків пальців. Принцип необхідності та пропорційності збору персональних даних;

– «Uzun v. Germany» (заява № 35623/05, рішення від 02/09/2010) - спостереження за шляхами пересування особи (GPS-дані) здійснювалося законно та було пропорційним;

– «Kennedy v. The United Kingdom» (заява № 26839/05, рішення від 18.05.2010) – Законність підстав та порядку проведення негласного спостереження (перегляд кореспонденції, прослуховування розмов);

- «Авілкіна та інші проти Російської Федерації» - за компетентними державними органами повинна зберігатися певна свобода розсуду стосовно встановлення справедливого

балансу між відповідними громадськими та приватними інтересами, які суперечать один іншому. Однак така свобода розсуду супроводжується європейським наглядом;

- «Суріков проти України» («Surikov v. Ukraine»; заява №42788/06; рішення від 26.04.2017р.) зазначено проте, що на сьогоднішній день був досягнутий певний рівень консенсусу на міжнародному рівні та, зокрема, між державами – членами Ради Європи стосовно фундаментальних принципів захисту даних та пов'язаних базових процедурних гарантій, які мають бути включені в національну правову систему, щоб виправдати необхідність будь-якого втручання;

- «С. і Марпер проти Сполученого Королівства» («S. and Marper v. United Kingdom»; заяви № 30562/04 та № 30566/04; рішення від 04.12.2008 р.) - захист персональних даних відіграє фундаментальне значення для реалізації права людини на повагу до приватного і сімейного життя, гарантованого ст. 8 Конвенції. Внутрішнє законодавство повинно забезпечувати відповідні гарантії для запобігання будь-якого використання персональних даних, яке може бути несумісним із гарантіями, передбаченими цією статтею.

4.3. Рекомендовано:

- У проєктах нормативно-правових актів, що розробляються ЦОВВ обов'язково необхідно визначати принципи, на яких ґрунтується обробка персональних даних, яка потребує врегулювання, зокрема, принципи адекватності, відповідності стосовно мети обробки персональних даних.

- Зважаючи на зміст принципів, які повинні визначатися у проєкті нормативно-правового акту стосовно обробки персональних даних, ЦОВВ – суб'єктам нормотворчої діяльності характер дій, що можуть вчинятися з персональних даних необхідно обмежити тією мірою, якою це необхідно для досягнення законної мети обробки персональних даних забезпечення прав суб'єктів персональних даних.

- Якщо проєкт нормативно-правового акту одночасно спрямований на визначення порядку обробки персональних даних та закріплення правового режиму публічного реєстру (бази даних), інформаційно-телекомунікаційної системи, з використання передбачається вчинення дій володільцем чи розпорядником щодо персональних даних, ЦОВВ повинен окремо визначити принципи формування та застосування інформаційного ресурсу, з використанням якого буде здійснюватися обробка персональних даних.

Типове порушення 5. Окремі нормативно-правові акти спрямовані на обмеження або звуження змісту прав суб'єктів персональних даних, зазначених у частині другій статті 8 Закону України «Про захист персональних даних».

5.1. Зміст нормативних вимог:

Згідно з положеннями статті 1 Конституції України: «Україна є незалежною, демократичною, соціальною, правовою державою». Конституційне визнання за Україною відповідного статусу забезпечується повсюдною дією принципу верховенства права, основоположним значенням прав і свобод людини і громадянина для встановлення змісту та спрямованості діяльності держави.

Цьому правилу, зокрема, кореспондує передбачена у частині першій статті 32 Конституції України норма, відповідно до якої: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України».

Як слідує з буквального змісту наведеної норми, перелік підстав для втручання в особисте сімейне життя, зокрема, шляхом збирання і обробки інформації про фізичну особу є імперативним і визначається виключно Конституцією України.

Згідно з приписами частини другою статті 32 Конституції України: «Не допускається 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 прав людини».

Вказана конституційна норма спирається на стандарти Ради Європи, закладені у статті 8 Конвенції Ради Європи «Про захист прав людини і основоположних свобод».

Згідно з вказаними положеннями Конвенції: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції».

Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб».

Таким чином, частина друга статті 32 Конституції України та частина друга статті 8 Конвенції Ради Європи «Про захист прав людини та основоположних свобод» визначили, вичерпний перелік підстав для обробки персональних даних без згоди суб'єкта персональних даних та обмеження їхніх прав в нормах національного законодавства України.

Як слідує зі змісту норми, передбаченої у частині першій статті 8 Закону України «Про захист персональних даних», особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

Основні види прав суб'єктів персональних даних закріплені частиною другою статті 8 згаданого Закону України, але їх перелік не є вичерпним і може розширюватися в нормах інших Законів України.

Звертаємо увагу, що відповідно до статті 92 Конституції України виключно законами визначаються права і свободи людини і громадянина, гарантії цих прав і свобод; основні обов'язки громадянина (пункт 1).

При цьому, частина друга статті 22 Конституції України містить важливу гарантію сутність якої виявляється в тому, що при прийнятті нових законів або внесення змін та доповнень до вже чинних не допускається звуження змісту та обсягу вже існуючих прав і свобод.

Відповідно до частини першої статті 1 Закону України «Про захист персональних даних», цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Частиною другою статті 1 вказаного Закону також передбачено, що цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Слід підкреслити, частиною першою статті 27 Закону України «Про захист персональних даних» закріплено важливу нормативну вимогу, відповідно до якої: «Положення щодо захисту персональних даних, викладені в цьому Законі, можуть доповнюватися чи уточнюватися іншими законами, за умови, що вони встановлюють вимоги щодо захисту персональних даних, що не суперечать вимогам цього Закону».

Отже, при прийнятті нормативно-правових актів, спрямованих на регулювання суспільних відносин у сфері обробки і захисту персональних даних не допускається зміна та/або звуження прав і свобод суб'єктів персональних даних, визначених Законом України «Про захист персональних даних», а також зміна вимог до обробки і захисту персональних даних, передбачених цим Законом, крім випадків, прямо передбачених в його нормах.

5.2. Правові позиції судової практики, на яких ґрунтується роз'яснення щодо запобігання викладеного типового порушення:

- «С. і Марпер проти Сполученого Королівства» («S. and Marper v. United Kingdom»; заяви № 30562/04 та № 30566/04; рішення від 04.12.2008 р.) - захист персональних даних відіграє фундаментальне значення для реалізації права людини на повагу до приватного і

сімейного життя, гарантованого ст. 8 Конвенції. Внутрішнє законодавство повинно забезпечувати відповідні гарантії для запобігання будь-якого використання персональних даних, яке може бути несумісним із гарантіями, передбаченими цією статтею;

- абзац другий пункту 3 мотивувальної частини Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012, лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці;

- «Про застосування Конституції України при здійсненні правосуддя», Постанова Пленуму Верховного Суду України від 01.11.1996 року № 9: «Конституційні права та свободи людини і громадянина є безпосередньо діючими. Вони визначають цілі і зміст законів та інших нормативно-правових актів, зміст і спрямованість діяльності органів законодавчої та виконавчої влади, органів місцевого самоврядування і забезпечуються захистом правосуддя».

5.3. Рекомендовано:

- У проєктах нормативно-правових актів ЦОВВ забороняється формулювати положення спрямовані на звуження змісту або переліку прав і свобод суб'єктів персональних даних, закріплених у частині другій статті 8 Закону України «Про захист персональних даних».

- За наявності у текстах чинних нормативно-правових актів положень, які обмежують або звужують права суб'єктів персональних даних, такі нормативно-правові акти доцільно визнати частково недійсними у порядку, встановленому законодавством України.

Типове порушення 6. Відсутність у проєктах нормативно-правових актів ЦОВВ спеціальних вимог щодо обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних в тих випадках, коли така обробка передбачається проєктом конкретного акту.

6.1. Нормативні вимоги:

Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації (далі Порядок повідомлення Уповноваженого), затверджений Наказом Уповноваженого від 08.01.2014 року № 1/02-14, у

пункті 1.2. визначає обробку персональних даних, що становить особливий ризик для прав і свобод суб'єктів як будь-яку дію або сукупність дій, а саме збирання, реєстрацію, накопичення, зберігання, адаптування, зміну, поновлення, використання і поширення (розповсюдження, реалізацію, передачу), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, 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 в 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.

Необхідно звернути увагу, щодо вказаної категорії персональних даних стаття 6 Конвенції Ради Європи № 108 передбачає для Держав-учасниць Конвенції зобов'язання, відповідно до яких, автоматизована обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних особливий ризик допускається лише за умови закріплення у нормах національного законодавства необхідних гарантій.

До таких гарантій Закон України «Про захист персональних даних» серед іншого відносить обов'язок володільця персональних даних письмово повідомляти Уповноваженого про випадки обробки персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних, а також заборону на обробку таких даних, крім випадків, прямо передбачених у частині другій статті 7 вказаного Закону.

Згідно з частиною другою статті 7 Закону України «Про захист персональних даних», обмеження щодо обробки персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних не поширюються на наступні випадки:

- здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

- необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

- необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

- здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;

- необхідна для обґрунтування, задоволення або захисту правової вимоги;

- необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних;

- стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

- стосується даних, які були явно оприлюднені суб'єктом персональних даних.

Вказаний перелік випадків, коли допускається обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних є вичерпним і не підлягає розширенню у підзаконних нормативно-правових актах.

Згідно з підпунктом 2.1. пункту 2 Порядку повідомлення Уповноваженого, володільць персональних даних повідомляє Уповноваженого Верховної Ради України з прав людини про здійснення ним будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, крім випадків, якщо:

- здійснюється обробка, єдиною метою якої є ведення реєстру для надання інформації населенню, який відкритий для населення в цілому;

- обробка здійснюється громадськими об'єднаннями, політичними партіями та/або організаціями, професійними спілками, об'єднаннями роботодавців, релігійними організаціями, громадськими організаціями світоглядної спрямованості за умови, що обробка стосується виключно персональних даних членів цих об'єднань та не передається без їх згоди;

- обробка необхідна для реалізації прав та виконання обов'язків володільця персональних даних у сфері трудових правовідносин відповідно до закону.

Таким чином, проєкт нормативно-правового акту може закріплювати правила обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних лише за умови забезпечення належних гарантій запобігання ризиків, пов'язаних зі здійсненням такої обробки.

6.2. Правові позиції судової практики, на яких ґрунтується роз'яснення щодо запобігання викладеного типового порушення:

- «Gaskin v. The United Kingdom» (заява № 10454/83, рішення від 07/07/1989) - Обмеження доступу особи до її персональних даних (документів щодо виховання дитини опікуном/прийомними батьками) з огляду на відсутність незалежного органу, який би розглядав клопотання щодо надання доступу;

- «K.H. and Others v. Slovakia» (заява № 32881/04, рішення від 06/11/2009) – Ненадання лікарнею заявникам копій їх медичної документації;

- «L.H. v. Latvia» (заява № 52019/07, рішення від 29/04/2014) - Збір інформації контролюючим органом із метою оцінки якості наданої пацієнту медичної допомоги лікарнею. Відсутність легітимної мети збору персональних даних. Надмірний об'єм зібраної інформації. Неврахування інтересів пацієнта;

– «Z. v. Finland» (заява № 22009/93, рішення від 25/02/1997) - Недостатність строків, впродовж яких обмежувався доступ до рішення суду, що містив чутливу інформацію про заявницю;

– «P.G. and J.H. v. The United Kingdom» (заява № 44787/98, рішення від 25/09/2001) Відбір та збереження зразків голосу.

6.3. Рекомендовано:

- У проєктах нормативно-правових актів, які спрямовані на врегулювання відносин щодо обробки персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних обов'язково необхідно визначати підстави для такої обробки з посиланням на приписи частини другої статті 7 Закону України «Про захист персональних даних», мету обробки, а також процедури повідомлення Уповноваженого про відповідну обробку.

- У проєкті нормативно-правового акту важливо передбачити положення щодо розмежування процедур обробки персональних даних, які становлять особливий ризик для прав та свобод суб'єктів персональних даних та персональних даних, обробка яких не тягне за собою відповідних наслідків.

- Якщо проєктом нормативно-правового акту передбачається врегулювання суспільних відносин щодо обробки персональних даних, що становить особливий ризик для прав і свобод суб'єкта персональних даних, такий акт повинен враховувати вимоги Порядку повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, затвердженого Наказом Уповноваженого від 08.01.2014 року № 1/02-14.

Типове порушення 7. Відсутність в проєктах нормативно-правових актів, які встановлюють порядок обробки персональних даних або правовий режим публічного реєстру (бази даних), інформаційно-телекомунікаційної системи положень щодо процедур призначення, статусу та повноважень відповідальної особи/структурного підрозділу з питань обробки персональних даних.

7.1. Зміст нормативних вимог:

Закон України «Про захист персональних даних» у частині другій статті 24 встановив важливу вимогу для правового регулювання відносин у сфері обробки та захисту персональних даних. Згідно з вказаною нормою, органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють

обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому, який забезпечує її оприлюднення.

За своїм правовим статусом структурний підрозділ з питань обробки персональних даних не є юридичною особою та, зазвичай, утворюється як департамент, відділ, управління з питань обробки персональних даних.

Відповідно до підпункту 2.2. пункту 2 Типового порядку, у випадках, передбачених Законом, володільць також визначає обов'язки та права осіб, відповідальних за організацію роботи, пов'язаної із захистом персональних даних під час їх обробки.

Згідно з частиною третьою статті 24 Закону України «Про захист персональних даних» та підпунктом 3.17. пункту 3 Типового порядку, відповідальна особа/структурний підрозділ виконує такі завдання:

- інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

- взаємодіє з Уповноваженим та визначеними ним посадовими особами його Секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

З метою виконання вказаних завдань відповідальна особа/структурний підрозділ:

- 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.

Вимоги відповідальній особі до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних, підпункт 3.19 пункту 3 Типового порядку.

Таким чином, зі змісту наведених норм слідує, що в тих випадках, коли проєкт нормативно-правового акту спрямований на врегулювання відносин щодо персональних даних, обробка яких супроводжується повідомленням Уповноваженого про таку обробку, ЦОВВ – суб'єкти нормотворчої діяльності обов'язково повинні включати до таких актів положення стосовно відповідальної особи/структурного підрозділу з питань обробки персональних даних.

7.2. Рекомендовано:

- Якщо проєкт нормативно-правового акту визначає порядок обробки персональних даних, обробка яких вимагає повідомлення Уповноваженого про такі дії з персональними даними, або нормативно-правовим актом затверджується положення про публічний реєстр (базу даних), інформаційно-телекомунікаційну систему, призначену для обробки категорії чутливих персональних даних, у проєкті такого нормативно-правового акту обов'язково повинні закріплюватися положення щодо статусу відповідальної особи/структурного підрозділу з відповідних питань;

- Проєкт нормативно-правового акту, який містить положення щодо відповідальної особи/структурного підрозділу з питань обробки персональних даних, обов'язково повинен містити положення щодо визначення його статусу, процедуру призначення (формування для структурних підрозділів), гарантії його діяльності;

- Важливо, щоб проєкт нормативно-правового акту, який містить положення щодо діяльності відповідальної особи/структурного підрозділу з питань обробки персональних даних встановлював порядок взаємодії цієї посадової особи/структурного підрозділу з Уповноваженим відповідно до вимог чинного законодавства України.