Проєкт Ради Європи
«Підтримка впровадження європейських стандартів прав людини в Україні»

24 квітня 2023 року

ПРАВОВИЙ ВИСНОВОК НА ПРОЄКТ ЗАКОНУ УКРАЇНИ «ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ» (№8153 ВІД 25 ЖОВТНЯ 2022 РОКУ)

ЗМІСТ

1. ВСТУП

Рада Європи здійснює реалізацію проєкту «Підтримка впровадження європейських стандартів прав людини в Україні» (далі – Проєкт), який фінансується в межах плану дій Ради Європи для України «Стійкість, відновлення та відбудова» (2023-2026). Мета Проєкту полягає у підтримці національних інституцій прав людини щодо ефективної реалізації їхнього мандату, включаючи надання експертної допомоги у приведенні національного законодавства у відповідність до європейських стандартів.

Правовий висновок підготовлений на запит Комітету Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій України, національних меншин і міжнаціональних відносин від 26 січня 2023 року.

Діана Шинкунієнє, Директор Інспекції з питань захисту персональних даних Литовської Республіки та Нана Ботчорішвілі, адвокат у сфері захисту персональних даних та приватності були залучені у якості міжнародних експертів Ради Європи до підготовки правового висновку на предмет відповідності проєкту Закону України «Про захист персональних даних» (надалі — «Проєкт Закону») стандартам Ради Європи та іншим європейським стандартам.

Правовий висновок обмежений лише вище зазначеним Проєктом Закону і не торкається всього пакету змін законодавства про захист персональних даних. Рада Європи готова долучитись до завершення цієї значної роботи шляхом подальшого обговорення ключових аспектів реформи у сфері захисту персональних даних з українськими органами влади.

Метою цього правового висновку є аналіз Проєкту Закону та надання рекомендацій щодо його вдосконалення. В основу цього правового висновку покладено стандарти Ради Європи та Європейського Союзу, зокрема оновлена Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS No. 108) із змінами, внесеними Протоколом CETS № 223 та прийнятою Комітетом міністрів на 128-й сесії Комітету міністрів (Ельсінор, 18 травня 2018 року), та Постанова (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних та скасування Директиви 95/46/ЕС (Загальний регламент захисту даних). Беручи до уваги,

що Проєктом Закону[1] пропонується імплементація положень правових актів ЄС, додатково для цілей підготовки цього висновку були взяті до уваги положення наступних правових актів ЄС: Директива (ЄС) 2016/680 Європейського парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів або виконання кримінальних покарань, а також про вільне переміщення таких даних (Директива про захист даних у правоохоронній діяльності), та Директива 2002/58/ЕС Європейського парламенту і Ради від 12 липня 2002 року про обробку персональних даних і захист приватного життя в секторі конфіденційності (Директива про конфіденційність та електронні комунікації).

З метою забезпечення узгодженості наданих рекомендацій автори цього правового висновку взяли до уваги висновок, підготовлений у 2020 році до попередньої редакції проєкту Закону України «Про захист персональних даних»[2], а також результати обговорення з українськими партнерами, які відбулись у 2021 році[3]. Авторам також відомо про проєкт Закону про наглядовий орган «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» (№ 6177 від 18.10.2021 р.), який перебуває на розгляді одного з Комітетів Верховної Ради України[4].

У разі прийняття, Проєкт Закону слугуватиме основою для захисту персональних даних як у державному, так і приватному секторах, а також для законодавчих органів при прийнятті правових актів, що регулюють обробку персональних даних та їх безпеку.

[1] Інформація, наведена в Пояснювальній записці до проєкту Закону України «Про захист персональних даних» (додаток 1), стор. 2, 3.
[2] Правовий висновок до проєкту Закону України «Про захист персональних даних» № 5628 від 07.06.2021 р. з рекомендаціями щодо приведення його у відповідність до стандартів Ради Європи та європейських стандартів, підготовлений Наташою Пірч Мусар та Діаною Шинкунієнє, 16 жовтня 2020 року (до реєстрації проєкту Закону в Верховній Раді України).
[3] Онлайн-консультації відбулись 29 квітня 2021 року, таблиця коментарів до проєкту Закону України «Про захист персональних даних» №5628 від 07.06.2021 р. та правовий висновок до нього, підготовлений в межах спільного проєкту Європейського Союзу та Ради Європи (Додаток 2).
[4] Інформація, наведена в пояснювальній записці до проєкту Закону України «Про захист персональних даних» №8153 від 25.10.2022 р.(Додаток 1, Стор. 8).

2. ПЕРЕЛІК СКОРОЧЕНЬ

Проєкт Закону	Проєкт Закону України «Про захист персональних даних»
Конвенція 108+	Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108), прийнята 28 січня 1981 року в Страсбурзі, з поправками, внесеними Протоколом CETS № 223
GDPR	Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних та скасування Директиви 95/46/ЕС (Загальний регламент про захист даних)
Директива про захист даних у правоохоронній діяльності	Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або судового переслідування кримінальних злочинів або виконання кримінальних покарань, а також про вільне переміщення таких даних
Директива про конфіденційність та електронні комунікації	Директива 2002/58/ЕС Європейського парламенту та Ради від 12 липня 2002 року про обробку персональних даних і захист конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації) з подальшими

	поправками, внесеними у 2006 та 2009 роках
Пояснювальний записка	Пояснювальна записка до Конвенції 108+, схвалена Комітетом міністрів на 128-й сесії (Ельсінор, 18 травня 2018 р.)
Таблиця коментарів	Таблиця коментарів до проєкту Закону України «Про захист персональних даних» №5628 від 07.06.2021 р. та правовий висновок до нього, підготовлений в межах спільного проєкту Європейського Союзу та Ради Європи (Додаток 2)

3. КОМЕНТАРІ ЗА СТАТТЯМИ ПРОЄКТУ ЗАКОНУ УКРАЇНИ «ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ»

3.1. ПРЕАМБУЛА ТА РОЗДІЛ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Преамбула Проєкту Закону відповідає Конвенції 108+ та GDPR.

Стаття 1. Сфера дії Закону

Стаття відповідає Конвенції 108+ та GDPR.

Стаття 2. Визначення термінів

Згідно з визначенням, наведеним у цій статті, термін «біометричні дані» означає персональні дані, отримані як результат спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи, які дають змогу ідентифікувати або верифікувати цю фізичну особу, в тому числі за такими параметрами як цифровий підпис особи, цифрове зображення особи, цифрові відбитки пальців. Формулювання «<...> в тому числі за такими параметрами, як цифровий підпис особи, цифрове зображення особи, цифрові відбитки пальців» передбачає, що самі ці параметри повинні розглядатися як біометричні дані. Однак такий підхід не є коректним. Слід зазначити, що цифровий підпис зазвичай означає електронний підпис, який не відноситься до біометричних даних (цей висновок може бути підкріплений положеннями частиною 6 тієї самої статті, яка передбачає, що термін «цифровий підпис» має використовуватися у значенні, передбаченому Законом України «Про електронні довірчі послуги»). Поняття «цифрові відбитки пальців» описує дані, що належать особі, яка користується інтернетом, застосовуючи різні цифрові пристрої. Згідно з п. 59 Пояснювальної записки, обробка зображень підпадатиме під визначення біометричних даних тільки в тому випадку, якщо дані обробляються за допомогою спеціального технічного засобу, який дає змогу здійснювати унікальну ідентифікацію або автентифікацію особи. Таким чином, само по собі цифрове зображення обличчя людини не має розглядатися як біометричні дані.

Згідно з визначенням біометричних даних, наведеним у пункті 14 статті 4 GDPR, термін «біометричні дані» **означає персональні дані, отримані як результат спеціальної технічної обробки**, що стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи, які забезпечують або підтверджують унікальну ідентифікацію цієї фізичної особи, наприклад, зображення обличчя або дактилоскопічні дані (відбитки пальців), є прикладами ознак фізичної особи, які мають пройти спеціальну технічну обробку, щоб вважатися біометричними даними.

Необхідно внести зміни до визначення терміну «біометричні дані», виключивши наступну частину - «в тому числі за такими параметрами як цифровий підпис особи, цифрове зображення особи, цифрові відбитки пальців», або використати формулювання, яке б не створювало розбіжностей. Рекомендуємо використати визначення терміну «біометричні дані», що наведений в Таблиці коментарів[5].

Відповідно до цієї статті, «обмеження обробки» означає позначення збережених персональних даних з метою обмеження їх подальшої обробки. Пункт 3 статті 4 GDPR і пункт 3 статті 3 Директиви про захист даних в правоохоронній діяльності передбачає, що «обмеження обробки» означає маркування збережених персональних даних з метою обмеження їх обробки у майбутньому.

Задля уникнення розбіжностей рекомендується внести зміни у визначення терміну «обмеження обробки», використовуючи слово «маркування» замість «позначення».

Визначення «правоохоронного органу», наведене у цій статті, передбачає, що «правоохоронний орган» — це державний орган, на який покладаються завдання щодо попередження, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, віднесених до його компетенції; забезпечення захисту прав і свобод людини, протидії злочинності, підтримання громадської безпеки та порядку; уповноважений виконувати кримінальні покарання; відкривати та проводити досудове розслідування та дізнання, забезпечувати процесуальне керівництво досудовим розслідуванням; державний орган спеціального призначення з правоохоронними функціями, який забезпечує національну безпеку України; розвідувальні та контррозвідувальні органи. Відповідно до визначення терміну «обробка персональних даних в правоохоронних цілях» з метою забезпечення захисту прав і свобод людини також є одним з елементів обробки персональних даних в правоохоронних цілях[6].

[5] **«Біометричні дані»**: персональні дані, отримані як результат спеціальної технічної обробки, які стосуються фізичних, фізіологічних характеристик фізичної особи та дають змогу ідентифікувати або верифікувати фізичну особу (Див. стор. 4).

[6] Згідно з частиною 1 статті 2 Проєкту Закону, «обробка персональних даних в правоохоронних цілях» означає обробку персональних даних правоохоронними органами, спрямовану на запобігання, виявлення, припинення, розкриття і розслідування кримінальних правопорушень, виконання кримінальних покарань; забезпечення захисту прав і свобод людини, протидію злочинності, підтримання громадської безпеки та порядку; відкриття та проведення досудового розслідування та дізнання, процесуальне керівництво досудовим розслідуванням; здійснення розвідувальної діяльності; забезпечення національної безпеки.

Відповідно до пункту 7 статті 3 Директиви про захист даних у правоохоронній діяльності термін «компетентний орган»" означає: а) будь-який державний орган, який має повноваження щодо попередження, розслідування, виявлення або підтримання кримінального обвинувачення та виконання кримінальних покарань, включно із захистом від загроз громадській безпеці та запобіганням їм; або б) будь-який інший орган або організація, яким законодавством держави-члена доручено здійснювати державну владу та офіційні повноваження з метою попередження, розслідування, виявлення або підтримання кримінального обвинувачення або виконання кримінальних покарань, включно з захистом від загроз громадській безпеці та запобіганням їх виникненню.

Зважаючи на те, що правоохоронні органи під час обробки персональних даних мають гарантувати дотримання прав людини, тим не менш, відповідно до Директиви про захист персональних даних у правоохоронній діяльності це не є завданням компетентних органів. Таким чином, рекомендується переглянути визначення терміну «правоохоронний орган» та терміну «обробка персональних даних в правоохоронних цілях», доповнивши наступним текстом – «гарантування законного дотримання прав і основоположних свобод людини» замість "забезпечення охорони прав і свобод людини".

Стаття 3. Законодавство про захист персональних даних

Ця стаття не потребує змін або доповнень.

Стаття 4. Принципи, пов’язані з обробкою персональних даних

Ця стаття не потребує змін або доповнень.

3.2. РОЗДІЛ II. ПІДСТАВИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 5. Підстави для обробки персональних даних

Згідно з частиною 5 статті 5 Проєкту Закону обробка персональних даних на підставі згоди суб’єкта персональних даних, а також з огляду на необхідність захисту життєво важливих інтересів суб’єкта персональних даних або іншої фізичної особи, може здійснюватися лише у випадку відсутності інших підстав, передбачених частиною 1 цієї статті. Відповідно до цього положення можна зробити висновок, що інші підстави для законної обробки мають пріоритет над підставами згоди і захисту життєво важливих інтересів.

Пунктом 2 статті 5 Конвенції 108+ передбачається, що обробка даних може здійснюватися на основі добровільної, конкретної, поінформованої та однозначної згоди суб’єкта даних або на

будь-якій іншій законній підставі, передбаченій законом. У пункті 1 статті 6 GDPR встановлені умови законності обробки. У Конвенції 108+ і GDPR не віддається пріоритет жодній з підстав для законної обробки даних, тобто всі правові підстави рівні.

Частина 5 статті 5 Проєкту Закону суперечить пункту 2 статті 5 Конвенції 108+ та пункту 1 статті 6 GDPR і тому має бути виключена.

Стаття 6. Згода на обробку персональних даних

Відповідно до пункту 1 частини 3 статті 6 Проєкту Закону згода не вважається добровільною, якщо суб'єкт персональних даних залежить від контролера, якому надає згоду, або підпорядковується йому. Слід зазначити, що у випадках підпорядкування (наприклад, у відносинах «роботодавець-працівник») добровільна згода можлива. Керівні принципи 05/2020 про згоду відповідно до Регламенту 2016/679, прийнятого 4 травня 2020 року Європейською Радою із захисту даних, передбачають, що характер відносин між роботодавцем і працівником не означає, що роботодавці ніколи не можуть покладатися на згоду як на законну підставу для обробки. Таким чином, за виняткових обставин добровільно надана згода все ж таки можлива (див. пункти 21, 22, 23, стор. 9)[7]. Частиною 2 статті 52 Проєкту Закону також передбачено можливість збору даних співробітників на підставі згоди. У такий спосіб пункт 1 частини 3 статті 6 суперечить цьому положенню.

Рекомендується внести зміни до формулювання пункту 1 частини 3 статті 6 Проєкту Закону, усунувши заборону на добровільно надану згоду, якщо існує залежність або підпорядкування між контролером даних і суб'єктом даних, оскільки це положення суперечитиме частині 2 статті 52 Проєкту Закону та Керівним принципам 05/2020 про згоду згідно Регламенту 2016/679.

Відповідно до частини 5 статті 6 Проєкту Закону, згода суб'єкта персональних даних на обробку його персональних даних вважається поінформованою, якщо до або в момент надання такої згоди суб'єкт персональних даних поінформований про таке:

1) підставу, мету, вид обробки його персональних даних;
2) персональні дані, які підлягають обробці;

[7] Доступно за посиланням: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf станом на 17 лютого 2023 року.

3) контактні дані контролера: постійне місцезнаходження та засоби зв'язку, які дають змогу суб'єкту персональних даних ідентифікувати такого контролера і оператора та безперешкодно зв'язатися з ними;

4) права, передбачені законодавством у сфері захисту персональних даних, і способи їх реалізації;

5) будь-яка інша інформація, необхідна для забезпечення чесної та прозорої обробки персональних даних.

Відповідно до положень пункту 2 статті 5 Конвенції 108+ обробка даних може здійснюватися на основі добровільної, конкретної, поінформованої та однозначної згоди суб'єкта даних. Зазначені вище Керівні принципи 05/2020 про згоду відповідно до Регламенту 2016/679, прийнятого 4 травня 2020 року Європейською Радою із захисту даних, передбачають, що для отримання чинної згоди суб'єкту даних має бути надана щонайменше така інформація:

i. дані про контролера;

ii. мета кожної з операцій щодо обробки, на які запитується згода;

iii. (тип) даних, що збиратимуться і використовуватимуться;

iv. наявність права відкликати згоду;

v. інформація про використання даних для автоматизованого прийняття рішень відповідно до положень пункту 2(c) статті 22 GDPR] (у відповідних випадках);

vi. можливі ризики передачі даних через відсутність рішення щодо відповідності та належних гарантій, як описано у статті 46 GDPR.

Слід зазначити, що надання інформації, наприклад, про права, передбачені законодавством у сфері захисту персональних даних та способи їх реалізації, не є необхідним для отримання поінформованої згоди.

Пропонується внести зміни до частини 5 статті 6 Проєкту Закону , встановивши чітку вимогу надавати інформацію про право відкликати згоду, про використання даних для автоматизованого прийняття рішень (у відповідних випадках), про можливі ризики передачі даних через відсутність рішення щодо відповідності та/або належних гарантій в третіх країнах (у відповідних випадках).

3.3. РОЗДІЛ III. СПЕЦІАЛЬНІ ВИМОГИ ЩОДО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 7. Особливі вимоги до обробки чутливих персональних даних

Відповідно до пункту 8 частини 2 статті 7 положення частини 1 цієї статті не застосовуються, якщо обробка необхідна для цілей профілактики захворювань або лікування професійних захворювань, для оцінки працездатності працівника, постановки медичного діагнозу, надання соціальних або послуг у сфері охорони здоров'я (включно з електронною системою охорони здоров'я), лікування або управління системою охорони здоров'я або соціальних послуг на основі закону або договору із медичним працівником із дотриманням умов і гарантій, передбачених частиною 2 цієї статті.

Оскільки відповідні гарантії захисту передбачені не саме в частині 2, а в частині 3, необхідно відредагувати частину 2, зробивши посилання на частину 3 статті 7 замість частини 2. Також частина 3 статті 7 має містити посилання на пункт 8 частини 2 цієї статті, оскільки умови (зобов'язання зберігати професійну таємницю) застосовуються лише в такому випадку відповідно до положень пункту 3 статті 9 GDPR.

Стаття 8. Обробка персональних даних, пов'язаних з притягненням до кримінальної відповідальності, правопорушень, кримінальних проваджень і судимості, а також пов'язаних із цим заходів безпеки

Згідно з частиною 2 статті 8 Проєкту Закону, обробка персональних даних, пов'язана із притягненням осіб до кримінальної відповідальності, правопорушеннями, кримінальними провадженнями і судимістю, а також пов'язаних із цим заходів безпеки, повинна здійснюватися контролюючим органом у затвердженому ним порядку.

У частині 1 статті 2 Проєкту Закону дається визначення терміну «контролюючий орган», а саме незалежний уповноважений орган, який здійснює нагляд і контроль за дотриманням вимог цього Закону, та повноваження якого передбачені цим Законом та Законом, який визначає орган, що здійснює державний контроль за дотриманням законодавства про захист персональних даних. Ведення реєстру судимостей, встановлення правил, що стосуються функціонування такого реєстру, не має входити до завдань органу з питань нагляду за дотриманням законодавства про захист персональних даних. Відповідно до статті 10 GDPR, будь-який повний реєстр судимостей повинен вестися лише під контролем офіційного органу.

Частина 2 статті 8 Проєкту Закону має бути узгоджена зі статтею 10 GDPR, якою

зобов'язання вести всеосяжний реєстр судимостей покладається на офіційний орган, але не на контролюючий орган.

Стаття 9. Обробка біометричних даних суб'єктами владних повноважень

Пункт 3 частини 1 статті 9 містить посилання на частину 2 статті 7 цього Проєкту Закону, який регулює загалом обробку особливих категорій персональних даних. Статтею 9 встановлюються конкретні умови обробки біометричних даних суб'єктами владних повноважень, тому посилання на статтю 7 є незрозумілим (тобто, чи може частина 2 статті 7 застосовуватися до обробки біометричних даних суб'єктами владних повноважень та якою мірою). З іншого боку, незрозумілий взаємозв'язок між частинами 1 та 2 статті 9.

Пропонується внести наступні зміни: 1) виключити або уточнити посилання на частину 2 статті 7 у пункті 3 частини 1 статті 9; 2) уточнити взаємозв'язок між частинами 1 і 2 статті 9 Проєкту Закону (наприклад, «Обробка біометричних даних суб'єктами владних повноважень є правомірною, якщо вона **відповідає умовам, викладеним у частині 1 цієї статті, і** здійснюється з такою метою <…>»).

Стаття 10. Здійснення відеоспостереження

Згідно з частиною 5 статті 10 Проєкту Закону контролер зобов'язаний розмістити попередження про те, що здійснюється відеоспостереження, у доступному місці державною мовою. Попередження повинно містити ім'я та контактні дані контролера та особи, яка здійснює відеоспостереження, якщо ця інша особа не є контролером. Незрозуміло, хто є «особою, яка здійснює відеоспостереження», і чому право суб'єкта даних на інформацію обмежується лише зібраними персональними даними (тобто попередженням про те, що здійснюється відеоспостереження), а також ім'ям і контактними даними контролера. Щодо обмежень, які стосуються прозорості обробки, то відповідно до пункту 1 статті 11 Конвенції 108+ не допускається жодних винятків з положень пункту 1 статті 8, що регулюють прозорість обробки, за винятком випадків, коли такий виняток передбачений законом, поважає суть основних прав і свобод та становить необхідний і відповідний у демократичному суспільстві захід захисту суспільних інтересів (таких як громадська безпека тощо). Слід зазначити, що інформація, яка стосується обробки даних методом відеоспостереження, може надаватися суб'єкту даних іншими способами, а не лише на попереджувальному знаку. Керівні принципи 3/2019 щодо обробки персональних даних за допомогою відеопристроїв, прийняті 29 січня 2020 року Європейською Радою з питань

захисту даних, передбачають, що: «З огляду на обсяг інформації, яка повинна надаватися суб'єкту даних, контролери даних можуть дотримуватися багаторівневого підходу, якщо вони вважають за краще використовувати комбінацію методів для забезпечення прозорості (ПР260, п. 35; ПР89, п. 22). Стосовно відеоспостереження, то найважливіша інформація повинна міститися власне на попереджувальному знаку (перший рівень), а додаткові обов'язкові відомості можуть надаватися в інші способи (другий рівень)»[8].

До частини 5 статті 10 Проєкту Закону слід внести поправки щодо заборони обмежувати право суб'єкта даних на інформацію лише зібраними персональними даними та ім'ям і контактними даними контролера.

Стаття 11. Обробка персональних даних в результаті аудіо-, відео- або фотофіксації публічних заходів

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 12. Обробка персональних даних з метою прямого маркетингу, передвиборної агітації та/або політичної реклами

У частині2 статті 12 Проєкту Закону встановлені умови, за яких обробка персональних даних з метою прямого маркетингу можлива без згоди суб'єкта персональних даних. Однією з цих умов є «контактні дані суб'єкта персональних даних, отримані внаслідок укладення та виконання договору, стороною якого є суб'єкт персональних даних, або для здійснення кроків, необхідних для укладення договору за запитом суб'єкта персональних даних». Слід зазначити, що відповідно до пункту 2 статті 13 Директиви про конфіденційність та електронні комунікації без попередньої згоди можуть використовуватися лише контактні дані електронної пошти: «Попри зазначене у пункті 1, якщо фізична або юридична особа отримує від своїх клієнтів їхні електронні контактні дані для електронної пошти, у контексті продажу товарів або послуг, відповідно до Директиви 95/46/ЕС, одна й та сама фізична чи юридична особа може використовувати ці електронні контактні дані для прямого маркетингу своїх власних аналогічних товарів або послуг. Це може здійснюватися за умови, що клієнтам чітко й недвозначно надається можливість заперечувати (безоплатно і зручним способом) проти такого використання електронних контактних даних під час їх збору та під час відправлення кожного повідомлення, якщо клієнт з самого початку не відмовився від такого

[8] Доступно за посиланням: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf від 24 лютого 2023 р., див. п. 111, с. 26.

використання».

Рекомендується переглянути частину 2 статті 12 Проєкту Закону в контексті пункту 2 статті 13 Директиви про конфіденційність та електронні комунікації, обмеживши сферу його застосування електронними контактними даними для електронної пошти.

Частиною 2 статті 12 Проєкту Закону також встановлена умова, що обробка персональних даних для цілей прямого маркетингу можлива без згоди суб'єкта персональних даних, за умови, що «ступінь втручання у приватне життя суб'єкта персональних даних не більше, ніж була необхідна з метою виконання первинного правочину». Слід зазначити, що сфера застосування пункту 2 статті 13 Директиви про конфіденційність та електронні комунікації не обмежується виконанням первинного контракту, тобто електронні контактні дані електронної пошти можуть використовуватися для прямого маркетингу аналогічних товарів або послуг після укладення первинного контракту.

Рекомендується переглянути частину 2 статті 12 Проєкту Закону в світлі пункту 2 статті 13 Директиви про конфіденційність та електронні комунікації, відмовившись від надмірних обмежень використання контактних даних (електронної пошти) для цілей прямого маркетингу.

Стаття 13. Обробка персональних даних з іншою метою, відмінної від тієї, для якої вони збиралися

У частині 1 статті 13 Проєкту Закону встановлюється перелік обставин, які необхідно враховувати під час визначення того, чи сумісна нова мета обробки з первинною. У пункті 49 Пояснювальної записки роз'яснюється, що: «Для з'ясування того, чи сумісна мета подальшої обробки з метою, для якої персональні дані збиралися початково, контролер, після виконання всіх вимог щодо законності початкової обробки, повинен взяти до уваги, *серед іншого*, будь-який зв'язок між цими цілями та метою очікуваної подальшої обробки; контекст, у якому були зібрані персональні дані, зокрема розумні очікування суб'єктів даних, що ґрунтуються на їхніх стосунках з контролером, щодо їх подальшого використання; характер персональних даних; наслідки передбачуваної подальшої обробки для суб'єктів даних; і наявність відповідних гарантій як під час початкової, так і під час передбачуваної подальшої обробки». У пункті 4(b) статті 6 GDPR, в якому описується контекст збору даних, робиться акцент на взаємовідносинах між суб'єктом даних і контролером даних; у пункті 4(c) статті 6 GDPR підкреслюється природа персональних даних, зокрема,

особливих категорій персональних даних і даних, пов'язаних із судимостями та правопорушеннями.

Рекомендується доповнити частину 1 статті 13 положеннями, що стосуються обґрунтованих очікувань суб'єктів даних, в основі яких лежать їхні взаємовідносини з контролером, а також, що стосуються характеру персональних даних (стосуються безпосередньо особливих категорій персональних даних і даних, пов'язаних із судимостями та правопорушеннями).

У частині 2 статті 13 Проєкту Закону передбачається (без зазначення жодних додаткових гарантій), що обробка з метою архівування в суспільних інтересах, для цілей наукових або історичних досліджень або для статистичних цілей повинна розглядатися як обробка, сумісна з початковою метою. У пункті 50 Пояснювальної записки роз'яснюється, що подальша обробка персональних даних, про яку йдеться у пункті 4(b) статті 5 Конвенції 180+, для цілей архівування в суспільних інтересах, наукових або історичних досліджень або для статистичних цілей *anpiopi* вважається сумісною за умови наявності інших гарантій (таких як, наприклад, анонімізація або псевдонімізація даних, за винятком випадків, коли необхідно збереження форми, яка забезпечує можливість ідентифікації; правила професійної таємниці; положення, що регулюють обмежений доступ і передачу даних для зазначених вище цілей, особливо щодо статистики та державних архівів; та інші технічні та організаційні заходи безпеки даних), і що операції загалом виключають будь-яке використання отриманої інформації для прийняття рішень або заходів, що стосуються конкретної особи. Пунктом 1 статті 89 GDPR також передбачаються гарантії та відступи, що стосуються обробки з метою архівування в суспільних інтересах, для цілей наукових або історичних досліджень або для статистичних цілей.

Частина 2 статті 13 Проєкту Закону потребує перегляду у контексті пункту 4(b) статті 5 Конвенції 108+ та пункту 1 статті 89 GDPR, а саме у частині, що стосується додаткових гарантій.

У частині 3 статті 13 Проєкту Закону зазначається, що якщо нова мета є несумісною з первинною метою, обробка персональних даних для нової мети повинна бути законною у визначених випадках (суб'єкт даних дав згоду, або така обробка необхідна для виконання юридичного обов'язку, передбаченого законом). У пункті декларативної частини 50 GDPR передбачено, що у тих випадках, коли суб'єкт даних дав згоду, або коли обробка ґрунтується

на законодавстві Європейського Союзу або держави-члена, що є необхідним і пропорційним заходом у демократичному суспільстві для захисту, зокрема, важливих цілей, що становлять загальний суспільний інтерес, контролеру має бути дозволено продовжувати обробку персональних даних незалежно від сумісності цілей. Це положення передбачає, що можна не проводити перевірку на сумісність цілей, якщо обробка з новою метою ґрунтується на згоді суб'єкта даних або необхідна для виконання юридичного зобов'язання, передбаченого законом.

Задля уникнення невизначеності буде доцільно внести зміни у формулювання частини 3 статті 13 Проєкту Закон, а саме «якщо нова мета є несумісною з первинною метою, обробка персональних даних з новою метою є правомірною у випадках <...>» до «пункту 1 статті 13 Проєкту Закону не застосовується і обробка персональних даних для нової мети має здійснюватися на підставі <...>» або подібним чином.

Стаття 14. Обробка персональних даних з метою архівування в суспільних інтересах, цілей наукового чи історичного дослідження, або для статистичних цілей

Частина 2 статті 14 Проєкту Закону залишає за контролером, який обробляє персональні дані для цілей наукового або історичного дослідження, право на власний розсуд обмежувати права суб'єкта даних, передбачених статтями 19 (Право суб'єкта персональних даних на доступ до персональних даних), 21 (Право суб'єкта персональних даних бути забутим), 22 (Право заперечувати проти обробки персональних даних), 24 (Право на обмеження обробки персональних даних) цього Закону, якщо їх застосування перешкоджатиме досягненню цих цілей, і таке обмеження необхідно для їх досягнення. По-перше, слід зазначити, що обмеження прав суб'єкта даних у цьому випадку має бути передбачено законом (див. пункт 1 статті 23 та пункт 2 статті 89 GDPR, пункт 2 статті 11 Конвенції 108+). По-друге, обмеження прав суб'єкта даних під час обробки персональних даних для статистичних цілей взагалі не передбачено у Проєкті Закону, хоча це мало б практичну цінність із урахуванням положень пункту 2 статті 89 GDPR, у яких воно згадується у контексті обмежень.

Частина 2 статті 14 Проєкту Закону має бути переглянута у спосіб, який би не залишав контролеру персональних даних можливості на власний розсуд обмежувати права суб'єкта даних. Доцільно передбачити у Проєкті Закону обмеження права суб'єкта даних під час обробки персональних даних для статистичних цілей.

Стаття 15. Обробка персональних даних для цілей журналістської або творчої діяльності

Згідно з частиною 2 статті 15 Проєкту Закону параграф перший цієї частини застосовується лише за умови, що контролер, який здійснює обробку персональних даних винятково для цілей журналістської або творчої діяльності, обґрунтовано вважає, що розкриття інформації здійснюється в суспільних інтересах, і шкода від розкриття такої інформації не перевищує суспільний інтерес, який переслідується її отриманням. Згідно з частиною 3, для цілей цієї статті під «журналістською діяльністю» слід розуміти діяльність журналістів і засобів масової інформації, їх працівників, як це визначено Законом України «Про інформацію».

У пункті 96 Пояснювальної записки підкреслюється, що: «Для врахування важливості права на свободу вираження поглядів у кожному демократичному суспільстві необхідно широко тлумачити поняття, які стосуються цієї свободи, а саме такої як журналістика». У цьому ж пункті, коли йдеться про свободу вираження поглядів, пояснюється, що свобода вираження поглядів включає свободу журналістського, науково-освітнього, художнього чи літературного вираження поглядів, а також право отримувати й поширювати інформацію. Зважаючи на це, можна зробити висновок, що сфера застосування статті 15 Проєкту Закону занадто вузька.

Рекомендується внести поправки до статті 15 Проєкту Закону, поширивши сферу її дії на «свободу вираження поглядів, включно зі свободою журналістського, науково-освітнього, художнього чи літературного вираження поглядів, а також право отримувати та поширювати інформацію».

Стаття 16. Обробка персональних даних після смерті суб'єкта персональних даних

Стаття не суперечить Конвенції 108+ та GDPR. Тож вона не викликає конкретних зауважень.

Стаття 17. Використання технології відстеження дій суб'єктів персональних даних в електронних комунікаціях і сервісах

У статті 17, а саме у її частинах 2 і 3, розглядаються умови, за яких персональні дані можуть законно оброблятися, зокрема, за попередньою згодою суб'єктів даних, якщо не застосовуються інші умови, при зборі за допомогою різних технологій відстеження. Розуміємо, що мета цієї статті полягає в інтеграції вимог, викладених у пункті 3 статті 5 Директиви про конфіденційність та електронні комунікації, яка містить стислі правила використання кукі-файлів та інших технологій відстеження на термінальному обладнанні

суб’єктів даних. Проте останнє положення встановлює вимоги до зберігання інформації або до отримання доступу до вже збереженої інформації на термінальному обладнанні абонента або користувача, а не до обробки персональних даних. Іншими словами, це більш конкретно стосується розміщення технологій відстеження на пристрої суб’єкта даних. Збір і обробка отриманих внаслідок нього персональних даних є окремою операцією, яка у будь-якому випадку регулюватиметься загальними положеннями про захист даних (наприклад, для ЄС — це GDPR).

Формулювання статті 17 необхідно переглянути, щоб узгодити його з пунктом 3 статті 5 Директиви про конфіденційність та електронні комунікації, встановивши умови зберігання інформації або отримання доступу до інформації на пристрої суб’єкта даних, але не обробки персональних даних у цьому контексті.

Відповідно до положень пункту 2 частини 3 статті 17 Проєкту Закону, суб’єкту даних має бути роз'яснено, що він/вона має право обирати, на яку технологією він/вона погоджується, якщо обробка здійснюється на підставі згоди. Згідно з визначенням, наведеним у пункті f статті 2 Директиви про конфіденційність та електронні комунікації, «згода» користувача або підписника відповідає згоді суб’єкта даних за Директивою 95/46/ЕС [GDPR], тобто це є «добровільно надана конкретна та поінформована вказівка на побажання користувача». Пунктом 3 статті 5 зазначеної вище Директиви передбачається, що зберігання інформації або отримання доступу до вже збереженої інформації на термінальному обладнанні підписника або користувача допускається лише за умови, що відповідний підписник або користувач дав свою згоду, отримавши чітку та вичерпну інформацію відповідно до положень Директиви 95/46/ЕС [GDPR], зокрема, про цілі обробки. Це означає, що згода дається на мету обробки, а не на використання технології. Для того, щоб згода була дійсною, інформація про обробку повинна бути чіткою та всеосяжною, що неможливо у випадку, якщо називається лише технологія. З іншого боку, вимога надавати користувачеві право обирати, з якою технологією він погоджується, здається недоречною або навіть надмірною.

З урахуванням положень пункту f статті 2 Директиви про конфіденційність та електронні комунікації рекомендується переглянути статтю 17 Проєкту Закону у частині, в якій вона передбачає право користувача (суб’єкта даних) обирати, на яку технологію він надає згоду, замінивши це правом обирати мету обробки.

Пунктом 2 частини 4 статті 17 Проєкту Закону передбачено зобов’язання для контролерів

або операторів, які здійснюють обробку персональних даних, зазначених у частині першій цієї статті, забезпечувати безумовну автоматизовану можливість для суб'єкта персональних даних вносити будь-які зміни до своїх персональних даних, обробка яких здійснюється. Слід зазначити, що пунктом 1(e) статті 9 Конвенції 108+ і статтею 16 GDPR передбачено право на виправлення неточних персональних даних, але не безумовне право вносити будь-які зміни.

Пункт2 частини 4 статті 17 Проєкту Закону в частині, якою передбачено безумовне право вносити будь-які зміни до персональних даних, обробка яких здійснюється, має бути переглянутий в контексті положень пункту 1(e) статті 9 Конвенції 108+ та статті 16 GDPR.

3.4. РОЗДІЛ IV. ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 18. Право на інформацію

Слід зазначити, що статті 13 і 14 GDPR не містять окремої вимоги надавати суб'єкту даних інформацію про оператора(-ів) (оператори належать до одержувачів персональних даних), а також про цілі та методи обробки, дії або комплекси дій, що виконуватимуться щодо персональних даних. З іншого боку, у цій статті бракує інформації про законні інтереси, що переслідуються контролером або третьою особою, а також, бракує вказівок на відповідні запобіжні заходи, що вживатимуться для транскордонної передачі, та можливі способи отримання копії. Також, на випадок прямого збору даних (стаття 13) GDPR не передбачає вимоги зазначати категорії даних, що обробляються. До того ж, пункт 4 статті 14 GDPR містить вимогу про те, що у разі подальшої обробки з метою, відмінною від початкової, суб'єкт даних повинен отримати попередню інформацію про це від контролера.

Рекомендується переглянути пункти 2, 4, 5 частини 1 статті 18 Проєкту Закону в контексті статей 13 і 14 GDPR, тобто тією мірою, якою стаття 18 передбачає додаткові вимоги до прозорості.

Статтю 18 Проєкту Закону слід доповнити, зокрема, інформацією про легітимний інтерес, що переслідується контролером або третьою особою, якщо обробка ґрунтується на положеннях пункту 6 частини 1 статті 5 цього Проєкту Закону, а також, стосовно транскордонної передачі, про відповідні запобіжні заходи, що вживатимуться, та можливі способи отримання копії.

Стосовно звільнення від зобов'язання щодо надання інформації, запропонованого частиною

4 статті 18 Проєкту Закону, можна зазначити, що у ній не передбачений випадок, коли надання інформації може унеможливити або серйозно ускладнити досягнення цілей обробки як передбачено пунктом 5(b) статті 14 GDPR. Також, навіть у випадках, коли застосовується звільнення від зобов'язання щодо надання інформації (тобто обробка виявляється неможливою, вимагатиме непропорційних зусиль або здатна унеможливити, або серйозно ускладнити досягнення цілей обробки), пунктом 5(b) статті 14 GDPR вимагається від контролера вжиття належних заходів захисту прав, свобод і легітимних інтересів суб'єкта даних, у тому числі шляхом оприлюднення інформації на широкий загал.

Рекомендується доповнити частину 4 статті 18 Проєкту Закону у частині, що стосується звільнення від зобов'язань щодо надання інформації, а також умов в контексті пункту 5(b) статті 14 GDPR.

Стаття 19. Право суб'єкта персональних даних на доступ до персональних даних

На відміну від пункту 4 статті 15 GDPR, у статті 19 Проєкту Закону відсутнє положення про те, що право на отримання копії персональних даних не повинно негативно позначатися на правах і свободах інших осіб.

Рекомендується доповнити статтю 19 Проєкту Закону положенням про те, що право на отримання копії персональних даних, про яке йдеться у частині 2, не повинно негативно позначатися на правах і свободах інших осіб.

Стаття 20. Право суб'єкта персональних даних на виправлення персональних даних

Відповідно до частини 3 статті 20 контролер зобов'язаний повідомити всіх одержувачів, яким були відкриті персональні дані, про задоволення вимоги про виправлення даних, окрім випадків, коли таке повідомлення становить для контролера надмірний тягар. Слід зазначити, що статтею 19 GDPR передбачені більш широкі зобов'язання щодо надання інформації: контролер зобов'язаний повідомляти про будь-яке виправлення чи видалення персональних даних або обмеження обробки, що здійснюється відповідно до положень статті 16, пункту 1 статті 17 та статті 18, кожному одержувачу, якому були відкриті персональні дані, окрім випадків, коли це виявляється неможливим або вимагає непропорційних зусиль. Контролер повинен за запитом суб'єкта персональних даних повідомити його про таких одержувачів.

Проєкт Закону необхідно узгодити із статтею 19 GDPR, додавши положення про

зобов'язання повідомляти одержувачів не лише про виправлення, але й про видалення персональних даних або про обмеження обробки, а також за запитом суб'єкта даних повідомляти його про таких одержувачів. Також варто зазначити про неможливість здійснити повідомлення відповідно до положень тієї ж статті GDPR.

Стаття 21. Право суб'єкта персональних даних бути забутим

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 22. Право заперечувати проти обробки персональних даних

Стаття 22 Проєкту Закону, що передбачає право заперечувати проти обробки персональних даних, не відповідає Конвенції 108+ і статті 21 GDPR у частині, що стосується визначеного способу обробки персональних даних та заперечення проти обробки для цілей прямого маркетингу. Відповідно до п. 79 Пояснювальної записки, результатом заперечення проти обробки даних для маркетингових цілей має бути безумовне видалення та вилучення персональних даних, на які поширюється таке заперечення. Слід зазначити, що у пунктах 2, 3 статті 21 GDPR також приділяється особлива увага праву на заперечення проти обробки персональних даних для цілей прямого маркетингу: суб'єкт даних може скористатися правом на таке заперечення у будь-який час, і контролер даних зобов'язаний без жодних умов припинити обробку персональних даних для цілей прямого маркетингу відразу після того, як отримає таке заперечення.

З огляду на пункти 2 і 3 статті 21 GDPR, статтю 22 Проєкту Закону слід доповнити додатковими положеннями, які більш чітко врегулюють право на заперечення: у випадку, коли персональні дані обробляються для цілей прямого маркетингу, суб'єкт даних повинен мати право у будь-який час заперечити проти обробки персональних даних для цілей такого маркетингу, який передбачає профайлінг в тій мірі, в якій він стосується прямого маркетингу. У разі заперечення проти обробки для цілей прямого маркетингу, персональні дані більше для таких цілей не оброблятимуться.

Стаття 23. Право на мобільність персональних даних

Положення статті 23 Проєкту Закону, що стосуються права на мобільність даних, видаються дуже складними для застосування на практиці й виходять за рамки положень статті 20 GDPR. Наприклад, нагляд за дотриманням порядку, викладеному у частині 3 статті 23 Проєкту Закону, що передбачає вимогу компенсації від суб'єкта даних за витрати, пов'язані з

реалізацією цього права, буде складним і для контролюючого органу. З іншого боку, така вимога компенсації від суб'єкта даних суперечить положенням пункту 5 статті 12 GDPR, де зазначається, що будь-яке повідомлення та будь-які дії, вчинені відповідно до статей, що регулюють права суб'єкта даних, повинні надаватися безкоштовно, за винятком випадків, коли запити від суб'єкта даних очевидно необґрунтовані або надмірні.

З урахуванням положень пункту 5 статті 12 та статті 20 GDPR, що встановлюють, відповідно, умови реалізації прав суб'єкта даних і права на мобільність даних, рекомендується виключити частину 3 статті 23 із Проєкту Закону.

Стаття 24. Право на обмеження обробки персональних даних

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень (за умови дотримання перелічених вище рекомендацій згідно зі статтею 20).

Стаття 25. Право на захист від автоматизованого прийняття рішень

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 26. Право суб'єкта персональних даних на захист своїх прав та відшкодування шкоди

Згідно з частиною 3 статті 26 Проєкту Закону контролер звільняється від відповідальності за шкоду, заподіяну суб'єкту персональних даних, якщо доведе, що події, які спричинили завдання такої шкоди, сталися не з його вини і він вжив усіх належних заходів для попередження порушення прав і заподіянню шкоди.

Частиною 4 статті 26 Проєкту Закону передбачено, що для компенсації шкоди, завданої суб'єкту персональних даних внаслідок обробки персональних даних спільними контролерами, суб'єкт персональних даних може звернутися зі скаргою або позовом до одного з таких контролерів. Відповідно до частини 5 статті 26 Проєкту Закону контролер, який відшкодував суб'єкту персональних даних шкоду, заподіяну діями оператора персональних даних, має право вимагати від такого оператора відшкодування в порядку регресу.

Слід зазначити, що у пункті 4 статті 82 GDPR йдеться не лише про контролерів, а й про операторів, які беруть участь у тій самій обробці («якщо більше ніж один контролер або оператор, або обидва контроле і оператор, беруть участь в одній і тій самій обробці, і якщо відповідно до положень пунктів 2 і 3 вони несуть відповідальність за будь-яку шкоду, заподіяну внаслідок обробки, кожен контролер або оператор даних несе відповідальність за

всю шкоду, щоб забезпечити суб'єкту даних ефективну компенсацію»). Пунктом 3 статті 82 GDPR передбачається, що оператор також звільняється від відповідальності, якщо виконуються умови цього пункту. Відповідно до пункту 5 статті 82 GDPR, якщо контролер або оператор сплатив повну компенсацію за заподіяну шкоду, такий контролер або оператор має право вимагати від інших контролерів або операторів, які беруть участь у тій самій обробці, ту частину компенсації, яка відповідає їхній частині відповідальності за шкоду.

Частиною 3 статті 26 Проєкту Закону не передбачено, що оператор звільняється від відповідальності за шкоду, заподіяну суб'єктові персональних даних. Положення частини 4 статті 26 Проєкту Закону обмежують можливість суб'єкта даних вимагати відшкодування збитків лише від контролера даних, який бере участь у обробці. Частиною 5 статті 26 Проєкту Закону не передбачається, що оператор, який відшкодував усі збитки, може вимагати компенсацію від контролера, який бере участь у тій самій обробці. Таким чином, положення частини 3, 4 і 5 статті 26 Проєкту Закону не відповідають положенням пунктів 3, 4 і 5 статті 82 GDPR. В свою чергучастину 3, 4 і 5 статті 26 Проєкту Закону слід доповнити положеннями, що стосуватимуться оператора.

Стаття 27. Порядок розгляду вимог суб'єкта персональних даних

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

3.5. РОЗДІЛ V ОБОВ'ЯЗКИ КОНТРОЛЕРА ТА ОПЕРАТОРА

Стаття 28. Загальні обов'язки контролера та оператора

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 29. Захист персональних даних за проєктуванням та замовчуванням

Стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 30. Спільні контролери

Частина 3 статті 30 передбачає, що: «Положення договору, що регулюють розподіл обов'язків щодо дотримання вимог до обробки персональних даних та впливають на права суб'єктів персональних даних, є інформацією, що становить суспільний інтерес, та надається у порядку, встановленому Законом України «Про доступ до публічної інформації». Суб'єкт персональних даних може здійснювати свої права щодо кожного з контролерів незалежно від

умов договору та ознайомитись зі змістом цього договору в порядку, встановленому Законом України «Про доступ до публічної інформації»».

Слід зазначити, що договір, укладений контролерами, які діють у приватному секторі, може містити комерційну таємницю, тому необґрунтовано розглядати його як інформацію, що становить суспільний інтерес. Пунктом 2 статті 26 GDPR передбачається, що суть угоди, укладеної спільними контролерами, має бути доступна суб'єкту даних, але не всім, як це можна припускати у випадку інформації, яка становить суспільний інтерес.

Положення частини 3 статті 30 Проєкту Закону необхідно переглянути у контексті захисту комерційної таємниці. Оскільки Проєкт Закону і Закон України «Про доступ до публічної інформації» мають різні цілі та сферу застосування, посилання на останній у Проєкті Закону варто переглянути. Рекомендується внести зміни до другого речення частини 3 статті 30 Проєкту Закону («Положення договору, що регулюють розподіл обов'язків щодо дотримання вимог до обробки персональних даних і стосуються прав суб'єктів персональних даних, вважаються інформацією, що становить суспільний інтерес, і повинні надаватися в порядку, визначеному Законом України «Про доступ до публічної інформації»»), висуваючи умову, що суть угоди має бути доступна суб'єкту даних, замість того, щоб вважатися інформацією, яка становить суспільний інтерес.

Стаття 31. Оператор персональних даних

Другим параграфом частини 8 статті 31 Проєкту Закону передбачається, що інформація про положення договору між контролером і оператором, на підставі якого здійснюється обробка, і які впливають на права суб'єктів персональних даних, надаються у порядку, визначеному Законом України «Про доступ до публічної інформації».

Як і в попередній статті, що регулює питання спільних контролерів, слід зазначити, що контролер і/чи оператор можуть діяти в приватному секторі, й договір, укладений ними може містити комерційну таємницю. З іншого боку, контролери і оператори, які необмежені Законом України «Про доступ до публічної інформації», не зобов'язані повідомляти інформацію на широкий загал. Таким чином, коли мова заходить про таких суб'єктів господарювання, договір не становитиме інформацію публічного характеру. З іншого боку, договір буде вважатися публічною інформацією, якщо він укладений контролером, на якого покладене таке зобов'язання вказаним вище законом; але у такому випадку не потрібно

включати спеціальне положення, що регулюватиме це питання, до цього Проєкту Закону, оскільки воно вже урегульовано Законом України «Про доступ до публічної інформації».

Положення частини 8 статті 31 Проєкту Закону необхідно переглянути в контексті захисту комерційної таємниці. Оскільки Проєкт Закону і Закон України «Про доступ до публічної інформації» мають різні цілі та сферу застосування, посилання на останній у Проєкті Закону потрібно переглянути. Рекомендується видалити параграф другий частини 8 статті 31 Проєкту Закону («Положення договору між контролером і оператором, на підставі якого здійснюється обробка, і які впливають на права суб'єктів персональних даних, надаються в порядку, встановленому Законом України «Про доступ до публічної інформації»»).

Стаття 32. Обробка персональних даних за дорученням котролера або оператора

Ця стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 33. Представник котролера або оператора

Ця стаття не суперечить Конвенції 108+ та GDPR. Тож вона не потребує змін або доповнень.

Стаття 34. Реєстрація операцій з обробки персональних даних

Ця стаття відповідає Конвенції 108+ та GDPR. Тож вона не потребує змін або доповнень.

Стаття 35. Безпека обробки персональних даних

Частина 1 статті 35 передбачає, що: «Контролер і оператор зобов'язані вживати належні заходи технічного та організаційного характеру для забезпечення належної безпеки обробки персональних даних такого рівня, який є співмірний ризику обробки персональних даних для прав і свобод суб'єктів персональних даних із дотриманням принципу пропорційності». Незрозуміло, що означає «принцип пропорційності» у контексті цієї статті. Слід зазначити, що відповідно до положень пункту 1 статті 7 Конвенції 108+ «контролер і, у відповідних випадках, оператор вживають відповідних заходів безпеки проти таких ризиків, як випадковий або несанкціонований доступ, знищення, втрата, використання, зміна чи розкриття персональних даних». У пунктах 62, 63 Пояснювальної записки зазначається, що під час прийняття рішення про заходи безпеки, як технічного, так й організаційного характеру, щодо кожної обробки слід брати до уваги таке: потенційні несприятливі наслідки

для фізичної особи, характер персональних даних, обсяг персональних даних, що обробляються, ступінь вразливості технічної архітектури, що використовується для обробки, необхідність обмеження доступу до даних, вимоги, що стосуються довгострокового зберігання, тощо; заходи безпеки повинні враховувати технічний рівень методів і прийомів захисту даних у сфері обробки даних, а їх вартість має бути співмірною серйозності та ймовірності потенційних ризиків.

Відповідно до положень пункту 1 статті 32 GDPR контролер і оператор вживають відповідних технічних та організаційних заходів, необхідних для забезпечення рівня безпеки, що відповідає ризику, беручи до уваги рівень техніки, витрати на впровадження та характер, обсяг, контекст і цілі обробки, а також ризик для прав і свобод фізичних осіб різного ступеня ймовірності та серйозності.

Не рекомендується вживати «принцип пропорційності» в контексті технічних та організаційних заходів, що спрямовані на забезпечення безпеки персональних даних. Беручи до уваги положення пункту 1 статті 32 GDPR, рекомендується доповнити цю статтю основними факторами, такими як стан технічного розвитку, витрати на впровадження, характер, обсяг, контекст і цілі обробки, а також ризик різного ступеня ймовірності та серйозності для прав і свобод фізичних осіб..

Стаття 36. Співпраця контролера та оператора з контролюючим органом

Ця стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 37. Повідомлення контролюючого органу про порушення безпеки персональних даних

Ця стаття відповідає Конвенції 108+ та GDPR. Тож вона не потребує змін або доповнень.

Стаття 38. Повідомлення суб'єкта персональних даних про порушення безпеки персональних даних

Ця стаття відповідає Конвенції 108+ та GDPR. Тож вона не потребує змін або доповнень.

Стаття 39. Оцінка впливу захисту даних

Ця стаття відповідає Конвенції 108+ та GDPR. Тож ця стаття не потребує змін або доповнень.

Стаття 40. Попередні консультації

У цій статті встановлюється умова, за якої контролер зобов'язаний провести попередню консультацію з контролюючим органом, якщо оцінка впливу відповідно до статті 39 Проєкту Закону свідчить про те, що обробка персональних даних призведе до високого ступеню ризику для суб'єктів даних. Вона відповідає Конвенції 108+ та GDPR з урахуванням наведених нижче коментарів.

Частиною 3 статті 40 передбачається, що після таких консультацій контролюючий орган надає контролеру рекомендації, але він також може прийняти інші рішення, не уточнюючи, саме які заходи це можуть бути. Наприклад, згідно з GDPR, відповідно до положень пункту 2 статті 36 та пункту 2(a) статті 58 контролюючий орган може попередити про те, що обробка, за якою здійснювалася оцінка впливу, може порушувати вимоги GDPR.

Якщо передбачається, що окрім рекомендацій контролюючий орган вживатиме інших заходів, то їх варто детальніше визначити у цій статті для контролерів з метою кращого розуміння та правової визначеності. Якщо такі заходи передбачаються законом, який регулює діяльність контролюючого органу, рекомендується зробити посилання на цей закон у цій статті.

Стаття 41. Відповідальна особа з питань захисту персональних даних

Цією статтею передбачено випадки, за яких контролер або оператор даних зобов'язані призначати відповідальну особу з питань захисту персональних даних. Один із таких випадків описаний у пункті 3 частини 1 статті 41, яким передбачається, що, якщо основна діяльність контролера або оператора полягає або пов'язана з обробкою великих масивів персональних даних, має бути призначена відповідальна особа з питань захисту даних. Такий сценарій обов'язкового призначення відповідальної особи з питань з захисту персональних даних є ширшим ніж той, що вимагається відповідною статтею GDPR (див. статтю 37). Останній дійсно вимагає призначення відповідальної особи з питань захисту даних у випадках обробки великих масивів персональних даних, але обмежує його контролерами або операторами, які обробляють великі масиви персональних даних спеціальних категорій (стаття 9) або дані, що стосуються кримінальних правопорушень (стаття 10 GDPR). Таким чином, загалом не має потреби у призначенні відповідальної особи з питань захисту персональних даних для широкомасштабної обробки всіх видів

даних.

З метою приведення пункту 3 частини 1 статі 41 у відповідність зі статтею 37 GDPR, потрібно внести зміни, якими встановлюватиметься, що призначення відповідальної особи з питань захисту персональних даних є необхідним у випадку обробки великих масивів даних лише тоді, коли основна діяльність контролера або оператора даних полягає в обробці спеціальних категорій даних або персональних даних, що пов'язані з судимостями і правопорушеннями.

У частині 7 статті 41 наводиться перелік осіб, які не можуть бути призначені відповідальними особами з питань захисту персональних даних. Серед них у статті згадуються особи, які не склали «кваліфікаційний іспит», без подальшого посилання на певні статті Проєкту Закону.

Оскільки кваліфікаційний іспит регулюється щонайменше статтею 42 Проєкту Закону, задля уникнення невизначеності бажано додати посилання на неї до цього положення.

Стаття 42. Кваліфікаційний іспит на посаду відповідальної особи з питань захисту персональних даних

Цією статтею передбачається, що особа може бути призначена відповідальною особою з питань захисту персональних даних у державному органі, якщо вона склала кваліфікаційний іспит і отримала сертифікат, виданий органом із сертифікації персоналу. Проте із Проєкту Закону незрозуміло, як здійснюватиметься процес організації іспитів, навчання та сертифікації на практиці, та як діятиме орган сертифікації. Проте, з цієї статті, а також із Перехідних положень (пункт 4 розділу XI) виходить, що ці елементи мають бути визначені контролюючим органом.

Для ясності рекомендується зробити посилання на відповідні положення або правовий акт, в якому можна ознайомитися з особливостями порядку організації кваліфікаційного іспиту. Також, необхідно узгодити між собою частину 1 статті 42 та пункту3 частини 7 статті 41: перша передбачає, що кваліфікаційний іспит застосовується лише у випадку державних органів, натомість у другому - зазначаються також контролери і оператори.

Стаття 43. Кодекс поведінки з питань захисту персональних даних

У цій статті викладено порядок прийняття та затвердження кодексу поведінки, який подібний до того, що передбачений статтею 40 GDPR.

Відповідно до частини 1 статті 43 кодекс поведінки визначається як добровільний захід. Натомість з положень частини 2 статті 43 виявляється, що певні типи організацій повинні прийняти кодекси поведінки в обов'язковому порядку. Таким чином, виникає питання щодо можливого протиріччя між цими двома статтями.

Для забезпечення правової визначеності необхідно досягнути узгодженості між частинами 1 та 2 статті 43, щоб пояснити, що зобов'язання певних організацій приймати кодекси поведінки виникає на додаток до добровільного прийняття кодексів поведінки іншими організаціями, на які не поширюється дія частини 2 статті 43.

Формулювання частини 3 статті 43 є нечітким, як зі змісту, так і мети, якої мають досягнути за допомогою кодексу поведінки, якщо брати до уваги положення пункту 2 статті 40 GDPR. Згідно з цим положенням GDPR, мета кодексу поведінки полягає у тому, щоб конкретизувати застосування GDPR щодо ряду елементів (сфера застосування, справедлива та прозора обробка тощо), які відповідають переліченим у частині 3 статті 43 Проєкту Закону.

Для більш точного відображення вимоги пункту 3 статті 40 GDPR, у частині 3 статті 43 слід зазначити, що кодекс поведінки має визначати застосування Проєкту Закону стосовно елементів, перелічених у цій статті.

Стаття 43 не передбачає вимогу про запровадження механізмів моніторингу застосування кодексу поведінки, в тому числі за допомогою органу контролю, як передбачено пунктом 4 статті 40 і статті 41 GDPR. За відсутності таких механізмів ефективність кодексу поведінки як засобу забезпечення дотримання законодавства про захист даних є сумнівною.

Статтю 43 необхідно доповнити вимогою щодо механізмів моніторингу, включаючи орган, застосування кодексу поведінки з урахуванням положень пункту 4 статті 40 і статті 41 GDPR.

3.6. РОЗДІЛ VI. ПЕРЕДАЧА ПЕРСОНАЛЬНИХ НА ТЕРІТОРІЮ ІНОЗЕМНИХ ДЕРЖАВ АБО МІЖНАРОДНИМ ОРГАНІЗАЦІЯМ

Стаття 44. Підстави для передачі персональних даних на територію іноземної держави або міжнародній організації

Стаття відповідає Конвенції 108+ та GDPR і не потребує внесення змін.

Стаття 45. Передача персональних даних на територію іноземної держави або міжнародній організації, які забезпечують належний рівень захисту персональних даних

У цій статті розглядається можливість передачі персональних даних до країн, які визнані належними, способи здійснення такої передачі і відповідні наслідки.

У частині 4 статті 45 зазначається, що під час передачі даних до держави, яка визнана належною, спеціальний дозвіл від контролюючого органу не потрібен. У статті також зазначається, що те саме застосовується, коли передача здійснюється «з» належної держави. Проте може виникнути питання, чому Проєктом Закону регулюватимуться потоки даних та їх передача з інших держав до України, оскільки це загалом виходить за межі Проєкту Закону.

Згадування про передачу даних «з» інших держав слід виключити, оскільки незрозуміло, чому потоки і передача даних з інших держав до України має регулюватись Проєктом Закону.

Стаття 46. Передача персональних даних на територію іноземної держави або міжнародній організації на підставі наданих гарантій захисту персональних даних

Стаття відповідає Конвенції 108+ та GDPR і не потребує внесення змін.

Стаття 47. Передача персональних даних на територію іноземної держави на підставі обов'язкових корпоративних правил

Стаття відповідає Конвенції 108+ та GDPR за умови виконання наступних коментарів і рекомендацій.

Частиною 1 статті 47 визначається група організацій, які можуть використовувати обов'язкові корпоративні правила. Проте, як видається, у ній йдеться про два типи визначень, що використовуються для цієї мети.

Для більшої ясності рекомендується об'єднати або уніфікувати у межах цієї статті визначення типів організацій, які можуть використовувати обов'язкові

корпоративні правила для передачі персональних даних.

У частині статті 47 зазначається, що обов'язкові корпоративні правила можуть передбачати інші заходи для забезпечення безпеки обробки персональних даних. Зміст цього положення і мета, на досягнення якої воно спрямоване, незрозумілі, і їх неможливо повністю оцінити, беручи також до уваги той факт, що GDPR не встановлює вимоги обов'язкових корпоративних правил, визначених у статті 47.

Необхідно роз'яснити положення частини 4 статті 47, з метою її більш детальної конкретизації її мети в контексті решти положень статті 47.

Стаття 48. Окремі випадки передачі персональних даних на територію іноземної держави або міжнародній організації

Пунктом 8 частини 1 статті 48 Проєкту Закону передбачається, що за відсутності належного рівня захисту та належних гарантій, передача персональних даних третій країні або міжнародній організації повинна відбуватися, якщо така передача необхідна для здійснення права на свободу вираження поглядів і «є пропорційною за певних обставин». У пункті 4(d) статті 14 Конвенції 108+ передбачається, що у такому випадку передача може відбуватися, якщо це є необхідним і пропорційним заходом у демократичному суспільстві, спрямованим на забезпечення свободи вираження поглядів. У контексті цього положення Конвенції 108+ незрозуміло, що передбачає фраза «пропорційний за конкретних обставин» відповідно до пункту 8 частини 1 статті 48 Проєкту Закону. «Конкретні обставини» не завжди можуть бути пов'язані з цінностями демократичного суспільства.

Положення пункту 8 частини 1 статті 48 Проєкту Закону мають бути узгоджені з пунктом 4(d) статті 14 Конвенції 108+, яка передбачає, що передача персональних даних третій країні або міжнародній організації повинна відбуватися, якщо така передача є необхідним і пропорційним заходом у демократичному суспільстві, спрямованим на забезпечення свободи вираження поглядів.

Стаття 49. Передача персональних даних на територію іншої держави в правоохоронних цілях

У цій статті встановлюються умови передачі персональних даних правоохоронними органами України третім країнам у правоохоронних цілях і, по суті, передбачається можливість такої передачі у випадку, якщо третя країна забезпечує належний рівень

захисту (частина 1 статті 49), або на підставі відповідного міжнародного договору (частини 2 статті 49). Слід зазначити, що пункт 1 статті 35 Директиви про захист даних у правоохоронній діяльності передбачає додаткові умови, яких потрібно дотримуватися при здійсненні міжнародної передачі даних в правоохоронних цілях. Зокрема, якщо передача необхідна саме в правоохоронних цілях, то вона здійснюється до компетентному органу. Також у ній передбачається можливість посилатися на відступи під час передачі (пункт 1(d) статті 35) і встановлюються вимоги для наступних передач (пункт 1(e) статті 35).

Статтю 49 слід переглянути і доповнити додатковими умовами, щоб визначити міжнародну передачу в правоохоронних цілях, з урахуванням положень статті 35 Директиви про захист даних у правоохоронній діяльності .

3.7. РОЗДІЛ VII. ПОРЯДОК ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІХ ОСІБ

У статті 50 розглядається порядок надання третім особам доступу до персональних даних, що знаходяться в розпорядженні розпорядника публічної інформації. Викликає певні запитання частина 5 статті 50, що пов’язано з нечіткості наведених положень. Доцільно було б об’єднати обидва пункти на користь правової визначеності, а також зазначити, що запит має бути відхилений, якщо будь-яка з умов попереднього пункту не виконується, особливо якщо запитувач не повідомив правову основу або законну мету отримання персональних даних. Якщо запит неповний, наприклад, у ньому бракує деяких необхідних елементів, запитувача попросять заповнити його протягом певного періоду, таким чином, щоб з міркувань економії часу, обидва і заявник, і компетентний орган, звільнились від тягаря повторного розгляду нового запиту, який знову може виявитися неповним.

Також, стосовно частини 7 статті 50, хочемо зазначити, що здається, що певний, порядок чи політика, яким встановлено обмеження на витрати на копіювання та друк, вже існує. Якщо це дійсно так, пропонуємо надати щонайменше описове посилання на цей порядок. Також варто надати можливість контролерам встановлювати вартість копіювання та друку самостійно у межах, визначених цим порядком.

Якщо такого порядку досі не існує, варто було зобов’язати контролюючий орган прийняти його впродовж певного періоду після набрання чинності цим Проєктом Закону.

Зрештою, також необхідно дослідити, чи поширюються обмеження, викладені у цій статті (наприклад, у частині 6), також й на випадки, коли персональні дані розкриваються в документах (обсягом більше 5 сторінок) відповідно до положень Закону України «Про доступ до публічної інформації». Якщо те, що передбачено стосовно таких витрат, має застосовуватися лише в частині доступу до персональних даних згідно цього Закону, це має бути чітко окреслено.

3.8 РОЗДІЛ VIII. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ РОБОТОДАВЦЕМ

Стаття 51. Загальні питання обробки персональних даних роботодавцем

У цій статті визначається загальний порядок, що застосовується до обробки персональних даних роботодавцем. Він не викликає жодних питань в світлі Конвенції 108+ або GDPR.

Стаття 52. Обробка персональних даних роботодавцем

У цій статті розглядаються більш конкретні умови обробки і передачі персональних даних роботодавцем у контексті трудових відносин. Коментар надається лише до тих положень статті, до яких виникають запитання, і/або які можуть потребувати внесення змін.

Відповідно до частини 2 статті 52 роботодавець може збирати дані про працівників, кандидатів на працевлаштування, державних службовців від інших осіб (джерел), тобто ймовірно третіх осіб, на підставі згоди працівника.

Оскільки у частині5 статті 51 розглядаються умови отримання згоди працівників, відповідне посилання має бути зроблено також у частині 2 статті 52, що забезпечить узгодженість між ними, а також те, що згода була отримана у належний спосіб.

До того ж, збір персональних даних працівників від третіх осіб може базуватись також і на інших правових підставах, і не лише на згоді, що залежить від мети обробки персональних даних, особливо у випадках, коли згода не може бути належною юридичною підставою, оскільки її неможливо отримати у законний спосіб (тобто коли умови для отримання згоди не можуть бути виконані). Загалом це відповідає підходу, передбаченому GDPR. Наприклад, якщо роботодавець запитує інформацію про вислугу років або досвід роботи, і така інформація необхідна для оформлення трудових відносин, її обробка може ґрунтуватися на заходах, що були необхідні до укладання трудового договору, і в такому випадку отримувати згоду не потрібно.

Рекомендується внести зміни до частини 2 статті 52, яка передбачає, що збір персональних даних з інших джерел також може базуватись на інших правових підставах, крім згоди (у відповідних випадках).

У частині 3 статті 52 передбачено, що персональні дані, які обробляються для цілей трудових відносин, повинні зберігатися протягом строку, необхідного для досягнення легітимної мети, що переслідується. У цій статті по суті повторно стверджується передбачений у Проєкті Закону принцип обмеженого зберігання, але не зазначається, як конкретно цей принцип має дотримуватися в контексті трудових відносин, що може викликати труднощі під час його застосування на практиці. Такі дані можуть зберігатися, наприклад, протягом строку, встановленого відповідними галузевими законами, або протягом строку, необхідного для здійснення дисциплінарного провадження або судового розгляду.

Задля запобігання неузгодженостей, рекомендується додати, що вимога зберігати персональні данні протягом строку, необхідного для досягнення легітимної мети, стосується персональних даних, що зберігаються у формі, яка дозволяє ідентифікувати суб'єктів даних відповідно до статті 5 (4) (e) Конвенції 108+ та статті 5 (1) (e) GDPR (стаття 5 (1) (e). Також рекомендується більш конкретно зазначити, як довго можуть зберігатися персональні дані працівників, наприклад, з посиланням на інші закони, які можуть передбачати конкретні строки зберігання та/або елементи, що дають змогу визначити такий строк зберігання (наприклад, строк позовної давності для судового розгляду), щоб полегшити застосування цього положення на практиці та забезпечити належне дотримання принципу обмеженого строку зберігання відповідно до зазначених вище статей Конвенції 108+ та GDPR.

У частині 6 статті 52 розглядається право (ймовірно, особи, яка є об’єктом внутрішнього розслідування роботодавця та інших зацікавлених працівників) на доступ до результатів такого внутрішнього розслідування. У ній зазначається, що такий доступ має бути наданий «не раніше спливу строку позовної давності». В такому випадку, цікавим є питання з чим узгоджується «строк позовної давності» і чи можна його вважати строком позовної давності для судового розгляду. Якщо так, то важко уявити собі ефективність такої можливості доступу, якщо це відбувається після закінчення такого періоду, і зацікавлені особи більше не можуть оскаржувати результати.

Частина 6 статті 52 потребує уточнення щодо строків, протягом яких особи можуть мати доступ до результатів розслідування, включно з посиланням на строк давності, щоб гарантувати, що така можливість доступу є ефективною, і що особи можуть за потреби законно оскаржити результати або домагатися їх перегляду.

Частина 8 статті 52, у якій йдеться про затвердження порядку обробки персональних даних роботодавцем, не зовсім зрозуміла, так само, як і мета, яку вона переслідує. Якщо порядок є рівнозначним внутрішньому регламенту, який визначає обов'язкові правила, як частину трудових відносин, у тому числі стосовно обробки персональних даних працівників, то доречним, серед інших, засобом, виходячи із статті 13 і 14 GDPR, виглядало би надання працівникам інформації про обробку їхніх персональних даних.

Частина 9 статті 52 стосується передачі державним органам персональних даних, зібраних роботодавцем для цілей трудових відносин.

Відповідно до ідеї, закладеної у GDPR, в частині 9 статті 52 рекомендується зазначити, що персональні дані передаються державним органам, якщо обробка необхідна для виконання юридичних зобов'язань роботодавця (див. пункт 1(c) статті 6 GDPR).

У частині 11 статті 52 очевидно розглядаються вимоги щодо доступу до публічної інформації та більш конкретно щодо доступу посадових осіб до даних.

Рекомендується додати до цього положення посилання на Закон України «Про доступ до публічної інформації», щоб положення частини 11 статті 52 застосовувалися у відповідності до вимог цього Закону.

Стаття 53. Обробка персональних даних працівників їхніми представниками

До цієї статті не виникає жодних конкретних зауважень, і вона не потребує змін.

Стаття 54. Особливі вимоги до обробки роботодавцем персональних даних працівників або кандидатів на працевлаштування

У частині 1 статті 54 йдеться про можливість роботодавця збирати інформацію про стан здоров'я працівників і кандидатів на працевлаштування, про яких докладніше йдеться також у частині 2 статті 54.

Пропонується додати до частини 1 статті 54 згадування про те, що обробка дозволена

за дотримання умов, викладених у частині 2 статті 54, що дозволить чітко встановити умови, за яких мають застосовуватися положення частини 1 статті 54.

У частині 2 статті 54 перелічені випадки, за яких роботодавець може збирати персональні дані про стан здоров'я кандидата на працевлаштування або працівника. Попри те, що така обробка буде дозволена Проєктом Закону, необхідно гарантувати, що вона в будь-якому випадку здійснюватиметься законно й у відповідності до інших положень/вимог Проєкту Закону (наприклад, матиме належну правову підставу).

Рекомендується доповнити частину 2 статті 54 вимогою здійснювати обробку справ, перелічених у цій частині у відповідності до інших умов, встановлених Проєктом Закону.

У частині 3 статті 54 йдеться про обробку генетичних даних працівників, а у частині 4 статті 54 додатково розкриваються умови обробки біометричних даних працівників. Важко передбачити обробку генетичних даних у трудових відносинах, у зв'язку із чим виникає запитання чи не мали автори Проєкту Закону намір урегулювати питання біометричних даних в частині 3 статті 54.

Сфера застосування та узгодженість частини 3 статті 54, особливо стосовно частини 4 статті 54, потребує перегляду, щоб ймовірно мова йшла про біометричні дані, які унікально ідентифікують особу, а не про генетичні дані.

Стаття 55. Прозорість обробки персональних даних в цілях трудових правовідносин

Ця стаття регулює права працівника на захист персональних даних. Коментарі надаються лише на ті положення, до яких виникають запитання, і/або які можуть потребують змін.

У частині 1 статті 55 йдеться про право працівника на інформацію (стаття 18 Проєкту Закону), в тому числі через право на доступ (стаття 19 Проєкту Закону), але не йдеться про інші права, передбачені Проєктом Закону.

У цій статті рекомендується зазначити всі права працівника на захист персональних даних, оскільки виокремлення одного або двох прав на практиці може призводити до невизначеності щодо того, чи користуються працівники всіма правами на захист персональних даних (стаття 20 та наступні Проєкту Закону) чи лише тими, які згадуються виключно у цій статті.

У частині 3 статті 55 йдеться про право працівників на отримання персональних даних про їх оцінювання та про право оскаржувати достовірність таких даних до органу управління та судах. Про можливість подання апеляції або скарги до контролюючого органу не йдеться.

Задля уникнення невизначеності частину 3 статті 55 слід доповнити положенням щодо права працівника подати апеляцію або скаргу до контролюючого органу.

Частиною 4 статті 55 встановлюється заборона на прийняття рішень, що мають суттєвий вплив на права та обов'язки працівника, на підставі автоматизовано обробки даних без врахування позиції працівника.

Для того, щоб забезпечити застосування цього положення у відповідності до порядку, яким більш загально урегульоване автоматизоване прийняття рішень цим Проєктом Закону (стаття 25), настійно рекомендується додати до цієї статті посилання на положення, якими передбачено автоматизоване прийняття рішень.

Частиною 7 статті 55 передбачається, що реалізація прав працівника, який є суб'єктом внутрішнього розслідування, може бути відстрочено до завершення розслідування. Такі обмеження прав і затримка в їх реалізації, як передбачено цією статтею, здаються досить широкими у контексті вимог GDPR, вимагаючи від контролера сприяння у реалізації прав суб'єктами даних (частина 2 статті 12), а також може порушуватись питання за статтею 11 Конвенції 108+, яка встановлює ліміти та умови для обмеження, які можуть бути передбачені вимогами щодо прозорості (наприклад, виняток передбачений законом і вважається таким, що є необхідним і пропорційним заходом у демократичному суспільстві). Також, якщо дані про суб'єкта даних збираються опосередковано, що може відбуватися у межах внутрішнього розслідування, суб'єкт персональних даних повинен отримати інформаційне повідомлення про обробку даних не пізніше ніж за 1 місяць відповідно до положень пункту 3(a) статті 14 GDPR. Водночас пункт 5(b) статті 14 також містить виняток, який передбачає можливість затримки у наданні інформації, у разі якщо це може серйозно перешкодити досягненню цілей обробки.

З огляду на ці елементи до частини 7 статті 55 потрібно внести зміни, зазначивши що у здійсненні прав, включаючи право на інформацію, може бути відмовлено, якщо це може серйозно перешкодити розслідуванню (наприклад, через ризик втрати доказів), але права можуть бути реалізовані відразу після усунення ризику.

3.8 РОЗДІЛ IX. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ ПРАВООХОРОННИМИ ОРГАНАМИ

У розділі IX йдеться про обробку персональних даних правоохоронними органами. У якості вступної ремарки слід нагадати, що Конвенція 108+ застосовується також до обробки персональних даних компетентними органами для правоохоронних цілей. Якщо говорити про ЄС, то GDPR не застосовується до такої обробки персональних даних, яка замість цього регулюється Директивою про захист даних у правоохоронній діяльності. Таким чином, з точки зору ЄС коментарі до цього розділу стосовно обробки даних в правоохоронних цілях, зроблені в світлі Директиви про захист даних у правоохоронній діяльності, а не GDPR. Проте варто звернути увагу, що на противагу Конвенції 108+, оскільки ні GDPR, ні Директива про захист даних у правоохоронній діяльності не застосовуються до обробки персональних даних з метою забезпечення національної безпеки, збереження державної таємниці або для цілей національної оборони (а саме, діяльність, яка зазвичай здійснюється розвідувальними службами), оскільки такі питання виходять за межі компетенції та законодавства ЄС. З огляду на ці роз'яснення, виникає кілька загальних зауважень до цього розділу, які наведені нижче.

По-перше, у положеннях цього розділу, що застосовуються до обробки персональних даних правоохоронними органами, згадуються «розвідувальні органи» без надання їх визначення, в той самий час, як запропоноване Проєктом Закону визначення «правоохоронного органу» вочевидь охоплює діяльність, яку зазвичай здійснюють розвідувальні органи. Беручі до уваги той факт, що у назві статті 56 зазначаються як правоохоронні, так і розвідувальні органи, у положеннях статті 56 правоохоронні і розвідувальні органи згадуються довільно. Водночас, у назві розділу IX не йдеться про розвідувальні органи, а стаття 57 та її зміст не містять чіткої вказівки на відповідні органи, про які йдеться у цих положеннях.

По-друге, сфера діяльності, що згадується у цьому розділі, зосереджена на обробці даних для «правоохоронних цілей» (див. частину2, 4 статті 56, частину 1 статті 57), але іноді також згадується обробка для «розвідувальних цілей» (частина 3 статті 56). Розуміємо це так, що, беручи до уваги визначення правоохоронного органу відповідно до Проєкту Закону, діяльність з розвідувальними цілями віднесена до категорії діяльності з правоохоронними цілями. Вітається те, що у Проєкті Закону йдеться про ці два види діяльності, однак варто наголосити, що на них можуть поширюватися різні вимоги законодавства про захист персональних даних відповідно до європейських стандартів захисту персональних даних. Зрештою, у цьому розділі не визначається, що слід розуміти

під «розвідувальними цілями». Обробка для таких цілей, зокрема у контексті Конвенції 108+, може здійснюватися з метою забезпечення національної безпеки, збереження державної таємниці або заходів забезпечення національної оборони. Визначення «обробки персональних даних для правоохоронних цілей», передбачене Проєктом Закону, охоплює деякі з таких видів діяльності, оскільки воно стосується «розвідувальних операцій» та «забезпечення національної безпеки». Проте, згідно з Директивою про захист даних у правоохоронній діяльності така діяльність і, загалом, розвідувальна діяльність не становить частину правоохоронних цілей, оскільки вони не регулюються законодавством ЄС, як це пояснювалося вище. У такий спосіб, застосовний режим захисту персональних даних, за можливих винятків, відрізнятиметься залежно від мети обробки (незважаючи на тип органу, що проводить таку діяльність), а саме, коли здійснюється обробка для правоохоронних цілей або для розвідувальної діяльності, у будь-якому випадку застосовується Конвенція 108+ до обох видів діяльності.

Оскільки обробка персональних даних у цих сферах, як для правоохоронних цілей, так і для цілей розвідувальної діяльності, може мати значний вплив на право особи на приватність та захист персональних даних, дуже важливо встановити чіткий порядок щодо цього, особливо стосовно обсягу та цілей, для яких такі дані можуть оброблятися.

Зважаючи на передбачені Проєктом Закону визначення «правоохоронного органу» та «обробки персональних даних для правоохоронних цілей», у цьому розділі необхідно уточнити, які положення застосовуються до яких органів (правоохоронних або розвідувальних) і для яких цілей (правоохоронної або розвідувальної), щоб уникнути розбіжностей і забезпечити правову визначеність та встановити застосовний режим із врахуванням можливих винятків щодо визначення мети обробки

До того ж, частиною 1 статті 56 встановлюється загальна вимога до правоохоронних і розвідувальних органів дотримуватися Проєкту Закону з урахуванням положень, передбачених статтею 57 щодо реалізації прав суб'єкта даних у зв'язку з обробкою персональних даних для правоохоронних цілей. Водночас у статті 56 повторно стверджуються деякі принципи захисту даних, яких повинні дотримуватися правоохоронні та розвідувальні органи, а саме принцип законності (частина 2 статті 56) та обмеження мети (частина 3 статті 56), але не згадуються інші принципи захисту даних, що застосовуються відповідно до Проєкту Закону. Також встановлюється одна специфічна вимога до правоохоронних і розвідувальних органів розмежовувати інформацію про різні

категорії суб'єктів персональних даних і обробляти її в окремих базах даних (частина 5 статті 56). Таке формулювання положень може створити неправильне враження про те, що лише такий порядок, про який йдеться у цьому розділі, застосовується до правоохоронних і розвідувальних органів, в той час, як ідея, що виникає з частини 1 статті 56, полягає в тому, що весь Проєкт Закону застосовується до нього з певними особливостями, викладеними у цьому розділі.

Для більшої ясності та правової визначеності до розділу IX або його статей слід додати, що ці положення застосовуються додатково до всіх інших положень Проєкту Закону, якщо не передбачено інше (наприклад, для здійснення прав суб'єкта персональних даних, про які йдеться у статті 57). З тих самих причин також настійно рекомендується доповнити цей розділ додатковими положеннями, що враховують певні особливості обробки персональних даних правоохоронними органами, де відповідні положення Проєкту Закону можуть бути не повною мірою релевантними (наприклад, обробка чутливих даних (див. статтю 10 Директиви про захист даних у правоохоронній діяльності), автоматизоване прийняття рішень (див. статтю 11 Директиви про захист даних у правоохоронній діяльності), відмінність між персональними даними і якістю персональних даних (див. статтю 7 Директиви про захист даних у правоохоронній діяльності) або накладати певні зобов'язання (протоколювання виконаних дій (див. статтю 25 Директиви про захист даних у правоохоронній діяльності) та обмеження, встановлені в тому числі на розвідувальні органи, але з неодмінним урахуванням вимог пункту 1 статті 11 Конвенції 108+.

Стаття 56. Вимоги до обробки персональних даних правоохоронними та розвідувальними органами

Частиною 1 статті 56 передбачається, що правоохоронні та розвідувальні органи повинні дотримуватися вимог Закону, *«з урахуванням»* положення, визначені статтею 57, у якій наведений порядок здійснення прав суб'єкта персональних даних. Так само у частині 4 статті 56 зазначається, що обробка персональних даних в правоохоронних цілях здійснюється *«з урахуванням»* принципів, визначених Законом. Вираз *«з урахуванням»* може бути витлумачений як не рівнозначний твердому зобов'язанню, хоча має бути гарантовано, що зазначений порядок у належний спосіб дотримується правоохоронними і розвідувальними органами, як і будь-яке зобов'язання за Проєктом Закону.

Рекомендується виключити з частини 1 і 4 статті 56 вираз «з урахуванням», щоб

показати чіткі зобов'язання правоохоронних і розвідувальних органів. У частині 4 статті 56 також має бути чітко зазначено, яких принципів слід дотримуватися, оскільки з поточного формулювання це незрозуміло.

Частина 2 статті 56 передбачає принцип законності відповідно до вимог Конвенції 108+ і узгоджується з відповідним положенням Директиви про про захист даних у правоохоронній діяльності (стаття 8).

Для повної узгодженості, щонайменше у стосунку до правоохоронних органів, у Проєкті Закону або в інших правових актах необхідно зазначити персональні дані, які обробляються, та цілі їх обробки.

Частиною 3 статті 56 передбачається принцип обмеження мети відповідно до вимог Конвенції 108+. У ній загалом враховані відповідні положення Директиви про захист даних у правоохоронній діяльності (пункти 1(b) та 2(a) і (b) статті 4), але все ж таки потрібні подальші роз'яснення.

Додатково до положення про те, що персональні дані не можуть використовуватися в подальшому, якщо це не дозволено виключно законом, у такому випадку необхідно також передбачати вимогу, яка б гарантувала, що така обробка є необхідною і пропорційною для подальшої мети. Зважаючи на можливі наслідки для осіб, чиї дані стають предметом обробки, встановлення таких обмежень є необхідним для запобігання будь-якому необґрунтованому використанню їхніх персональних даних та гарантуватиме дотримання принципу обмеження мети. До того ж, у цьому положенні має бути чітко зазначено, що персональні дані не обробляються у спосіб, несумісний з початковою метою. Такі зміни приведуть положення частини 3 статі 56 у відповідність із пунктами 1(b) і 2(a) статті 4 Директиви про захист даних у правоохоронній діяльності Також, рекомендуємо авторам Проєкту Закону розглянути можливість включення положення, що стосується цілей використання даних, які б були сумісними.

У частині 5 статті 56 встановлюється вимога до правоохоронних і розвідувальних органів розмежовувати інформацію про різні категорії суб'єктів персональних даних і обробляти її в окремих базах даних, що аналогічно передбаченому статтею 6 Директиви про захист даних у правоохоронній діяльності .

Рекомендуємо роз'яснити у пункті 3 частини 5 цієї статті хто є «іншими учасниками кримінального провадження» і в такий спосіб привести її у відповідність до пункту (d) статті 6 Директиви про захист даних у правоохоронній діяльності (тобто особи, які можуть бути викликані для дачі свідчень у зв'язку із кримінальними правопорушеннями або подальшим кримінальними провадженнями; особи, які можуть надати інформацію про кримінальні правопорушення, або про спільників або пов'язаних із підозрюваними або засудженими осіб).

Стаття 57. Особливості реалізації прав суб'єктів персональних даних у зв'язку з обробкою персональних даних в цілях правоохоронної діяльності

Ця стаття регулює обмеження, які можуть накладатися на права суб'єктів персональних даних під час обробки їхніх персональних даних для правоохоронних цілей, і умови накладення таких обмежень.

Якщо конкретніше, то частиною 1 статті 57 передбачається обмеження прав, про які йдеться у статтях 18 (право на інформацію), 19 (право на доступ) і 21–24 (право бути забутим, заперечувати, на перенесення, на обмеження), і надається перелік цілей, права щодо яких можуть бути обмежені відповідно до закону.

Проте у частині 1 статті 57 не згадується право на виправлення персональних даних (стаття 20 Проєкту Закону), яке необхідно додати, якщо тільки для цього права не передбачено жодних обмежень. До того ж, право на мобільність (стаття 23 Проєкту Закону) видається недоречним у контексті обробки для правоохоронних цілей, і посилання на відповідну статтю задля уникнення невірного тлумачення слід виключити. Стосовно умов, за яких права можуть обмежуватися, загальне посилання на те, що це буде здійснюватися в порядку, передбаченому законом, здається недостатнім і має бути доповнено вимогами, викладеними щодо цього у пункті 1 статті 11 Конвенції 108+. Згідно останнього, зокрема, більш конкретно вимагається, щоб обмеження також враховувало суть основних прав і свобод та було необхідним і пропорційний заходом у демократичному суспільстві.

У частині 2 статті 57 загально представлено, у який спосіб рішення про обмеження реалізації прав мають прийматися в кожному окремому випадку. Це передбачає дотримання балансу між необхідністю досягнення мети правоохоронної діяльності та необхідністю забезпечення права суб'єкта персональних даних, що, вочевидь, загалом

відповідає вимогам Конвенції 108+ та Директиви про захист даних у правоохоронній діяльності.

Однак, необхідно встановити зв'язок між частиною 2 та частиною 1 статті 56, зробивши на неї посилання, оскільки в останній викладаються всеосяжні та обов'язкові умови, включно із допустимою метою обмеження, яких повинні дотримуватися компетентні органи, встановлюючи обмеження щодо прав окремих осіб. Також слід визначити (в Проєкті Закону або в інших правових актах), у який спосіб можуть вводитися обмеження щодо кожного окремого права, оскільки вони не завжди вводитимуться і застосовуватимуться однаково (наприклад, право на доступ не передбачає тих самих обмежень, що й право на інформацію). За відсутності таких роз'яснень, незрозуміло чи можна все ще розглядати обмеження, як таке, що відповідає вимозі пункту 1 статі 11 Конвенції 108+, головним чином, умові, що воно має бути «передбачено законом».

До частини 3 та 4 статті 57 особливих зауважень не виникає.

У якості заключної ремарки до цього розділу, звертаємо увагу на наступні, прийняті Радою Європи документи, які можуть стати корисним керівництвом під час розгляду зазначених вище рекомендацій та їх реалізації:

- Рекомендація (87) 15, що регулює використання персональних даних у секторі поліції, прийнята 17 вересня 1987 року;
- Практичний посібник щодо використання персональних даних у секторі поліції, прийнята 15 лютого 2018 року.

3.9 Розділ X. Відповідальність за порушення законодавства у сфері захисту персональних даних

У цьому розділі викладаються загальні умови та порядок накладення штрафів у разі порушення вимог Проєкту Закону.

Стаття 58. Відповідальність за порушення законодавства у сфері захисту персональних даних

Частина 1 статті 58 додатково до відповідальності, яка настає за цим Законом, також міститься загальне посилання на «інші закони України».

Для забезпечення правової визначеності для контролерів і операторів даних, в цій частині необхідно дати роз'яснення про інші закони України, які можуть слугувати

підставою для притягнення до відповідальності у разі порушень у сфері захисту персональних даних, і особливо, якщо інші закони також передбачають санкції за порушення вимог Проєкту Закону.

У частині 2 статті 58 згадується про *«заходи»*, які можуть застосовуватися контролюючим органом у разі порушень у сфері захисту персональних даних, але не уточнюється характер або зміст цих заходів, і те, чи можливі інші заходи, крім штрафів, як це зазначено у цьому розділі. У Пояснювальній записці до Проєкту Закону, а також у Проєкті Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» (№ 6177 від 18.10.2021)[9] можуть бути передбачені інші заходи, такі як адміністративні санкції, але в цьому у нас нема повної впевненості. У певних випадках необхідні заходи, відмінні від штрафів (наприклад, заборона обробки), для забезпечення ефективних, пропорційних та стримуючих санкцій, як це передбачено Конвенцією 108+ (див. параграф 100 Пояснювальної записки та статтю 12 Конвенції 108+), а також GDPR (див. пункт 1 статті 83).

Необхідно більш детально визначити заходи, які можуть застосовуватися контролюючим органом у разі порушень вимог Проєкту Закону, а також зазначити чи можливі інші види санкцій, окрім штрафів (наприклад, попередження, наказ про припинення обробки тощо, як це передбачено пунктом 2 статті 58 GDPR), для більшої правової визначеності, а також для встановлення порядку ефективних і належних санкцій та заходів відповідно до Конвенції 108+ і GDPR.

У частині 4 статті 58 йдеться про права та засоби правового захисту, доступні суб'єкту персональних даних, незалежно від відповідальності, яка може бути накладена на сторону відповідно до Проєкту Закону.

Задля уникнення невизначеності, у статті також варто зазначити, що у такому випадку суб'єкт персональних даних має право подати скаргу до контролюючого органу.

[9] Проєкту Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» № 6177 від 18.10.2021, доступний за посиланням: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992

Стаття 59. Відповідальність контролерів та операторів за порушення законодавства у сфері захисту персональних даних

У статті 59 передбачені суми та порогові значення штрафів, які можуть накладатися контролюючим органом у разі порушення вимог Проєкту Закону. Зокрема, тут застосовується підхід, схожий на той, що застосовується GDPR (стаття 83), відповідно до якого встановлюються різні порогові значення штрафів (виражені у фіксованих сумах або відсотках від річного обороту, включно з максимальними лімітами для загальних сум) залежно від порушення та чи було воно вчинено фізичною або юридичною особою. При цьому також враховується, чи призвело недодержання вимог законодавства до порушення прав суб'єкта персональних даних і чи має воно повторний характер. У такий спосіб ця стаття, вочевидь, встановлює загалом ефективний, пропорційний та стримувальний порядок накладення штрафів відповідно до Конвенції 108+ (див. параграф 100 Пояснювальної записки та статтю 12 Конвенції 108+), а також GDPR (див. пункт 1 статті 83) щодо цього питання. Окремі положення, тим не менш, викликають питання, що викладені нижче, і можуть потребувати внесення змін.

У частинах 1 і 2 статті 59, якими встановлюється нижній поріг штрафів, передбачені різні порогові значення залежно від того, чи призвело недотримання вимог законодавства до порушення прав суб'єкта персональних даних. Така відмінність, що стосується наявності або відсутності порушення прав суб'єктів персональних даних, не визначається частиною 3 статті 59, положення якої передбачають вищий поріг штрафів. У будь-якому випадку, ні Конвенція 108+, ні GDPR не проводять такої відмінності і встановлення різних порогових значень і накладання штрафів, залежно від того, чи було порушення прав чи ні, може бути поставлено під сумнів. Попри те, що при накладенні санкцій потрібно враховувати, серед інших факторів, наявність конкретного порушення права суб'єктів даних, недотримання законодавства про захист персональних даних у більшості випадків також призводитиме певною мірою до порушення права суб'єктів даних на приватність або захист даних і не завжди кваліфікується як «право» за змістом статей 19–24 Проєкту Закону (наприклад, це може бути втручання у приватне життя, неможливість відкликати згоду, або тільки матеріальна шкода тощо).

Якщо тільки розробники Проєкту Закону не мають наміру досягти певної мети, рекомендується усунути відмінність між пороговими значеннями залежно від того, чи мало місце порушення прав суб'єктів даних чи ні, як це передбачено частинами 1 і 2 статті 59, і залишити лише частину 2 статті 59, щонайменше для забезпечення

узгодженості з частиною 3 статті 59. Натомість, на посилення статті 59, пропонуємо доповнити її додатковими положеннями, якими встановити, що штрафи мають накладатися з урахуванням обставин кожного окремого випадку та визначити фактори, які мають братися до уваги контролюючим органом, аналогічно викладеному в пункті 2 статті 83 GDPR. З цією метою рекомендується щонайменше перенести до тексту статті обставини, що перелічені в Пояснювальній записці до Проєкту Закону щодо накладення штрафів (тобто *«характер, тяжкість і тривалість порушення та його наслідки, заходи, вжиті для забезпечення виконання вимог Проєкту Закону, та будь-які заходи, спрямовані на запобігання негативних наслідків, що виникли внаслідок порушення, або на пом'якшення їхнього впливу»*).

Незрозуміла сфера застосування частини 4 статті 59, у якій йдеться про порядок накладення штрафів за порушення *«інших положень»* Проєкту Закону, крім тих, які перелічені в частинах 1–3 статті 59.

Рекомендується більш детально роз'яснити, про які інші положення може йти мова в частині 4 статті 59, оскільки в іншому випадку актуальність цього положення видається незрозумілою.

Стаття 60. Строки давності для застосування відповідальності за цим Законом

Ця стаття передбачає строк давності тривалістю 3 роки для відповідальності, до якої можуть притягнути за порушення вимог Проєкту Закону. Іншими словами, відповідно до Проєкту Закону контролер та оператор персональних даних не буде притягнутий до відповідальності, якщо після виявлення або вчинення порушення законодавства про захист персональних даних мине 3 роки. Ні Конвенція 108+, ні GDPR не передбачають можливості встановлення строку давності для накладення штрафів або інших видів санкцій у разі порушення законодавства про захист даних. Дійсно, строк позовної давності тривалістю 3 роки є досить коротким періодом, який може значно послабити ефективність Проєкту Закону і особливо стримувальний характер порядку притягнення до відповідальності контролерів або операторів персональних даних, як передбачено статтею 59. Контролери або оператори персональних даних точно намагатимуться знайти способи приховати порушення, якщо знатимуть про можливість уникнення відповідальності після закінчення строку тривалістю 3 роки. Додатково, Керівництво 04/2022 щодо нарахування адміністративних штрафів за GDPR, прийняте Європейською Радою із захисту даних 12 травня 2022 року, встановлює, що порушення, скоєні в

минулому, можуть все ще представляти інтерес для введення санкцій, якщо оцінювати роботу контролерів або операторів з точки зору санкційної процедури і, саме тому, не потребує встановлення обмеженого періоду (тим не менш в національному законодавстві деяких країн ЄС досі існують такі періоди обмеження). Таким чином виявляється, що періоди обмеження можуть, певною мірою, заважати контролюючому органу діяти ефективно під час оцінки порушень, здійсненних контролером або оператором.

З цих причин настійно рекомендується виключити статтю 60 або встановити період позовної давності більше, ніж три роки для того, щоб контролюючий орган мав можливість ефективно діяти та враховувати усі порушення, скоєні контролером або оператором протягом відповідного періоду часу в рамках санкційної процедури.

3.10 РОЗДІЛ XI. ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

У цьому розділі викладаються положення, що стосуються формальних аспектів Проєкту Закону (таких як набрання законом чинності, правил перехідного періоду), а також передбачається низка змін до інших законодавчих актів України у певних сферах або секторах (трудовий кодекс, поховання та похоронна справа, електронна комерція, електронна система охорони здоров'я, електронні засоби зв'язку). Ці поправки до інших законодавчих актів спрямовані на введення простої вимоги щодо дотримання положень Проєкту Закону там, де це доречно, або передбачають певні зобов'язання у зазначених актах законодавства. У зв'язку з цим формальні аспекти (пункти 1–4 цього розділу) і введення вимоги щодо дотримання Проєкту Закону в певні законодавчі акти України (пункти 5.1–5.4 цього розділу) не викликають зауважень. Стосовно положень, що запроваджують особливі зобов'язання в певних сферах або секторах, що згадуються в цьому розділі (пункт 5), оскільки Конвенція 108+[10] та GDPR не встановлюють конкретних правил обробки персональних даних у таких сферах або секторах, коментарі надаються лише за потреби та з загальної точки зору на основі цих текстів. Однак, у питаннях, що стосуються електронних засобів зв'язку і тих, що пов'язані з недоторканністю приватного життя і конфіденційністю під час обробки персональних даних у цьому контексті, ми даємо коментарі з погляду Директиви про конфіденційність та електронні засоби зв'язку. Звертаємо увагу, що наші коментарі надаються, наскільки це

[10] Проте Рада Європи прийняла Рекомендацію № R(95) 4 від 7 лютого 1995 року про захист персональних даних у сфері телекомунікаційних послуг, з особливим акцентом на телефонні послуги, яка певною мірою і досі залишається актуальною. У такий спосіб, наша думка також підкріплюється положеннями цієї Рекомендації.

можливо, лише на базі витягів із законодавства, що представлені у цьому розділі, без повного знання цих законодавчих актів, про які йде мова, або доступу до них.

Пункт 5.5 Перехідних положень щодо статті 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення» (Відомості Верховної Ради України, 2018, № 5, стор. 31) – Стаття 11. Електронна система охорони здоров'я

Ця стаття, вочевидь, стосується функціонування електронної системи охорони здоров'я. Більш конкретно, відповідно до підпункту 2 пункту 5 Перехідних положень Проєкту Закону, статті 11 передбачає, що доступ до даних про пацієнта, що містяться в електронній системі охорони здоров'я, надається лікареві, з яким пацієнт уклав декларацію, або іншому медичному персоналу, на який поширюється зобов'язання відповідно до статті 40 Закону України «Основи законодавства України про охорону здоров'я».

Ми припускаємо, що в даному випадку інший медичний персонал пов'язаний лікарською таємницею або іншими зобов'язаннями щодо дотримання конфіденційності, які передбачені зазначеним українським законодавством, але задля уникнення будь-яких сумнівів, про це має бути чітко зазначено у цій статті задля гарантування того, що, дійсно, існують відповідні гарантії доступу до даних пацієнта, які кваліфікуються як дані особливої категорії згідно статті 6(1) Конвенції 108+ та статті 9(1) GDPR. Також варто передбачити чи потрібно запроваджувати додаткові запобіжники в законі відповідно до статті 6(1) GDPR та статті 6(2) Конвенції 108+, задля усунення будь-яких можливих ризиків для обробки даних пацієнтів, включно із тими, що по'вязані із безпекою (наприклад, встановити в Проєкті Закону вимоги безпеки щодо функціонування та доступу електронної системи охорони здоров'я).

Підпунктом 4 пункту 5 щодо статті 11 передбачається, що уповноважений орган зобов'язаний опублікувати *«дані, накопичені в електронній системі охорони здоров'я, на офіційному веб-сайті»* на умовах, які визначаються Кабінетом Міністрів України і мають бути затверджені контролюючим органом. Також зазначено, що дані (ймовірно той самий їх набір, що і згаданий у попередньому реченні) перед публікацією мають бути повністю знеособлені відповідно до вимог Закону України «Про захист персональних даних».

До цієї статті не виникає жодних конкретних зауважень і рекомендацій.

Підпункт 6 пункту 5 Перехідних положень стосується змін до Закону України «Про електронні комунікації» (Офіційний вісник України, офіційне видання 2021 р., № 6, стор. 10, стаття 306, код Закону 102665/2021)

Попередньо та загально зауважимо, що у статтях, викладених відповідно до цього пункту, використовуються певні ключові поняття, такі як «дані трафіку», «дані про місцезнаходження», «додаткова послуга», «користувач», «кінцевий користувач», «споживач», але без надання їм визначень, які можуть викликати запитання щодо їх застосовності.

З метою забезпечення ясності і правової визначеності, настійно рекомендується включити визначення згаданих вище понять, що гарантуватиме належне застосування викладених у цьому пункті положень, зважаючи на відповідні значення цих термінів, що наведені у Директиві про конфіденційність та електронні комунікації, а також Конвенції Ради Європи про кіберзлочинність, включаючи додаткові протоколи до неї (так звана Будапештська Конвенція).

З загальної перспективи, також незрозуміло, хто може накладати санкції або в інший спосіб притягувати до відповідальності організації за порушення положень, викладених у цьому пункті. Відповідно до статті 15a Директиви про конфіденційність та електронні комунікації примусове виконання та інші форми відповідальності за дотримання таких положень вимагає ефективного, пропорційного та стримувального санкційного порядку. Таке примусове виконання може здійснюватися контролюючим органом.

Необхідно доповнити положення, що стосуються Закону України «Про електронні комунікації», щоб уточнити, як виконуватимуться викладені нижче положення, з урахуванням вимог статті 15a Директиви про конфіденційність та електронні комунікації.

Стаття 31. Безпека електронних комунікацій

Частина 1 статті 31 відповідає вимозі, викладеній у пункті 1 статті 4 Директиви про конфіденційність та електронні комунікації.

Частиною 2 статті 31, яка стосується ризиків, що мають оцінюватися для запровадження відповідних заходів безпеки, передбачено визначення таких ризиків та зазначається, що

під ними слід розуміти будь-які дії, в тому числі, серед іншого, *«послуги або товари»*.

Якщо не було допущено помилку під час перекладу, це згадування про «послуги та товари» слід виключити, оскільки в цьому контексті воно вочевидь не має сенсу. До того ж, для забезпечення ефективного і повного захисту приватного життя фізичних осіб, положення має містити чіткий перелік ризиків із зазначенням того, що це може становити ризик для змісту повідомлення /кореспонденції, а також для будь-яких пов'язаних із таким повідомленням /кореспонденцією даних (наприклад, даних трафіку).

У частині 3 статті 31 перелічуються загальні заходи, якими гарантується безпека комунікації відповідно до тих, що наведені в статті 4 Директиви про конфіденційність та електронні комунікації, зі змінами від 2009 року. Проте у пункті 2 частини 3 статті 31, яким передбачено зобов'язання попереджати певні загрози персональним даним, що відповідає обсягу визначення порушення персональних даних, однак, не зазначається, що ці загрози /дії можуть бути незаконними або випадковими, як це передбачено статтею 4 Директиви про конфіденційність та електронні комунікації, а також визначенням порушення персональних даних, наведеного в GDPR і, власне, в Проєкті Закону.

Для забезпечення відповідності визначення порушення безпеки персональних даних, що міститься в Проєкті Закону до Директиви про конфіденційність та електронні комунікації, а також для забезпечення охоплення повного спектру ризиків щодо персональних даних, яким необхідно запобігти, у пункті 2 частини 3 статті 31 варто вказати на випадковий або незаконний характер безпекових загроз/дій щодо персональних даних.

Положення пункту 3 частини 3 статті 31, яким передбачається впровадження організаційних та інших заходів безпеки, є незрозумілим в частині згаданого *«затвердження»* таких заходів (ким? як?), а також посилання на *«законодавство про захист інформації та захист персональних даних»*.

Рекомендується роз'яснити це положення, а саме, що мається на увазі або що очікується під затвердженням заходів безпеки та зазначити назву Проєкту Закону замість фрази «законодавство про захист інформації та персональних даних», щоб уникнути будь-якого невірного тлумачення.

Стаття 31[1]. Повідомлення споживачів та кінцевих користувачів про ризик для безпеки електронних комунікаційних мереж та/або послуг

Розуміємо, що це положення стосується зобов'язань постачальників електронних комунікаційних мереж та/або послуг повідомляти споживачів і користувачів електронних комунікаційних послуг про виникнення ризику для безпеки, що впливає на такі послуги. Оскільки це зобов'язання стосується ризиків для безпеки, у такий спосіб воно видається відмінним від зобов'язання повідомляти про порушення безпеки для персональних даних, передбаченого статтями 37 і 38 Проєкту Закону.

Оскільки ризик безпеки електронних комунікаційних мереж та/або послуг, як це визначено у частині 2 статті 31, може на практиці також призводити до витоку персональних даних в розумінні Проєкту Закону, у тексті слід уточнити, що зобов'язання щодо повідомлення, передбачені в статті 31[1], не обмежуються і тому застосовуються додатково до зобов'язань щодо повідомлення про порушення безпеки персональних даних відповідно до статей 37 і 38 Проєкту Закону, щоб забезпечити правову визначеність для постачальників електронних комунікаційних мереж та послуг. Також, для забезпечення належного інформування споживачів і користувачів, у тому числі для того, щоб вони могли оцінити будь-які ризики для приватності та захисту даних, у положенні має бути зазначений зміст повідомлення, яке має бути направлено фізичним особам, зокрема, характер ризику і можливі наслідки для фізичних осіб.

Стаття 31[2] Таємниця приватного спілкування

У цій статті передбачені зобов'язання, спрямовані на забезпечення таємниці приватного спілкування, а також можливі обмеження, аналогічні до тих, передбачених статтею 5 Директиви про конфіденційність та електронні комунікації.

У якості попереднього коментаря до цієї статті, варто зазначити, що стаття 5 Директиви про конфіденційність та електронні комунікації, якою встановлюється принцип конфіденційності комунікації, не розрізняє «приватну» та іншу комунікацію та передбачає вимогу конфіденційності для будь-якого типу комунікацій. Те саме стосується визначення «комунікації» відповідно до пункту (d) статті 2 Директиви про конфіденційність та електронні комунікації.

В тій міри, в якій поняття «приватне спілкування» може створити невизначеність щодо типу комунікацій, які захищені або не захищені положеннями статті 31², рекомендується замінити його лише на «комунікації» відповідно до Директиви про конфіденційність та електронні комунікації.

Частиною 1 статті 31² встановлюється загальна вимога щодо забезпечення таємниці приватного спілкування. Хоча у статті передусім розглядається «приватне спілкування», у ній також йдеться про листування, телефонні розмови, телеграфну чи іншу кореспонденцію, але не уточнюється, чи слід включати ці повідомлення також у категорію «приватних повідомлень».

Варто додатково дати роз'яснення цієї статті, визначивши, чи слід включати «листування, телефонні розмови, телеграфну чи іншу кореспонденцію» також у категорію приватної комунікації і, в такий спосіб, користуватися тими самими заходами захисту. До того ж, до елементів, на які поширюється таємниця приватної комунікації, слід додати особу відправника /одержувача, назву повідомлення та будь-які вкладення (у відповідних випадках), оскільки секретність для окремих осіб неможливо забезпечити, якщо ці елементи не включені у статтю.

До частини 2 статті 31², у якій зазначається зобов'язання постачальників електронних комунікаційних мереж та/або послуг та інших осіб, залучених у процес діяльності електронних комунікацій, захищати таємницю приватного спілкування навіть після припинення їх діяльності, не виникає зауважень, оскільки це відповідає загальній вимозі забезпечення конфіденційності комунікацій, як це передбачено статтею 5 Директиви про конфіденційність та електронні комунікації.

Частиною 3 статті 31² розглядається можливість для постачальників електронних комунікаційних мереж та/або послуг отримувати, використовувати та передавати інформацію про приватне спілкування іншим особам в обсязі, необхідному для надання електронних комунікаційних послуг. Стаття має широкий сенс і підвищує ризик необґрунтованого використання і передачі даних про приватне спілкування усупереч вимозі конфіденційності комунікацій згідно статті 5 Директиви про конфіденційність та електронні комунікації.

Зважаючи на положення пункту 1 статті 5 Директиви про конфіденційність та електронні комунікації, у статті необхідно, по-перше, зазначити операції, які можуть

розглядатися як необхідні для надання послуг електронних комунікацій, і, по-друге, зазначити, що інші особи, яким може передаватися інформація про приватне спілкування, повинні дотримуватися суворих зобов'язань щодо дотримання та забезпечення конфіденційності такого спілкування.

Частиною 4 статті 31^2 передбачається заборона на втручання в приватне спілкування і встановлюється порядок, який допускає у певних випадках виключення з цієї заборони, дотримуючись загалом того самого підходу, що й, відповідно, у Директиві про конфіденційність та електронні комунікації (пункт 1 статті 5 і пункт 22 декларативної частини). Водночас, можна розширити види втручання, що перелічені у цій статті (прослуховування, записування, зберігання та передача інформації), щоб забезпечити усебічний і ефективний захист приватного спілкування.

З цією метою статтю слід доповнити посиланням на «запис на плівку» і «будь-який інший тип втручання» відповідно до пункту 1 статті 5 Директиви про конфіденційність та електронні комунікації.

До того ж, це положення містить загальну вказівку на те, що втручання може дозволятися, якщо це необхідно для надання електронних комунікаційних послуг, але без зазначення який саме вид діяльності може бути цим дозволений. Відповідно до пункту 1 статті 15 Директиви про конфіденційність та електронні комунікації та пункту 22 її декларативної частини, допустимі лише обмежені технічні операції (технічне зберігання, яке необхідно для передачі повідомлення і протягом необхідного строку), і під час їх виконання в будь-якому випадку вимагається забезпечення конфіденційності повідомлень.

З метою обмеження втручання, необхідного для надання електронних комунікаційних послуг згідно положень пункту 1 статті 15 Директиви про конфіденційність та електронні комунікації, у цьому положенні слід додатково визначити, якими можуть бути необхідні операції, а також наголосити, що навіть у таких випадках має гарантуватися конфіденційність.

Також це положення у широкому сенсі передбачає, що втручання може бути дозволено законом без подальшого уточнення цілей, заради яких це може відбуватися, і, більш загально, умов або конкретних правил, що застосовуються в такому випадку. Проте згідно з положеннями пункту 1 статті 5 Директиви про конфіденційність та електронні комунікації, конфіденційність спілкування може порушуватися лише за умови дотримання суворих та специфічних умов, як це додатково зазначено у пункті 1 статті 15 тієї самої

Директиви. Відповідно до цього останнього положення, обмеження має становити необхідний, належний та пропорційний у демократичному суспільстві захід, спрямований на забезпечення національної безпеки (тобто державної безпеки), оборони, громадської безпеки та запобігання, виявлення, розкриття та розслідування кримінальних правопорушень або несанкціонованого використання системи електронних комунікацій. Всі ці дії мають здійснюватися відповідно до вимог національного законодавства. Слід зазначити, що це також відображає підхід й умови, передбачені Конвенцією 108+ (стаття 11) та GDPR (стаття 23), коли застосовуються обмеження щодо певних положень або прав щодо захисту персональних даних. Останні положення, на наш погляд, також слід брати до уваги, коли мова йде про втручання в таємницю приватного спілкування, оскільки воно пов'язане з персональними даними. Задля забезпечення відповідності стандартам ЄС, включаючи, більш загально, частину 2 статі 8 Конвенції про захист прав людини і основоположних свобод, якою встановлюються умови, за яких можливе втручання у приватне життя, головним чином у сфері комунікацій, національне законодавство має, зокрема, визначати цілі, для яких може здійснюватися втручання, відповідно до обмежених цілей, передбачених пунктом 1 статті 15 Директиви про конфіденційність та електронні комунікації та статті 23 GDPR (наприклад, виявлення, розкриття та розслідування кримінальних правопорушень), ким воно може здійснюватися (тобто, відповідними контролерами /компетентними органами), форма, в якій воно здійснюватиметься (включаючи будь-який попередній судовий чи адміністративний дозвіл), дані, які можуть збиратися чи бути доступні, період їх зберігання, а також гарантії (наприклад, контроль) і права окремих фізичних осіб.

Частина 4 статті 31^2 потребує доопрацювання для того, щоб більш детально визначити прийнятні межі втручання компетентними органами у таємницю приватного спілкування з урахуванням вимог Директиви про конфіденційність та електронні комунікації (пункт 1 статті 15), GDPR (стаття 23), Конвенції 108+ (стаття 11) та Конвенції про захист прав людини і основоположних свобод (частина 2 статті 8). Якщо конкретніше, то необхідно визначити цілі, для яких може здійснюватися втручання, форма його здійснення, особу, яка його здійснюватиме, до яких даних здійснюватиметься доступ, або які дані зберігатимуться і як довго, а також гарантії і права окремих фізичних осіб у цьому контексті. Принцип 2.5 Рекомендації № R(95)4 також може виконувати функцію корисного керівництва у цьому випадку.

Мета частини 5 статті 31^2 незрозуміла, однак її сенс міг бути втрачений під час перекладу. Ми певною мірою розуміємо, що ця частина передбачає зобов'язання постачальників електронних комунікаційних мереж та/або послуг повідомляти споживача або користувача під час або до укладання договору про надання послуг про той факт, що постачальник отримує інформацію про приватне спілкування, записує або зберігає її, проте незрозуміло, чому постачальник може здійснювати такі дії (крім надання послуги). До того ж, зазначається, що інформація про приватне спілкування має видалятися якомога швидше, наскільки це технічно можливо, і в тих випадках, коли інформація не є необхідною для надання послуги. Імовірно, це положення може певною мірою стосуватися обробки даних трафіку, яке додатково регулюється статтею 119^1, або обробки даних про місцезнаходження відповідно до положень статті 119^2.

Незрозуміло, який конкретний сценарій або зобов'язання має охоплюватися частиною 4 цієї статті та яка сфера її застосування, та чи можливий її зв'язок зі статтями 119^1 та 119^2, які розглядаються далі. Ми не можемо далі це прокоментувати.

Частиною 6 статті 31^2 дозволяється запис приватного спілкування та пов'язаних з ним даних під час здійснення підприємницької діяльності в цілях надання доказів здійсненої оплати та умов, за яких це може відбуватися. Це положення по суті відповідає положенням пункту 2 статті 5 Директиви про конфіденційність та електронні комунікації, але для повної відповідності потребує уточнення.

Статтю варто доповнити вказівкою про те, що записане спілкування має бути видалено якомога швидше і в будь-якому випадку не пізніше закінчення періоду, протягом якого транзакція може бути законно оскаржена відповідно до положень пункту 2 статті 5 та пункту 23 декларативної частини Директиви про конфіденційність та електронні комунікації.

У частині 7 статті 31^2 йдеться про повідомлення про запис спілкування, але незрозуміло, якого запису спілкування це стосується.

Якщо частина 7 статті 31^2 має на меті визначити зобов'язання щодо повідомлення про запис спілкування, як це передбачено частиною 6 статті 31^2, то необхідно про це прямо зазначити в цій частині, щоб забезпечити чіткий зв'язок між двома статтями. В іншому випадку зміст частини 7 статті 31^2 може потребувати подальшого уточнення сфери її застосування.

Частиною 8 статті 31^2 передбачається можливість для уповноважених осіб постачальника електронних комунікаційних мереж обробляти персональні дані споживачів або користувачів за умови, що вони беруть на себе зобов'язання про нерозголошення конфіденційної інформації, яка стала їм відома у зв'язку з їх професійною діяльністю. Точна мета цього положення незрозуміла. Дійсно, можна припустити, що співробітникам постачальника електронних комунікаційних мереж в будь-якому випадку потрібно буде обробляти певні персональні дані споживачів або користувачів, наприклад, для надання послуги або виставлення рахунків, і це не потребує окремого регулювання у законі, оскільки загальні положення Проєкту Закону в будь-якому випадку застосовуватимуться до такої обробки персональних даних, за винятком випадків, коли це положення має на меті виконання конкретного сценарію або зобов'язання. У зв'язку із цим може виникнути питання, чому існує конкретне посилання на конфіденційну інформацію споживачів і користувачів разом з вимогою про те, щоб уповноважена особа взяла на себе зобов'язання щодо нерозголошення. Імовірно, це положення може певною мірою стосуватися обробки даних трафіку, яка додатково регулюється статтею 119^1, або обробки даних про місцезнаходження відповідно до положень статті 119^2.

Пункт 8 статті 31^2 може потребувати перегляду для уточнення сфери його застосування і можливого зв'язку з положеннями статей 119^1 і 119^2, що розглядаються далі.

Стаття 31^3. Порядок надання інформації на запити про надання доступу до персональних даних споживача та/або кінцевого користувача електронних комунікаційних послуг та збереження інформації про такі запити

Ця стаття, ймовірно, регулює надання постачальниками електронних комунікаційних мереж та послуг інформації про персональні дані і приватне спілкування споживачів або користувачів за запитами компетентних органів. Однак, обсяг таких запитів та органи державної влади невизначені, і тому, її неможливо повністю оцінити, оскільки частина 1 статті 31^3 містить посилання на статтю Проєкту Закону або окреме законодавство, які не включені в представлений на розгляд текст.

В тій мірі, в який надання компетентним органам інформації про приватне спілкування споживачів або користувачів, а також персональних даних за запитом, як це зазначено в частині 2 статті 31^3, буде вважатися втручанням, наші коментарі

будуть такими самими, як і ті, що й викладені на ту саму тему щодо частини 4 статті 31^2 (див. вище). До речі, варто також визначити, як саме мають бути сформульовані положення, а саме частини 2 статті 31^3 та частини 4 статті 31^2, оскільки зрештою вони стосуються одного й того самого питання. Наприклад, частина 2 статті 31^3 може містити посилання на частину 4 статті 31^2, в якій визначаються умови, за яких може надаватися доступ до інформації про приватне спілкування або персональні дані споживачів та користувачів.

У частині 3 статті 31^3 йдеться про записи, які повинні зберігатися постачальниками електронних комунікаційних мереж та/або послуг щодо запитів, отриманих від компетентних органів, що відповідає змісту пункту 1(b) статті 15 Директиви про конфіденційність та електронні комунікації щодо цього.

Стаття 117. Каталоги номерів (телефонні довідники)

У цій статті розглядається порядок включення персональних даних споживачів і кінцевих користувачів у телефонні довідники та права споживачів і користувачів у цьому зв'язку. Це виявляється, переважно, з положень частини 1 та2 статті 117, зміст яких подібний змісту статті 12 Директиви про конфіденційність та електронні комунікації, що стосується того самого питання, і тому, зауважень тут не виникає. Положення частини 3 статті 117, якими передбачається право споживачів та кінцевих користувачів забороняти використання їх персональних даних для дзвінків з комерційною або дослідницькою метою, збігаються з принципом 7.8 Рекомендації № R(95)4 і не потребують внесення змін.

В частині 4 статті 117, зокрема, зазначається, що інформація про перевірку, виправлення або видалення персональних даних, як це зазначено у частині 2 статті 117 (за яким споживачам і користувачам надаються такі права), не повинна включатися до телефонного довідника. Однак, це положення незрозуміле і може навіть дещо суперечити частині 2 статті 117, якщо його розуміти як таке, що забороняє включення запитаних споживачами та кінцевими користувачами виправлень, видалення персональних даних. Припускаємо, що це не є метою цієї статті.

Заборона, що встановлюється частиною 4 статті 117, потребує уточнення, зокрема, задля уникнення суперечностей щодо права на захист персональних даних, яке гарантується споживачам та користувачам відповідно до частини 2 статті 117.

Стаття 119. Захист інформації про споживача, кінцевого користувача та надані електронні комунікаційні послуги

У статті наводиться обмежений перелік цілей, для яких постачальники електронних комунікаційних мереж та/або послуг можуть збирати і зберігати необхідні персональні дані споживачів або кінцевих користувачів (частина 1 статті 119). У ній також встановлюється, що одержана кінцевими користувачами інформація про електронні комунікаційні послуги, «може» надаватися в порядку, визначеному «цим Законом із дотриманням вимог Закону України «Про захист персональних даних»». Використання слова «може» означає, що надання інформації у такий спосіб є лише опцією, в той час, як будь-яка інформація про обробку персональних даних кінцевих користувачів електронних комунікаційних послуг надається відповідно до національного законодавства в сфері захисту персональних даних, в тому числі Проєкту Закону.

Рекомендується замінити слово «може» на чітке зобов'язання надавати кінцевим користувачам інформацію про обробку їхніх персональних даних відповідно до Проєкту Закону. До того ж, оскільки цілі обробки, що викладені у цій статті, тісно пов'язані з темами, що розглядаються в наступних статтях (119[1], 119[2], 119[3], 119[4], 119[5]), зокрема, стосовно обробки даних трафіку або даних про місцезнаходження кінцевих користувачів, пропонується зазначити у статті 119, що обробка повинна здійснюватися на умовах, викладених у наступних статтях.

Стаття 119[1]. Дані трафіку

У цій статті встановлюються умови обробки постачальником електронних комунікаційних мереж та/або послуг даних трафіку споживачів або кінцевих користувачів, які, зазвичай, видаляються або знеособлюються відразу після того, як в них зникає потреба для цілей надання електронних комунікаційних послуг, крім випадків, передбачених цією статтею. Стаття здебільшого відображає ті самі умови, викладені у статті 6 Директиви про конфіденційність та електронні комунікації, однак є ряд зауважень та рекомендацій до неї, що викладені нижче.

Окрім винятків, що стосуються зберігання даних трафіку, пункт 1 частини 1 статті 119[1] передбачає таку можливість на підставі закону, що згадується в широкому сенсі і без

додаткових умов. Припускаємо, що така можливість має на меті збереження певних даних трафіку з метою передачі компетентним органам, наприклад, для кримінального розслідування, судового розгляду або для забезпечення громадської безпеки. Так само, коли йдеться про втручання у таємницю приватного спілкування, доступ до даних трафіку і їх зберігання, як виняток, може здійснюватися відповідно до статті 6 Директиви про конфіденційність та електронні комунікації лише за дотримання суворих та особливих умов, зазначених у пункті 1 статті 15 цієї Директиви[11]. Тож у цьому випадку наші коментарі та рекомендації будуть однаковими. У декількох словах, як це пояснювалося вище, обмеження має становити необхідний, належний та пропорційний у демократичному суспільстві захід, спрямований на досягнення певних і обмежених цілей, повагу фундаментальних прав і свобод, та має бути передбачений національним законодавством. Це також відповідає вимогам Конвенції 108 + (стаття 11) та GDPR (стаття 23).

Статтю 119[1] необхідно доповнити, визначивши порядок доступу компетентних органів до даних трафіку з урахуванням вимог Директиви про конфіденційність та електронні комунікації, GDPR та Конвенції 108+, що викладені вище. Для забезпечення відповідності пункту 1(b) статті 15 Директиви про конфіденційність та електронні комунікації у статті необхідно передбачити вимогу до постачальників послуг встановлювати внутрішні процедури надання відповідей на запити про доступ до персональних даних користувачів та зобов'язання надавати компетентним органам за запитом інформацію про ці процедури, кількість отриманих запитів, наведене правове обґрунтування та їхню відповідь.

Інший виняток, встановлений пунктом 4 частини 1 статті 119[1] стосується зберігання даних трафіку для розрахунку оплати електронних комунікаційних послуг, що додатково регулюється частиною 3 статті 119[1].

[11] Проте зверніть увагу, що це положення Директиви про конфіденційність та електронні комунікації посилається на іншу Директиву ЄС про зберігання даних трафіку (2006/24/ЕС) від 15 березня 2006 року, у якій йдеться про зберігання даних, згенерованих або таких, що оброблялися у зв'язку з наданням постачальником електронних комунікаційних мереж та/або послуг , але яку Суд ЄС визнав у 2014 році недійсною (справа С-293/12 і С-594/12, «Цифрові права, Ірландія» (Digital Rights Ireland), 08 квітня 2014 р.), і яка більше не застосовується. У такий спосіб, чинний порядок з цього питання, якій слід враховувати, виходить із практики Суду ЄС, включно зі справою «Цифрові права, Ірландія» (Digital Rights Ireland), яка вже згадувалася, а також включно зі справою С-203/15 «Теле 2 Сверіґе / Ватсон» (Tele 2 Sverige/Watson) від 21 грудня 2016 року, справою С-511/18, «Ла Квадратюр ду Нет» (La Quadrature du Net), 06 жовтня 2020 року.

Задля уникнення невірного тлумачення умов, що застосовуються в такому випадку, пропонується зазначити у пункті 4 частини 1 статті 119[1], що таке використання здійснюватиметься на умовах, викладених у пункті 3 статті 119[1].

У пункті 5 частини 1 статті 119[1] йдеться про надання послуг маркетингу або інших додаткових електронних комунікаційних послуг, що також регулюється частиною 2 статті 119[1].

Задля уникнення невірного тлумачення умов, що застосовуються в такому випадку, пропонується зазначити у пункті 5 частини 1 статті 119[1], що таке використання здійснюватиметься на умовах, викладених у частині2 статті 119[1].

Частина 2 статті 119[1] передбачає особливі умови, яких повинні дотримуватися при використанні даних трафіку з метою надання маркетингових або додаткових послуг, за умови згоди споживача, що, по суті, відповідає вимогам, передбаченим пунктом 3 статті 6 Директиви про конфіденційність та електронні комунікації.

У цьому положенні також має бути чітко визначено, що згода в такому випадку має бути поінформованою і отримана відповідно до тих самих вимог, які викладені в Проєкті Закону, щоб гарантувати, що вона отримана у спосіб, який відповідає вимогам щодо захисту персональних даних. У статті також має бути чітко зазначено право споживачів або кінцевого користувача відкликати згоду відповідно до статті 6 Директиви про конфіденційність та електронні комунікації.

Частина 3 статті 119[1] передбачає особливі умови, яких потрібно дотримуватися при використанні даних трафіку, зокрема, для розрахунку оплати за маркетингові або додаткові послуги, що мають надаватися за згоди споживача, що по суті відповідає вимогам, передбаченим пунктом 2 статті 6 Директиви про конфіденційність та електронні комунікації.

Для подальшого обмеження такого використання відповідно до пункту 2 статті 6 Директиви про конфіденційність та електронні комунікації і для забезпечення дотримання принципів обмеження мети, мінімізації даних і обмеженого зберігання, передбачених Конвенцією 108+ (пункт 4 стаття 5) і GDPR (пункт 1(a)–(c) статті 5), статтю слід доповнити, зазначивши, що обробка для розрахунку оплати і здійснення платежу допустима лише до закінчення періоду, протягом якого рахунок можна

законно оскаржити або здійснення платежу. Оскільки в цих положеннях не йдеться про питання виставлення деталізованих рахунків, в той час, як це передбачено статтею 7 Директиви про конфіденційність та електронні комунікації, рекомендується додати порядок, що регулює це питання до частини 3 статті статті 119[1] Проєкту Закону.

Частиною 4 статті 119[1] вимагається, що обробка даних трафіку може здійснюватися лише уповноваженими особами постачальника електронних комунікаційних мереж та/або сервісів у для певних цілей. Це положення відповідає положенням пункту 5 статті 6 Директиви про конфіденційність та електронні комунікації, і не викликає зауважень.

Стаття 119[2]. Дані про місцезнаходження споживача та/або кінцевого користувача

У цій статті викладаються умови обробки даних про місцезнаходження споживачів або кінцевих користувачів постачальником електронних комунікаційних мереж та/або послуг. Ці положення здебільшого відповідають умовам статті 9 Директиви про конфіденційність та електронні комунікації з урахуванням наступних зауважень і рекомендацій, що докладно наведені нижче.

Частиною 1 статті 119[2] передбачено, що додатково та в міру необхідності під час надання «*додаткових послуг*» споживачеві або кінцевому користувачеві, дані про місцезнаходження споживача можуть оброблятися на підставі закону або в тих випадках, коли такі дані знеособлені, і споживач або кінцевий користувач дав на це згоду. Проте до цього положення виникає кілька запитань.

За винятком випадків, коли обробка здійснюється відповідно до закону (див. наші коментарі нижче), стаття може встановлювати сукупні умови для надання додаткових послуг споживачам та кінцевим користувачам, якими вимагається знеособлення персональних даних та отримання згоди цих фізичних осіб. Варто зазначити, що такі сукупні умови не вимагаються у пункті 1 статті 6 Директиви про конфіденційність та електронні комунікації, оскільки у такому випадку отримується згода фізичної особи на надання додаткової послуги, або анонімізуються дані про місцезнаходження перед їх подальшим використанням. Важко передбачити, як можуть надаватися додаткові послуги, якщо дані про місцезнаходження знеособлюються (за умови, що це означає те саме, що й «робити анонімними»).

Рекомендується переглянути формулювання цього положення згідно із пункту 1 статті 6 Директиви про конфіденційність та електронні комунікації в такий спосіб, щоб передбачити, що для надання додаткових послуг потрібна або згода на обробку даних про місцезнаходження, або дані про місцезнаходження анонімізовані.

Щодо посилання у цьому положенні на обробку даних про місцезнаходження відповідно до закону, ми припускаємо, що така обробка має на меті охопити ситуації зберігання даних про місцезнаходження з метою передачі компетентним органам, наприклад, для кримінального розслідування, судового розгляду або для забезпечення громадської безпеки. І так само, стосовно інших, розглянутих вище, винятків із дозволеної законом обробки (таємниця приватних повідомлень, зберігання даних трафіку), цей виняток може застосовуватися лише для певних цілей і має бути додатково передбачений законом відповідно до пункту 1 статті 15 цієї Директиви. Тож наші зауваження та рекомендації збігаються з викладеними вище щодо таємниці приватних повідомлень і збереження даних трафіку.

Цю статтю необхідно доповнити, щоб більш конкретно деталізувати порядок доступу компетентних органів до даних про місцезнаходження з урахуванням вимог Директиви про конфіденційність та електронні комунікації, GDPR і Конвенції 108+, що викладені вище. Якщо конкретніше, то необхідно зазначити мету, форму, виконавця і період збору, надання і зберігання таких даних, а також гарантії і права окремих фізичних осіб у цьому контексті. До того ж, для забезпечення відповідності пункту 1(b) статті 15 Директиви про конфіденційність та електронні комунікації у статті необхідно передбачити вимогу до постачальників послуг встановлювати внутрішні процедури реагування на запити про доступ до персональних даних користувачів та зобов'язання за запитом компетентних органів надавати інформацію про ці процедури, кількість отриманих запитів, наведене правове обґрунтування та їхню відповідь.

Частиною 2 статті 119^2 встановлюються вимоги до інформаційного повідомлення споживача або кінцевого користувача щодо отримання його згоди (як зазначено в частині 1 статті 119^2) на обробку його персональних даних. У такий спосіб, цим положенням встановлюється вимога, яка дуже схожа до викладеної у пункті 1 статті 9 Директиви про конфіденційність та електронні комунікації. Проте незрозуміло, чому у положенні йдеться про згоду на обробку «персональних даних», а у частині 1 статті 119^2

йдеться про згоду на обробку «даних про місцезнаходження». І так само, елементи інформаційного повідомлення, яке має надаватися, стосуються не даних про місцезнаходження, а персональних даних, натомість стаття 119^2 відповідно до статті 6 Директиви про конфіденційність та електронні комунікації зосереджена на даних про місцезнаходження.

Необхідно переглянути і доповнити формулювання частини 2 статті 119^2, замінивши вираз «персональні дані» на «дані про місцезнаходження», в тому числі коли йдеться про можливість відкликання згоди і тип даних, що обробляються. Також пропонується встановити зв'язок з частиною 1 статті 119^2, оскільки у частині 2 статті 119^2 додатково визначається вимога, викладена у частині 1 статті 119^2. Ця стаття також має вказувати, що згода в такому випадку має бути поінформованою та отримана відповідно до тих самих вимог, які викладені в Проєкті Закону, що гарантуватиме її отримання у спосіб, який відповідає вимогам щодо захисту персональних даних.

У частині 3 статті 119^2 йдеться про право споживачів та кінцевих користувачів відкликати згоду на обробку персональних даних щодо кожного з'єднання з мережею або кожного випадку передачі даних. Ця частина відповідає вимозі, викладеній у пункті 2 статті 9 Директиви про конфіденційність та електронні комунікації, і не викликає зауважень.

У частині 4 статті 119^2 передбачено, що обробка даних про місцезнаходження за цією статтею може здійснюватися особами, уповноваженими постачальником електронних комунікаційних мереж та/або послуг, для певних викладених у статті цілей. Стаття сформульована у тому ж ключі, що й пункт 3 статті 9 Директиви про конфіденційність та електронні комунікації, проте з використанням терміну «може» нею встановлюється більше можливостей для обробки уповноваженими особами, ніж це передбачено Директивою про конфіденційність та електронні комунікації, у якій йдеться про «обмежене» коло осіб. До того ж, цілі, для яких дозволена обробка даних про місцезнаходження відповідно до цієї статті (виставлення рахунків, управління трафіком, відповіді на запити споживачів та/або кінцевих користувачів, встановлення випадків шахрайства, надання маркетингових послуг або інших додаткових послуг), не відповідають меті, викладеній у пункті 3 статті 9 Директиви про конфіденційність та електронні комунікації (надання послуг з доданою вартістю).

У статті має чіткіше визначатися, що обробка даних про місцезнаходження дозволена лише уповноваженим особам для виключних цілей. Також для забезпечення відповідності із пунктом 3 статті 9 Директиви про конфіденційність та електронні комунікації необхідно змінити цілі, для яких дані про місцезнаходження можуть оброблятися і в цьому контексті зазначити лише додаткові послуги або послуги з доданою вартістю, як зазначено в пункті 3 статті 9 Директиви про конфіденційність та електронні комунікації.

Стаття 119^3. Надання даних про місцезнаходження споживача та/або кінцевого користувача

У частині 1 статті 119^3 розглядаються ситуації, коли у постачальників електронних комунікаційних мереж та/або послуг може виникнути необхідність повідомити про місцезнаходження кінцевого користувача уповноваженим органам або іншим особам для захисту життєво важливих інтересів зацікавлених осіб, як зазначено в цьому положенні, відповідно до визначеного Законом України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112». Відповідно до неофіційного перекладу назви вказаного вище закону, ми припускаємо, що під уповноваженими органами слід розуміти всі служби екстреної допомоги (включаючи, наприклад, органи поліції, службу швидкої медичної допомоги, службу цивільного захисту населення, аварійну газову та пожежну служби, а також службу спасіння). Можливість зазначати місцезнаходження фізичних осіб за обставин, наведених у цій статті, також передбачена пунктом (b) статті 10 Директиви про конфіденційність та електронні комунікації та частина 1 статті 119^3 їй відповідає.

Частиною 2 статті 119^3 встановлюється зобов'язання постачальників електронних комунікаційних мереж та/або послуг швидко реагувати на «обґрунтовані запити», але не уточнюючи, від кого ці запити можуть надходити і якою, зокрема, має бути їх форма, щоб вважатися обґрунтованими. До того ж, те саме положення передбачає, що постачальник електронних комунікаційних мереж та/або послуг несе відповідальність за дотримання «закону» (без зазначення того, про який закон у цьому випадку йде мова) під час надання даних.

Необхідно уточнити положення, що стосується обґрунтованих запитів, про які йде мова, щоб зазначити, від кого вони можуть надходити, а також за яких умов вони вважаються обґрунтованими. Також необхідно переглянути останнє речення цієї

статті, оскільки зобов'язання, яке воно має на меті встановити, не є визначеним.

Стаття 119[4]. Відстеження зловмисних або небажаних викликів абоненту

Ця стаття регулює умови відстеження зловмисних або небажаних викликів, що даватиме змогу абоненту, який може отримувати такі виклики, встановити особу автора цих викликів. Слід зазначити, що як виняток із виключення представлення ідентифікації лінії абонента, який здійснює виклик, пунктом (a) статті 10 Директиви про конфіденційність та електронні комунікації передбачається загальне зобов'язання постачальників електронних комунікаційних послуг щодо впровадження прозорих процедур, що стосуються запитів абонентів на відстеження зловмисних або небажаних викликів, а також зберігання та надання даних, що містять ідентифікацію лінії абонента, який здійснює виклик. У ньому не уточнюється, як має функціонувати зазначена процедура та інші пов'язані з нею умови, оскільки ці аспекти визначаються національним законодавством. Тож формально стаття 119[4], вочевидь, досягає цієї мети і відповідає пункту (a) статті 10 Директиви про конфіденційність та електронні комунікації.

Проте, хотілося б звернути увагу на зміст статті, оскільки вона може викликати деякі питання щодо приватності абонента, який має бути ідентифікований після запиту, отриманого відповідно до цих положень. Якщо конкретніше, то оскільки ця стаття встановлює як умову лише те, що ініціатор запиту має довести необхідність встановлення особи абонента для захисту своїх прав у судах без додаткових умов або критеріїв того, що вважається прийнятним доказом, який має бути представлений у такому випадку (наприклад, велика кількість отриманих викликів, шкідливий зміст повідомлень та будь-який інший елемент, що підтверджує фактичний законний інтерес до отримання ідентифікації), ризик полягатиме в тому, що кожен, хто вдає з себе жертву зловмисних викликів, базуючись лише на двох або трьох викликах, і стверджує, що це необхідно для цілей судового розгляду, може легко отримати ідентифікаційні дані іншого абонента у незаконний спосіб.

Тому настійно рекомендується встановити додаткові умови для більш суворого визначення ініціаторів зловмисних викликів, щоб запобігти неправомірному використанню такої процедури і неналежному порушенню приватності абонентів.

Додатково звертаємо увагу на те, що це положення опосередковано посилається на ідентифікацію або обмеження телефонної лінії абонента, але не конкретизує порядок, який буде застосований щодо цього. У Директиві про конфіденційність та електронні комунікації безпосередньо розглядається це питання і встановлюються умови його реалізації відповідно до положень статті 8.

Рекомендується додати окреме положення, що регулює представлення та обмеження ідентифікації абонента та під'єднаної лінії відповідно до статті 8 Директиви про конфіденційність та електронні комунікації.

Стаття 119^5 Небажані виклики та повідомлення абоненту

Ця стаття регулює умови відстеження небажаних викликів і повідомлень, яке даватиме змогу абоненту, який може отримувати такі виклики або повідомлення, встановити особу їх автора. Як і у випадку з зловмисними викликами, що розглядалися вище, Директивою про конфіденційність та електронні комунікації передбачається таке зобов'язання постачальників електронних комунікаційних послуг впроваджувати прозорі процедури, що стосуються запитів абонентів на відстеження зловмисних або небажаних викликів, а також зберігання та надання даних, що містять ідентифікацію лінії абонента, який здійснює виклик. У ньому не уточнюється, як має функціонувати зазначена процедура та інші пов'язані з нею умови, оскільки ці аспекти визначаються національним законодавством. Тож формально стаття 119^5 досягає цієї мети і відповідає пункту (a) статті 10 Директиви про конфіденційність та електронні комунікації.

Проте, хотілося б звернути увагу на зміст статті, який подібно до зловмисних викликів, також може викликати деякі запитання щодо приватності абонента, який буде ідентифікований після отриманого відповідно до цих положень запиту. Більш конкретно якщо стаття вимагає від ініціатора запиту зобов'язатися використовувати дані про особу абонента лише для захисту своїх прав у судах без додаткових умов або критеріїв того, що вважається прийнятним доказом, який має бути представлений у такому випадку абонентом, який звертається із запитом (наприклад, велика кількість отриманих викликів, зміст повідомлень, що свідчить про їх неприємний характер, та будь-який інший елемент, що підтверджує фактичний законний інтерес до отримання ідентифікації), стаття може використовуватись в неправомірний спосіб. Насправді, ризик полягатиме в тому, що

кожен, хто вдає з себе жертву зловмисних дзвінків на підставі, навіть, двох або трьох викликів, і стверджує, що це необхідно для цілей судового розгляду, може легко отримати ідентифікаційні дані іншого абонента у незаконний спосіб.

Настійно рекомендується встановити додаткові умови для визначення більш суворої процедури ідентифікації авторів зловмисних викликів або повідомлень, щоб запобігти неправомірному використанню такої процедури і неналежному порушенню приватності абонентів.

Як заключне зауваження до положень, що стосуються електронних комунікаційних мереж, зазначимо, що вони не стосуються проблеми автоматичної переадресації дзвінків, як це передбачено статтею 11 Директиви про конфіденційність та електронні комунікації. Згідно з цим положенням, абоненти повинні мати можливість просто і безплатно припинити автоматичну переадресацію виклику третьою стороною на пристрій абонента.

Розробники Проєкту Закону мають розглянути можливість включення положення, подібного до положення статті 11 Директиви про конфіденційність та електронні комунікації.

4. ВИСНОВКИ

Проєкт Закону містить розширену версію положень, що встановлюють всеосяжну правову базу для захисту даних. Порівняно з попередньою редакцією, він розглядає додаткові та ключові питання, такі як режим відповідальності за порушення вимог Проєкту Закону, та розглядає конкретні дії щодо обробки даних, у тому числі щодо обробки даних для правоохоронних цілей і, у певних секторах, зокрема, електронні комунікаційні мережі.

Загальний передбачений Проєктом Закону підхід досить близький до того, який виходить з європейських стандартів. У зв’язку з цим можна відзначити, що деякі положення відповідають Конвенції 108 + та GDPR, а також іншим відповідним стандартам, і не потребують поправок. Деякі положення рекомендується переглянути, уточнити або внести до них правки, щоб гарантувати їх відповідність європейським стандартам і, зокрема, Конвенції 108+ і GDPR.

Особливої уваги заслуговують такі моменти:

- Положення, що регулюють обробку персональних даних, як частини електронних комунікацій, передбачають рамки, що гарантують конфіденційність повідомлень, які включають можливість дозволеного законом втручання. Умови, що застосовуються до таких втручань, які додатково не визначені в Проєкті Закону, слід більш конкретно врегулювати або в Проєкті Закону, або в іншому законодавчому акті, беручи до уваги вимоги європейських стандартів щодо цього питання. Те саме стосується доступу компетентних органів до даних про місцезнаходження фізичних осіб, який у Проєкті Закону розглядається лише в загальних рисах.

- У межах статей, що стосуються обробки персональних даних постачальниками електронних комунікаційних мереж та/або послуг, Проєкт Закону включає положення, що регулюють умови обробки даних трафіку користувачів таких послуг. У ньому в загальних рисах розглядається можливість доступу компетентних органів до таких даних, але не регламентуються умови, за яких може відбуватися таке зберігання. Питання збереження даних трафіку має регулюватися конкретною правовою базою та належними гарантіями згідно з відповідними правовими актами України, якщо це становить втручання в захист даних і права суб'єктів персональних даних. Тут повинні враховуватися європейські стандарти у цій сфері, включно з Конвенцією 108+, а з боку ЄС — відповідна практика Суду ЄС з цього питання.

- У межах процесу доопрацювання та прийняття Проєкту Закону настійно рекомендується розглянути цей Проєкт Закону разом із Проєктом Закону, що регулює діяльність контролюючого органу, оскільки ці два акти дуже тісно пов'язані і не можуть реалізовуватися один без іншого відповідно до Конвенції 108+ та GDPR. Існування та функціонування контролюючого органу є ключовим компонентом ефективної системи захисту даних.

Зрештою, хотілося б відзначити, що обробка персональних даних може також регулюватися іншими законами, що регулюють конкретні питання (вибори, політичні кампанії, працевлаштування, електронні комунікації тощо) додатково до загального закону про захист персональних даних. У такий спосіб, систематичні зміни, що стосуються законодавчого процесу, могли б значно сприяти підвищенню якості правових

актів, що регулюють обробку персональних даних у різних галузях, і водночас вищому рівню захисту персональних даних в Україні, уникаючи потенційних протиріч принципів права. Щодо законності обробки, то підстава для обробки, про яку йдеться у пункті (c) (дотримання юридичних зобов'язань) та пункті (e) (виконання завдання в суспільних інтересах) статті 6 (1) GDPR, має бути встановлена законом. Зазначений закон має визначати мету обробки, а також може містити конкретні положення для адаптації застосування правил GDPR (типи даних, що обробляються; відповідні суб'єкти персональних даних тощо). Тому радимо зобов'язати державні установи, які беруть участь в законодавчому процесі, включати в законодавчі акти, що регулюють обробку персональних даних, мету обробки, про яку йде мова, і, залежно від обставин, іншу відповідну інформацію. Це зобов'язання може бути закріплене в Проєкту Закону або в інших правових актах України, що регулюють законодавчий процес.
