



Ministry  
of Digital Transformation  
of Ukraine



**USAID**  
ВІД АМЕРИКАНСЬКОГО НАРОДУ

# "Аналіз законодавства про захист персональних даних України" Додатки до Звіту

підготовлений АО "Саєнко Харенко"  
14 вересня 2020 року



Підготовка цього Попереднього Звіту стала можливою завдяки підтримці американського народу, наданої через Агентство США з міжнародного розвитку (USAID) в рамках Програми "Конкурентоспроможна економіка України" (через Субконтракт №: №: CEP-2020-064 для реалізації грантової діяльності "Аналіз законодавства про захист персональних даних України"). Думки авторів не обов'язково відображають погляди Агентства США з міжнародного розвитку або уряду Сполучених Штатів Америки.

## I. ДОДАТКИ

### ДОДАТОК I. ПЕРЕЛІК РІШЕНЬ ЄС ЩОДО АДЕКВАТНОСТІ

No.	Країна	Дата	Застереження/виключення
1.	Швейцарія <sup>1</sup>	26.07.2000	Жодних застережень
2.	Канада <sup>2</sup>	20.12.2001	Застосовується тільки до приватних організацій, які займаються обробкою персональних даних в процесі комерційної діяльності
3.	Аргентина <sup>3</sup>	30.06.2003	Жодних застережень
4.	Бейлівік Гернси <sup>4</sup>	12.11.2003	Жодних застережень
5.	Острів Мен <sup>5</sup>	28.04.2004	Жодних застережень
6.	Бейлівік Джерсі <sup>6</sup>	08.05.2008	Жодних застережень
7.	Фарерські острови <sup>7</sup>	05.03.2010	Не поширюється на діяльність з обробки персональних даних, що здійснюється органами влади Королівства Данії
8.	Андора <sup>8</sup>	19.10.2010	Жодних застережень
9.	Ізраїль <sup>9</sup>	31.01.2011	Не застосовується для неавтоматизованої обробки персональних даних
10.	Уругвай <sup>10</sup>	21.08.2012	Жодних застережень
11.	Нова Зеландія <sup>11</sup>	19.12.2012	Жодних застережень
12.	Програма по захисту конфіденційності США (Privacy Shield) <sup>12</sup>	12.07.2016	Застосовується лише для компаній в США, які включені до Списку Privacy Shield <sup>13</sup> (рішення <b>визнане недійсним</b> )
13.	Японія <sup>14</sup>	23.01.2019	Застосовується лише для передачі даних з ЄС до операторів, що займаються обробкою персональної інформації в Японії <sup>15</sup>

<sup>1</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 26 липня 2000 про адекватний захист персональних даних, наданий в Швейцарії.](#)

<sup>2</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 20 грудня 2001 о про адекватний захист персональних даних, наданий Канадським Актом про захист персональних даних і електронні документи.](#)

<sup>3</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 30 червня 2003 про адекватний захист персональних даних в Аргентині.](#)

<sup>4</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 21 листопада 2003 про адекватний захист персональних даних в Гернси.](#)

<sup>5</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 28 квітня 2004 про адекватний захист персональних даних на Острові Мен.](#)

<sup>6</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 8 травня 2008 про адекватний захист персональних даних в Джерсі.](#)

<sup>7</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 5 березня 2010 про адекватний захист персональних даних забезпечений Фарерським Актом про обробку персональних даних.](#)

<sup>8</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 19 жовтня 2010 про адекватний захист персональних даних в Андоррі.](#)

<sup>9</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 31 січня 2011 року про адекватний захист персональних даних в Ізраїлі щодо автоматизованої обробки персональних даних.](#)

<sup>10</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС від 21 серпня 2012 про адекватний захист персональних даних в Східній Республіці Уругвай щодо автоматизованої обробки персональних даних.](#)

<sup>11</sup> [19 грудня 2012 про адекватний захист персональних даних в Новій Зеландії.](#)

<sup>12</sup> [Рішення Європейської Комісії Рішення Європейської Комісії ЄС \(EU\) 2016/1250 від 12 липня 2016 о про адекватний захист персональних даних наданий ЄС-США Рішення про захист Конфіденційності.](#)

<sup>13</sup> [Рішення Суду Європейського Союзу у справі C-311/18 - Уповноважений із захисту даних проти Facebook Ірландія і Максиміліан Шремс визнав у пункті 201 Рішення про захисту конфіденційності недійсним. В даний час EDBP оцінює адекватність захисту передачі даних до США. Відповідно до EDBP і його членів, передача даних в США є "можливою лише після оцінки адекватності до передачі даних відповідно до механізму SCC", "не рекомендується", "під питанням", "можливий на додаткових законних підставах передбачених статтею 46 GDPR", "якомога швидше підтверджено іншою правовою основою \(наприклад, SCCs, BCRs, і виключення\), в іншому випадку особисті дані не можуть бути передані в США".](#)

<sup>14</sup> [Рішення Європейської комісії \(EU\) 2019/419 від 23 січня 2019 про адекватний захист персональних даних в Японії на основі Акту про Захист Персональних Даних \(далі – "Японське рішення"\).](#)

<sup>15</sup> Ст. 1(2) Японського рішення не охоплює передачу даних одержувачам, що належать до однієї з наступних категорій, в тій межі що всі або частина цілей обробки персональних даних відповідає одній із перелічених цілей:

- установи радіомовлення, видавці газет, комунікаційні агенції чи інші організації ЗМІ (включаючи будь-яких осіб, які здійснюють діяльність у сфері преси як свою діяльність), якщо вони обробляють персональні дані для цілей преси;
- особи, які професійній діяльності займаються письмом, якщо це включає персональні дані;
- університети та будь-які інші організації або групи, спрямовані на академічні дослідження, або будь-яка особа, що належить до такої організації чи групи, якщо вони обробляють персональні дані з метою академічних досліджень;
- релігійні органи, якщо вони обробляють особисті дані для цілей релігійної діяльності (включаючи всі пов'язані з цим діяльності); і
- політичні органи, якщо вони обробляють особисті дані для цілей своєї політичної діяльності (включаючи всю пов'язану з цим діяльність).

## ДОДАТОК II. ПРАВА СУБ'ЄКТІВ ДАНИХ

Юрисдикція	Закон	Стаття
Європейський Союз	Загальний регламент захисту даних (EU) 2016/679	Розділ 3 GDPR визначає перелік прав суб'єктів даних, а саме: <ul style="list-style-type: none"> <li>– право бути проінформованим (ст. 12-14)</li> <li>– право на доступ (ст. 15)</li> <li>– право на виправлення (ст. 16)</li> <li>– право на видалення ("право бути забути") (ст. 17)</li> <li>– право обмежувати обробку (ст. 18)</li> <li>– право на переносимість даних (ст. 20)</li> <li>– право заперечувати (ст. 21)</li> <li>– права щодо автоматизованого прийняття рішень та профілювання (ст. 22).</li> </ul>
Німеччина	Німецький Федеральний закон про захист даних від 30 червня 2017 року	Розділ 2 і 3 закону описують права суб'єктів даних, а саме: <ul style="list-style-type: none"> <li>– Стаття 32. Інформація, яка надається, якщо особисті були отримані від суб'єкта даних;</li> <li>– Стаття 33. Інформація, яка надається, якщо особисті дані не були отримані від суб'єкта даних;</li> <li>– Стаття 34. Право суб'єкта даних на доступ;</li> <li>– Стаття 35. Право стирання;</li> <li>– Стаття 36. Право заперечувати;</li> <li>– Стаття 37. Автоматизоване індивідуальне прийняття рішень, включаючи профілювання;</li> <li>– Стаття 57. Право на доступ;</li> <li>– Стаття. Право на уточнення і стирання і обмеження обробки;</li> <li>– Стаття 60. Право подавати скаргу до Федерального уповноваженого; та</li> <li>– Стаття 61. Засоби правового захисту проти рішень Федерального уповноваженого, або якщо він чи вона не вживають заходів</li> </ul>
Велика Британія	Закон про Захист Даних 2018	Розділ 3 частина 3 DPA 2018 встановлює права фізичних осіб на свої дані. Деякі права суб'єкта даних недоступні у частині 3, такі як право на переносимість даних та право на заперечення. <ul style="list-style-type: none"> <li>– право отримувати інформацію про збір та використання персональних даних.</li> <li>– права доступу суб'єктом даних до інформації про обробку даних.</li> <li>– право на виправлення недостовірних або неповних даних, коли обробка даних порушує принципи захисту даних. Будь яке виправлення недостовірних персональних даних що стосуються особи повинні бути здійснені без затримки і протягом місяця від отримання такого запиту.</li> <li>– право на видалення персональних даних та обмеження їх обробки, якщо немає вагомих причин для їх подальшої обробки.</li> <li>– права щодо автоматизованого прийняття рішень.</li> </ul> <p>Пар. 4 Частини 1 Додатку 2 до DPA 2018 містить нові виключення щодо прав суб'єктів даних з метою підтримання ефективного імміграційного контролю або розслідування чи</p>

		виявлення діяльності, яка могла його підірвала.
Каліфорнія, США	Закон про Конфіденційність Споживачів у Каліфорнії від 2018	Права суб'єктів даних за CCPA не перераховані в одній окремій статті та не структуровані, так як у GDPR. Вони розділені на наступні категорії і впливають із контексту: (1) право на повідомлення <sup>16</sup> ; (2) право на розкриття та доступ <sup>17</sup> ; (3) право opt out/opt in щодо продажу персональних даних <sup>18</sup> ; (4) право вимагати видалення/стирання (право бути забутим) <sup>19</sup> ; і (5) право на однакові сервіси і ціну <sup>20</sup> .
Ізраїль	Закон про захист конфіденційності, 5741-1981 (PPL)	PPL не містить однієї статі, яка містить перелік всіх прав суб'єктів даних. Однак, наступні права впливають із контексту: <ul style="list-style-type: none"> <li>– право на доступ до даних/копій даних (в PPL Стаття 13(a) Право досліджувати інформацію). (a) Кожна особа наділена правом досліджувати самостійно, або через уповноважену ним у письмовій формі на це особу, або його опікуна будь-яку інформацію, яка зберігається про нього в базі даних</li> <li>– право виправляти помилки (Стаття 14(a)). Людина, яка в процесі дослідження інформації про нього є неправильною, не повною, не чіткою, чи застарілою може вимагати від власника бази даних, або якщо такий власник не резидент, то від співвласника, змінити або видалити інформацію</li> <li>– право на видалення даних, обмежене прямим маркетингом (Стаття 17F(b) PPL). Кожна особа має право вимагати, у письмовій формі, від власника бази даних, що використовується для прямої розсилки, про видалення інформації про нього з бази даних.</li> </ul>
Туреччина	Турецький закон про Захист Даних № 6698	<b>Права Суб'єктів Даних</b> Стаття 11 – (1) кожна особа має право звернутися до контролера даних для того щоб: <ol style="list-style-type: none"> <li>a) дізнатись про обробку його/її персональні дані,</li> <li>b) вимагати інформацію про те чи обробляться його/її персональні дані,</li> <li>c) знати мету обробки його/її персональних даних і чи дані використовуються у відповідності з метою,</li> <li>ç) знати про третіх сторін, яким передаються його персональні дані в межах країни чи закордон,</li> <li>d) вимагати виправлення неповних чи неправильних даних, якщо такі є,</li> <li>e) вимагати стирання чи видалення його/її персональних даних відповідно до умов передбачених статтею 7,</li> <li>f) вимагати звітування про операції, що здійснюються відповідно до підпунктів (d) і (e) третім сторонам, яким його/її персональні дані будуть передаватись,</li> <li>g) заперечувати проти рішення, що базується виключно автоматизованій обробці,</li> <li>h) вимагати компенсацію за шкоду, що виникає у зв'язку з незаконною обробкою його/її даних.</li> </ol>

<sup>16</sup> CCPA §§ 1798.100(a)- (b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130, і 1798.135.

<sup>17</sup> CCPA §§ 1798.100(d), 1798.110, 1798.115.

<sup>18</sup> CCPA §§ 1798.105, 1798.115(d), 1798.120 і 1798.135(a)-(b).

<sup>19</sup> CCPA §§ 1798.105, 1798.115(d), 1798.120(a), (d), 1798.135.

<sup>20</sup> CCPA § 1798.125.

**ДОДАТОК III. ВИМОГИ ЩОДО ОБРОБКИ ЧУТЛИВИХ ДАНИХ ПЕРЕДБАЧЕНІ НАЦІОНАЛЬНИМ ЗАКОНОДАВСТВОМ**

<b>Конкретні вимоги, пов'язані з обробкою чутливих даних, визначені в національному законодавстві</b>					
<b>Вимоги / особливості</b>	<b>Німеччина</b>	<b>Ізраїль</b>	<b>Каліфорнія (ССРА)</b>	<b>Велика Британія</b>	<b>Туреччина</b>
<b>Концепція чутливих даних</b>	Представлена відповідно до GDPR	Представлена	Не представлена згідно ССРА. Врегульована правилами та в межах HIPAA <sup>21</sup> .	Представлена відповідно до GDPR	Представлена
<b>Спеціальне регулювання щодо медичних, біометричних та генетичних даних</b>	Врегульовано ст. 22 BDSG <sup>22</sup> та GDPR.	Представлено <sup>23</sup>	Представлено <sup>24</sup>	Врегульовано ст. 10 DPA <sup>25</sup> та GDPR.	Представлено <sup>26</sup>
<b>Призначення DPO</b>	Обов'язкове відповідно до GDPR	Вимагається відповідно до PDS (ст.17 (b)) <sup>27</sup>	Не вимагається	Обов'язкове відповідно до GDPR	Вимагається реєстрація контролера відповідно до TDPL (ст. 16(2)) <sup>3</sup>
<b>Ведення реєстру чутливих даних</b>	Не встановлюється	Вимагається	Вимагається	Не встановлюється	Вимагається
<b>Повідомлення про порушення щодо персональних даних</b>	Вимагається незалежно від типу даних ст.22 BDSG.	Вимагається у випадку тяжких порушень (PDS 11(b)(1))	Вимагається	Вимагається згідно ст. 67 DPA.	Вимагається незалежно від типу даних <sup>28</sup>

<sup>21</sup> [HIPAA - Закон про Портативність та Підзвітність Медичного Страхування](#) від 1996 року, який регулює конфіденційність даних та безпеку у відносинах медичного страхування.

<sup>22</sup> [Федеральний Закон про Захист Даних \(BDSG\)](#) ст.22.

<sup>23</sup> ["Положення про Захист Конфіденційності \(Безпека даних\) - 2017.pdf"](#) (не офіційний переклад). Положення про Захист Конфіденційності визначає чотири категорії баз даних, які різняться в залежності від чутливості даних, способів використання даних, кількості осіб, які мають доступ до бази даних, та кількості суб'єктів даних.

<sup>24</sup> [HIPAA - Закон про Портативність та Підзвітність Медичного Страхування](#) від 1996 року, який регулює конфіденційність даних та безпеку у відносинах медичного страхування.

<sup>25</sup> [Закон про Захист Даних Великобританії від 2018 року.](#)

<sup>26</sup> Положення про Обробку та Захист Конфіденційності Особистих Даних про Здоров'я від 20 жовтня 2016 року.

<sup>27</sup> ["Положення про Захист Конфіденційності \(Безпека даних\) – 2017.pdf"](#) (не офіційний переклад). Положення про Захист Конфіденційності встановлює чотири категорії баз даних, які різняться в залежності від чутливості даних, способів використання даних, кількості осіб, які мають доступ до бази даних, та кількості суб'єктів даних.

<sup>28</sup> [Рішення Ради від 24.01.2019 № 2019/10 про Процедури та Принципи Повідомлення про Порушення Персональних Даних.](#)

<p><b>Правова основа для обробки біометричних даних державними органами</b></p>	<p>Відповідно до Розділу 22 BDSG для державних органів:</p> <ul style="list-style-type: none"> <li>– у зв'язку із виконання обов'язків із соціальної безпеки та захисту;</li> <li>– питання, пов'язані зі здоров'ям;</li> <li>– публічний інтерес у сфері охорони здоров'я;</li> <li>– відповідно до невідкладного публічного інтересу;</li> <li>– для запобігання загрозам публічній безпеці та шкоді гарантіям загального благополуччя;</li> <li>– у зв'язку із невідкладними причинами, пов'язаними з безпекою або кризовим менеджментом.</li> </ul> <p>Додаткові правові підстави для державних органів наведені в Розділах 23, 25, 27, 28.</p> <p>Підхід BDSG у питаннях обробки біометричних</p>	<p>Підхід PPL до правової основи обробки даних базується в основному на концепції згоди з повідомленням за винятком декількох виключень:</p> <ul style="list-style-type: none"> <li>– потреби юстиції та національної безпеки;</li> <li>– ведення бази біометричних даних національних ідентифікуючих документів Національним органом з біометричних баз даних.</li> </ul> <p>Слабкий підхід ізраїльського законодавства до обробки чутливих персональних даних наразі переглядається законотворцем і національним ДРА з метою внесення змін до законодавства для приведення його у відповідність до GDPR<sup>29</sup>.</p>	<p>ССРА не розглядає детально правові підстави обробки даних. Він регулює питання комерційного використання персональних даних.</p> <p>За загальним правилом, отримання згоди на обробку даних не вимагається.</p> <p>Споживачам надане право "opt-out" щодо продажу їх даних (однак немає можливості видалити дані), але лише у випадках, коли ці дані є предметом фінансового стимулу (наприклад, для продажу).</p>	<p>Охоплюється Статтями 6 і 9 GDPR.</p>	<p>TDPL забороняє обробку даних спеціального характеру (біометричних даних) відповідно до Статті 6(2) без надання однозначної згоди.</p> <p>У той же час такі дані можуть оброблятися без згоди у таких випадках:</p> <ul style="list-style-type: none"> <li>– якщо це передбачено законом;</li> <li>– для цілей охорони здоров'я.</li> </ul>
---	--	---	---	---	---

<sup>29</sup> "У пошуках адекватності: Ізраїль та США намагаються адаптуватися стандартів захисту даних ЄС", травень 2020 року.

	даних відображає підхід, викладений у Статтях 6 і 9 GDPR.				
--	--	--	--	--	--