Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Бакалаврська кваліфікаційна робота на тему

«Засіб для формування політики захисту даних вебсайту відповідно до GDPR»

Виконала: студентка 4 курсу групи 1БС-21б
спеціальності 125 Кібербезпека
_____ Дарина МАЛЬЦЕВА
Керівник: к. т. н., доц., доцент каф. ЗІ
_____ Олеся ВОЙТОВИЧ
«16» червня 2025 р.
Рецензент: к. т. н., доц., доцент каф. ПЗ
_____ Володимир МАЙДАНЮК
«16» червня 2025 р

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«16» червня 2025 р.

Вінниця ВНТУ – 2025 року

Міністерство освіти і науки України
Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти І (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітня програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«24» березня 2025 року

ЗАВДАННЯ

НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Дарині МАЛЬЦЕВІЙ

1. Тема роботи: «Засіб для формування політики захисту даних вебсайту відповідно до GDPR»
керівник роботи: Олеся ВОЙТОВИЧ, к.т.н., доцент кафедри ЗІ,
затверджені наказом ректора ВНТУ від 20 березня 2025 року №97.

2. Строк подання студентом роботи 16 червня 2025 року

3. Вихідні дані роботи:
- засіб для формування політики захисту даних вебсайту
- аналіз вебсайтів, для яких генерується політика
- програмна реалізація веб-застосунку

4. Зміст текстової частини: Вступ. Аналіз предметної області. Розробка засобу для формування політики GDPR. Реалізація засобу для політики GDPR. Висновки. Список використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Основні принципи обробки персональних даних GDPR. Недоліки генераторів шаблонів політики GDPR. Алгоритм роботи засобу для генерування основних положень GDPR. Визначення рівня критичності захисту персональних даних. Визначення рівня критичності передачі особистих даних третім сторонам. Визначення необхідності генерації положення про захист фінансових даних користувачів. Структура застосунку. Алгоритм генерації основних положень GDPR.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	О. ВОЙТОВИЧ, к.т.н., доц. каф.ЗІ	24.03.25	10.06.25
2	О. ВОЙТОВИЧ, к.т.н., доц. каф.ЗІ	14.05.25	10.06.25
3	О. ВОЙТОВИЧ, к.т.н., доц. каф.ЗІ	30.05.25	10.06.25

7. Дата видачі завдання 24 березня 2025 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Аналіз завдання. Вступ	24.03.25 – 30.03.25	
2	Аналіз інформаційних джерел за напрямком бакалаврської кваліфікаційної роботи	31.03.25 – 13.04.25	
3	Розробка рішень, моделей, алгоритмів	14.04.25 – 04.05.25	
4	Практична реалізація, моделювання, експериментування, результати	05.05.25 – 14.05.25	
5	Аналіз виконання БКР, висновки	15.05.25 – 18.05.25	
6	Оформлення пояснювальної записки	19.05.25 – 26.05.25	
7	Попередній захист БКР	27.05.25 – 30.05.25	
8	Виправлення зауважень, перевірка на наявність текстових запозичень, підготовка ілюстративного матеріалу	31.05.25 – 10.06.25	
9	Представлення БКР до захисту, рецензування	11.06.25 – 13.06.25	

Студент _____ Дарина МАЛЬЦЕВ

Керівник роботи _____ Олеся ВОЙТОВИ

АНОТАЦІЯ

Бакалаврська кваліфікаційна робота складається з 63 сторінок формату А4, на яких є 8 рисунків, 3 таблиці, список використаних джерел містить 27 найменування.

Бакалаврська кваліфікаційна робота присвячена розробці програмного засобу для формування політики захисту даних сайту відповідно до GDPR. Під час аналізу особливостей регламенту GDPR було відокремлено його важливість в сучасному світі. Також досліджено основні положення регламенту, особливості його використання для різних цілей бізнесу, особливості контролю та покарання за недотримання GDPR.

Розроблено засіб для генерування основних положень регламенту GDPR для вебсайтів підприємств з різним профілем. Засіб являє собою окремий сайт з короткими інформативними відомостями про регламент, набір видів вебсайтів, для яких може потенційно застосовуватись GDPR та набір основних положень двома мовами – українською та англійською, відповідно до вибору користувача.

Засіб написаний за допомогою інструментів HTML та CSS, з використанням мови програмування JavaScript.

Ключові слова: GDPR, захист даних, персональні дані, GDPR для вебсайтів, регламент ЄС, регламент захисту даних.

ABSTRACT

The Bachelor's thesis consists of 63 pages in A4 format, containing 8 figures, 3 tables, and the list of references includes 27 entries.

The Bachelor's thesis is dedicated to the development of a software tool for creating a data protection policy for a website in accordance with the GDPR. The analysis of the GDPR regulation highlighted its importance in the modern world. The main provisions of the regulation were also studied, including its application for various business purposes, as well as the features of control and penalties for non-compliance with the GDPR.

The tool is developed to generate the main provisions of the GDPR regulation for different types of websites. The tool is a separate website with brief informational details about the regulation, a set of website types for which the GDPR may potentially apply, and a set of key provisions in both Ukrainian and English, according to the user’s selection.

The website is written using HTML and CSS tools, with JavaScript programming language.

Keywords: GDPR, data protection, GDPR for websites, EU regulation, data protection regulation.

ЗМІСТ

ВСТУП

У сучасному цифровому середовищі питання захисту персональних даних набуло критично важливого значення. Зростання кількості вебсайтів, мобільних додатків і онлайн-сервісів призвело до постійного обміну конфіденційною інформацією між користувачами та провайдерами послуг. У зв’язку з цим законодавчі ініціативи, зокрема Загальний регламент про захист даних (GDPR), стали ключовими орієнтирами для розробників, підприємств і юридичних структур у сфері забезпечення цифрової безпеки.

GDPR встановлює чіткі вимоги до збору, зберігання, обробки та передачі персональних даних, що зобов’язує вебресурси адаптувати свої політики конфіденційності до європейських стандартів. І хоча регламент був прийнятий у ЄС, його дія фактично стала глобальною — адже кожен ресурс, що обробляє дані громадян Європейського Союзу, повинен його дотримуватися. Водночас у багатьох країнах, зокрема й в Україні, спостерігається зростаючий попит на локалізовані рішення, які дозволяють швидко і без юридичної плутанини реалізовувати політики конфіденційності.

Метою роботи є покращення захисту персональних даних, що збираються, обробляються та зберігаються різними сервісами шляхом створення простого та зрозумілого вебзастосунку для генерування політики безпеки та основних положень GDPR для різного типу вебсайтів.

Для досягнення цієї мети передбачені наступні завдання:

- проаналізувати особливості положень GDPR, санкції за порушення та відповідальних сторін;
- проаналізувати вже існуючі рішення для генерації політики інформаційної безпеки за особливостями GDPR;
- створити логіку роботи вебзастосунку на основі попередньо проведеного аналізу;

- технічна реалізація вебзастосунку та проведення тестування системи для впевненості у коректності роботи генератора положень загального регламенту про захист даних.

Результати роботи були апробовані через публікацію тез: GDPR: основні положення та використання в сучасному світі. Всеукраїнська науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії: тези доп., 2025., Вінниця. - URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2025 (дата звернення 12.05.2025)

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз загального регламенту захисту даних (GDPR)

Регламент загального захисту даних (General Data Protection Regulation, або GDPR) - це ключовий нормативний акт у сфері захисту персональних даних, ухвалений Європейським Союзом 27 квітня 2016 року. Він набув чинності 25 травня 2018 року та став обов'язковим до виконання на території всіх країн-членів ЄС. Прийняття цього документу стало відповіддю на стрімкий розвиток цифрових технологій, глобалізацію обміну даними, зростання кількості сервісів, що збирають, зберігають і аналізують персональні дані користувачів. Головна мета GDPR полягає в тому, щоб надати фізичним особам - тобто суб'єктам персональних даних — більше прав і можливостей для контролю за тим, як їхні дані збираються, обробляються, зберігаються та передаються. Таким чином, регламент спрямований на забезпечення більшої прозорості, підзвітності та безпеки у сфері обробки персональних даних [1].

Однією з визначальних особливостей GDPR є його екстериторіальна дія. Це означає, що вимоги регламенту поширюються не лише на компанії, зареєстровані у країнах ЄС, а й на будь-які інші організації та фізичних осіб, незалежно від їхнього географічного розташування, якщо вони так чи інакше здійснюють обробку персональних даних громадян Європейського Союзу. Зокрема, якщо вебсайт або онлайн-платформа надає свої послуги користувачам, які перебувають на території ЄС, або веде маркетинг, націлений на громадян ЄС, - така діяльність автоматично підпадає під дію GDPR. Це положення суттєво підвищує значення дотримання регламенту для бізнесу, IT-сфери, освітніх ініціатив, медіа та будь-яких інших суб'єктів, що функціонують у глобальному цифровому просторі.

GDPR встановлює сім основних принципів обробки персональних даних (рис. 1.1):

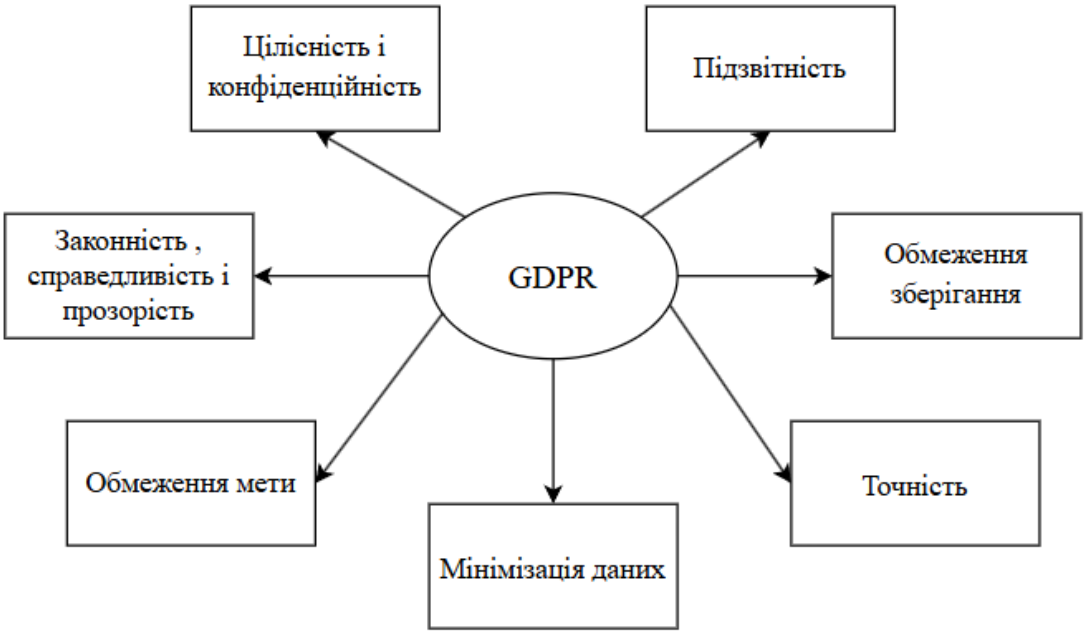


Рисунок 1.1 - Основні принципи обробки персональних даних GDPR

Рисунки в цій бакалаврській кваліфікаційній роботі було виконано за допомогою онлайн конструктора-редактора блоксхем draw.io [2].

1) законність, справедливість і прозорість - обробка персональних даних має здійснюватися на законних підставах, без введення в оману, та у зрозумілий спосіб для суб'єкта даних. Користувач має чітко розуміти, які саме дані збираються, з якою метою, хто ними оперує та як довго вони будуть зберігатися.

2) обмеження мети - персональні дані повинні збиратися лише з конкретними, явно визначеними та законними цілями. Подальша обробка цих даних не повинна суперечити первинним цілям. Якщо можуть бути якісь винятки, про них потрібно попередньо повідомити користувачів та задокументувати цей випадок.

3) мінімізація даних - необхідно забезпечити, щоб обсяг персональних даних, що збираються та обробляються, був не більшим, ніж потрібно для досягнення конкретної мети. Збір надлишкових або зайвих даних є

порушенням принципу мінімізації і може бути підставою для санкцій з боку наглядових органів.

4) точність - персональні дані мають бути точними, актуальними та, за необхідності, оновлюватися. Організації повинні вживати розумних заходів для виявлення та виправлення неточностей або вилучення застарілої інформації. Наприклад, це може стосуватися адрес доставки, контактної інформації чи платіжних реквізитів.

5) обмеження зберігання - дані не повинні зберігатися довше, ніж це необхідно для реалізації цілей, для яких вони були зібрані. Після закінчення цього строку дані мають обов’язково бути безпечно видалені або анонімізовані. У межах реалізації цього принципу часто запроваджується політика життєвого циклу даних (data retention policy), яка визначає терміни зберігання для кожної категорії інформації.

6) цілісність і конфіденційність - організації зобов’язані забезпечити належний рівень безпеки персональних даних, включаючи захист від несанкціонованого доступу, випадкової втрати, знищення або пошкодження. Це досягається шляхом впровадження технічних та організаційних заходів, зокрема шифрування, обмеження доступу, багаторівневої автентифікації та регулярного аудиту систем безпеки.

7) підзвітність - контролери персональних даних повинні не лише дотримуватись вищезазначених принципів, але й бути здатними документально підтвердити це. Тобто організація повинна мати внутрішню документацію - записи про обробку даних та засоби для демонстрації відповідності GDPR - наприклад, шляхом ведення реєстрів обробки, проведення оцінки впливу на захист даних чи призначення відповідальних осіб [3].

Загальний регламент про захист даних (GDPR) також визначає широкий спектр прав суб’єктів персональних даних, реалізація яких є обов’язковою для всіх організацій, що здійснюють їх обробку, незалежно від фізичного розташування офісу компанії. Це означає, що кожна компанія, організація або

ресурс, який працює з персональними даними фізичних осіб, які є громадянами Європейського союзу, має не лише технічно їх захищати, а й забезпечити користувачам можливість повноцінно реалізувати свої права (див. табл. 1.1) [4].

Таблиця 1.1 – Ключові права суб’єктів персональних даних

Право	**Опис**
Право доступу до своїх персональних даних	Користувач має право отримати підтвердження того, чи здійснюється обробка його персональних даних, а також доступ до самих даних і додаткову інформацію: мету обробки, категорії даних, отримувачів, строк зберігання тощо.
Право на виправлення неточностей	У разі виявлення неточної або неповної інформації користувач має право вимагати її виправлення чи доповнення без зайвих зволікань. Це особливо важливо для уникнення юридичних та репутаційних ризиків.
Право на видалення персональних даних (право бути забутим)	Особа може вимагати видалення своїх даних, якщо вони більше не потрібні для досягнення цілей, для яких були зібрані, або якщо дані обробляються незаконно. Організація зобов’язана задовольнити таку вимогу, якщо немає правових підстав для збереження інформації.
Право на обмеження обробки	У певних випадках суб’єкт даних може вимагати обмежити обробку своїх персональних даних, наприклад, коли оскаржується точність даних або якщо обробка є незаконною, але особа не бажає їх видалення.
Право на переносимість даних	Користувач має право отримати свої персональні дані в структурованому, загальновживаному форматі, а також передати їх іншому контролеру, якщо обробка здійснюється на підставі згоди або договору, і автоматизовано.
Право на заперечення проти обробки	У будь-який момент користувач може висловити заперечення щодо обробки своїх даних на підставі законного інтересу або з метою прямого маркетингу.

Для того щоб ці права були дійсно реалізовані, власники вебсайтів зобов’язані створити зрозумілий та доступний документ, тобто політику конфіденційності. Вона є головним каналом комунікації між оператором персональних даних та користувачем. Від якості цього документа залежить не лише відповідність вимогам GDPR, а й рівень довіри користувачів до сайту. У сучасному цифровому середовищі користувачі все частіше звертають увагу на те, як саме їхні дані обробляються, і відсутність належної політики може стати бар’єром на шляху до використання ресурсу або навіть викликати негативну реакцію з боку аудиторії [5].

Політика конфіденційності повинна містити таку обов’язкову інформацію:

– які саме дані збираються – перелік типів персональних даних, які обробляються в рамках функціонування вебсайту (наприклад: ім’я, електронна пошта, номер телефону, IP-адреса, поведінкові дані на сайті, файли cookie тощо). Також важливо чітко розмежовувати обов’язкові для збору дані (наприклад, необхідні для реєстрації) та ті, що надаються добровільно. Це дозволяє користувачу усвідомлено контролювати обсяг особистої інформації, яку він передає;

– на якій правовій підставі здійснюється обробка – згідно з GDPR, існує шість правових підстав для обробки персональних даних. Політика повинна чітко вказувати, яка саме з них застосовується у кожному конкретному випадку. Наприклад, при підписці на розсилку - це буде згода, при оформленні замовлення - виконання договору, а при зберіганні історії переглядів - законний інтерес. Надзвичайно важливо, щоб ця інформація була викладена у зрозумілій формі, адже саме вона дозволяє визначити законність обробки даних;

– хто має доступ до даних – користувач повинен бути проінформований про всіх осіб або компанії, які отримують доступ до його персональних даних. Це можуть бути сторонні підрядники, сервіси аналітики (наприклад, Google Analytics), платіжні системи або хостинг-провайдери.

Якщо дані передаються за межі Європейського економічного простору, має бути зазначено, в які саме країни, на якій підставі та з якими гарантіями безпеки;

– як довго дані зберігаються – політика має чітко пояснювати строки або критерії зберігання персональних даних. Наприклад, дані можуть зберігатися до моменту відкликання згоди користувача, протягом строку дії договору, або ж згідно з вимогами локального податкового чи бухгалтерського законодавства. Важливо зазначити, що після завершення періоду зберігання дані повинні бути безпечно знищені або анонімізовані;

– які права має користувач і як ними скористатися – політика повинна надавати чіткий алгоритм дій для користувача, що хоче реалізувати свої права, гарантовані GDPR. Це включає контактні дані відповідальної особи, електронну адресу для звернень, строки обробки запитів, а також можливі умови ідентифікації користувача для уникнення зловживань. Наявність простої й зрозумілої інструкції з реалізації прав формує довіру до сервісу та демонструє відкритість компанії.

Таким чином, політика конфіденційності виконує не лише юридичну, але й важливу інформаційну та комунікаційну функцію, дозволяючи користувачам приймати обґрунтовані рішення щодо передачі своїх даних, а також розуміти, як ці дані будуть оброблятися. Вона виступає своєрідною «візитівкою» цифрового ресурсу в очах відвідувача. Наявність чіткої, логічно структурованої та доступно сформульованої політики не лише сприяє дотриманню правових норм, але й підвищує репутацію вебсайту як надійного, етичного та відповідального учасника інформаційного простору. У контексті загальносвітової цифровізації та зростання рівня кіберзагроз, така прозорість є однією з головних умов ефективної цифрової взаємодії [6].

1.2 Відповідальність за порушення регламенту

Важливою складовою ефективного функціонування Регламенту GDPR є чітко визначена система відповідальності за його порушення, що охоплює як фінансові, так і репутаційні наслідки для організацій, які не дотримуються встановлених вимог. Сам факт існування реальних санкцій є потужним інструментом тиску, який змушує компанії, установи та інші суб'єкти господарювання ретельно ставитись до збирання, обробки, зберігання та захисту персональних даних. На відміну від декларативних норм, які не мають реального впливу, система відповідальності в межах GDPR побудована на прозорих механізмах контролю та чітких наслідках за недотримання. Це дозволяє створити дієвий превентивний механізм, що стимулює впровадження політик конфіденційності, засобів захисту даних, систем аудиту та постійного моніторингу інформаційних потоків. У цьому контексті відповідальність стає не лише елементом правового тиску, а й невіддільною частиною сучасної стратегії з інформаційної безпеки - адже захист даних напряму пов'язаний із довірою користувачів, репутацією бренду та загальною стійкістю цифрової інфраструктури [7].

Уже сьогодні існує низка гучних випадків, коли великі компанії зазнали значних збитків через порушення GDPR. Наприклад, British Airways у 2020 році була оштрафована на 20 мільйонів фунтів стерлінгів за витік даних понад 400 тисяч клієнтів. Компанія Google отримала штраф у 50 мільйонів євро за непрозору політику згоди на обробку персональних даних у Франції. Ці приклади свідчать про те, що відповідальність за порушення GDPR - це не теоретична загроза, а реальна практика сучасного регулювання. Для сфери інформаційної безпеки це означає, що технічні рішення повинні не лише працювати, а й бути юридично обґрунтованими та відповідати принципам захисту даних за замовчуванням. Захист персональної інформації - це вже не конкурентна перевага, а обов'язковий мінімум, ігнорування якого може

коштувати компанії не лише грошей, а й довіри користувачів, партнерів та інвесторів [8].

Порушення вимог Регламенту GDPR можуть проявлятися у найрізноманітніших формах і охоплюють як технічні, так і організаційні аспекти обробки персональних даних. У більшості випадків такі порушення виникають внаслідок недостатнього розуміння норм регламенту, недосконалого внутрішнього контролю або нехтування елементарними принципами інформаційної безпеки. Вони можуть мати як навмисний, так і ненавмисний характер, однак незалежно від мотивації порушення тягнуть за собою серйозні наслідки - від попереджень до багатомільйонних штрафів [9].

Серед найпоширеніших типів порушень варто виокремити кілька ключових категорій:

1) обробка персональних даних без належної правової підстави. Одним з основних принципів GDPR є законність обробки, тобто наявність чіткої правової основи (наприклад, згоди суб'єкта даних, виконання договору чи законного інтересу). Проте багато організацій досі обробляють дані користувачів без явної згоди або не обґрунтовують правову підставу належним чином. Часто порушується також принцип мінімізації - збираються надмірні обсяги інформації, не релевантні для конкретної мети.

2) недотримання обов'язку інформування. Згідно з регламентом, кожен користувач повинен бути чітко і в зрозумілій формі поінформований про те, які саме дані збираються, з якою метою, хто є їхнім контролером, які права має суб'єкт даних тощо. Втім, у багатьох випадках політики конфіденційності залишаються або надто загальними, або незрозумілими з юридичної точки зору, або взагалі відсутні. Це порушення вважається критичним, оскільки воно прямо зачіпає право особи на прозорість.

3) недостатній рівень безпеки обробки даних. Організації зобов'язані впроваджувати відповідні технічні та організаційні заходи безпеки, однак на практиці часто зустрічається використання застарілих систем, слабких паролів, відсутність шифрування або резервного копіювання. Такі технічні

вразливості відкривають шлях для витоків, несанкціонованого доступу, маніпуляцій або повної втрати персональних даних.

4) ігнорування прав суб'єктів даних. GDPR гарантує кожному користувачеві низку прав - зокрема право на доступ до своїх даних, їхнє виправлення, обмеження обробки або повне видалення (право на забуття). У випадках, коли компанії не відповідають на такі запити, не дотримуються встановлених строків або повністю ігнорують вимоги користувачів, відбувається суттєве порушення принципів регламенту.

5) несвоєчасне повідомлення про інциденти безпеки. GDPR зобов'язує контролерів даних повідомляти про витік або порушення захисту персональних даних протягом 72 годин з моменту виявлення інциденту. Нерідко компанії приховують подібні інциденти з міркувань репутації або через відсутність внутрішніх процедур реагування, що лише погіршує ситуацію і вважається грубим порушенням обов'язків перед як наглядовими органами, так і самими суб'єктами даних.

Залежно від характеру, обсягу, навмисності та наслідків порушення, GDPR передбачає диференційований підхід до накладення санкцій. Регламент встановлює два основні рівні адміністративних штрафів, які можуть застосовуватись окремо або в поєднанні з іншими заходами впливу. Їх мета - не лише покарати винних, а й запобігти повторним порушенням, підвищити рівень обізнаності, а також стимулювати організації до системного впровадження стандартів безпеки (рис. 1.2) [10].

1) перший рівень санкцій – цей рівень штрафу застосовується у випадках менш тяжких порушень, до яких належать:

– відсутність або неналежне ведення обов'язкової документації щодо обробки даних;

– недостатня співпраця з наглядовими органами;

– невиконання зобов'язань з обліку даних (наприклад, відсутність реєстру обробки);

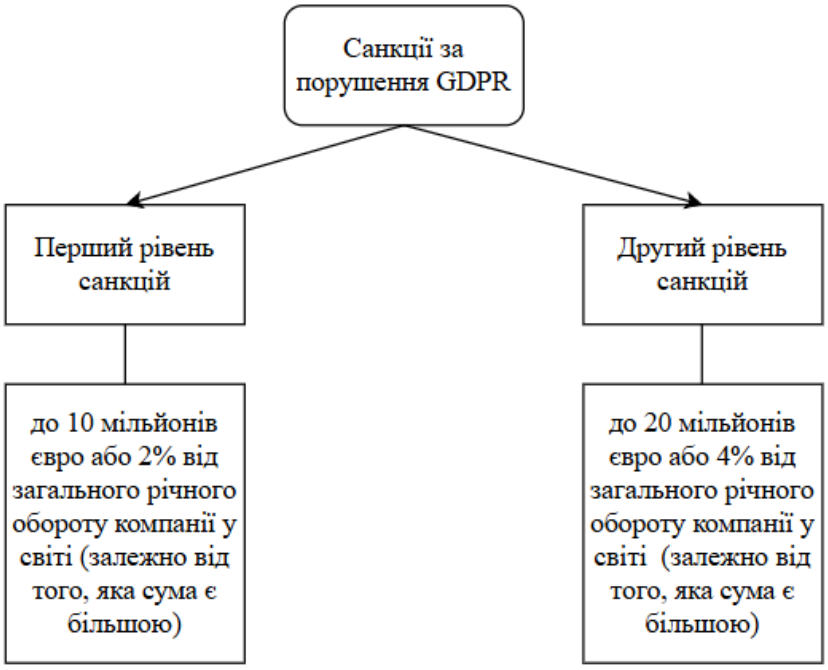


Рисунок 1.2 – Санкції за порушення GDPR

– порушення вимог до зберігання даних або принципу прозорості, які не спричинили серйозних наслідків для суб’єктів даних.

2) другий рівень санкцій – цей рівень стосується найсерйозніших порушень, серед яких:

– порушення основних принципів обробки даних, таких як законність, прозорість, цільове обмеження, мінімізація;

– обробка персональних даних без згоди або з порушенням прав суб’єкта;

– незаконна передача даних третім країнам без належного рівня захисту;

– ігнорування запитів користувачів або невиконання їхніх прав відповідно до статей 12–22 GDPR.

Окрім штрафів, GDPR передбачає й інші заходи адміністративного впливу, які можуть мати не менш серйозні наслідки для організації:

– тимчасова або повна заборона на обробку персональних даних;

– обмеження певних видів діяльності або вимога до внесення технічних змін у системи;

– зобов’язання повідомити громадськість про факт порушення, що особливо болісно для репутації бренду;

– вимога компенсувати завдану шкоду постраждалим суб’єктам даних.

Таким чином, відповідальність за порушення Регламенту GDPR є не лише формальною вимогою, а й одним із ключових механізмів впливу на діяльність організацій у сфері захисту персональних даних. Жорсткі санкції, що передбачають значні фінансові штрафи, а також можливість репутаційних втрат, змушують компанії системно підходити до питання безпеки інформації, розглядаючи її не лише як технічну проблему, а й як складову правового та управлінського процесу.

У контексті інформаційної безпеки це означає, що ефективна реалізація вимог GDPR неможлива без поєднання технічних заходів із чіткими політиками та процедурами, що регламентують обробку персональних даних. Важливим аспектом стає підвищення рівня правової грамотності персоналу, а також створення культури дотримання конфіденційності у всіх підрозділах організації. Саме комплексний підхід - який включає розробку внутрішніх політик, впровадження інструментів кіберзахисту, регулярний аудит та навчання працівників - забезпечує не лише відповідність вимогам законодавства, а й сприяє сталому та безпечному розвитку цифрових сервісів [11].

Отже, відповідальність за порушення GDPR є не стільки покаранням, скільки стимулом для організацій підвищувати стандарти захисту персональних даних, інтегруючи правові та технічні рішення у свою щоденну діяльність. Лише так можна гарантувати дотримання прав суб’єктів даних і зменшити ризики виникнення інформаційних інцидентів у сучасних умовах цифровізації.

1.3 Огляд існуючих рішень для автоматичного створення політик конфіденційності

У зв’язку з активним розвитком цифрових технологій, глобалізацією електронної комерції та посиленням вимог до захисту персональних даних, зростає потреба у швидкому й ефективному створенні юридично коректної документації для вебсайтів. Одним із найважливіших документів, що забезпечують дотримання вимог законодавства, є політика конфіденційності. Вона повинна бути доступною, зрозумілою та юридично точною, оскільки відображає, які саме персональні дані збирає сайт, з якою метою, на якій правовій підставі й як саме вони обробляються [12].

З огляду на складність і юридичну відповідальність, яку передбачає створення такого документа, виникла потреба в спеціалізованих інструментах, які б допомогли веброзробникам, власникам бізнесу та адміністраторам ресурсів автоматизувати процес формування політик. Як відповідь на цей запит, на ринку з’явилася низка онлайн-сервісів, які реалізують функціонал автоматичних генераторів політик конфіденційності.

Такі генератори, як правило, представляють собою вебінтерфейси з інтерактивними формами, де користувач покроково вводить інформацію про свій вебсайт (тип зібраних даних, використання сторонніх сервісів, розташування серверів тощо), а система на основі шаблонів створює готовий текст документа. Це дозволяє навіть непрофесіоналам отримати юридично обґрунтований текст без залучення юристів, що значно економить ресурси та час.

Найбільш відомі серед них:

– Termly - одна з найпопулярніших платформ, яка пропонує цілий набір інструментів для створення не лише політики конфіденційності, а й умов використання, cookie-банерів, угод про обробку даних (DPA) тощо. Сервіс підтримує вимоги різних законодавств, зокрема GDPR (ЄС), CCPA

(Каліфорнія, США) та інших міжнародних актів. Перевагами Termly є інтуїтивно зрозумілий інтерфейс, автоматичне оновлення політик відповідно до змін у законодавстві та можливість інтеграції з платформами типу WordPress. Проте головним недоліком залишається англомовність сервісу та обмеження функціоналу у безкоштовній версії [13].

– Iubenda - ще один потужний гравець у цій сфері, що орієнтований на розробників і юридичні департаменти. Iubenda дозволяє гнучко налаштовувати політику згідно з технічними особливостями сайту або застосунку. Сервіс підтримує автоматичну синхронізацію, має API, бібліотеку шаблонів і можливість ведення кількох мовних версій. Незважаючи на функціональність, цей інструмент є складним у використанні для новачків, а більшість можливостей доступні лише за підпискою [14].

– PrivacyPolicies.com, FreePrivacyPolicy.com, GetTerms.io - сервіси, які пропонують більш спрощені генератори. Вони підійдуть для невеликих проєктів і забезпечують базовий рівень відповідності. Як правило, користувач заповнює форму з запитаннями, на основі яких створюється шаблон тексту. Після цього можна завантажити або вбудувати готову політику на сайт. Однак ці сервіси мають обмежену гнучкість, не завжди дозволяють змінювати юридичні формулювання, і часто вимагають плату за додаткові функції, зокрема за можливість завантаження документів без водяних знаків або HTML-форматування [15-17].

Попри широку доступність онлайн-інструментів для автоматичного створення політик конфіденційності, питання їх ефективності та універсальності залишається відкритим. На перший погляд, подібні сервіси значно спрощують процес підготовки юридичних документів, особливо для непрофесійної аудиторії - розробників-початківців, малих підприємців або власників персональних блогів. Однак, при більш детальному аналізі виявляється, що не всі генератори здатні забезпечити належний рівень відповідності законодавчим вимогам та реальним потребам конкретного вебресурсу.

Саме тому доцільно розглянути характерні обмеження таких рішень, які стають критичними у випадках, коли йдеться про локалізовані, вузькоспеціалізовані або освітні вебпроєкти. Далі буде проведено огляд ключових проблем, пов’язаних із використанням популярних сервісів генерування політик, що дозволило чітко сформулювати вимоги до нового інструменту, створеного в межах бакалаврської кваліфікаційної роботи (рис 1.3).

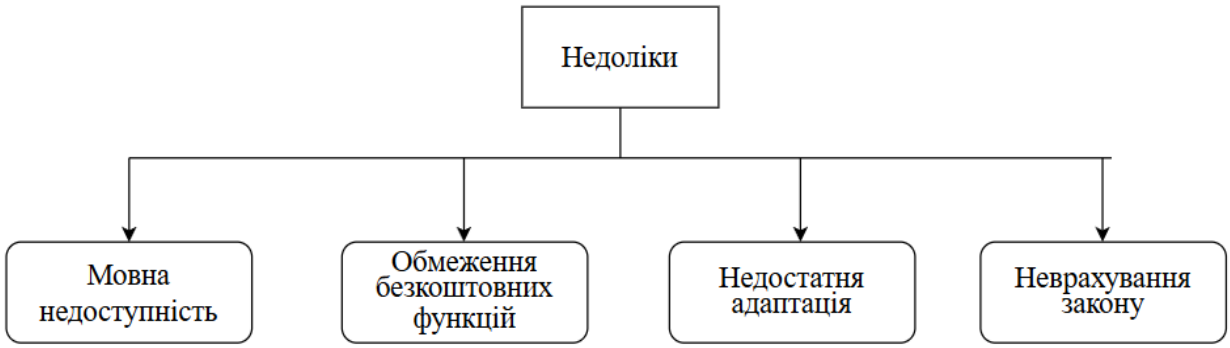


Рисунок 1.3 – Недоліки генераторів шаблонів політики GDPR

1) мовна недоступність - переважна більшість сервісів підтримує лише англійську мову або інші західноєвропейські мови. Українська версія зазвичай відсутня або реалізована машинним перекладом, що викликає юридичні ризики через неправильне трактування термінології та порушення стилістичної відповідності нормативним актам.

2) обмеження безкоштовних функцій - у багатьох випадках базовий функціонал дозволяє згенерувати лише узагальнений документ, без можливості вказати специфіку сайту або типову поведінку користувача. До того ж, інтеграція з сайтом, багатомовність, автоматичні оновлення або видалення логотипу сервісу доступні лише за підпискою.

3) недостатня адаптація до функціональних особливостей конкретного ресурсу - наприклад, політика, створена за допомогою шаблону, може не враховувати наявність контактних форм, реєстрації, авторизації через

соціальні мережі, аналітичних трекерів, e-commerce модулів або інтеграцій з платіжними системами.

4) неврахування національного законодавства - окрім дотримання вимог GDPR, онлайн-ресурси, що діють у конкретній юрисдикції, повинні також враховувати положення національного законодавства про захист персональних даних. Це можуть бути нормативні акти щодо обробки персональних даних неповнолітніх, зберігання даних у сфері освіти, вимоги щодо отримання згоди або обмеження передачі інформації за кордон. Більшість іноземних генераторів політик конфіденційності не мають функціоналу, який би дозволяв врахувати специфіку локального правового середовища, що може призвести до невідповідності політики вимогам конкретної держави.

Отже, аналіз існуючих інструментів для створення політик конфіденційності засвідчує потребу в новому, більш адаптованому та зручному рішенні. Попри наявність великої кількості генераторів юридичних документів, більшість із них орієнтовані на англомовний ринок, мають обмежену функціональність у безкоштовних версіях, не враховують специфіку окремих типів вебресурсів і недостатньо гнучкі у налаштуваннях. Ці фактори створюють бар’єри для багатьох користувачів, особливо тих, хто працює в умовах обмежених ресурсів або не має юридичної підготовки.

Таким чином, виникає об’єктивна потреба в універсальному, безкоштовному та інтуїтивно зрозумілому інструменті, який дозволяв би ефективно формувати політики конфіденційності відповідно до вимог міжнародного законодавства у сфері захисту персональних даних, зокрема GDPR.

Серед ключових вимог до такого інструменту можна виділити такі.

– Мовна адаптивність. Надзвичайно важливо, щоб користувач мав змогу створити політику конфіденційності рідною або зрозумілою мовою. Це підвищує рівень прозорості та довіри з боку відвідувачів вебресурсу, адже дозволяє їм чітко ознайомитися з тим, як обробляються їхні персональні дані.

Крім того, це сприяє кращому розумінню юридичних обов’язків самими розробниками.

– Гнучка персоналізація відповідно до функціональності сайту або додатку. Сучасні вебресурси відрізняються великою різноманітністю - від простих блогів до складних e-commerce платформ із системами авторизації, збором статистики, інтеграцією сторонніх API, формами зворотного зв’язку, онлайн-чатами тощо. Усі ці елементи передбачають різні обсяги та типи обробки персональних даних. Тому інструмент повинен дозволяти точно враховувати, які саме функції використовуються, щоб створений документ дійсно відображав реальні процеси обробки.

– Відповідність міжнародним стандартам і нормативним вимогам. Найбільш розповсюдженим стандартом сьогодні є Загальний регламент про захист даних (GDPR), що регулює порядок обробки персональних даних на території Європейського Союзу та впливає на всі компанії й проєкти, які працюють із європейськими громадянами. Інструмент має враховувати ключові положення цього регламенту, включаючи правові підстави обробки, забезпечення прав суб’єктів даних, прозорість процесів, передачу даних третім сторонам, зберігання та безпеку інформації.

– Доступність для широкого кола користувачів. Не всі розробники мають змогу користуватися дорогими SaaS-платформами чи наймати юридичних консультантів. Особливо це стосується студентів, фрілансерів, стартапів або представників малого бізнесу, для яких простота, швидкість та безкоштовний доступ до базової функціональності мають вирішальне значення. Інструмент повинен бути максимально зручним у використанні, без потреби у спеціальній підготовці.

Враховуючи вищезазначене, можна стверджувати, що існує значний попит на зручний генератор політик конфіденційності, який дозволить автоматизувати процес створення правового документа, водночас забезпечуючи юридичну точність, структурованість та відповідність регламентам. Такий підхід сприятиме поширенню культури захисту

персональних даних, підвищенню рівня довіри до цифрових сервісів і зниженню ризиків для розробників у сфері дотримання законодавства.

1.4 Порівняння створеного сервісу з генерації політик GDPR із вже існуючими застосунками

У найближчому майбутньому наявність чіткої, доступної та адаптованої під конкретну аудиторію політики конфіденційності може стати базовим очікуванням користувачів - так само, як наявність мобільної версії сайту, інтерфейсу кількома мовами чи підтримки безпечного з'єднання (HTTPS). Особливо це стосується освітніх, соціальних, медіа- та комерційних проєктів, де обробка даних є не лише неминучою, а й критичною для ефективного функціонування. У цьому контексті реалізація вимог конфіденційності — це не лише дотримання букви закону, а й прояв поваги до цифрових прав особи та відповідальності перед спільнотою користувачів.

Аналіз основних положень GDPR, принципів обробки персональних даних і сучасних викликів, пов'язаних із впровадженням політик конфіденційності, свідчить про те, що дотримання вимог цього регламенту є не лише юридичним обов'язком, а й складовою загальної стратегії кібербезпеки цифрових сервісів. У сучасному інформаційному середовищі, де обсяг і чутливість даних постійно зростають, захист персональної інформації набуває вирішального значення для збереження довіри користувачів і запобігання кібератакам.

Більшість доступних інструментів створення політик конфіденційності мають обмежену адаптивність, не враховують специфіку окремих типів сайтів, недостатньо прозоро формулюють положення, і часто не враховують новітні ризики в сфері захисту інформації. Також бракує рішень, які б дозволяли створювати змістовні, двомовні та функціонально адаптовані розділи політики - з орієнтацією не лише на правову відповідність, а й на практичну безпеку даних.

Ці проблеми вирішуються за допомогою інструменту, який генерує основні положення політики конфіденційності залежно від функціональності конкретного вебресурсу. Його особливістю є поєднання юридичної точності та фокус на питаннях кіберзахисту: кожне положення структуроване так, щоб не лише відповідати GDPR, але й сприяти мінімізації цифрових ризиків. Додаткова підтримка української та англійської мов дозволяє охопити широку аудиторію користувачів - від фахівців і розробників до освітніх установ і локальних проєктів (табл. 2.2).

Таблиця 2.2 – Порівняльна характеристика створеного сервісу із вже існуючими інструментами

Характеристика	Termly	lubenda	PrivacyPolicies.com / FreePrivacyPolicy.com / GetTerms.io	Розроблений сайт
1	2	3	4	5
Підтримка GDPR	Так	Так	Так	Так
Інші законодавчі акти (CCPA тощо)	Так	Так	Обмежено	Ні
Типи документів	Політика конфіденційності, умови використання, cookie-банери, DPA	Політика конфіденційності, умови, API, багатомовність	Політика конфіденційності, умови використання	Лише GDPR політика для обраного типу сайту
Мовна підтримка	Англійська	Багатомовність	Англійська	Англійська, українська
Можливість вибору типу сайту/ресурсу	Обмежено	Гнучке налаштування	Обмежено	Широкий вибір
Інтерфейс	Інтуїтивний	Складний	Простий	Простий
Автоматичне оновлення політик	Так	Так	Ні	Ні
Інтеграції з CMS/платформами	Так (WordPress тощо)	API та інші інтеграції	Ні	Ні
Кастомізація юридичних формулювань	Обмежена	Висока	Обмежена	Обмежена

1	2	3	4	5
Безкоштовний функціонал	Обмежений	Обмежений	Так	Так
Завантаження PDF без водяних знаків	Платно	Платно	Платно	Безкоштовно (через сапорт)
Підтримка клієнтів (сапорт)	Так	Так	Обмежена	Так
Цільова аудиторія	Бізнес, середні та великі сайти	Юридичні департаменти, розробники	Малі проєкти, стартапи	Малі та середні локальні проєкти, користувачі без юридичної підготовки

Що є у розробленого сервісу, але відсутнє у конкурентів:

1) двомовність з підтримкою української мови (локалізація під український ринок).

2) широкий перелік типів вебсайтів для вибору, що допомагає сформувати релевантну політику відповідно до специфіки.

3) простий і зрозумілий інтерфейс, який не вимагає спеціальних юридичних знань.

4) можливість отримати готовий pdf* документ через контакт із сапорт-центром без додаткових оплат.

5) орієнтованість саме на GDPR, що робить сервіс максимально сфокусованим на актуальних вимогах Європейського регламенту.

6) врахування саме українського національного законодавства, що робить політику максимально наближеною до українсьокого бізнесу.

Розроблений вебсервіс є прикладом ефективного, локалізованого підходу до реалізації вимог GDPR у цифровому просторі, зокрема в українському сегменті малого та середнього бізнесу. Основною перевагою платформи є її простота та зручність у використанні: користувачеві достатньо лише обрати тип вебсайту, вказати бажану мову (українську чи англійську), після чого отримати адаптований текст політики конфіденційності, який

відповідає ключовим вимогам Європейського регламенту про захист персональних даних.

Окремо варто відзначити функцію персоналізованої підтримки через сапорт-центр: користувач може отримати готову політику у форматі PDF із можливістю подальшого редагування або впровадження. Це дозволяє адаптувати документ під конкретні потреби бізнесу, уникаючи типових шаблонів, що часто зустрічаються у безкоштовних генераторах.

На відміну від великих міжнародних платформ, які часто не мають української локалізації, потребують глибокого заповнення форм, а також обмежують доступ до функцій у безкоштовних версіях, розроблений сервіс вирізняється фокусом саме на локального користувача. Підтримка української мови, чітке структурування політик залежно від типу вебсайту та можливість оперативного отримання документу роблять платформу особливо привабливою в контексті українського ринку.

Таким чином, сервіс не лише виконує прикладну функцію, але й сприяє підвищенню загального рівня правової обізнаності користувачів щодо вимог захисту персональних даних. Це поєднання простоти, адаптивності та доступності робить платформу унікальною та надзвичайно корисною для цільової аудиторії.

1.5 Постановка завдання

Попри чітко сформульовані положення Регламенту GDPR та наявність онлайн-інструментів, які спрощують створення відповідної документації, реалізація політик конфіденційності на практиці залишається складним і багатовимірним завданням. Це особливо актуально в умовах стрімкої цифровізації, коли обсяги оброблюваних персональних даних зростають, а способи їх збору, зберігання та передачі стають дедалі складнішими [18].

У цьому контексті варто звернути увагу на кілька ключових викликів, з якими стикаються сучасні учасники цифрового середовища під час

впровадження ефективних та відповідних вимогам законодавства політик конфіденційності. До таких учасників належать розробники вебресурсів, фахівці з інформаційної безпеки, юристи, адміністратори освітніх і некомерційних платформ, а також малі підприємці та фрилансери, які часто не мають спеціалізованих юридичних знань або доступу до професійних консультацій. Їхня робота ускладнюється тим, що політика конфіденційності повинна бути не лише формальною вимогою, а й реально діючим документом, який враховує технічні особливості ресурсу, мовні нюанси цільової аудиторії, а також стрімко змінюваний ландшафт нормативно-правових актів у сфері захисту персональних даних.

Підготовка такого документа потребує глибокого розуміння принципів обробки даних, можливостей технічної інфраструктури, специфіки конкретного типу сайту, а також вміння поєднати ці елементи у доступну й юридично коректну форму. Як наслідок, реалізація вимог конфіденційності перетворюється на складний міждисциплінарний процес, який вимагає узгодженої співпраці між різними фахівцями, доступу до якісних інструментів підтримки та гнучких підходів до автоматизації.

Хоча GDPR встановлює загальні принципи та вимоги, практична реалізація політик конфіденційності значною мірою залежить від інтерпретації норм. Це призводить до різноманітності підходів: один сайт може подавати політику як юридичний документ на 15 сторінок, тоді як інший - у вигляді стислого пояснення на пів сторінки. Через це виникає складність в оцінці відповідності - як для користувача, так і для наглядових органів. Крім того, вимоги GDPR часто поєднуються з нормами інших юрисдикцій. Це створює додатковий виклик у формуванні універсальних політик, що враховують багаторівневу нормативну базу.

Політика конфіденційності - це не лише юридичний інструмент, а й засіб інформування. Однак на практиці вона часто є малозрозумілою для кінцевого користувача. Адже, значна частина користувачів не читає політику

конфіденційності взагалі, через складність викладу. Це свідчить про необхідність адаптувати форму подачі до рівня обізнаності користувача.

Не кожна організація, особливо на етапі стартапу чи малого бізнесу, має у своєму штаті фахівця з питань захисту персональних. Як наслідок - складання політики конфіденційності покладається на сторонні сервіси, автоматизовані генератори або загальні шаблони з інтернету.

Окремим викликом є механізм отримання згоди на обробку персональних даних. GDPR вимагає, щоб згода була вільною, конкретною, поінформованою і однозначною. Проте на практиці реалізація цього принципу викликає багато питаньЗвідси випливає потреба у впровадженні механізмів прозорого, зручного та документованого отримання згоди.

У таких випадках важливо надавати прості, структуровані та локалізовані інструменти, які дозволяють власникам сайтів хоча б на базовому рівні забезпечити відповідність вимогам законодавства.

Таким чином, грамотне впровадження політик конфіденційності - це не просто відповідь на регуляторні виклики, а стратегічний інструмент цифрової етики та побудови довіри у відносинах між користувачем і платформою. Політика конфіденційності поступово втрачає статус суто формального документа і перетворюється на важливий елемент цифрової репутації, що впливає на сприйняття ресурсу не менше, ніж його дизайн, функціональність або технічна надійність.

Отже, застосування подібного інструменту забезпечує не лише відповідність нормам GDPR, а й формує культуру обережного ставлення до персональних даних як до цінного ресурсу, який потребує системного й грамотного захисту.

2 РОЗРОБКА ЗАСОБУ ДЛЯ ФОРМУВАННЯ ПОЛІТИКИ GDPR

2.1 Огляд засобу для формування основних положень GDPR

У сучасних реаліях цифрової економіки захист персональних даних набуває особливої ваги, адже кількість інформації, що збирається і обробляється різноманітними вебресурсами, стрімко зростає. Відповідність вимогам GDPR стає необхідною умовою для законного функціонування вебсайтів, незалежно від їхнього масштабу чи географічного розташування. Однак підготовка політики конфіденційності, що враховує всі нюанси обробки персональних даних, залишається складним і ресурсозатратним процесом. Це потребує комплексних знань у сфері законодавства, розуміння технічних аспектів обробки даних, а також врахування специфіки діяльності конкретного ресурсу.

Для спрощення цього процесу розроблено спеціалізований вебінструмент, який надає можливість автоматизованого формування основних положень політики конфіденційності відповідно до вимог GDPR. Користувачам пропонується вибрати тип свого вебресурсу - наприклад, корпоративний сайт, інтернет-магазин, блог чи мобільний застосунок - а також обрати мову генерації: українську або англійську. На основі цих виборів система автоматично формує адаптований перелік ключових положень, які необхідно врахувати у політиці конфіденційності для обраного виду ресурсу.

Особливістю цього інструменту є те, що він не створює повний текст політики, а забезпечує базовий каркас, що містить найважливіші юридичні та організаційні вимоги, які мають бути включені до документа. Такий підхід дозволяє мінімізувати ризики пропуску критично важливої інформації, сприяє уніфікації підходів до захисту персональних даних і одночасно залишає простір для індивідуального доопрацювання політики відповідно до унікальних характеристик кожного ресурсу. Це особливо актуально для малих

підприємств, стартапів, некомерційних організацій та освітніх платформ, які часто не мають змоги залучати висококваліфікованих юристів (рис. 2.1).

Рисунок 2.1 – Алгоритм роботи засобу для генерування основних положень GDPR

Алгоритм, відображає логіку роботи вебзасобу для генерації основних положень політики конфіденційності згідно з вимогами GDPR. Основне завдання системи – надати користувачеві можливість сформувати ключові пункти, які мають бути обов’язково присутні в політиці конфіденційності, залежно від типу вебсайту та вибраної мови.

Робота програми базується на простій, покроковій взаємодії з користувачем. Спочатку користувач обирає тип вебресурсу, який він розробляє або адмініструє. Це можуть бути, наприклад, особисті блоги, комерційні сайти, інтернет-магазини, навчальні платформи чи інформаційні портали. Потім він обирає, які саме персональні дані будуть надаватись його клієнтом. Для кращої специфікації у користувача також система запитує про передачу персональних даних третім сторонам та про наявність будь-яких фінансових операцій на сайті. Після цього обирається мова формування положень - українська або англійська. На основі цих параметрів система підбирає відповідний шаблон із бази варіантів, адаптований під потреби конкретного типу сайту та мовну специфіку.

Після генерації положень користувач отримує готовий текст, який може бути використаний як основа для подальшого створення повноцінної політики конфіденційності. Однак для отримання файлу з цими положеннями, система пропонує звернутися до служби підтримки, що дозволяє забезпечити додатковий рівень контролю, перевірки коректності запиту та консультації з питань інтеграції тексту в структуру вебресурсу.

Для визначення рівня критичності захисту персональних даних громадян ЄС, обов’язковим кроком для формування основних положень GDPR є вказання, які саме персональні дані збираються сайтом:

- ПІБ;
- email;
- номер телефону;
- домашня адреса;
- IP-адреса;
- платіжна інформація;
- дані геолокації;
- спеціалізовані дані користувача (дані, які є спеціалізованими саме для цього виду сайту і є обов’язковими для вказання).

Для визначення рівня критичності захисту даних система фактично підраховує загальну кількість персональних даних, які збирається сайтом про свого потенційного користувача. В реальності кожний бізнес збирає про своїх користувачів мінімум 3 типи персональних даних – ім’я, номер телефону та якфсь спеціалізовані дані, які необхідні для нормальної та повноцінної роботи вебсайту, бази даних та й компанії в загальному. Отже рівень захищеності особистих конфіденційних даних користувачів буде здебільшого – середній або високий (рис. 2.2).

Рисунок 2.2 - Визначення рівня критичності захисту персональних даних

Також особливу увагу варто приділити факту передачі персональних даних користувачів третім сторонам. Сайт однієї компанії може обмінюватись

даними із сайтом іншої компанії для досягнення цілі. Отже, організація має взяти на себе відповідальність за збереження конфіденційності, цілісності і доступності персональних даних клієнтів. Особливо критичною є передача даних компаніям які не працюють в ЄС та не підпорядковуються положенням GDPR (рис. 2.3).

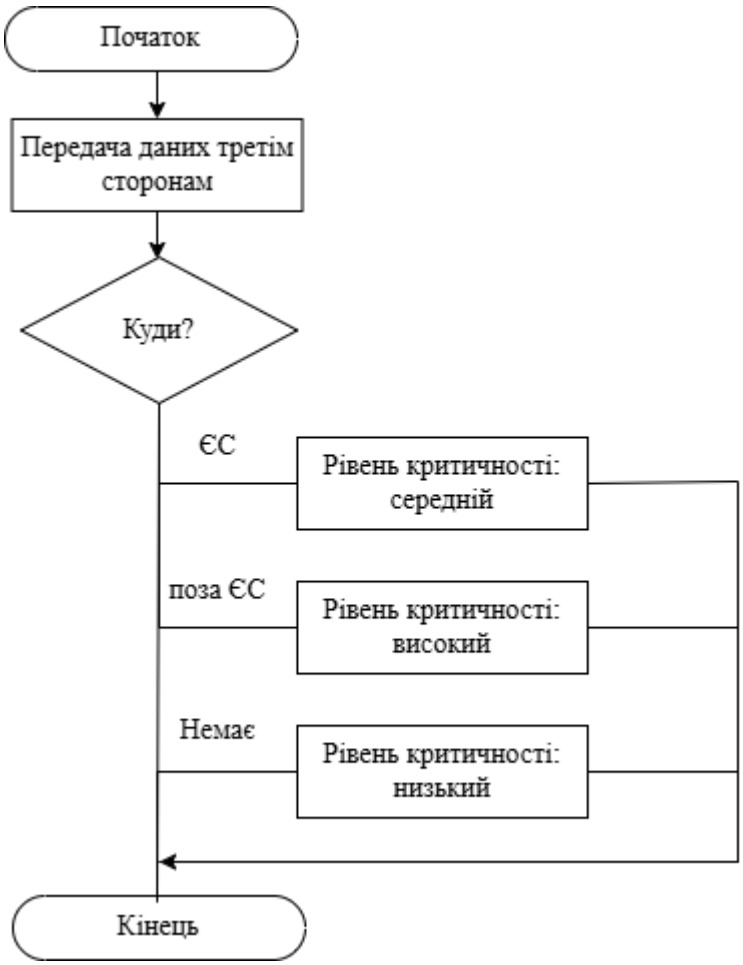


Рисунок 2.3 - Визначення рівня критичності передачі особистих даних третім сторонам

Застосунок також збирає дані про планування проведення сайтом будь-яких фінансових операцій. Фінансові операції та фінансові дані користувачів потребують відповідного належного захисту, що також має бути передбачено політикою конфіденційності згідно загального регламенту захисту персональних даних (рис. 2.4).

Рисунок 2.4 - Визначення необхідності генерації положення про захист фінансових даних користувачів

Такий підхід не лише спрощує процес створення юридично релевантного контенту, але й підвищує якість взаємодії з користувачем, забезпечуючи персоніфікований супровід та зменшуючи ймовірність помилок. У результаті, засіб виступає ефективним інструментом підвищення кібербезпеки та забезпечення належного рівня захисту персональних даних на етапі впровадження політик конфіденційності.

Завдяки такій автоматизації власники вебсайтів отримують ефективний інструмент, що не лише економить час і ресурси, а й підвищує рівень кібербезпеки, забезпечуючи належний захист персональних даних. Це важливо не лише з погляду відповідності законодавству, а й для зміцнення довіри користувачів, адже прозорість у питанні обробки їхніх персональних даних є одним із ключових чинників сучасної цифрової етики.

2.2 Аналіз основних положень GDPR для кожного виду вебсайту

GDPR передбачає уніфікований підхід до захисту персональних даних, однак його практична реалізація потребує врахування особливостей

конкретного типу вебресурсу. Залежно від функціонального призначення сайту, категорій користувачів, які ним користуються, характеру зібраних даних і мети їх обробки, змінюються і вимоги до структури та змісту політики конфіденційності. Наприклад, інтернет-магазини обробляють не лише базові контактні дані, а й платіжну інформацію; освітні платформи можуть працювати з персональними даними неповнолітніх; корпоративні сайти зазвичай не збирають великі масиви даних, однак зобов'язані інформувати про використання форм зворотного зв'язку чи аналітики. Таким чином, створення універсального шаблону є малоефективним – натомість необхідний інструмент, здатний адаптувати положення GDPR до специфіки конкретного ресурсу [19].

Створений вебзастосунок для генерації основних положень GDPR дозволяє власникам бізнесу, підприємцям, програмістам, спеціалістам з інформаційної безпеки, юристам чи студентам та викладачам отримати саме той перелік вимог, який необхідний їм для конкретно їхнього продукту.

Застосунок дає можливість отримати положення для таких видів вебсайтів та сервісів:

- інтернет-магазини (E-commerce Sites);
- сайти соціальних мереж (Social Networking Sites);
- новинні сайти (News Websites);
- сайти компаній та корпорацій (Corporate Websites);
- блоги та інформаційні портали (Blogs & Information Portals);
- освітні платформи (Educational Platforms);
- медичні сайти та платформи для запису до лікаря (Medical Websites & Appointment Platforms);
- сайти пошуку роботи (Job Portals);
- платформи для бронювання (Booking Sites);
- форуми та дискусійні платформи (Discussion Forums);
- сайти зі збором донатів (Donation Platforms);

– рекламні платформи (Advertising Platforms);
– маркетплейси (Online Marketplaces);
– сайти особистих послуг (Personal Services Websites).

І хоча низка положень регламенту GDPR є універсальними та обов'язковими для всіх типів вебсайтів і онлайн-сервісів - наприклад, принципи прозорості, законності обробки даних чи дотримання прав суб'єктів персональних даних - окремі елементи політики конфіденційності все ж мають суттєві відмінності залежно від контексту. У деяких випадках певні положення набувають критичного значення з юридичної точки зору: наприклад, політика щодо cookies для сайтів, що використовують розгорнуту систему аналітики, або правила згоди на обробку даних для сервісів, орієнтованих на неповнолітню аудиторію. Водночас, інші положення - такі як чітке пояснення прав користувача або зрозуміле формулювання мети обробки - мають більше значення з точки зору довіри користувача до ресурсу та дотримання принципів цифрової етики. Саме тому грамотне структурування і персоналізація основних положень відповідно до виду вебресурсу є ключовою умовою ефективної реалізації політики конфіденційності, що поєднує юридичну силу з доступністю й прозорістю для аудиторії (табл. 2.1) [20].

Таблиця 2.1 – Вебсайти та основні положення GDPR для них

Тип вебсайту	Опис діяльності	Основні положення GDPR
Інтернет-магазини	Продають товари та послуги онлайн, збирають персональні дані для замовлень (ПІБ, адреси доставки, платіжні дані).	Прозорість щодо збору та обробки даних, явна згода на збереження платіжних даних, можливість видалення облікових записів, шифрування під час обробки платіжних даних.
Сайти соціальних мереж	Платформи для обміну інформацією, фото, відео, особистими повідомленнями між користувачами.	Забезпечення конфіденційності профілів, право користувачів на видалення даних (право на забуття), контроль над тим, хто може переглядати дані.
Новинні сайти	Платформи для публікації статей, новин та аналітики, збір даних користувачів через	Збір мінімальних даних для коментарів, явна згода на підписку на розсилки, політика конфіденційності щодо

Тип вебсайту	Опис діяльності	Основні положення GDPR
	підписку на розсилки або коментарі.	використання даних для аналітики.
Сайти компаній та корпорацій	Представницькі сайти для інформування клієнтів і партнерів про компанію, з можливістю контактів і запитів.	Прозорість щодо обробки контактної інформації, згода на отримання маркетингових матеріалів, право на доступ до персональних даних.
Блоги та інформаційні портали	Сайти для публікації статей, часто із можливістю коментарів та підписки.	Збір даних через коментарі та підписки, чітка політика щодо використання файлів cookie та інших технологій відстеження.
Освітні платформи	Сайти, що надають освітні матеріали, курси або сертифікацію, збирають дані студентів.	Збір лише необхідної інформації для навчання, забезпечення права на виправлення або видалення даних, забезпечення захищеності платіжних даних.
Сайти медичних послуг	Сайти для надання медичних послуг або інформації, включаючи записи на прийоми або обробку медичних даних.	Посилений захист персональних даних, обробка чутливої інформації тільки з явною згодою, право на видалення медичних записів.
Сайти пошуку роботи	Платформи для розміщення резюме та вакансій, де користувачі можуть передавати свої особисті дані для пошуку роботи.	Прозорість щодо того, як використовуються персональні дані кандидатів, забезпечення права на видалення або виправлення резюме.
Платформи для бронювання	Сайти для бронювання послуг, таких як готелі, квитки, тощо, які збирають дані для бронювання.	Обмежений доступ до персональних даних, шифрування під час передачі платіжних даних, явна згода на обробку особистої інформації для бронювання.
Форуми, а також дискусійні платформи	Сайти, що надають можливість користувачам обмінюватися думками, питаннями та відповідями.	Контроль за видимістю персональних даних у профілях, явна згода на обробку при реєстрації, можливість видалення профілю і даних.
Сайти зі збором донатів	Платформи для збору благодійних внесків або пожертв, де користувачі можуть залишати свої платіжні та контактні дані.	Захист персональних та платіжних даних, явна згода на обробку даних для збору пожертв, забезпечення права на відкликання згоди.
Рекламні платформи	Сайти для управління рекламними кампаніями, що збирають дані про користувачів для таргетування.	Чітка згода на використання даних для персоналізації реклами, забезпечення права на доступ до даних і відкликання згоди.
Маркетплейси	Платформи для продажу товарів та послуг від	Забезпечення прозорості щодо використання даних продавців та

Тип вебсайту	Опис діяльності	Основні положення GDPR
	різних продавців, що збирають дані як покупців, так і продавців.	покупців, зокрема у контексті аналітики, право на видалення облікових записів та платіжної інформації.
Сайти особистих послуг	Платформи для надання особистих послуг, таких як консультації, тренінги, коучинг, із збором контактної та платіжної інформації клієнтів.	Згода на обробку даних клієнтів, шифрування під час передачі платіжних даних, право на виправлення або видалення персональної інформації.

Аналіз основних типів вебресурсів, таких як інтернет-магазини, соціальні мережі, новинні портали, освітні платформи, медичні сайти та інші, дозволяє зробити важливий висновок про універсальність і водночас специфічність застосування положень Регламенту GDPR. Незалежно від функціонального призначення та сфери діяльності, кожен із цих сайтів оперує персональними даними користувачів, що вимагає ретельного дотримання вимог щодо їх збору, обробки, зберігання та захисту.

Водночас особливості обробки даних суттєво відрізняються залежно від типу платформи та характеру інформації, що збирається. Наприклад, інтернет-магазини перш за все зосереджені на забезпеченні безпеки платіжних даних і наданні користувачам контролю над їх обліковими записами, у той час як сайти соціальних мереж повинні акцентувати увагу на конфіденційності профілів та реалізації права на «забуття». Медичні та освітні платформи працюють із найбільш чутливою інформацією, що потребує підвищеного рівня захисту і суворого дотримання принципів явної згоди [21].

Комплексне впровадження положень GDPR у кожному конкретному випадку потребує не лише загальних знань і технічних рішень, а й адаптації політик конфіденційності під особливості конкретного виду вебсайту. У цьому контексті особливо корисними є автоматизовані інструменти, що допомагають власникам сайтів швидко і точно формувати основні положення щодо обробки персональних даних відповідно до вимог регламенту.

Однією з ключових переваг створеного сервісу є інтеграція норм українського законодавства у сфері захисту персональних даних. Зважаючи на те, що платформа орієнтована передусім на український ринок, важливо було забезпечити відповідність не лише європейському Регламенту GDPR, а й вимогам Закону України «Про захист персональних даних» [22]. У результаті користувачі отримують політики конфіденційності, які враховують особливості українського правового поля – зокрема, термінологію, порядок згоди суб'єкта даних, обов'язки володільця персональних даних та порядок реалізації прав користувача.

Це дозволяє користувачам платформи бути впевненими в тому, що підготовлена політика не лише підвищує рівень довіри з боку відвідувачів сайту, але й забезпечує юридичну коректність у випадках звернень контролюючих органів або можливих конфліктів. Особливо це актуально для сайтів, що працюють виключно на території України або обробляють дані громадян України. Таким чином, сервіс виконує подвійну роль — одночасно забезпечує відповідність міжнародним (GDPR) і національним (українське законодавство) стандартам, що робить його комплексним і релевантним інструментом для вітчизняних онлайн-проєктів.

Наявність вебресурсу, який автоматично генерує індивідуальні рекомендації та положення GDPR для різних типів сайтів, значно спрощує цей процес. Такий підхід дозволяє не лише економити час і зусилля при розробці політик конфіденційності, а й знижує ризики невідповідності нормативним вимогам, оскільки кожен тип сайту отримує адаптовані, актуальні та законодавчо обґрунтовані рекомендації.

Отже, застосування автоматизованих систем для формування політик GDPR є важливим кроком у підвищенні рівня захисту персональних даних, забезпеченні юридичної відповідності та створенні довіри користувачів, що сприяє ефективному та безпечному функціонуванню цифрових сервісів у різних сферах діяльності.

2.3 Врахування українського законодавства до генерації положень GDPR

У процесі розробки вебсервісу генерації політик конфіденційності особлива увага приділялася не лише забезпеченню відповідності положенням Загального регламенту про захист даних (GDPR), але й адаптації створених документів до правових реалій України. Адже вітчизняні компанії, вебсайти та онлайн-сервіси, що працюють на українському ринку, в першу чергу підпадають під юрисдикцію національного законодавства. Основним нормативним актом, який регламентує правила обробки та захисту персональних даних в Україні, є Закон України «Про захист персональних даних», прийнятий у 2010 році [23].

Цей закон закладає базові принципи обробки персональної інформації, включаючи законність, прозорість, цілеспрямованість збору даних, мінімізацію обсягу інформації, а також обов'язковість отримання згоди суб'єкта на обробку його персональних даних. Закон також гарантує фізичним особам низку прав: право знати про джерела збору інформації, право доступу до власних даних, право на уточнення або знищення неточних чи неправомірно зібраних даних, а також право відкликати свою згоду на обробку.

У межах вебзастосунку було реалізовано механізм, що дозволяє формувати політики конфіденційності, які враховують вимоги як GDPR, так і українського законодавства. Зокрема, до шаблонів політик було включено посилання на Закон України «Про захист персональних даних», уточнення прав суб'єктів даних згідно з українським законодавством, а також опис обов'язків володільця персональних даних відповідно до національних норм. Окрему увагу приділено специфіці згоди: якщо за GDPR вона має бути «вільно надана, конкретна, інформована і недвозначна», то Закон України деталізує механізми надання та відкликання згоди, включаючи можливість її

оформлення письмово або в електронній формі із застосуванням електронного підпису.

Включення положень українського закону в функціонал сервісу також дозволяє краще врахувати потреби малого і середнього бізнесу, що не має постійної юридичної підтримки, але прагне дотримуватися вимог чинного законодавства. Завдяки локалізованому підходу, користувачі можуть отримати не просто шаблон, а документ, який справді відповідає нормам права та інформує відвідувачів сайту про всі ключові аспекти обробки їхніх персональних даних.

Таким чином, розроблений застосунок не лише адаптується до стандартів Європейського Союзу, а й виступає актуальним і практичним інструментом для українських суб’єктів господарювання. Це наближає юридичну культуру українського цифрового простору до міжнародного рівня, водночас забезпечуючи відповідність національним нормам і сприяючи формуванню довіри з боку користувачів.

3 РЕАЛІЗАЦІЯ ЗАСОБУ ДЛЯ ФОРМУВАННЯ ПОЛІТИКИ GDPR

3.1 Обгрунтування вибору інструментів та середовища для реалізації засобу

Під час розробки програмного засобу для автоматизованого формування основних положень політики конфіденційності відповідно до вимог Загального регламенту про захист даних (GDPR) було здійснено ретельний вибір інструментів програмування та середовища розробки. Основна мета полягала у створенні зручного, ефективного та масштабованого рішення, яке забезпечує високу швидкодію, кросбраузерну сумісність, адаптивність до різних типів пристроїв, а також максимальну прозорість реалізованих процесів для кінцевого користувача.

Для структурування вмісту вебсторінок під час реалізації програмного засобу було використано мову розмітки HTML (HyperText Markup Language), яка є загальновизнаним стандартом для побудови каркасу вебресурсів. Саме HTML забезпечує основу будь-якого сучасного вебзастосунку, дозволяючи визначити ієрархічну структуру сторінки, впорядкувати елементи контенту, розмістити логічно взаємопов’язані блоки та забезпечити базову взаємодію з користувачем. Зокрема, за допомогою HTML реалізовано основну архітектуру сайту — від заголовків сторінок і описового тексту до інтерактивних елементів, таких як випадаючі списки вибору типу сайту та мови, кнопки підтвердження, блоки відображення згенерованої політики конфіденційності, а також навігаційні та службові елементи інтерфейсу [24].

HTML дає змогу створити семантично зрозумілу структуру, що покращує доступність контенту для користувачів, включаючи людей з обмеженими можливостями, а також забезпечує кращу індексацію сторінок у пошукових системах. Це особливо важливо у контексті прозорості інформаційної взаємодії, яка прямо стосується вимог GDPR — зокрема,

зобов’язання інформувати користувача про обробку його даних зрозумілою, прозорою мовою.

Оформлення візуального вигляду вебресурсу було реалізовано за допомогою каскадних таблиць стилів (CSS — Cascading Style Sheets). Цей інструмент дозволяє відокремити логіку представлення вмісту від його структурної частини, що, своєю чергою, значно спрощує подальший супровід, оновлення та розвиток вебпроєкту. За допомогою CSS були створені стилі, які відповідають вимогам сучасного вебдизайну — зокрема, було забезпечено зрозуміле та контрастне візуальне оформлення, зручне розташування елементів, легкість навігації та приємна кольорова палітра, яка не відволікає від головного — інформації про конфіденційність та права користувача [25].

Особлива увага приділялася адаптивності інтерфейсу, яка реалізована через медіазапити та гнучку систему сіток. Завдяки цьому вебресурс коректно відображається на екранах з різним розширенням: від великих моніторів до смартфонів. Це критично важливо з огляду на вимоги GDPR щодо забезпечення доступності інформації незалежно від технічних засобів користувача — політика конфіденційності повинна бути не лише юридично правильною, а й легкою для сприйняття на будь-якому пристрої.

Для реалізації логіки взаємодії між елементами сторінки, обробки вибору користувача, а також динамічного формування контенту політики конфіденційності була використана мова програмування JavaScript. Саме JavaScript дозволяє забезпечити гнучку логіку поведінки сторінки без необхідності взаємодії з сервером, що робить рішення більш автономним, швидким та зручним у використанні. Наприклад, обробка вибору типу сайту та мови відбувається миттєво, без перезавантаження сторінки, що позитивно впливає на досвід користувача [26].

JavaScript також дозволив реалізувати перевірки правильності введення, адаптивну генерацію тексту політики відповідно до заданих параметрів, а також забезпечити інтерактивність інтерфейсу.

У якості середовища розробки було обрано Visual Studio Code (VS Code) — потужний, легкий у використанні редактор коду з широкими можливостями розширення. Серед його основних переваг можна виділити:

- підтримку великої кількості мов програмування, включаючи HTML, CSS, JavaScript;
- розширення (плагіни), що автоматизують форматування коду, підсвічують синтаксис, допомагають у виявленні помилок;
- інтеграцію з системами контролю версій, такими як Git;
- вбудований термінал, що значно спрощує процес налагодження.

VS Code також має активну спільноту та велику кількість навчальних ресурсів, що значно скорочує час на пошук рішень у разі виникнення труднощів під час розробки [27].

Для перегляду та тестування вебзастосунку використовувався браузер Google Chrome, який було обрано через його надійність, популярність серед користувачів та підтримку всіх сучасних вебтехнологій. Важливою перевагою є наявність інструментів розробника (DevTools), які дозволяють швидко знаходити та виправляти помилки, перевіряти адаптивність верстки та налагоджувати роботу скриптів.

Альтернативним варіантом було використання фреймворків, таких як React або Vue.js, однак зважаючи на порівняно невелику складність логіки додатку та потребу в швидкому розгортанні рішення, було вирішено застосувати чистий JavaScript без додаткових бібліотек. Такий підхід дозволив зменшити обсяг коду, уникнути залежностей, а також забезпечити вищу швидкодію і простоту переносу/інтеграції на інші проєкти чи серверні платформи.

Таким чином, вибрані інструменти — HTML, CSS, JavaScript, середовище розробки Visual Studio Code та браузер Chrome для тестування — були обрані на основі принципів простоти, ефективності, масштабованості та орієнтованості на кінцевого користувача. Сукупне використання цих технологій дозволило створити інтуїтивно зрозумілий, динамічний та

функціональний вебінструмент, що не лише автоматизує створення політик конфіденційності згідно з GDPR, але й відповідає високим стандартам кібербезпеки та захисту персональних даних.

3.2 Програмна реалізація вебзастосунку

Ідеєю вебзастосунку є генерація основних положень GDPR для різних видів вебсайтів. Для початку користувачу необхідно пояснити основи GDPR, можливості його використання, для яких типів бізнесу він має застосовуватись та в чому різниця між положеннями в залежності від типу вебсайту, а також загальна інформація про санкції, які накладаються на організації в разі недотримання чи якимось чином ухилення від виконання політики конфіденційності GDPR.

Умовно сайт можна поділити на дві частини: теоретична та технічна (рис. 3.1).

Теоретична частина застосунку написана українською мовою для відкриття дверей до положень GDPR саме для українського бізнесу. Опис регламенту починається з відповіді на запитання «Що це?». Далі для кращої впевненості користувача сайт пропонує короткий опис типів бізнесу, які мають підпорядковуватись положенням GDPR, у разі оброки персональних даних громадян ЄС. Також, для заохочення власників бізнесу дотримуватись вимог регламенту вкінці теоретичної частини розміщений коротки опис типів санкцій для порушення положень регламеннту, особливо якщо ці порушення привели до витоку конфіденційних даних клієнтів бізнесу.

Друга частина застосунку – технічна чатина – це фактично набір запитань, на які користувач має відповісти, аби сайт міг «зрозуміти» які основні положення GDPR має дотримуватись саме його бізнес. Користувач має відповісти на 5 простих запитань: тип вебсайту, які конфіденційні дані клієнтів збираються, чи планується передача цих даних третім сторонам, чи

планується проведення будь-яких фінансових операцій та якою мовою генерувати положення регламенту (українка чи англійська).

Рисунок 3.1 – Структура застосунку

Кожне питання – це окремий блок, на якому користувач зобов’язаний вказати (обрати) один або декілька із запропонованих варіантів. Після кожного блоку користувач має натиснути кнопку «Продовжити» аби перейти до генерації самих положень.

```
<script>
        function goToStep(stepNumber) {
            // Приховуємо всі кроки
             const steps = document.querySelectorAll('.survey-
step');
             steps.forEach(step => {
                step.style.display = 'none';
            });

            // Показуємо потрібний крок
            const nextStep = document.getElementById('step' +
stepNumber);
            if (nextStep) {
                nextStep.style.display = 'block';
            }
        }
    </script>
```

Для генерації основних положень GDPR користувачу надано на вибір 14 видів бізнесу, для яких регламент буде дещо відрізнятись, враховуючи специфіку роботи бізнесу, збору необхідної інформації та особливостей потенційного клієнта. Вибір типу бізнесу був реалізований за допомогою випадаючого списку.

Для визначення рівня критичності захищеності персональних даних клієнтів бізнесу надано для обрання 8 типів персональних даних. Також варто зауважити, що для кожного бізнесу існує своя категорія клієнтських персональних даних, які мають бути обов’язково зібрані для належного функціонування системи.

Особлива увага має бути приділена сайтам у яких планується введення фінансових операцій, а також передача конфіденційних даних користувачів третім сторонам, особливо, якщо представники третьої сторони знаходяться за сежами Європейського союзу та мають повне право не підпорядковуватись GDPR. Для таких випадків система генерує окремі положення регламенту, які слід взяти до уваги.

Також для користувача був реалізований вибір мови для генерації основних положення GDPR. Застосунок дає можливість згенерувати основні положення GDPR як українською, так і англійською мовою.

```
 function generateBaseInfo(language) {
    const t = translations[language];
    return `
        <p><strong>${t.labels.dataSensitivity}:</strong>
${t.dataSensitivity[surveyData.dataSensitivity]}</p>
        <p><strong>${t.labels.dataTransferLevel}:</strong>
${t.dataTransferLevel[surveyData.dataTransferLevel]}</p>
        <p><strong>${t.labels.hasFinancialOperations}:</strong>
${t.hasFinancialOperations[surveyData.hasFinancialOperations]}</
p>
    `;
}
```

Генерація самої політики відбувається в декілька етапів (рис. 3.2).

На рисунку представлено алгоритм генерації, який фатично можна описати як збір усієї необхідної інформації для генерування основних положень GDPR, генерування самої політики та адаптація її під користувача.

При встановленні типів особистих даних клієнта, які можуть збиратись сайтом, обраховується рівень критичності захисту цих даних.

```
function goToStep(stepNumber) {
        document.querySelectorAll('.survey-step').forEach(step
=> step.style.display = 'none');
        document.getElementById(`step${stepNumber}`).style.displ
ay = 'block';

        // При переході з кроку 2 – обчислюємо критичність
        if (stepNumber === 3) {
            const checkboxes =
document.querySelectorAll('input[name="dataType"]:checked');
            let totalScore = 0;
            checkboxes.forEach(box => {
                totalScore += parseInt(box.value);
            });

            if (totalScore >= 0 && totalScore <= 2) {
                surveyData.dataSensitivity = 'low';
            } else if (totalScore >= 3 &&  totalScore <= 4) {
                surveyData.dataSensitivity = 'medium';
            } else if (totalScore >= 5) {
                surveyData.dataSensitivity = 'high';
            }
        }
```

```
}
```

Рисунок 3.2 – Алгоритм генерації основних положень GDPR

Також обраховується рівень критичності при передачі даних третім сторонам, особливо, якщо це відбувається не на території ЄС.

```
const transfer = document.getElementById('dataTransfer').value;
        if (transfer === 'no') {
            surveyData.dataTransferLevel = 'low';
        } else if (transfer === 'eu') {
            surveyData.dataTransferLevel = 'medium';
        } else if (transfer === 'other') {
            surveyData.dataTransferLevel = 'high';
        }
```

Для користувача продумана можливість завантаження основних положень регламенту у форматі pdf*. Для цього їм надаються контактні дані служби підтримки, куди вони можуть написати запит та отримати перелік положень в доступному та сприйнятному для читання вигляді.

```
<!-- Генерація текстового поля -->
    <div id="generated-text-container" style="display: none;">
        <div id="generated-text"></div>
        <div class="button-container">
            <button id="download-button" class="styled-
button">Download</button>
        </div>
    </div>
<script>
        document.getElementById("download-
button").addEventListener("click", function() {
            alert("To download the pdf* file contact our support
centre support@gmail.com");
        });
    </script>
```

За допомогою вище вказаних функцій, стилістики та алгоритмів було створено вебзастосунок, для генерації основних положень GDPR з урахуванням особливостей типу бізнесу, планування роботи бізнесу, зручної мови для впровадження політики, а ткож українського законодавства.

3.3 Тестування та приклад роботи вебзастосунку

На завершальному етапі розробки будь-якого веборієнтованого рішення особливої уваги заслуговує процес тестування – він дозволяє впевнитися у правильності реалованої логіки, коректному відображенні інтерфейсу та стабільності взаємодії з користувачем. У контексті створення вебзастосунку, що забезпечує формування політики конфіденційності згідно з вимогами GDPR, тестування є не лише технічним, а й юридично значущим процесом. Адже кожна помилка в інтерфейсі або логіці може призвести до некоректного відображення ключової інформації, що, у свою чергу, може спричинити порушення вимог Регламенту.

Проведення тестування дозволяє перевірити, наскільки вебресурс є інтуїтивно зрозумілим для користувача, чи всі блоки сторінки функціонують відповідно до призначення, а також чи забезпечено доступність і

читабельність основних елементів — таких як розділи «Що таке GDPR», «Сфери застосування», «Відповідальність за порушення» тощо. Крім цього, перевіряється відповідність зовнішнього вигляду сторінки обраному дизайну, з урахуванням адаптивності та кросбраузерності, що є важливим у забезпеченні доступу до політики конфіденційності з будь-якого пристрою.

Вебсайт створений в темних і світлих відтінках для підтримки сучасного і одночасно класичного стилю (рис.3.1 і 3.2).

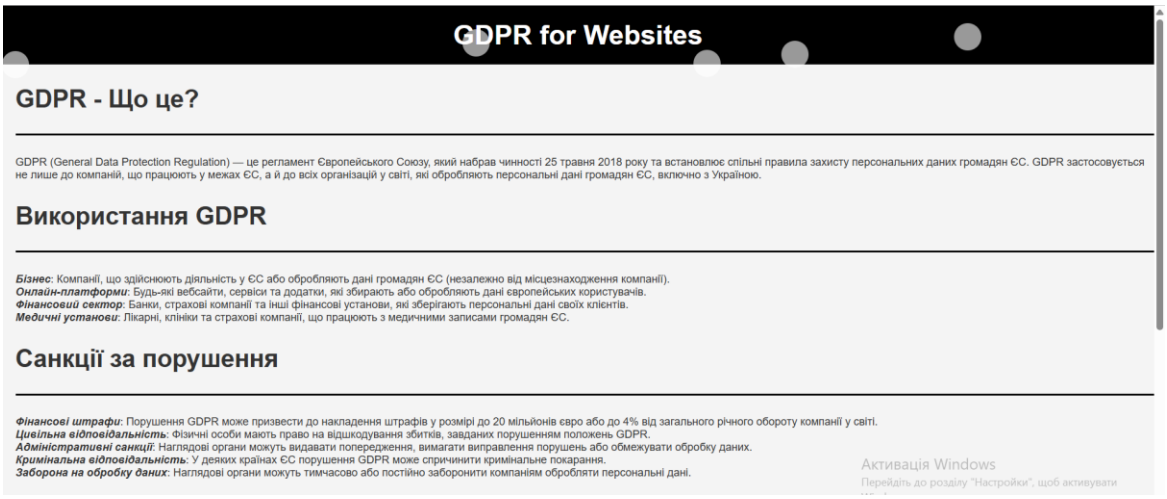


Рисунок 3.3 – Вигляд створеного застосунку, 1 частина

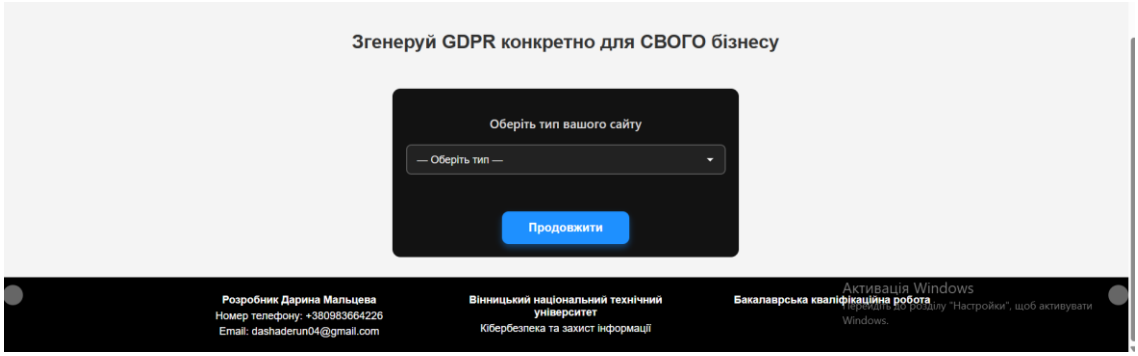


Рисунок 3.4 – Вигляд створеного застосунку, 2 частина

Однією з ключових функціональних можливостей реалізованого вебзастосунку є форма генерації основних положень політики конфіденційності відповідно до вимог GDPR, адаптованих під конкретний тип вебсайту. Для цього передбачено зручний випадаючий список, у якому користувач має змогу обрати тип ресурсу, до якого відноситься його сайт (рис. 3.5).

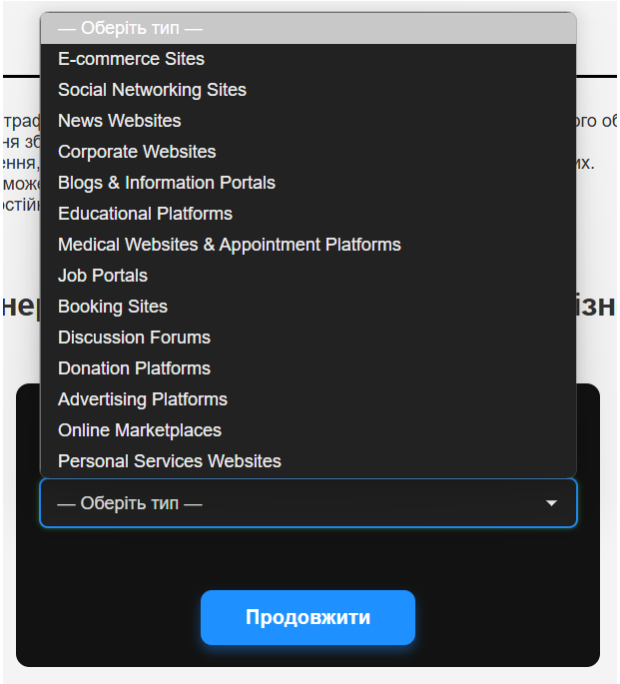


Рисунок 3.5 – Випадаючий список для вибору типу вебсайту

Наступним кроком користувачу необхідно обрати, які саме персональні дані його клієнтів будуть збиратись системою. Для цього реалізований select-box з типами конфіденційних даних та спеціалізованими даними для конкретного типу бізнесу (рис. 3.6).

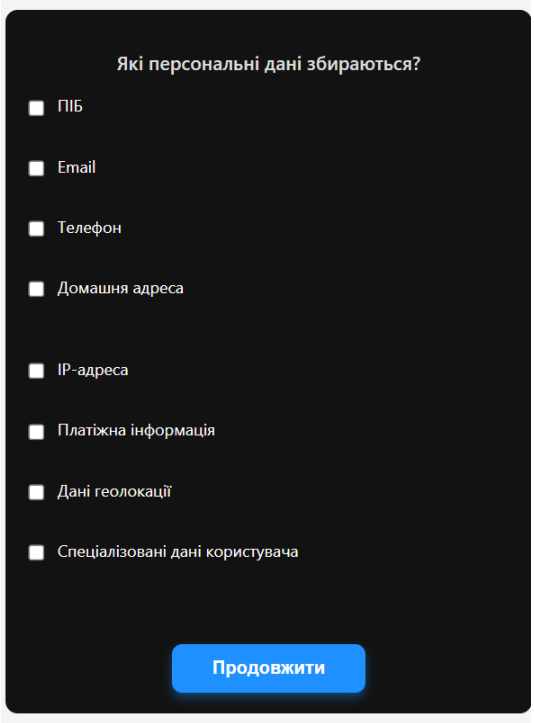


Рисунок 3.6 – Вибір типів персональних даних клієнта

Далі користувачу необхідно відповісти на запитання про передачу персональних даних його клієнта третім сторонам. Для цього реалізований зручний випадючий список з трьома пунктами для вибору (рис. 3.7)

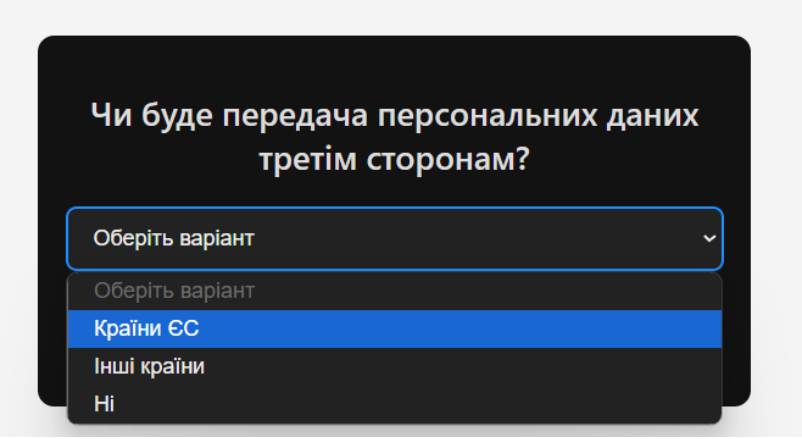


Рисунок 3.7 – Запит про передачу персональних даних третім сторонам

Після цього, система питає в користувача про наявність будь-яких фінансових операцій, адже від цього напрям залежить ступніь захищеності й платіжних даних клієнта. Це опитування також реалізовано зручним та зрозумілим випадаючим списком (рис. 3.8).

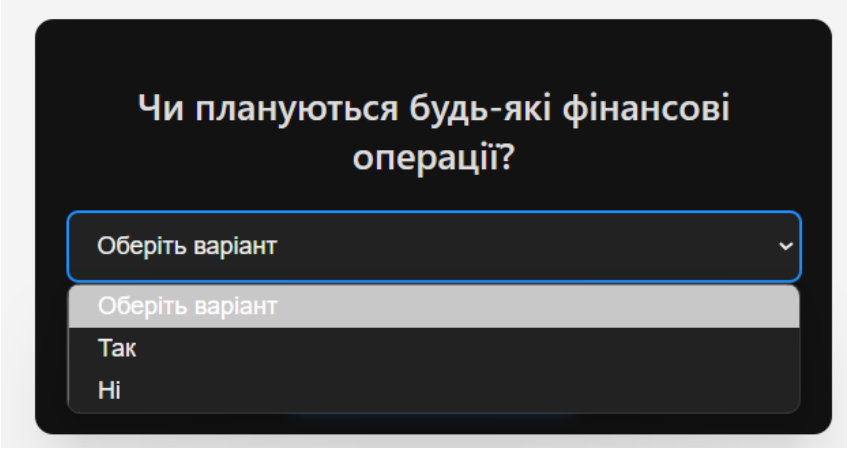


Рисунок 3.8 – Опитування про наявність будь-яких фінансових операцій

Закриває опитування вибір мови генерації положень. Застосунок пропонує згенерувати GDPR двома мовами – українськолю та англійською (рис. 3.9).

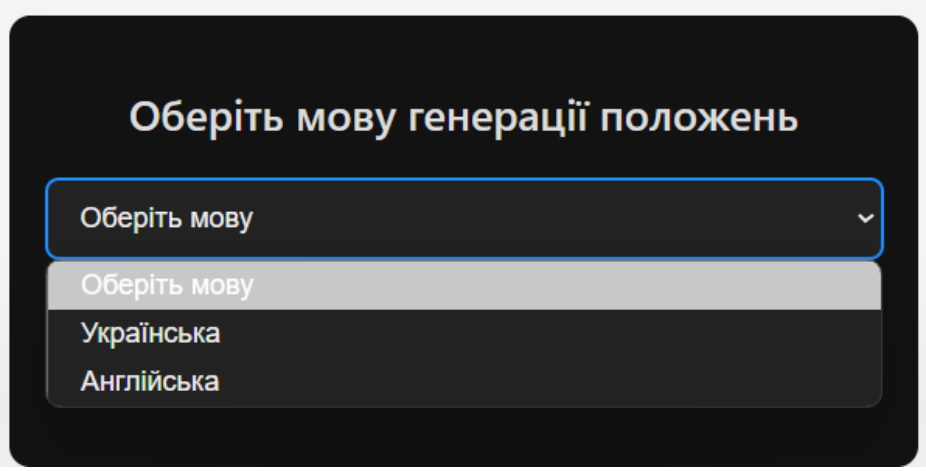


Рисунок 3.9 – Вибір мови для генерації основних положень GDPR

Після проведення опитування, користувачу пропонується натиснути на кнопку «Генерувати», після чого система починає підбір релевантних положень саме для цього типу бізнесу з усіма його вище вказаними особливостями (рис 3.10).

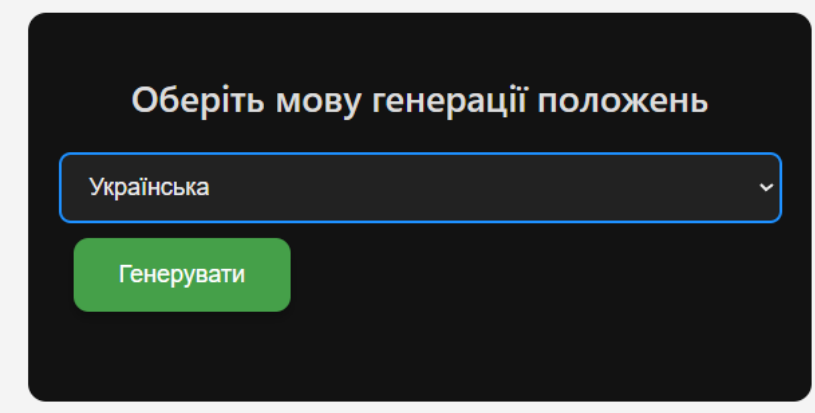
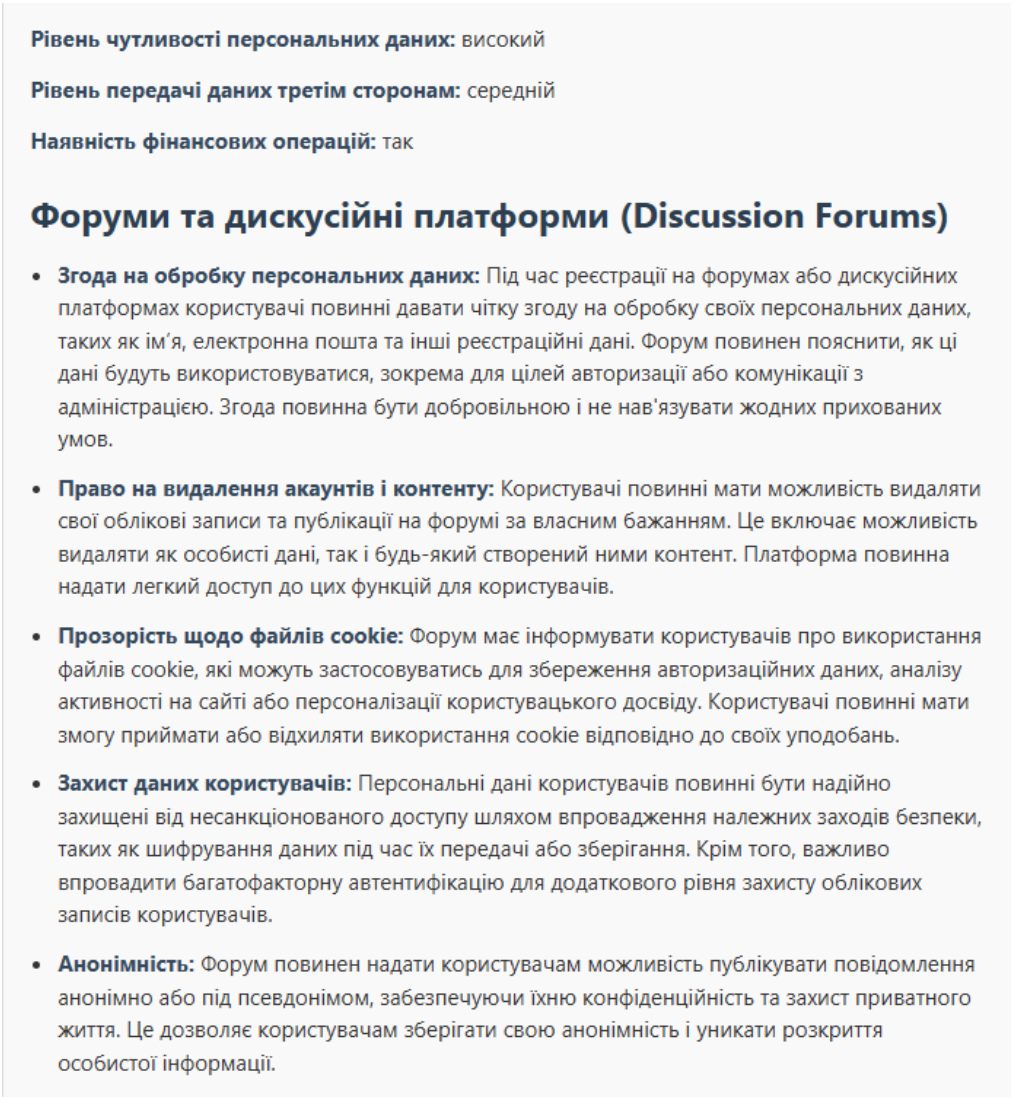


Рисунок 3.10 – Кнопка для генерації GDPR

Приклад згенерованого списку положень для «Форуми та дискусійні платформи» українською мовою (рис. 3.11 – 3.12).



Рівень чутливості персональних даних: високий

Рівень передачі даних третім сторонам: середній

Наявність фінансових операцій: так

Форуми та дискусійні платформи (Discussion Forums)

- **Згода на обробку персональних даних:** Під час реєстрації на форумах або дискусійних платформах користувачі повинні давати чітку згоду на обробку своїх персональних даних, таких як ім'я, електронна пошта та інші реєстраційні дані. Форум повинен пояснити, як ці дані будуть використовуватися, зокрема для цілей авторизації або комунікації з адміністрацією. Згода повинна бути добровільною і не нав'язувати жодних прихованих умов.
- **Право на видалення акаунтів і контенту:** Користувачі повинні мати можливість видаляти свої облікові записи та публікації на форумі за власним бажанням. Це включає можливість видаляти як особисті дані, так і будь-який створений ними контент. Платформа повинна надати легкий доступ до цих функцій для користувачів.
- **Прозорість щодо файлів cookie:** Форум має інформувати користувачів про використання файлів cookie, які можуть застосовуватись для збереження авторизаційних даних, аналізу активності на сайті або персоналізації користувацького досвіду. Користувачі повинні мати змогу приймати або відхиляти використання cookie відповідно до своїх уподобань.
- **Захист даних користувачів:** Персональні дані користувачів повинні бути надійно захищені від несанкціонованого доступу шляхом впровадження належних заходів безпеки, таких як шифрування даних під час їх передачі або зберігання. Крім того, важливо впровадити багатофакторну автентифікацію для додаткового рівня захисту облікових записів користувачів.
- **Анонімність:** Форум повинен надати користувачам можливість публікувати повідомлення анонімно або під псевдонімом, забезпечуючи їхню конфіденційність та захист приватного життя. Це дозволяє користувачам зберігати свою анонімність і уникати розкриття особистої інформації.

Рисунок 3.11 – Основні положення GDPR для «Форуми та дискусійні платформи» українською мовою (частина 1)

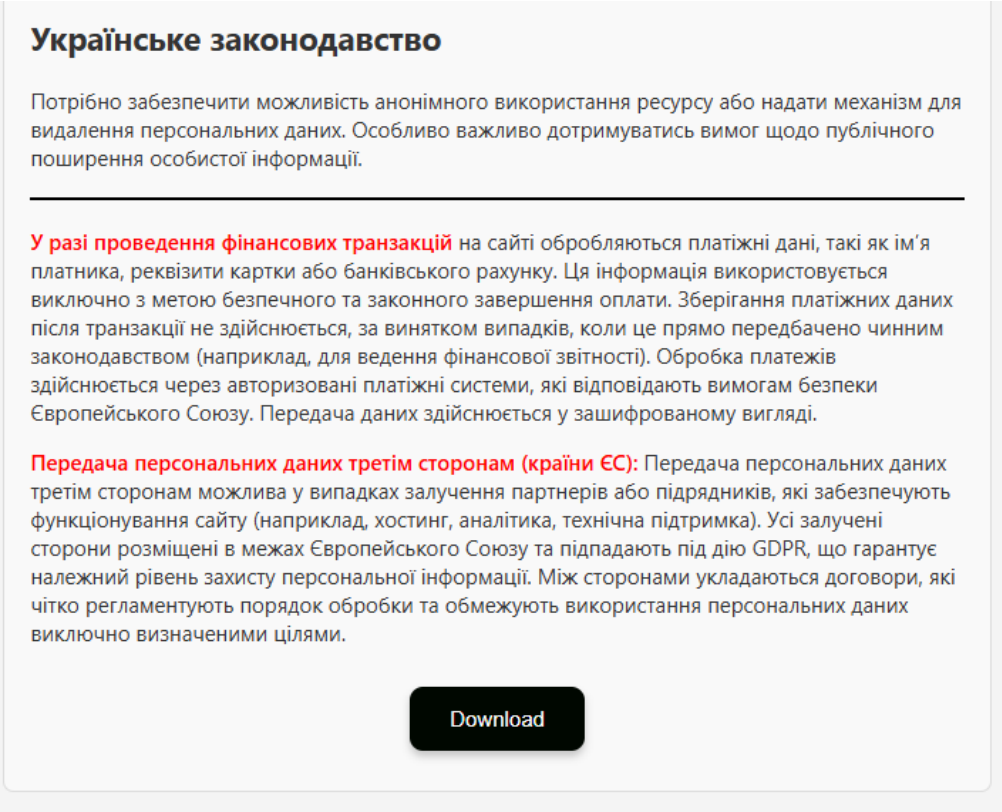
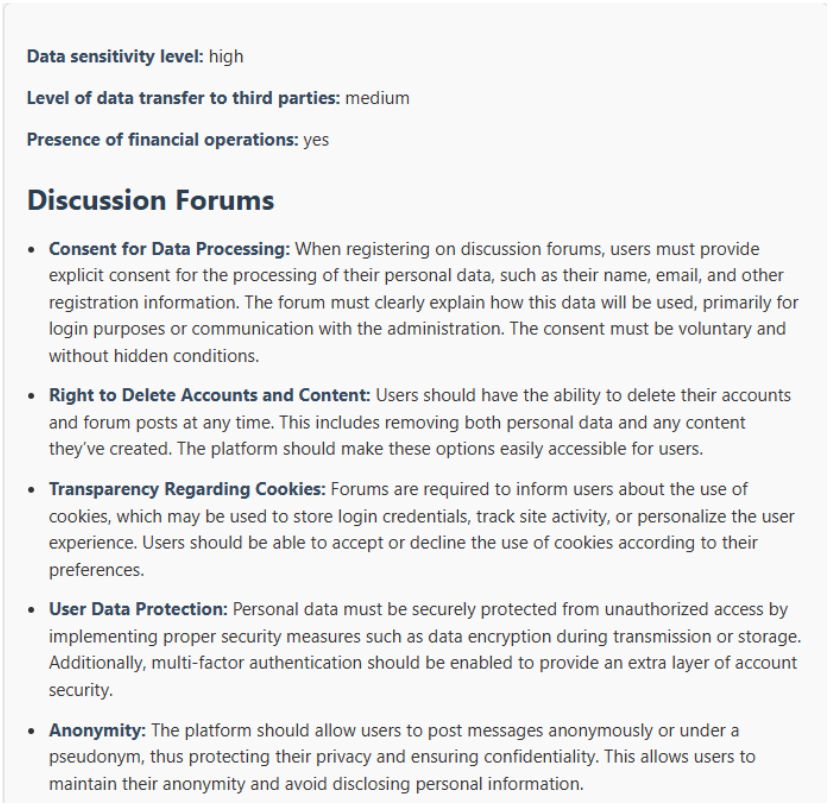


Рисунок 3.12 – Основні положення GDPR для «Форуми та дискусійні платформи» українською мовою (частина 2)

Можна побачити, що окрім GDPR система також додає декілька порад щодо дотримання українського законодавства, адже застосунок розрахований на український ринок для захисту конфіденційних даних громадян України.

Окремо від загальних правил, які слід дотримуватись система також дає поради стосовно проведення фінансових транзакцій (так як це було вище вказано користувачем), а також про передачу конфіденційних даних клієнта третім сторонам, які знаходяться на території Європейського союзу, адже ця особливість була попередньо також вказана користувачем. Варто зазначити, що яки персональні дані клієнта передавались за межі ЄС – система надала інші поради стосовно даних дій бізнесу.

Також було проведено тестування перекладу тексту на англійську мову (рис. 3.13 – 3.14).



Data sensitivity level: high

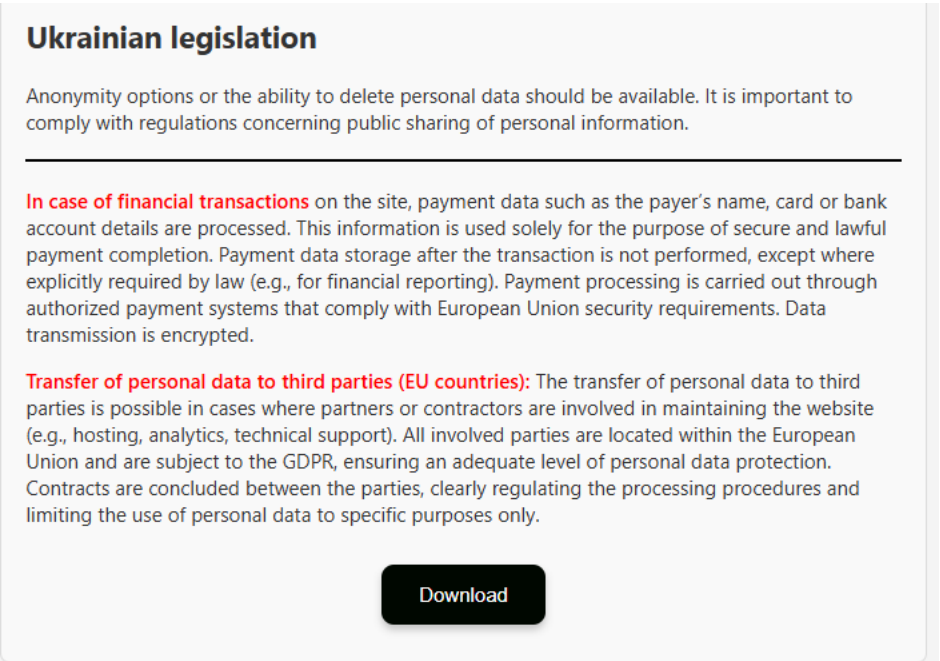
Level of data transfer to third parties: medium

Presence of financial operations: yes

Discussion Forums

- **Consent for Data Processing:** When registering on discussion forums, users must provide explicit consent for the processing of their personal data, such as their name, email, and other registration information. The forum must clearly explain how this data will be used, primarily for login purposes or communication with the administration. The consent must be voluntary and without hidden conditions.
- **Right to Delete Accounts and Content:** Users should have the ability to delete their accounts and forum posts at any time. This includes removing both personal data and any content they've created. The platform should make these options easily accessible for users.
- **Transparency Regarding Cookies:** Forums are required to inform users about the use of cookies, which may be used to store login credentials, track site activity, or personalize the user experience. Users should be able to accept or decline the use of cookies according to their preferences.
- **User Data Protection:** Personal data must be securely protected from unauthorized access by implementing proper security measures such as data encryption during transmission or storage. Additionally, multi-factor authentication should be enabled to provide an extra layer of account security.
- **Anonymity:** The platform should allow users to post messages anonymously or under a pseudonym, thus protecting their privacy and ensuring confidentiality. This allows users to maintain their anonymity and avoid disclosing personal information.

Рисунок 3.13 – Основні положення GDPR для «Форуми та дискусійні платформи» англійською мовою (частина 1)



Ukrainian legislation

Anonymity options or the ability to delete personal data should be available. It is important to comply with regulations concerning public sharing of personal information.

In case of financial transactions on the site, payment data such as the payer's name, card or bank account details are processed. This information is used solely for the purpose of secure and lawful payment completion. Payment data storage after the transaction is not performed, except where explicitly required by law (e.g., for financial reporting). Payment processing is carried out through authorized payment systems that comply with European Union security requirements. Data transmission is encrypted.

Transfer of personal data to third parties (EU countries): The transfer of personal data to third parties is possible in cases where partners or contractors are involved in maintaining the website (e.g., hosting, analytics, technical support). All involved parties are located within the European Union and are subject to the GDPR, ensuring an adequate level of personal data protection. Contracts are concluded between the parties, clearly regulating the processing procedures and limiting the use of personal data to specific purposes only.

Download

Рисунок 3.14 – Основні положення GDPR для «Форуми та дискусійні платформи» англійською мовою (частина 2)

Кнопка «Download», виконана в мінімалістичному стилі з чорним фоном і білим текстом, відіграє роль завершального етапу взаємодії користувача з вебзастосунком. Вона логічно завершує процес генерації адаптованого тексту політики конфіденційності відповідно до обраного типу сайту та мови (рис. 3.15).

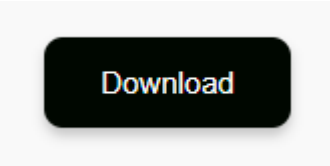


Рисунок 3.15 – Кнопка «Download»

При натисканні на кнопку Download користувач не отримує безпосереднього завантаження файлу. Натомість з’являється інформаційне повідомлення з інструкцією — для отримання політики конфіденційності у форматі pdf* необхідно зв’язатися з службою підтримки (рис. 3.16).

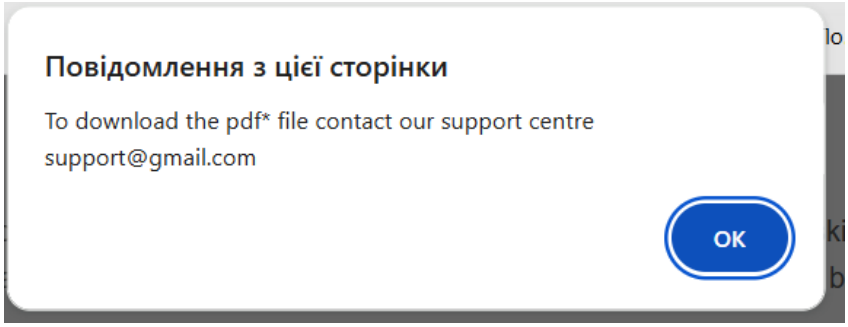


Рисунок 3.16 – Повідомлення про можливості завантаження pdf* файлу

3.4 Висновки до розділу

У результаті проведеного тестування вебзастосунку було підтверджено, що всі основні функції працюють коректно, а структура інтерфейсу відповідає принципам зручності та логічної побудови взаємодії з користувачем. Сайт має чітко виражену інформаційну частину, яка ознайомлює користувача з основними положеннями та важливістю регламенту GDPR. Цей вступний блок відіграє важливу роль у формуванні загального розуміння того, чому

дотримання політик конфіденційності є обов’язковим для сучасних вебресурсів.

Однією з ключових функціональних складових є можливість вибору типу вебсайту із заздалегідь підготовленого списку, який включає різні категорії, зокрема: e-commerce, соціальні мережі, новинні портали, медичні сайти, блоги, маркетплейси тощо. Такий підхід дозволяє врахувати специфіку кожного типу ресурсу та автоматизовано сформувати відповідні положення політики конфіденційності відповідно до вимог GDPR. Завдяки цьому користувач отримує персоналізований результат без необхідності глибокого занурення в юридичні нюанси регламенту.

Додатково реалізовано мовну адаптацію вебзастосунку, що дає змогу обрати мову інтерфейсу з випадного списку. Наразі підтримується, зокрема, українська мова, що є особливо важливим у контексті локалізації для українських користувачів та організацій, які прагнуть адаптувати свою діяльність відповідно до європейських норм захисту персональних даних. Багатомовність ресурсу підвищує його доступність та зручність використання для ширшої аудиторії.

Загалом, вебзастосунок демонструє ефективне поєднання інформативності, адаптивності та автоматизації процесу формування політик конфіденційності, що робить його корисним інструментом для власників різних типів онлайн-ресурсів, які прагнуть відповідати сучасним вимогам у сфері захисту персональних даних.

ВИСНОВКИ

У ході виконання бакалаврської кваліфікаційної роботи було всебічно досліджено правові, організаційні та технічні аспекти реалізації політик конфіденційності відповідно до вимог Загального регламенту про захист даних (GDPR), а також проведено порівняльний аналіз існуючих рішень у сфері автоматизації цього процесу. Основною метою роботи було створення зручного онлайн-сервісу, який би дозволяв генерувати GDPR-сумісні політики конфіденційності для різних типів вебресурсів з урахуванням актуальних потреб малого та середнього бізнесу, а також українських користувачів.

У першому розділі роботи було проаналізовано нормативно-правову базу у сфері захисту персональних даних, приділено увагу основним принципам та вимогам GDPR, зокрема правам суб’єктів даних, механізмам отримання згоди та зобов’язанням контролерів. Також були висвітлені актуальні виклики, що постають перед власниками вебсайтів при імплементації політик конфіденційності, включаючи складність формулювання юридично коректних текстів, багатомовність, а також необхідність адаптації до конкретного функціоналу вебресурсу.

Другий розділ був присвячений опису структури й функціоналу розробленого сервісу. Користувачі можуть обрати тип вебсайту, мову політики (українську або англійську) та отримати згенерований документ у форматі PDF. Інтерфейс платформи розроблено максимально доступним і зрозумілим, що дозволяє уникнути складнощів навіть недосвідченим користувачам. Особливою перевагою сервісу є підтримка української локалізації та врахування норм вітчизняного законодавства, зокрема Закону України «Про захист персональних даних», що підвищує його релевантність для українського бізнес-середовища.

У третьому розділі було представлено технічну реалізацію застосунку, описано обрані інструменти й технології, принципи архітектури, а також проведено базове тестування роботи сервісу. Наведено приклади генерації

політик для різних типів сайтів, протестовано процес вибору параметрів, створення тексту політики та формування кінцевого PDF-файлу. Результати тестування підтвердили стабільну та коректну роботу основного функціоналу, що свідчить про готовність сервісу до використання.

Порівняльна аналітика із провідними світовими сервісами, такими як Termly, Iubenda, PrivacyPolicies.com, засвідчила, що попри менший функціональний обсяг, створена платформа має вагомі переваги для своєї цільової аудиторії — простота використання, українська мова, адаптовані юридичні формулювання та можливість персональної консультації. Завдяки підтримці як європейського, так і українського законодавства, сервіс виступає практичним інструментом забезпечення правової відповідності онлайн-ресурсів та сприяє підвищенню рівня кібергігієни в національному інформаційному середовищі.

Отже, розроблений застосунок успішно вирішує поставлені у роботі завдання та має значний потенціал до подальшого розвитку. У перспективі можливим напрямом удосконалення є впровадження адаптивної генерації політик на основі складніших логік, інтеграція з популярними CMS-платформами, розширення підтримки на інші нормативні акти (зокрема DPA або CCPA), а також створення особистого кабінету для зберігання згенерованих документів і моніторингу змін законодавства. Таким чином, дипломна робота не лише має прикладну цінність, але й демонструє, як інструменти автоматизації можуть допомогти бізнесу дотримуватися законодавчих норм у сфері захисту персональних даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. J. Kaufmann, M. Schmidl, Baker& McKenzie. GDPR National Legislation Survey: Munich, 2017. 31c.

2. Diagrams constructor. URL: https://app.diagrams.net/ (дата звернення 18.05.2025)

3. Mind. GDPR працює: 7 принципів захисту даних інтернет-користувачів. URL: https://mind.ua/openmind/20256738-gdpr-pracyue-7-principiv-zahistu-danih-internet-koristuvachiv (дата звернення 19.05.2025)

4. Corewin. Права та вимоги запитів суб'єктів даних за GDPR. URL: https://corewin.ua/blog/how_can_netwrix_help_you_respond_to_gdpr_requests/ (дата звернення 19.05.2025)

5. Блохін, Максим Юрійович. "General data protection regulation (gdpr) як потенційне джерело вдосконалення вітчизняного законодавства у сфері захисту персональних даних." Часопис цивілістики 42 (2021): 44-48.

6. Legal Support. Privacy Policy | Політика Конфіденційності. URL: https://legal-support.top/politika-konfidencijnosti/ (дата звернення 19.05.2025)

7. GDPR Text. Стаття 82 GDPR. Право на відшкодування та відповідальність. URL: https://gdpr-text.com/uk/read/article-82/ (дата звернення 20.05.2025)

8. Юридична газета online. Найбільші штрафи за порушення норм GDPR. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vchimosya-na-pomilkah-naybilshi-shtrafi-za-porushennya-norm-gdpr.html (дата звернення 20.05.2025)

9. Webpromo. Порушення вимог GDPR: причини, наслідки та приклади. URL: https://web-promo.ua/ua/blog/porushennya-vimog-gdpr-prichini-naslidki-ta-prikladi/ (дата звернення 20.05.2025)

10. Webnauts. Регламент GDPR для захиту особистих даних. URL: https://webnauts.pro/uk/blog/reglament-gdpr-dlya-zahystu-osobystyh-danyh/ (дата звернення 20.05.2025)

11. Головацький, Назарій Тарасович. "Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України." (2024).

12. ScienceDirect. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. URL: https://www.sciencedirect.com/science/article/pii/S0167404821002261 (дата звернення 20.05.2025)

13. Termly. URL: https://termly.io/ (дата звернення 21.05.2025)

14. Iubenda. URL: https://www.iubenda.com/ (дата звернення 21.05.2025)

15. PrivacyPolicies. URL: https://www.privacypolicies.com/blog/gdpr/ (дата звернення 21.05.2025)

16. FreePrivacyPolicies. URL: https://www.freeprivacypolicy.com/ (дата звернення 21.05.2025)

17. GetTerms. URL: https://getterms.io/ (дата звернення 21.05.2025)

18. Ieee Xplore. Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. URL: https://ieeexplore.ieee.org/abstract/document/10540423 (дата звернення 21.05.2025)

19. Тугарова, Оксана Кузьмівна, and Тарас Ющук. "НАТІЛЬНІ ТЕХНОЛОГІЇ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІДПОВІДНО ДО НОРМ GDPR." The 1 st International scientific and practical conference “Modern problems of science, education and society”(March 26-28, 2023) SPC “Sci-conf. com. ua”, Kyiv, Ukraine. 2023. 1016 p.. 2023.

20. CQR. Загальні положення про захист даних (GDPR). URL: https://cqr.company/ua/wiki/compliance/general-data-protection-and-regulation-gdpr/ (дата звернення 22.05.2025)

21. Шепета, Олена Василівна, and Сергій Вікторович Мельник. "ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЗАСТОСУНКАХ ВІДСТЕЖЕННЯ ЗДОРОВ’Я MHEALTH ВІДПОВІДНО ДО НОРМ GDPR." The 6 th International

scientific and practical conference “Progressive research in the modern world”(March 2-4, 2023) BoScience Publisher, Boston, USA. 2023. 663 p.. 2023.

22. Верховна Рада України. Про захист персональних даних. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 03.06.2025)

23. Кульчій, І. О. GDPR: зміни режиму в законодавстві України про захист персональних даних. Diss. Національний університет" Полтавська політехніка імені Юрія Кондратюка", 2023.

24. CSS in UA. Довідник по HTML тегам. URL: https://css.in.ua/html/tags (дата звернення 30.05.2025)

25. CSS in UA. Довідник по CSS властивостям. URL: https://css.in.ua/css/propertiess (дата звернення 30.05.2025)

26. CSS in UA. Довідник по JavaScript. URL: https://css.in.ua/js/objects (дата звернення 30.05.2025)

27. Romul. Знайомство з Visual Studio Code. URL: https://romul.name/blog/znayomstvo-z-visual-studio-code/ (дата звернення 30.05.2025)

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Засіб для формування політики захисту даних вебсайту відповідно до GDPR

Автор роботи: Мальцева Дарина Вадимівна

Тип роботи: бакалаврська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ, група 1 БС-21б

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism **0,6** %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

√ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

Завідувач кафедри ЗІ д. т. н., проф. _____ Володимир ЛУЖЕЦЬКИЙ

Гарант освітньої програми «Безпека інформаційних та комунікаційних систем» к. т. н., доц. _____ Леонід КУПЕРШТЕЙН

Особа, відповідальна за перевірку _____ Валентина КАПЛУН

З висновком експертної комісії ознайомлений(-на)

Керівник _____ Олеся ВОЙТОВИЧ

Здобувач _____ Дарина МАЛЬЦЕВА

Додаток Б

Текст коду веб-застосунку

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>GDPR for Websites</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f4f4f4;
      color: #333;
      margin: 0;
    }
    .header {
      background-color: #000;
      color: white;
      text-align: center;
      padding: 20px 0;
      position: relative;
    }
    .header h1 {
      font-size: 2.5rem;
      margin: 0;
    }
    .header .circle {
      position: absolute;
      background-color: rgba(255, 255, 255, 0.6);
      width: 40px;
```

```
    height: 40px;
    border-radius: 50%;
}
.header .circle:nth-child(1) {
    top: 20%;
    left: 10%;
}
.header .circle:nth-child(2) {
    top: 40%;
    left: 40%;
}
.header .circle:nth-child(3) {
    top: 30%;
    right: 15%;
}
.header .circle:nth-child(4) {
    top: 60%;
    right: 30%;
}
.header .circle:nth-child(5) {
    top: 75%;
    left: 60%;
}
.subheader {
    margin: 30px 0;
    font-size: 1.5rem;
    text-align: left;
    padding-left: 20px;
}
hr {
```

```
    border: none;
    border-top: 3px solid black;
    margin: 20px 0;
}
.subheader-container {
    text-align: center;
    margin-top: 40px;
}
.subheader-title {
    font-size: 28px; /* Розмір шрифту */
    font-weight: bold;
    color: #333; /* Колір тексту */
    font-family: 'Arial', sans-serif;
    position: relative;
    display: inline-block;
}

.subheader-title:before {
    left: 0;
}
.subheader-title:after {
    right: 0;
}
.custom-select {
    width: 100%;
    padding: 12px;
    border-radius: 10px;
    border: 1px solid #ccc;
    background-color: #2c2c2c;
    color: #ffffff;
```

```
        font-size: 1em;
        margin-bottom: 25px;
        appearance: none;
        -webkit-appearance: none;
        -moz-appearance: none;
        background-image: url("data:image/svg+xml;charset=US-
ASCII,%3Csvg%20fill%3D'%23ffffff'%20height%3D'24'%20viewBox%3D'0%200%2024%2024'%20widt
h%3D'24'%20xmlns%3D'http%3A//www.w3.org/2000/svg'%3E%3Cpath%20d%3D'M7%2010l5%205
%205-5z'/%3E%3C/svg%3E");
        background-repeat: no-repeat;
        background-position-x: 98%;
        background-position-y: center;
    }
    .custom-select:focus {
        outline: none;
        border-color: #4caf50;
        box-shadow: 0 0 5px rgba(76, 175, 80, 0.5);
    }
    .continue-button {
        display: block;
        margin: 0 auto;
        padding: 12px 28px;
        font-size: 1em;
        background-color: #4caf50;
        border: none;
        border-radius: 30px;
        color: white;
        cursor: pointer;
        transition: background-color 0.3s ease;
    }
    .continue-button:hover {
```

```
    background-color: #45a049;
}
footer {
    background-color: #000;
    color: white;
    padding: 20px 0;
    display: flex;
    justify-content: center;
    align-items: center;
    flex-direction: column;
    position: relative;
}
.footer-content {
    display: flex;
    justify-content: space-around;
    width: 80%;
    max-width: 1200px;
}
.footer-column {
    text-align: center;
    width: 30%;
}
.footer-column p {
    margin: 5px 0;
}
.footer-column a {
    color: #fff;
    text-decoration: none;
}
```

```
.footer-column a:hover {
    text-decoration: underline;
}
.footer-circles {
    position: absolute;
    top: 10%;
    display: flex;
    justify-content: space-between;
    width: 100%;
}
.footer-circles .circle {
    background-color: rgba(255, 255, 255, 0.4);
    width: 30px;
    height: 30px;
    border-radius: 50%;
}
#generated-text-container {
    background-color: #f9f9f9; /* світлий фон */
    border: 1px solid #ddd;    /* тонка межа */
    padding: 20px;
    border-radius: 8px;
    max-width: 700px;
    margin: 20px auto;
    font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
    color: #333;
}
#generated-text-container h3 {
    color: #2c3e50;
    font-size: 1.6em;
    margin-bottom: 15px;
```

```
}
#generated-text-container ul {
    list-style-type: disc;
    padding-left: 20px;
}
#generated-text-container li {
    margin-bottom: 12px;
    line-height: 1.5;
}
#generated-text-container strong {
    color: #34495e;
}
.button-container {
    text-align: center;
    margin-top: 20px;
}
.styled-button {
    background-color: #000700;
    border: none;
    color: white; /* Білий текст */
    padding: 15px 30px; /* Відступи для кнопки */
    text-align: center;
    text-decoration: none;
    display: inline-block;
    font-size: 16px;
    margin: 10px;
    cursor: pointer;
    border-radius: 10px; /* Закруглені кути */
    box-shadow: 0 4px 6px rgba(0, 0, 0, 0.2); /* Легка тінь */
    transition: background-color 0.3s ease; /* Анімація при наведенні */
```

```
}
.styled-button:hover {
    background-color: #45a049; /* Трохи темніший відтінок при наведенні */
}
.survey-step {
    max-width: 480px;
    margin: 30px auto;
    padding: 20px;
    background: #121212;
    color: #fff;
    border-radius: 12px;
    box-shadow: 0 0 15px rgba(255, 255, 255, 0.1);
    font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
}
.survey-step h2, .survey-step h3 {
    margin-bottom: 20px;
    font-weight: 600;
    text-align: center;
    color: #ddd;
}
.red-start {
    color: red;
    font-weight: 600;
}
.custom-select, select {
    width: 100%;
    padding: 12px 15px;
    font-size: 16px;
    border-radius: 8px;
    border: 2px solid #555;
```

```
    background-color: #222;
    color: #eee;
    outline: none;
    cursor: pointer;
    transition: border-color 0.3s ease;
}
.custom-select:hover, select:hover,
.custom-select:focus, select:focus {
    border-color: #1e90ff;
}
label {
    display: block;
    margin: 8px 0;
    font-size: 16px;
    cursor: pointer;
    user-select: none;
}
input[type="checkbox"] {
    margin-right: 10px;
    transform: scale(1.2);
    vertical-align: middle;
    cursor: pointer;
}
.continue-button, .next-button {
    display: block;
    margin: 30px auto 0;
    background-color: #1e90ff;
    color: #fff;
    border: none;
    padding: 14px 40px;
```

```
            font-size: 18px;
            font-weight: 600;
            border-radius: 10px;
            cursor: pointer;
            transition: background-color 0.25s ease;
            box-shadow: 0 5px 10px rgba(30, 144, 255, 0.4);
        }
        .continue-button:hover, .next-button:hover {
            background-color: #0f68d1;
            box-shadow: 0 8px 15px rgba(15, 104, 209, 0.7);
        }
        .survey-step {
            margin-bottom: 30px;
        }
    </style>

</head>
<body>
    <div class="header">
        <h1>GDPR for Websites</h1>
        <div class="circle"></div>
        <div class="circle"></div>
        <div class="circle"></div>
        <div class="circle"></div>
        <div class="circle"></div>
    </div>

    <div class="subheader">
        <h2>GDPR - Що це?</h2>
        <hr>
```

```
</div>

<p style="padding-left: 20px;">
    GDPR (General Data Protection Regulation) — це регламент Європейського Союзу, який набрав чинності 25 травня 2018 року та встановлює спільні правила захисту персональних даних громадян ЄС. GDPR застосовується не лише до компаній, що працюють у межах ЄС, а й до всіх організацій у світі, які обробляють персональні дані громадян ЄС, включно з Україною.
</p>

<div class="subheader">
    <h2>Використання GDPR</h2>
    <hr>
</div>

<!-- Текст про використання GDPR -->
<p style="padding-left: 20px;">
    <strong><em>Бізнес</em></strong>: Компанії, що здійснюють діяльність у ЄС або обробляють дані громадян ЄС (незалежно від місцезнаходження компанії).<br>
    <strong><em>Онлайн-платформи</em></strong>: Будь-які вебсайти, сервіси та додатки, які збирають або обробляють дані європейських користувачів.<br>
    <strong><em>Фінансовий сектор</em></strong>: Банки, страхові компанії та інші фінансові установи, які зберігають персональні дані своїх клієнтів.<br>
    <strong><em>Медичні установи</em></strong>: Лікарні, клініки та страхові компанії, що працюють з медичними записами громадян ЄС.<br>
</p>

<div class="subheader">
    <h2>Санкції за порушення</h2>
    <hr>
</div>

<!-- Текст про відповідальність -->
```

```
  <p style="padding-left: 20px;">
    <strong><em>Фінансові штрафи</em></strong>: Порушення GDPR може призвести до накладення штрафів у розмірі до 20 мільйонів євро або до 4% від загального річного обороту компанії у світі.<br>
    <strong><em>Цивільна відповідальність</em></strong>: Фізичні особи мають право на відшкодування збитків, завданих порушенням положень GDPR.<br>
    <strong><em>Адміністративні санкції</em></strong>: Наглядові органи можуть видавати попередження, вимагати виправлення порушень або обмежувати обробку даних.<br>
    <strong><em>Кримінальна відповідальність</em></strong>:  У деяких країнах ЄС порушення GDPR може спричинити кримінальне покарання.<br>
    <strong><em>Заборона на обробку даних</em></strong>: Наглядові органи можуть тимчасово або постійно заборонити компаніям обробляти персональні дані.<br>
  </p>

  <div class="subheader-container">
    <h2 class="subheader-title">Згенеруй GDPR конкретно для СВОГО бізнесу</h2>
  </div>

  <!-- Крок 1: Тип вебсайту -->
<div id="step1" class="survey-step">
  <h3>Оберіть тип вашого сайту</h3>
  <select id="siteType" class="custom-select">
    <option disabled selected value="">— Оберіть тип —</option>
    <option value="ecommerce">E-commerce Sites</option>
    <option value="social">Social Networking Sites</option>
    <option value="news">News Websites</option>
    <option value="corporate">Corporate Websites</option>
    <option value="blogs">Blogs & Information Portals</option>
    <option value="education">Educational Platforms</option>
    <option value="medical">Medical Websites & Appointment Platforms</option>
    <option value="jobs">Job Portals</option>
```

```
      <option value="booking">Booking Sites</option>
      <option value="forums">Discussion Forums</option>
      <option value="donation">Donation Platforms</option>
      <option value="advertising">Advertising Platforms</option>
      <option value="marketplace">Online Marketplaces</option>
      <option value="services">Personal Services Websites</option>
   </select>

   <button class="continue-button" onclick="goToStep(2)">Продовжити</button>
</div>

<!-- Крок 2: Дані користувача -->
<div id="step2" class="survey-step" style="display:none;">
   <h3>Які персональні дані збираються?</h3>
   <label><input type="checkbox" name="dataType" value="1"> ПІБ</label><br>
   <label><input type="checkbox" name="dataType" value="2"> Email</label><br>
   <label><input type="checkbox" name="dataType" value="3"> Телефон</label><br>
   <label><input type="checkbox" name="dataType" value="4"> Домашня адреса</label><br><br>
   <label><input type="checkbox" name="dataType" value="5"> IP-адреса</label><br>
   <label><input type="checkbox" name="dataType" value="6"> Платіжна інформація</label><br>
   <label><input type="checkbox" name="dataType" value="7"> Дані геолокації</label><br>
   <label><input type="checkbox" name="dataType" value="8"> Спеціалізовані дані користувача</label><br><br>
   <button class="continue-button" onclick="goToStep(3)">Продовжити</button>
</div>

<!-- Крок 3: Передача даних третім сторонам -->
<div class="survey-step" id="step3" style="display: none;">
   <h2>Чи буде передача персональних даних третім сторонам?</h2>
```

```
    <select id="dataTransfer">
        <option value="" disabled selected>Оберіть варіант</option>
        <option value="eu">Країни ЄС</option>
        <option value="other">Інші країни</option>
        <option value="no">Ні</option>
    </select>
    <button class="continue-button" onclick="goToStep(4)">Продовжити</button>
</div>

<!-- Крок 4: Фінансові операції -->
<div class="survey-step" id="step4" style="display: none;">
    <h2>Чи плануються будь-які фінансові операції?</h2>
    <select id="financialOperations">
        <option value="" disabled selected>Оберіть варіант</option>
        <option value="yes">Так</option>
        <option value="no">Ні</option>
    </select>
    <button class="continue-button" onclick="goToStep(5)">Продовжити</button>
</div>

<!-- Крок 5: Вибір мови генерації -->
<div class="survey-step" id="step5" style="display: none;">
    <h2>Оберіть мову генерації положень</h2>
    <select id="languageSelect">
        <option value="" disabled selected>Оберіть мову</option>
        <option value="ukrainian">Українська</option>
        <option value="english">Англійська</option>
    </select>
    <button class="styled-button" onclick="submitSurvey()">Генерувати</button>
    <div id="result" class="generated-text" style="margin-top: 30px;"></div>
```

```
</div>

  <!-- Генерація текстового поля -->
<div id="generated-text-container" style="display: none;">
  <div id="generated-text"></div>
  <div class="button-container">
   <button id="download-button" class="styled-button">Download</button>
  </div>
</div>

  <footer>
    <div class="footer-content">
      <div class="footer-column">
        <p><strong>Розробник Дарина Мальцева</strong></p>
        <p>Номер телефону: <a href="tel:+380983664226">+380983664226</a></p>
        <p>Email: <a
href="mailto:dashaderun04@gmail.com">dashaderun04@gmail.com</a></p>
      </div>
      <div class="footer-column">
        <p><strong>Вінницький національний технічний університет</strong></p>
        <p>Кібербезпека та захист інформації</p>
      </div>
      <div class="footer-column">
        <p><strong>Бакалаврська кваліфікаційна робота</strong></p>
      </div>
    </div>
    <div class="footer-circles">
      <div class="circle"></div>
      <div class="circle"></div>
    </div>
```

```
</footer>

<script>
   function goToStep(stepNumber) {
      // Приховуємо всі кроки
       const steps = document.querySelectorAll('.survey-step');
       steps.forEach(step => {
         step.style.display = 'none';
      });

      // Показуємо потрібний крок
      const nextStep = document.getElementById('step' + stepNumber);
      if (nextStep) {
         nextStep.style.display = 'block';
      }
   }
</script>

<script>
const translations = {
   ukrainian: {
      dataSensitivity: {
         ow: 'низький',
         medium: 'середній',
         high: 'високий'
      },
      dataTransferLevel: {
         low: 'низький',
         medium: 'середній',
         high: 'високий'
```

```
    },
    hasFinancialOperations: {
      yes: 'так',
      no: 'ні'
    },
    labels: {
      dataSensitivity: 'Рівень чутливості персональних даних',
      dataTransferLevel: 'Рівень передачі даних третім сторонам',
      hasFinancialOperations: 'Наявність фінансових операцій'
    }
  },
  english: {
    dataSensitivity: {
      low: 'low',
      medium: 'medium',
      high: 'high'
    },
    dataTransferLevel: {
      low: 'low',
      medium: 'medium',
      high: 'high'
    },
    hasFinancialOperations: {
      yes: 'yes',
      no: 'no'
    },
    labels: {
      dataSensitivity: 'Data sensitivity level',
      dataTransferLevel: 'Level of data transfer to third parties',
      hasFinancialOperations: 'Presence of financial operations'
```

```
        }
    }
};
  const surveyData = {
    siteType: '',
    dataSensitivity: '',
    dataTransferLevel: '',
    hasFinancialOperations: '',
    language: ''
  };

  function goToStep(stepNumber) {
    document.querySelectorAll('.survey-step').forEach(step => step.style.display = 'none');
    document.getElementById(`step${stepNumber}`).style.display = 'block';

    // При переході з кроку 2 – обчислюємо критичність
    if (stepNumber === 3) {
      const checkboxes = document.querySelectorAll('input[name="dataType"]:checked');
      let totalScore = 0;
      checkboxes.forEach(box => {
        totalScore += parseInt(box.value);
      });

      if (totalScore >= 0 && totalScore <= 2) {
        surveyData.dataSensitivity = 'low';
      } else if (totalScore >= 3 &&  totalScore <= 4) {
        surveyData.dataSensitivity = 'medium';
      } else if (totalScore >= 5) {
        surveyData.dataSensitivity = 'high';
      }
```

```
    }
  }

  function generateBaseInfo(language) {
  const t = translations[language];
  return `
    <p><strong>${t.labels.dataSensitivity}:</strong>
${t.dataSensitivity[surveyData.dataSensitivity]}</p>
    <p><strong>${t.labels.dataTransferLevel}:</strong>
${t.dataTransferLevel[surveyData.dataTransferLevel]}</p>
    <p><strong>${t.labels.hasFinancialOperations}:</strong>
${t.hasFinancialOperations[surveyData.hasFinancialOperations]}</p>
  `;
}

  function submitSurvey() {
    // Крок 1
    const siteType = document.getElementById('siteType').value;
    surveyData.siteType = siteType;

    // Крок 3
    const transfer = document.getElementById('dataTransfer').value;
    if (transfer === 'no') {
      surveyData.dataTransferLevel = 'low';
    } else if (transfer === 'eu') {
      surveyData.dataTransferLevel = 'medium';
    } else if (transfer === 'other') {
      surveyData.dataTransferLevel = 'high';
    }

    // Крок 4
```

```
const finOps = document.getElementById('financialOperations').value;
surveyData.hasFinancialOperations = finOps;

// Крок 5
const language = document.getElementById('languageSelect').value;
surveyData.language = language;

let baseInfo = '';
let detailedPolicy = '';

// Тут підставляється додатковий блок з відповідями:
baseInfo = generateBaseInfo(language);

// Показ тексту
const financialNoteUa = `
  <p>
  <span class="red-start">У разі проведення фінансових транзакцій</span> на сайті обробляються платіжні дані, такі як ім’я платника, реквізити картки або банківського рахунку. Ця інформація використовується виключно з метою безпечного та законного завершення оплати. Зберігання платіжних даних після транзакції не здійснюється, за винятком випадків, коли це прямо передбачено чинним законодавством (наприклад, для ведення фінансової звітності).

  Обробка платежів здійснюється через авторизовані платіжні системи, які відповідають вимогам безпеки Європейського Союзу. Передача даних здійснюється у зашифрованому вигляді.

  </p>
`;
const financialNoteEn = `
  <p>
  <span class="red-start">In case of financial transactions</span> on the site, payment data such as the payer’s name, card or bank account details are processed. This information is used solely for the purpose of secure and lawful payment completion. Payment data storage after the transaction is not performed, except where explicitly required by law (e.g., for financial reporting).
```

Payment processing is carried out through authorized payment systems that comply with European Union security requirements. Data transmission is encrypted.

`;

const dataTransferEuUa = `

Передача персональних даних третім сторонам (країни ЄС):

Передача персональних даних третім сторонам можлива у випадках залучення партнерів або підрядників, які забезпечують функціонування сайту (наприклад, хостинг, аналітика, технічна підтримка). Усі залучені сторони розміщені в межах Європейського Союзу та підпадають під дію GDPR, що гарантує належний рівень захисту персональної інформації. Між сторонами укладаються договори, які чітко регламентують порядок обробки та обмежують використання персональних даних виключно визначеними цілями.

`;

const dataTransferNonEuUa = `

У разі передачі персональних даних за межі ЄС:

У разі потреби передати персональні дані організаціям, розташованим за межами Європейського Союзу, така передача здійснюється лише за наявності належних правових гарантій. Це можуть бути рішення Європейської Комісії про адекватний рівень захисту, стандартні договірні положення або інші правові механізми, передбачені GDPR.

У разі відсутності вказаних гарантій передача можлива лише після отримання чітко вираженої згоди суб’єкта даних з попереднім інформуванням про потенційні ризики.

`;

const dataTransferEuEn = `

Transfer of personal data to third parties (EU countries):

The transfer of personal data to third parties is possible in cases where partners or contractors are involved in maintaining the website (e.g., hosting, analytics, technical support). All involved parties are located within the European Union and are subject to the GDPR, ensuring an adequate level of personal data protection. Contracts are concluded

between the parties, clearly regulating the processing procedures and limiting the use of personal data to specific purposes only.

`;

const dataTransferNonEuEn = `

In case of transfer of personal data outside the EU:

If it is necessary to transfer personal data to organizations located outside the European Union, such transfer is carried out only with appropriate legal safeguards. These may include an adequacy decision by the European Commission, standard contractual clauses, or other legal mechanisms under the GDPR.

If such guarantees are absent, the transfer is only possible after obtaining the data subject's explicit consent, with prior information on potential risks.

`;

if (siteType === 'ecommerce' && language === 'ukrainian') {

detailedPolicy = `

<h3>Інтернет-магазини (E-commerce Sites)</h3>

Прозорість обробки даних: Інтернет-магазин повинен чітко інформувати користувачів про те, які саме персональні дані збираються під час використання платформи. Це включає в себе дані, необхідні для обробки замовлень, оплат, доставки, а також для поліпшення користувацького досвіду. Важливо, щоб користувачі розуміли, як їхні дані будуть використовуватися, на який термін вони будуть зберігатися, і хто саме буде мати до них доступ. Усі етапи збору та обробки повинні бути прозорими та зрозумілими для кінцевих користувачів.

Згода на обробку платіжних даних: При здійсненні платіжних операцій користувачі повинні надавати явну згоду на обробку своїх платіжних даних, таких як банківські реквізити, платіжні картки та інші фінансові дані. Ці дані мають бути використані виключно для виконання конкретного замовлення або для надання певних послуг, і не можуть бути використані для інших цілей без додаткової згоди. Всі платіжні операції повинні бути захищені на всіх етапах процесу з використанням надійних механізмів шифрування.

Право на забуття: Користувачі Інтернет-магазинів повинні мати можливість безперешкодно вимагати видалення своїх персональних даних, включаючи історію покупок, платіжні реквізити та іншу інформацію, що була зібрана під час взаємодії з сайтом. Це право, яке гарантує користувачам, що їхні дані не

зберігатимуться без їхньої згоди після завершення покупки або іншої операції, для якої ці дані були надані.

Шифрування даних: Для забезпечення безпеки персональних даних, зокрема платіжної інформації, всі транзакції та дані користувачів повинні бути захищені за допомогою сучасних методів шифрування під час їхньої передачі через Інтернет. Це гарантує, що дані користувачів не будуть доступні третім особам, і допомагає зберігати довіру клієнтів до платформи.

Мінімізація збору даних: Інтернет-магазин має дотримуватись принципу мінімізації збору даних, що означає збір тільки тих даних, які необхідні для виконання конкретних операцій, наприклад, адреса доставки, платіжні реквізити та контактна інформація. Збір додаткових або зайвих даних повинен бути обмежений або взагалі виключений.

Cookies та інші технології відстеження: Інтернет-магазини повинні отримувати явну згоду користувачів на використання файлів cookie або інших технологій відстеження для збору даних про поведінку користувача на сайті. Якщо ці технології не є критично необхідними для роботи платформи, їх використання повинно бути чітко роз'яснене, і користувачі повинні мати можливість налаштувати або відмовитися від їх використання.

<h2>Українське законодавство</h2>

Необхідно дотримуватись вимог Закону України «Про захист персональних даних» щодо отримання згоди на обробку даних, а також враховувати положення Закону «Про електронну комерцію». Слід чітко визначити мету збору персональної та платіжної інформації та забезпечити її належний захист.

<hr>

`;

} else if (siteType === 'ecommerce' && language === 'english') {

detailedPolicy = `

<h3>E-commerce Sites</h3>

Transparency in data processing: E-commerce sites must clearly inform users about the personal data they collect, how it will be used (for payments, deliveries, etc.), and how long it will be stored. This information must be provided in a clear and understandable manner, ensuring that users know exactly how their data will be processed and by whom. Full transparency regarding the purpose, collection, and usage of personal data is essential.

Consent for processing payment data: When processing payment data, explicit consent must be obtained from users. This includes information like credit card details, bank account numbers, and other financial data. Such data should only be used for fulfilling a specific order or providing a service, and not for any other purposes without further consent. All payment transactions must be secured using reliable encryption methods.

Right to be forgotten: Users must have the right to request the deletion of their account, along with any personal data stored on the site, including order history, payment details, and any other information provided during interactions with the platform. This ensures that users can control their data and have it removed once it is no longer necessary for fulfilling the transaction.

Data encryption: To ensure the security of personal data, especially payment information, all transactions and user data must be encrypted during transmission over the Internet. This guarantees that the data remains confidential and cannot be accessed by unauthorized third parties, providing users with the confidence that their information is protected.

Data minimization: E-commerce sites should collect only the data that is necessary for completing an order, such as delivery address, payment details, and contact information. The collection of excessive or unnecessary data should be avoided, and only essential information should be gathered for the purpose of fulfilling the order.

Cookies and other tracking technologies: E-commerce platforms must obtain explicit consent from users for the use of cookies and other tracking technologies that collect data on user behavior. If these technologies are not essential for the functionality of the site, users must be clearly informed and given the option to accept or reject their use.

<h2>Ukrainian legislation</h2>

Compliance with the Law of Ukraine "On Personal Data Protection" is required, particularly regarding the collection and processing of personal and payment information. The Law "On Electronic Commerce" should also be considered. It is important to clearly state the purpose of data collection and ensure adequate security measures.

<hr>

`;

} else if (siteType === 'social' && language === 'ukrainian') {

detailedPolicy = `

<h3>Сайти соціальних мереж (Social Networking Sites)</h3>

Захист конфіденційності профілів: Соціальні мережі повинні забезпечувати можливість для користувачів самостійно керувати рівнем конфіденційності свого профілю. Це включає опції вибору, хто саме має доступ до їхньої особистої інформації — будь то публіка, лише друзі або конкретні особи. Користувачі повинні мати змогу налаштовувати параметри конфіденційності, щоб обмежувати доступ до свого контенту, фотографій, дописів та іншої особистої інформації. Це важливий аспект захисту даних і приватного життя у рамках використання соціальних платформ.

Згода на обробку особистих даних: Всі дані, що збираються в процесі реєстрації або використання платформи, повинні бути оброблені лише після надання користувачем явної та чіткої згоди. Це стосується як основної інформації профілю, так і таких елементів, як фотографії, геолокаційні дані, повідомлення та інші особисті дані. Соціальна мережа повинна детально пояснити користувачам, для яких цілей використовуються їхні дані, і забезпечити можливість надання згоди на кожен окремий вид обробки.

Право на видалення даних: Користувачі повинні мати можливість видалити свій профіль разом із усією інформацією, яку вони надавали на платформі, включаючи фотографії, публікації, коментарі та інші особисті дані. Це право, закріплене в GDPR, дає можливість користувачам контролювати свої особисті дані та забезпечує їх повне видалення з системи, якщо користувач більше не хоче бути присутнім на платформі або використовувати її.

Аудит безпеки: Соціальні мережі повинні проводити регулярні аудити безпеки для виявлення та усунення вразливостей, які можуть призвести до несанкціонованого доступу до персональних даних користувачів. Це включає перевірку захищеності баз даних, систем доступу, захисту від хакерських атак та інших потенційних загроз. Аудити безпеки мають бути документованими, а результати — використовуватися для постійного вдосконалення захисту.

Захист від зловживань: Платформи повинні впроваджувати механізми для швидкого звітування про порушення конфіденційності або зловживання. Користувачі мають легко знаходити ці механізми і використовувати їх для повідомлення про підозрілу або шкідливу діяльність. Це допоможе швидко реагувати на потенційні загрози і захищати як окремих користувачів, так і цілі спільноти від неправомірного використання їхніх даних.

<h2>Українське законодавство</h2>

<p>

Слід враховувати особливості обробки персональних даних великого обсягу та чутливої інформації. Важливо надати користувачам можливість самостійно керувати своїми даними (редагування, видалення) відповідно до Закону України «Про захист персональних даних».

```
            </p>
            <hr>
        `;
    } else if (siteType === 'social' && language === 'english') {
        detailedPolicy = `
            <h3>Social Networking Sites</h3>
            <ul>
                <li><strong>Profile Privacy Protection:</strong> Social networks must provide users with the ability to control the visibility of their profiles. This includes settings to make profiles public, private, or visible only to specific individuals. Users should be able to customize their privacy settings to limit access to personal content such as photos, posts, and other personal information. This ensures that individuals maintain control over their personal data and the exposure of their online presence.</li>
                <li><strong>Consent for Personal Data Processing:</strong> All personal data collected during the registration and use of the social network must be processed only after obtaining explicit consent from the user. This includes profile information, photos, geolocation data, messages, and other personal details. The social platform must clearly explain to users the purposes for which their data will be used and allow them to provide consent for each specific type of data processing.</li>
                <li><strong>Right to Data Erasure:</strong> Users must have the ability to delete their profile, along with all the personal information they have shared on the platform, including photos, posts, comments, and other data. This right ensures that users can control their personal data and have it fully removed from the system if they no longer wish to participate or use the platform. It empowers users to safeguard their digital footprint.</li>
                <li><strong>Regular Security Audits:</strong> Social networks must perform regular security audits to identify and eliminate vulnerabilities that could lead to unauthorized access to user data. These audits should include assessments of database protection, access control systems, defense against hacking attempts, and other potential security risks. Documented audits help ensure ongoing improvements in the security measures protecting user data.</li>
                <li><strong>Protection Against Abuse:</strong> Platforms must implement mechanisms that allow users to easily report privacy violations or instances of misuse. These mechanisms should be user-friendly and accessible, enabling quick responses to suspicious or harmful activities. This helps protect individual users and entire communities from data misuse and unauthorized activities.</li>
            </ul>
            <h2>Ukrainian legislation</h2>
            <p>
```

Special attention must be given to the processing of large volumes of personal and sensitive data. Users should be granted control over their data (editing, deletion) in accordance with the Law of Ukraine "On Personal Data Protection".

</p>

<hr>

`;

} else if (siteType === 'news' && language === 'ukrainian') {

detailedPolicy = `

<h3>Новинні сайти (News Websites)</h3>

Збір мінімальних даних для коментарів: Якщо новинний сайт дозволяє коментарі під статтями, він повинен обмежити збір персональних даних до мінімуму. Наприклад, сайт може збирати лише ім’я користувача та електронну пошту, необхідні для ідентифікації коментатора. Важливо, щоб новинний ресурс мав чітку політику конфіденційності, яка пояснює, як використовуються ці дані, як довго вони зберігаються, та які права мають користувачі щодо обробки їхніх даних. Ця політика має бути доступною на сайті, а користувачі повинні бути ознайомлені з нею перед додаванням коментарів.

Згода на підписку на розсилки: У разі, якщо новинний сайт пропонує підписку на інформаційні розсилки, важливо отримати явну згоду користувачів на використання їхніх електронних адрес для цього. Розсилка новин або будь-якої іншої маркетингової інформації без прямої згоди користувачів є порушенням GDPR. При оформленні підписки повинні використовуватися методи подвійної підтвердження (double opt-in), щоб упевнитись, що користувач дійсно бажає отримувати листи. Користувачі також повинні мати можливість легко відписатися від розсилки в будь-який момент.

Право на доступ до даних: Відповідно до GDPR, користувачі повинні мати право отримати доступ до персональних даних, які зберігає новинний сайт. Це може включати дані реєстрації, історію коментарів, підписки на розсилки та іншу персональну інформацію. Новинний сайт повинен надати чіткі інструкції щодо того, як користувачі можуть звернутися за такою інформацією, а також виконати цей запит в установлені строки. Крім того, користувачі мають право вимагати виправлення або видалення своїх даних.

Політика щодо файлів cookie: Новинні сайти часто використовують файли cookie для збору даних про поведінку користувачів, аналізу трафіку, покращення роботи сайту та надання персоналізованої реклами. Відповідно до GDPR, сайти повинні чітко інформувати користувачів про використання файлів cookie. Перед тим, як розмістити будь-які файли cookie (окрім тих, що є необхідними для роботи сайту), потрібно отримати згоду від користувача. Політика щодо файлів cookie повинна містити детальну інформацію про те, які файли cookie використовуються, для чого вони

потрібні, як довго зберігаються дані, і як користувачі можуть керувати своїми налаштуваннями щодо файлів cookie.

<h2>Українське законодавство</h2>

Під час збору особистих даних для коментування чи підписки необхідно інформувати користувачів про мету обробки та забезпечити збереження їхніх прав. Також варто дотримуватись принципів прозорості та мінімізації даних.

<hr>

`;

} else if (siteType === 'news' && language === 'english') {

detailedPolicy = `

<h3>News Websites</h3>

Collecting Minimal Data for Comments: If a news website allows user comments under its articles, it should limit the collection of personal data to the bare minimum necessary. For example, the website might collect only a username and an email address for the purpose of identifying the commenter. It’s essential for the website to have a clear privacy policy that explains how this data will be used, how long it will be stored, and what rights users have concerning their data. This policy should be accessible on the site, and users should be made aware of it before submitting any comments.

Consent for Newsletter Subscriptions: If a news website offers newsletter subscriptions, it’s important to obtain explicit consent from users before using their email addresses for that purpose. Sending newsletters or any other marketing communications without explicit user consent is a violation of GDPR. News websites should employ a double opt-in method to confirm that users genuinely wish to subscribe. Users must also have the option to easily unsubscribe from newsletters at any time.

Right to Access Data: Under GDPR, users have the right to access the personal data that a news website holds about them. This might include registration details, comment history, subscription preferences, and other personal information. The website must provide clear instructions on how users can request access to their data, and the site should fulfill these requests within a reasonable timeframe. Additionally, users have the right to request corrections or deletions of their personal data.

Cookie Policy Transparency: Many news websites use cookies to track user behavior, analyze site traffic, improve user experience, and provide personalized advertising. Under GDPR, websites must clearly inform users about the use of

cookies. Before placing any non-essential cookies (those not necessary for basic site functions), explicit consent must be obtained from the user. The cookie policy should provide detailed information about what types of cookies are used, their purposes, how long the data will be stored, and how users can manage their cookie preferences.

<h2>Ukrainian legislation</h2>

When collecting personal data for commenting or newsletter subscriptions, users must be informed of the purpose of processing. Transparency and data minimization principles must be followed.

<hr>

`;

} else if (siteType === 'corporate' && language === 'ukrainian') {

detailedPolicy = `

<h3>Сайти компаній та корпорацій (Corporate Websites)</h3>

Прозорість збору даних: Компанійські сайти часто використовують контактні форми, форми зворотного зв'язку або підписки на інформаційні матеріали. Важливо, щоб такі сайти чітко та прозоро інформували відвідувачів про те, які персональні дані збираються, для чого вони використовуються, і як довго зберігатимуться. Наприклад, у формі зворотного зв'язку слід чітко зазначити, що електронна пошта та ім'я використовуються виключно для надання відповіді на запит. Ця інформація повинна бути легко доступною у вигляді політики конфіденційності на сайті.

Згода на отримання маркетингових матеріалів: Якщо компанія планує використовувати зібрані контактні дані для розсилки інформаційних або рекламних матеріалів, потрібно отримати чітку згоду від користувачів. Це можна зробити шляхом надання користувачу опції погодитися або відмовитися від отримання маркетингових повідомлень під час введення контактних даних. Використання електронної пошти для рекламних цілей без явної згоди користувачів порушує вимоги GDPR, тому важливо застосовувати подвійне підтвердження (double opt-in) для розсилок.

Право на виправлення та видалення: Сайти компаній повинні забезпечити користувачам можливість виправляти або видаляти свою персональну інформацію, яка зберігається на сайті. Наприклад, якщо користувач оновлює свою контактну інформацію або бажає видалити свій обліковий запис, компанія повинна забезпечити цей процес без зайвих труднощів і в найкоротші терміни. Користувачі також

мають право вимагати видалення своїх даних, якщо вони більше не потрібні компанії для виконання договірних зобов'язань.

Інформаційна безпека: Один із ключових аспектів відповідності GDPR – це захист персональних даних від несанкціонованого доступу або витоку. Компанії зобов'язані впроваджувати надійні механізми безпеки для захисту даних клієнтів, партнерів та співробітників. Це включає використання SSL-сертифікатів для захисту передачі даних, шифрування конфіденційної інформації та регулярне оновлення систем безпеки для запобігання потенційним кіберзагрозам. Також компанія повинна регулярно проводити аудити безпеки, щоб впевнитися, що всі дані захищені належним чином.

<h2>Українське законодавство</h2>

У разі використання форм зворотного зв’язку, збору резюме або контактної інформації необхідно чітко вказати мету збору та обсяг обробки. Важливо уникати надмірного збору даних та забезпечити належне зберігання.

<hr>

`;

} else if (siteType === 'corporate' && language === 'english') {

detailedPolicy = `

<h3>Corporate Websites</h3>

Transparency in Data Collection: Corporate websites often use contact forms, feedback forms, or subscription fields to collect personal data. It is crucial that these websites clearly and transparently inform visitors about what personal data is being collected, why it is being collected, and how long it will be retained. For example, in a feedback form, it should be clearly stated that the email and name provided will only be used to respond to the inquiry. This information should be readily accessible through a privacy policy linked directly on the website.

Consent for Marketing Communications: If a company intends to use collected contact details for distributing informational or promotional materials, explicit consent must be obtained from users. This can be done by providing users with an option to agree or decline to receive marketing messages at the time of submitting their contact details. Sending marketing emails without users’ explicit consent violates GDPR, so employing a double opt-in system for newsletters and promotional materials is essential.

Right to Rectification and Erasure: Corporate websites must allow users to rectify or delete their personal data stored on the site. For instance, if a user updates their contact details or requests the deletion of their account, the company must ensure that this process is straightforward and executed promptly. Additionally, users have the right to request the erasure of their data if it is no longer necessary for the company to fulfill any contractual obligations.

Data Security: A key aspect of GDPR compliance is ensuring the security of personal data to prevent unauthorized access or breaches. Companies are required to implement robust security measures to protect the personal information of clients, partners, and employees. This includes using SSL certificates to secure data transmission, encrypting sensitive information, and regularly updating security systems to mitigate potential cyber threats. Companies should also conduct regular security audits to ensure that all data is properly protected.

<h2>Ukrainian legislation</h2>

For feedback forms, resume submissions, or contact data collection, the purpose and scope of data processing must be clearly specified. Excessive data collection should be avoided, and proper data storage ensured.

<hr>

`;

} else if (siteType === 'blogs' && language === 'ukrainian') {

detailedPolicy = `

<h3>Блоги та інформаційні портали (Blogs & Information Portals)</h3>

Згода на використання коментарів: Якщо блог дозволяє коментарі від користувачів, важливо забезпечити їх інформування щодо збору персональних даних. Це можуть бути такі дані, як ім'я, електронна пошта або інші ідентифікаційні відомості. Блог повинен чітко пояснювати, для чого будуть використовуватися ці дані, наприклад, для публікації коментарів, відповідей на них, або сповіщення про нові відповіді. Окрім цього, має бути отримана явна згода від користувача на обробку їхніх персональних даних перед їхнім публікуванням.

Політика щодо файлів cookie: Багато блогів використовують файли cookie для збору аналітичних даних, відстеження поведінки користувачів або надання персоналізованих рекомендацій. Відповідно до вимог GDPR, такі сайти повинні інформувати користувачів про використання файлів cookie і пояснювати, які саме дані збираються. Крім того, до початку збору даних потрібно

отримати згоду користувача на використання cookie-файлів. Це також передбачає надання користувачам можливості відмовитися від певних типів файлів cookie.

Збір мінімальних даних: Згідно з принципом мінімізації даних, блоги та інформаційні портали повинні збирати лише ті персональні дані, які є необхідними для виконання конкретних функцій. Наприклад, для публікації коментарів на блозі достатньо імені та електронної адреси користувача. Якщо сайт пропонує підписку на оновлення блогу чи нові статті, слід обмежитися лише збиранням електронної пошти та уникати збору зайвої інформації, якщо це не є необхідним для надання послуги.

Право на видалення даних: Користувачі повинні мати можливість видалити свої персональні дані, зокрема коментарі та іншу інформацію, яку вони залишають на блозі. Адміністратори блогу зобов'язані забезпечити прозорий та легкий механізм видалення облікових записів або окремих даних, відповідно до запитів користувачів.

<h2>Українське законодавство</h2>

Слід дотримуватись правил збору персональних даних через підписки або коментарі. Користувачам потрібно надавати інформацію про те, як їхні дані будуть зберігатися і використовуватися, відповідно до українського законодавства.

<hr>

`;

} else if (siteType === 'blogs' && language === 'english') {

detailedPolicy = `

<h3>Blogs & Information Portals</h3>

Consent for Using Comments: If a blog allows users to post comments, it is essential to inform them about the collection of personal data. This may include data such as name, email address, or other identifying details. The blog should clearly explain how this information will be used, for example, to publish comments, respond to them, or notify users of new replies. In addition, explicit consent must be obtained from the user for processing their personal data before posting comments.

Cookie Policy: Many blogs use cookies to collect analytical data, track user behavior, or offer personalized recommendations. According to GDPR, such websites must inform users about the use of cookies and explain what specific data is being collected. Moreover, users' consent must be obtained before collecting cookie data. This also includes providing users with the option to decline certain types of cookies.

Data Minimization: In accordance with the data minimization principle, blogs and information portals should collect only the personal data that is necessary for specific functions. For example, to post a comment on a blog, only a name and an email address should be required. If the site offers subscriptions to blog updates or new articles, collecting only the email address should suffice, avoiding unnecessary data collection unless essential for the service.

Right to Data Deletion: Users should have the ability to delete their personal data, including comments and other information they leave on the blog. Blog administrators are obliged to provide a transparent and user-friendly mechanism for account deletion or data removal upon users' requests.

<h2>Ukrainian legislation</h2>

When collecting data via comments or subscriptions, it is necessary to inform users about how their data will be stored and used, in line with Ukrainian legal requirements.

<hr>

`;

} else if (siteType === 'education' && language === 'ukrainian') {

detailedPolicy = `

<h3>Освітні платформи (Educational Platforms)</h3>

Згода на обробку персональних даних: Освітні платформи повинні надавати студентам чітку та детальну інформацію щодо того, які персональні дані збираються під час реєстрації або використання платформи. Це можуть бути такі дані, як ім’я, контактна інформація, академічна історія та інші пов'язані з навчанням відомості. Важливо, щоб студенти були проінформовані про те, як ці дані будуть використовуватися, наприклад, для створення облікового запису, відстеження успішності, надання доступу до курсів чи індивідуального навчального плану. Крім того, студенти повинні надавати явну згоду на обробку їхніх даних до моменту їх використання.

Мінімізація збору даних: Збирати необхідний мінімум даних є одним із основних принципів GDPR. Освітні платформи повинні обмежити збір персональної інформації лише тими даними, які є безпосередньо необхідними для надання освітніх послуг. Наприклад, ім’я, електронна пошта та платіжна інформація — це мінімальний набір, необхідний для створення облікового запису студента, оплати курсів та надання доступу до навчальних матеріалів. Жодні інші додаткові дані, які не мають

прямого відношення до навчального процесу, не повинні збиратися без належного обґрунтування.

Захист платіжної інформації: Освітні платформи, що використовують платіжні дані для покупки курсів чи підписок, зобов'язані гарантувати безпеку цих даних. Фінансова інформація студентів повинна бути зашифрована та зберігатися у захищеному середовищі, що запобігає несанкціонованому доступу. Всі транзакції мають бути захищені за допомогою надійних механізмів шифрування і відповідати найкращим практикам у галузі фінансової безпеки. Це передбачає також регулярний аудит систем безпеки, щоб уникнути будь-яких ризиків.

Право на виправлення і видалення даних: Користувачі освітніх платформ, включаючи студентів, повинні мати повне право на доступ до своїх персональних даних, можливість їх змінювати або видаляти, якщо цього вимагає студент. Це включає, наприклад, можливість виправити контактну інформацію або оновити платіжні реквізити. Також студенти повинні мати право видалити свій обліковий запис разом із усіма пов'язаними з ним даними, якщо вони більше не бажають використовувати платформу.

<h2>Українське законодавство</h2>

У разі роботи з даними неповнолітніх необхідно враховувати додаткові вимоги щодо згоди батьків або законних представників. Також важливо захищати дані про академічну успішність та особисту інформацію учнів і студентів.

<hr>

`;

} else if (siteType === 'education' && language === 'english') {

detailedPolicy = `

<h3>Educational Platforms</h3>

Consent for Processing Personal Data: Educational platforms must provide students with clear and detailed information regarding what personal data is being collected when they register or use the platform. This may include data such as name, contact information, academic records, and other learning-related details. It is crucial that students are informed about how this data will be used, for instance, to create accounts, track progress, or provide access to courses or personalized learning plans. Moreover, explicit consent must be obtained from students for the processing of their data before it is used.

Data Minimization: Collecting the minimum necessary data is a core GDPR principle. Educational platforms should limit the collection of personal

information to only what is directly necessary for providing educational services. For example, name, email, and payment information are the minimum required to create a student account, pay for courses, and provide access to learning materials. No additional data not directly related to the learning process should be collected without a valid reason.

Protection of Payment Information: Educational platforms that use payment data for course purchases or subscriptions are required to ensure the security of this information. Students' financial data must be encrypted and stored in a secure environment to prevent unauthorized access. All transactions should be protected by robust encryption mechanisms and adhere to the best practices in financial security. This also includes regular security audits to mitigate any potential risks.

Right to Rectification and Data Deletion: Users of educational platforms, including students, must have full rights to access their personal data and the ability to correct or delete it as needed. This includes, for example, the ability to update contact information or change payment details. Additionally, students should have the right to delete their accounts and all associated data if they no longer wish to use the platform.

<h2>Ukrainian legislation</h2>

If data on minors is processed, additional requirements apply, including parental or legal guardian consent. Academic and personal data must be protected in accordance with privacy laws.

<hr>

`;

} else if (siteType === 'medical' && language === 'ukrainian') {

detailedPolicy = `

<h3>Медичні сайти та платформи для запису до лікаря (Medical Websites & Appointment Platforms)</h3>

Обробка чутливих даних: Медичні сайти обробляють надзвичайно чутливу інформацію, таку як стан здоров’я пацієнтів, діагнози, історія хвороб, медичні рецепти та інші дані, що підпадають під категорію спеціальних персональних даних за GDPR. Тому, відповідно до вимог Регламенту, ці дані повинні бути максимально захищеними за допомогою надійного шифрування як під час їх передачі, так і зберігання. Доступ до таких даних має надаватися виключно уповноваженим особам, а платформи повинні проводити регулярні перевірки та аудити безпеки для запобігання несанкціонованому доступу.

Згода на обробку медичних даних: Збір медичних даних вимагає явної та інформованої згоди користувача. Медичні сайти та платформи повинні забезпечувати прозорість у тому, як і для чого використовуються медичні дані користувачів. Перед реєстрацією на сайті або наданням будь-яких медичних послуг, користувачі повинні бути чітко проінформовані про мету збору даних та надавати свою згоду на їх обробку. Усі дії з обробки даних повинні бути документованими та відповідати вимогам GDPR.

Право на видалення даних: Відповідно до принципів GDPR, користувачі медичних платформ мають право вимагати видалення своїх медичних даних після надання медичних послуг або в інших випадках, передбачених законодавством. Це право включає можливість видалити інформацію про попередні консультації, діагнози, рецепти та інші чутливі дані. Медичні платформи повинні створити зрозумілі та доступні інструменти для видалення даних за запитом користувача, при цьому забезпечуючи дотримання всіх юридичних зобов'язань щодо зберігання даних.

Мінімізація збору даних: Медичні сайти та платформи повинні збирати лише ті дані, які є безпосередньо необхідними для надання медичних послуг. Наприклад, для запису на прийом до лікаря достатньо збирати лише ім’я, контактні дані, причину звернення та інформацію про історію лікування, якщо вона необхідна. Зайва інформація, яка не є критичною для надання медичної допомоги або консультації, не повинна збиратися без вагомих підстав.

Захист конфіденційності: Для забезпечення належного рівня конфіденційності пацієнтів, медичні сайти повинні впроваджувати додаткові механізми захисту. До таких заходів можна віднести двофакторну аутентифікацію для медичного персоналу, що має доступ до медичних даних пацієнтів, регулярне оновлення систем безпеки, а також моніторинг спроб несанкціонованого доступу до системи. Це гарантує, що лише медичний персонал, якому дозволено працювати з персональними даними пацієнтів, зможе мати доступ до цієї інформації.

<h2>Українське законодавство</h2>

Слід дотримуватись норм щодо захисту медичної та конфіденційної інформації згідно з законодавством України. Чутливі дані повинні оброблятись виключно з явною згодою та з обмеженим доступом.

<hr>

`;

} else if (siteType === 'medical' && language === 'english') {

detailedPolicy = `

<h3>Medical Websites & Appointment Platforms</h3>

Processing of Sensitive Data: Medical websites handle extremely sensitive data, such as patients' health conditions, diagnoses, medical history, prescriptions, and other information classified as special personal data under GDPR. As per the Regulation, these data must be secured using robust encryption both during transmission and while being stored. Access to such data must be strictly limited to authorized personnel, and platforms should conduct regular audits and security checks to prevent unauthorized access.

Consent for Processing Medical Data: The collection of medical data requires explicit and informed consent from users. Medical websites and platforms must ensure full transparency regarding how and why users' medical data are collected and used. Before registering on the site or accessing any medical services, users must be clearly informed about the purpose of the data collection and must provide their consent for the data processing. All data processing activities must be properly documented and comply with GDPR requirements.

Right to Erasure: In line with GDPR principles, users of medical platforms have the right to request the deletion of their medical data after receiving medical services or in other cases permitted by law. This right includes the possibility to delete information about past consultations, diagnoses, prescriptions, and other sensitive data. Medical platforms must provide clear and accessible tools for users to request data deletion while ensuring they comply with any legal obligations regarding data retention.

Data Minimization: Medical websites and platforms should collect only the information that is strictly necessary for providing medical services. For example, when scheduling an appointment, the platform should only collect the patient’s name, contact information, reason for the visit, and relevant medical history if required. Excessive or irrelevant data not essential for providing medical assistance or consultations should not be collected without valid justification.

Confidentiality Protection: To ensure the privacy of patients, medical websites should implement additional security mechanisms. These may include two-factor authentication for medical personnel accessing patient records, regular updates to security systems, and monitoring for unauthorized access attempts. These measures help ensure that only authorized medical professionals with permission to handle personal data can access sensitive patient information.

<h2>Ukrainian legislation</h2>

Processing of medical and confidential information must comply with Ukrainian legislation. Sensitive data should only be handled with explicit consent and access must be strictly limited.

```
        <hr>
      `;
    } else if (siteType === 'jobs' && language === 'ukrainian') {
      detailedPolicy = `
        <h3>Сайти пошуку роботи (Job Portals)</h3>
        <ul>
```

Згода на обробку персональних даних: Сайти пошуку роботи обробляють широкий спектр особистих даних користувачів, включаючи резюме, контактну інформацію, професійні навички, та інші відомості, що можуть бути конфіденційними. Відповідно до вимог GDPR, перед реєстрацією на такій платформі кандидати повинні надати свою явну та інформовану згоду на обробку своїх персональних даних. Цей процес має бути прозорим, і користувачі повинні мати доступ до інформації про те, як будуть використовуватись їхні дані, та з якою метою.

Право на видалення даних: Кандидати повинні мати можливість видалити свої профілі, резюме та іншу особисту інформацію, коли вони більше не хочуть використовувати платформу або завершили процес пошуку роботи. Платформи повинні забезпечити легкий доступ до цієї функції та дотримуватись вимог щодо повного видалення даних з усіх систем. Важливо, щоб користувачі також могли видалити всю інформацію, яку вони надали потенційним роботодавцям через платформу.

Мінімізація збору даних: Сайти пошуку роботи повинні збирати лише ті персональні дані, які є критично необхідними для успішного пошуку роботи. Це можуть бути такі дані, як професійні кваліфікації, досвід роботи, рівень освіти та контактна інформація. Всі додаткові відомості повинні бути запитувані тільки у випадку, коли вони безпосередньо впливають на можливість отримання конкретної вакансії. Принцип мінімізації даних допомагає зменшити ризики, пов'язані з безпекою та конфіденційністю.

Захист персональних даних: Персональні дані кандидатів, зокрема резюме, контактні дані та інша інформація, повинні бути надійно захищені відповідно до вимог GDPR. Це означає, що платформи повинні використовувати передові технології шифрування для захисту даних під час їх передачі та зберігання. Також важливо, щоб ці платформи регулярно проводили аудити безпеки, щоб уникнути можливих витоків даних або несанкціонованого доступу.

Передача даних третім сторонам: У багатьох випадках платформи пошуку роботи передають персональні дані кандидатів роботодавцям або рекрутерам. GDPR вимагає, щоб цей процес був повністю прозорим. Кандидати повинні бути чітко проінформовані про можливість передачі їхніх даних третім сторонам, а також повинні мати можливість дати або відкликати свою згоду на таку передачу. Роботодавці також повинні зобов'язуватися зберігати дані відповідно до вимог конфіденційності та безпеки.

```
        </ul>
```

```
            <h2>Українське законодавство</h2>
            <p>
            Під час обробки персональних даних кандидатів необхідно дотримуватись вимог щодо конфіденційності та інформування про передачу даних третім особам (роботодавцям). Також потрібно чітко визначити строки зберігання резюме.
            </p>
            <hr>
          `;
        } else if (siteType === 'jobs' && language === 'english') {
          detailedPolicy = `
            <h3>Job Portals</h3>
            <ul>
              <li><strong>Consent for Data Processing:</strong> Job portals process a wide range of personal data, including resumes, contact information, professional skills, and other confidential information. Under GDPR, candidates must give explicit and informed consent for the processing of their personal data before registering and using the platform. This process should be transparent, ensuring that users are fully aware of how their data will be used and for what purpose.</li>
              <li><strong>Right to Data Deletion:</strong> Candidates must have the ability to delete their profiles, resumes, and any personal information when they no longer wish to use the platform or have completed their job search. Platforms must offer easy access to this feature and comply with GDPR by fully erasing data from all systems. It is also important for users to be able to delete any information shared with potential employers through the platform.</li>
              <li><strong>Data Minimization:</strong> Job portals should collect only the personal data necessary for a successful job search, such as professional qualifications, work experience, education level, and contact details. Any additional information should be requested only when directly relevant to a specific job application. The principle of data minimization helps reduce security and privacy risks.</li>
              <li><strong>Protection of Personal Data:</strong> Personal data of candidates, including resumes, contact information, and other details, must be securely protected in accordance with GDPR requirements. This means that platforms should use advanced encryption technologies to safeguard data during transmission and storage. Regular security audits should be conducted to prevent potential data breaches or unauthorized access.</li>
              <li><strong>Data Sharing with Third Parties:</strong> In many cases, job portals share candidates' personal data with employers or recruiters. GDPR mandates that this process be fully transparent. Candidates should be clearly informed of the possibility that their data may be shared with third parties and must have the option to give or withdraw consent
```

for such sharing. Employers must also adhere to privacy and security standards when handling the data they receive.

<h2>Ukrainian legislation</h2>

When handling candidate data, it is necessary to ensure confidentiality and inform about the possibility of transferring data to third parties (employers). Data retention periods must also be clearly defined.

<hr>

`;

} else if (siteType === 'booking' && language === 'ukrainian') {

detailedPolicy = `

<h3>Платформи для бронювання (Booking Sites)</h3>

Згода на обробку персональних даних: Платформи для бронювання повинні отримувати явну згоду користувачів на обробку їхніх персональних даних перед завершенням будь-якої транзакції. Це означає, що користувачам повинно бути надано чітке пояснення, які дані збираються (наприклад, ім’я, контактні дані, платіжна інформація) і як ці дані будуть використовуватись. Згода повинна бути добровільною та обґрунтованою, без прихованих умов або автоматичних налаштувань, як, наприклад, попередньо встановлені чекбокси.

Захист фінансової інформації: Платіжні дані користувачів (кредитні картки, банківські реквізити) повинні бути надійно захищені за допомогою сучасних технологій шифрування, щоб уникнути несанкціонованого доступу третіх осіб. Важливо, щоб ці дані зберігалися безпечно і були доступні тільки уповноваженим особам.

Право на видалення та виправлення даних: Користувачі повинні мати можливість видалити свої персональні дані після завершення процесу бронювання, якщо вони більше не потрібні для надання послуги. У разі виявлення помилок у персональних даних, користувач має право їх виправити. Це дає можливість користувачам підтримувати актуальність своїх даних та запобігати потенційним проблемам через неправильну інформацію.

Політика cookie: Платформи зобов’язані інформувати користувачів про використання файлів cookie, які можуть бути застосовані для збереження історії бронювань, налаштування персоналізованих пропозицій або для аналітики щодо використання сайту. Користувачі повинні мати можливість приймати

рішення про використання cookie або відмовлятися від них відповідно до своїх уподобань.

Мінімізація збору даних: Відповідно до GDPR, платформи повинні збирати лише ті дані, які є абсолютно необхідними для виконання конкретної задачі. Наприклад, для процесу бронювання можуть знадобитися тільки паспортні дані та контактна інформація. Будь-які додаткові дані, які не мають прямого відношення до процесу, не повинні запитуватися або зберігатися.

<h2>Українське законодавство</h2>

Слід зазначати мету збору персональних даних при оформленні бронювань, а також інформувати користувачів про умови передачі інформації третім особам (наприклад, готелям чи перевізникам) згідно з українським законодавством.

<hr>

`;

} else if (siteType === 'booking' && language === 'english') {

detailedPolicy = `

<h3>Booking Sites</h3>

Consent for Data Processing: Booking platforms must obtain explicit consent from users before processing their personal data during transactions. This means users should be provided with a clear explanation of what data is collected (such as names, contact information, and payment details) and how this data will be used. The consent must be voluntary and fully informed, with no hidden conditions or pre-selected checkboxes.

Protection of Financial Information: User payment data (such as credit card details and bank information) must be securely protected using advanced encryption technologies to prevent unauthorized access by third parties. It’s essential that this data is stored safely and is only accessible to authorized personnal.

Right to Delete and Correct Data: Users should have the ability to delete their personal data once the booking process is completed, provided it is no longer necessary for the service. In case of errors, users have the right to correct their personal information, ensuring accuracy and preventing potential issues that might arise from incorrect data.

Cookie Policy: Booking platforms are required to inform users about their use of cookies, which may store booking history, personalize offers, or track

user behavior for analytical purposes. Users should have the option to accept or reject the use of cookies in line with their preferences.

Data Minimization: Under GDPR, booking platforms must collect only the data necessary to fulfill specific purposes. For example, only passport data and contact information may be required for the booking process. Any additional data that is not directly related to the service should not be requested or stored.

<h2>Ukrainian legislation</h2>

Users must be informed about the purpose of personal data collection during booking, including conditions for sharing data with third parties (e.g., hotels, carriers), in accordance with Ukrainian law.

<hr>

`;

} else if (siteType === 'forums' && language === 'ukrainian') {

detailedPolicy = `

<h3>Форуми та дискусійні платформи (Discussion Forums)</h3>

Згода на обробку персональних даних: Під час реєстрації на форумах або дискусійних платформах користувачі повинні давати чітку згоду на обробку своїх персональних даних, таких як ім’я, електронна пошта та інші реєстраційні дані. Форум повинен пояснити, як ці дані будуть використовуватися, зокрема для цілей авторизації або комунікації з адміністрацією. Згода повинна бути добровільною і не нав'язувати жодних прихованих умов.

Право на видалення акаунтів і контенту: Користувачі повинні мати можливість видаляти свої облікові записи та публікації на форумі за власним бажанням. Це включає можливість видаляти як особисті дані, так і будь-який створений ними контент. Платформа повинна надати легкий доступ до цих функцій для користувачів.

Прозорість щодо файлів cookie: Форум має інформувати користувачів про використання файлів cookie, які можуть застосовуватись для збереження авторизаційних даних, аналізу активності на сайті або персоналізації користувацького досвіду. Користувачі повинні мати змогу приймати або відхиляти використання cookie відповідно до своїх уподобань.

Захист даних користувачів: Персональні дані користувачів повинні бути надійно захищені від несанкціонованого доступу шляхом

впровадження належних заходів безпеки, таких як шифрування даних під час їх передачі або зберігання. Крім того, важливо впровадити багатофакторну автентифікацію для додаткового рівня захисту облікових записів користувачів.

Анонімність: Форум повинен надати користувачам можливість публікувати повідомлення анонімно або під псевдонімом, забезпечуючи їхню конфіденційність та захист приватного життя. Це дозволяє користувачам зберігати свою анонімність і уникати розкриття особистої інформації.

<h2>Українське законодавство</h2>

Потрібно забезпечити можливість анонімного використання ресурсу або надати механізм для видалення персональних даних. Особливо важливо дотримуватись вимог щодо публічного поширення особистої інформації.

<hr>

`;

} else if (siteType === 'forums' && language === 'english') {

detailedPolicy = `

<h3>Discussion Forums</h3>

Consent for Data Processing: When registering on discussion forums, users must provide explicit consent for the processing of their personal data, such as their name, email, and other registration information. The forum must clearly explain how this data will be used, primarily for login purposes or communication with the administration. The consent must be voluntary and without hidden conditions.

Right to Delete Accounts and Content: Users should have the ability to delete their accounts and forum posts at any time. This includes removing both personal data and any content they've created. The platform should make these options easily accessible for users.

Transparency Regarding Cookies: Forums are required to inform users about the use of cookies, which may be used to store login credentials, track site activity, or personalize the user experience. Users should be able to accept or decline the use of cookies according to their preferences.

User Data Protection: Personal data must be securely protected from unauthorized access by implementing proper security measures such as data encryption during transmission or storage. Additionally, multi-factor authentication should be enabled to provide an extra layer of account security.

Anonymity: The platform should allow users to post messages anonymously or under a pseudonym, thus protecting their privacy and ensuring confidentiality. This allows users to maintain their anonymity and avoid disclosing personal information.

<h2>Ukrainian legislation</h2>

Anonymity options or the ability to delete personal data should be available. It is important to comply with regulations concerning public sharing of personal information.

<hr>

`;

} else if (siteType === 'donation' && language === 'ukrainian') {

detailedPolicy = `

<h3>Сайти зі збором донатів (Donation Platforms)</h3>

Згода на обробку персональних і фінансових даних: Перш ніж донори зможуть здійснити пожертву, вони мають надати свою чітку згоду на обробку персональних даних, таких як ім’я, електронна пошта, та фінансову інформацію. Це включає інформацію про платіжні карти або банківські реквізити, що використовуються для переказу коштів. Важливо, щоб ця згода була добровільною та свідомою, і щоб донор був поінформований про те, які дані збираються та з якою метою.

Прозорість щодо використання коштів: Донори повинні мати доступ до чіткої інформації про те, як саме будуть використані їхні кошти. Це включає в себе надання детальної інформації про конкретні проекти, на які спрямовані їхні пожертви, і звіти про те, як платформа розподіляє фінанси. Окрім цього, донори мають знати, які персональні дані збираються під час пожертвувань і як ці дані будуть використовуватися.

Захист фінансових даних: Всі фінансові операції, що здійснюються через платформу, повинні бути захищені за допомогою сучасних методів шифрування. Це гарантує, що дані платіжних карток або банківські реквізити захищені від несанкціонованого доступу третіх осіб. Крім того, платформи повинні впроваджувати додаткові заходи безпеки, такі як двофакторна аутентифікація, щоб підвищити рівень захисту фінансової інформації.

Право на видалення даних: Після завершення пожертвування донори повинні мати можливість видалити свої персональні та фінансові дані з платформи. Це право надається користувачам для забезпечення контролю над

їхніми особистими даними та зниження ризиків їхнього неправомірного використання у майбутньому.

Мінімізація збору даних: Платформи повинні збирати лише мінімально необхідну кількість персональних даних, щоб виконати процес пожертвування. Це означає, що збирання зайвої інформації, яка не є безпосередньо необхідною для транзакцій, слід уникати. Наприклад, для пожертви потрібні лише ім'я, контактні дані та платіжна інформація.

<h2>Українське законодавство</h2>

Необхідно прозоро вказати, як будуть використовуватись персональні дані донорів. У разі залучення платіжних сервісів — слід переконатись, що обробка відбувається відповідно до чинного фінансового та інформаційного законодавства України.

<hr>

`;

} else if (siteType === 'donation' && language === 'english') {

detailedPolicy = `

<h3>Donation Platforms</h3>

Consent for Processing Personal and Financial Data: Before donors can make a donation, they must provide explicit consent for the processing of their personal data, such as their name, email, and financial information. This includes details about their payment cards or bank accounts used for the transfer of funds. It's crucial that this consent is voluntary and informed, ensuring that donors are fully aware of what data is being collected and for what purposes.

Transparency Regarding the Use of Funds: Donors should have access to clear information about how their donations will be used. This includes providing detailed reports on the specific projects or causes that their donations support and how the platform distributes the funds. Additionally, donors should be informed about what personal data is collected during the donation process and how it will be used.

Financial Data Protection: All financial transactions conducted through the platform must be protected using advanced encryption methods. This ensures that payment card information or bank account details are kept secure from unauthorized access by third parties. Moreover, platforms should implement additional security measures, such as two-factor authentication, to further safeguard financial data.

Right to Data Deletion: After completing a donation, donors should have the option to delete their personal and financial data from the platform. This right is provided to users to maintain control over their personal data and reduce the risk of misuse in the future.

Data Minimization: Platforms should only collect the minimum amount of personal data necessary to complete the donation process. This means avoiding the collection of excessive information that is not directly required for the transaction. For example, a donation may only require the donor's name, contact details, and payment information.

<h2>Ukrainian legislation</h2>

Users must be clearly informed about how their personal data will be used. If payment services are involved, their data processing must comply with Ukrainian financial and information laws.

<hr>

`;

} else if (siteType === 'advertising' && language === 'ukrainian') {

detailedPolicy = `

<h3>Рекламні платформи (Advertising Platforms)</h3>

Згода на обробку даних: Перш ніж користувачі можуть створити рекламний обліковий запис або використовувати інструменти таргетованої реклами, вони повинні надати явну згоду на обробку своїх персональних даних. Це може включати в себе збір таких даних, як контактна інформація, місцезнаходження, вік, інтереси та інші поведінкові фактори, що використовуються для побудови рекламних стратегій. Важливо, щоб згода користувачів була добровільною і щоб вони отримали інформацію про те, як будуть використовуватись їхні дані.

Політика щодо файлів cookie: Рекламні платформи мають обов'язково інформувати користувачів про використання файлів cookie. Ці файли використовуються для збору даних про поведінку користувачів, таких як сторінки, які вони відвідують, товари, які вони переглядають, або контент, яким вони цікавляться. Ці дані аналізуються для таргетингу реклами та покращення взаємодії з користувачами, тому політика використання cookie повинна бути прозорою та легко доступною.

Право на виправлення або видалення даних: Користувачі повинні мати можливість вимагати виправлення неправильної інформації або видалення свого облікового запису на рекламній платформі. Це стосується як особистої

інформації, яка надається для створення облікових записів, так і даних, зібраних під час використання реклами. Крім того, платформи повинні надавати чіткі інструкції щодо процесу видалення даних або внесення змін.

Прозорість щодо збору даних: Для користувачів важливо розуміти, які саме дані збираються і як вони використовуються для цілей реклами. Рекламні платформи повинні чітко вказувати інформацію, яка збирається для таргетованої реклами, зокрема вік, стать, місцезнаходження, інтереси, а також їхню поведінку в мережі. Така прозорість забезпечує довіру користувачів і надає їм можливість робити обґрунтований вибір.

Захист даних: Персональні дані, зібрані для рекламних цілей, повинні бути захищені від несанкціонованого доступу. Рекламні платформи повинні використовувати сучасні методи шифрування для захисту цих даних і забезпечити їхнє використання лише з дозволу користувача. Це гарантує, що дані не будуть передані третім особам або використані в небажаних цілях.

<h2>Українське законодавство</h2>

Варто враховувати обмеження щодо автоматизованої обробки та профілювання. Користувачам потрібно надавати вибір щодо персоналізованої реклами та збору аналітичних даних, дотримуючись принципів інформованої згоди.

<hr>

`;

} else if (siteType === 'advertising' && language === 'english') {

detailedPolicy = `

<h3>Advertising Platforms</h3>

Consent for Data Processing: Before users can create advertising accounts or use targeted advertising tools, they must give explicit consent for the processing of their personal data. This may include collecting information such as contact details, location, age, interests, and other behavioral factors used for building advertising strategies. It is essential that users' consent is voluntary and that they are informed about how their data will be used.

Cookie Policy: Advertising platforms are required to inform users about the use of cookies. These files are used to gather data on user behavior, such as the pages they visit, the products they view, or the content they engage with. This data is analyzed for ad targeting and improving user interaction. Therefore, the cookie usage policy should be transparent and easily accessible.

Right to Rectification or Deletion of Data: Users must have the ability to request the correction of inaccurate information or the deletion of their advertising accounts. This applies to both the personal information provided during account creation and the data collected while using advertising services. Additionally, platforms should provide clear instructions on how users can delete their data or make necessary changes.

Transparency in Data Collection: It is crucial for users to understand what specific data is being collected and how it is used for advertising purposes. Advertising platforms must clearly state the types of information collected for targeted advertising, including age, gender, location, interests, and browsing behavior. Such transparency fosters user trust and enables them to make informed decisions.

Data Protection: Personal data collected for advertising purposes must be safeguarded against unauthorized access. Advertising platforms should implement modern encryption methods to protect this data and ensure its use is strictly with the user's consent. This guarantees that the data will not be shared with third parties or used for purposes other than those intended by the user.

<h2>Ukrainian legislation</h2>

Restrictions regarding automated processing and profiling must be considered. Users should be given the option to consent to personalized advertising and data collection in accordance with the principle of informed consent.

<hr>

`;

} else if (siteType === 'marketplace' && language === 'ukrainian') {

detailedPolicy = `

<h3>Маркетплейси (Online Marketplaces)</h3>

Згода на обробку даних: Покупці та продавці на маркетплейсах повинні надати свою згоду на обробку персональних даних, перш ніж вони зможуть створити обліковий запис або брати участь у транзакціях. Цей процес включає згоду на зберігання інформації, такої як ім'я, адреса електронної пошти, контактні дані та платіжна інформація, яка є необхідною для належної реєстрації, підтвердження особи та забезпечення безпечних транзакцій. Маркетплейси повинні гарантувати, що користувачі добре інформовані про те, як їхні дані будуть використовуватися і зберігатися.

Захист фінансових та персональних даних: Під час здійснення покупок або продажу на маркетплейсах особисті дані та платіжна інформація повинні бути захищені від несанкціонованого доступу за допомогою шифрування та надійних заходів безпеки. Це включає використання захищених платіжних шлюзів і шифрування всіх фінансових транзакцій. Маркетплейс також повинен надавати додаткові заходи захисту, такі як двофакторна аутентифікація, щоб забезпечити максимальний рівень безпеки даних.

Право на видалення акаунтів: Після завершення угод користувачі повинні мати можливість видалити свої облікові записи та особисті дані з платформи. Це право на «забуття» є важливим аспектом захисту конфіденційності та особистої безпеки користувачів. Платформи повинні розробити простий і зрозумілий процес видалення даних, який дозволить покупцям і продавцям без зусиль керувати своєю присутністю на платформі.

Мінімізація збору даних: Платформи для продажу товарів та послуг повинні збирати лише мінімум даних, необхідних для здійснення угод. Це означає, що інформація, яка збирається, повинна бути обмежена контактною інформацією, ім'ям та платіжними даними. Маркетплейси не повинні збирати або зберігати зайві персональні дані, що не мають прямого відношення до угод. Такий підхід мінімізує ризики та покращує захист конфіденційності.

Прозорість щодо використання даних: Користувачі повинні мати доступ до інформації про те, як їхні дані використовуються маркетплейсом. Це стосується не лише даних, які використовуються для транзакцій, але й інформації, яка може бути застосована для оцінки покупок, надання відгуків або покращення користувацького досвіду. Прозорість у використанні даних допомагає підвищити довіру між користувачами та платформою, а також сприяє дотриманню стандартів захисту даних.

<h2>Українське законодавство</h2>

Збір інформації про продавців та покупців повинен відбуватись лише з конкретною метою. Слід враховувати правила щодо електронної комерції, оплати та збереження транзакційних даних у відповідності до українських вимог.

<hr>

`;

} else if (siteType === 'marketplace' && language === 'english') {

detailedPolicy = `

<h3>Online Marketplaces</h3>

Consent for Data Processing: Buyers and sellers on online marketplaces must provide consent for the processing of their personal data before they can create accounts or engage in transactions. This process includes consent for storing information such as names, email addresses, contact details, and payment information, which is necessary for proper registration, identity verification, and secure transactions. Marketplaces must ensure that users are fully informed about how their data will be used and stored.

Protection of Financial and Personal Data: When conducting purchases or sales on online marketplaces, personal data and payment information must be protected from unauthorized access through encryption and robust security measures. This includes the use of secure payment gateways and encryption for all financial transactions. Additionally, marketplaces should offer enhanced security measures such as two-factor authentication to ensure maximum data protection.

Right to Delete Accounts: After completing transactions, users should have the ability to delete their accounts and personal data from the platform. This right to "be forgotten" is a crucial aspect of safeguarding user privacy and personal security. Marketplaces should provide a simple and clear process for data deletion, allowing both buyers and sellers to easily manage their presence on the platform.

Data Minimization: Online marketplaces should only collect the minimum amount of data necessary for conducting transactions. This means that the collected information should be limited to contact details, names, and payment information. Marketplaces should not collect or store excess personal data that is not directly relevant to the transaction process. Such an approach minimizes risks and enhances privacy protection.

Transparency Regarding Data Usage: Users must have access to information about how their data is being used by the marketplace. This includes not only data used for transactions but also information that may be applied for evaluating purchases, providing reviews, or improving the user experience. Transparency in data usage helps build trust between users and the platform and ensures adherence to data protection standards.

<h2>Ukrainian legislation</h2>

Information about sellers and buyers must only be collected for specific, declared purposes. The requirements of Ukrainian laws on electronic commerce, payment operations, and transaction data storage should be strictly followed.

<hr>

```
    `;
  } else if (siteType === 'services' && language === 'ukrainian') {
    detailedPolicy = `
      <h3>Сайти особистих послуг (Personal Services Websites)</h3>
      <ul>
        <li><strong>Згода на обробку даних:</strong> Користувачі, які реєструються на сайтах особистих послуг, повинні надати свою згоду на обробку персональних даних. Це може включати такі дані, як ім’я, контактні дані, адресу, інформацію про замовлення та інші важливі деталі, необхідні для надання послуг. Без згоди користувача ці дані не можуть бути зібрані або використані. Користувачам повинні бути надані детальні умови щодо обробки даних перед підтвердженням згоди.</li>
        <li><strong>Мінімізація збору даних:</strong> Платформа повинна збирати лише ті дані, які є абсолютно необхідними для виконання замовлення або надання послуг. Наприклад, для бронювання або організації послуг може бути необхідним лише ім'я, контактна інформація та деталі замовлення. Зайві дані, які не є критичними для надання послуг, не повинні збиратися, що дозволяє мінімізувати ризики для конфіденційності та безпеки користувача.</li>
        <li><strong>Захист персональних даних:</strong> Персональні дані користувачів, які замовляють послуги на таких платформах, повинні бути захищені за допомогою відповідних заходів безпеки, таких як шифрування даних, щоб запобігти їхньому несанкціонованому доступу або зловживанню. Платформи повинні використовувати надійні механізми захисту для забезпечення збереження інформації користувачів та уникнення потенційних витоків.</li>
        <li><strong>Право на видалення даних:</strong> Після завершення надання послуг користувачі мають право на повне видалення своїх персональних даних з платформи. Це включає видалення облікових записів та всіх збережених даних про замовлення. Платформа повинна забезпечувати легкий і доступний механізм видалення даних на вимогу користувача, що відповідає принципам захисту конфіденційності та положенням GDPR.</li>
        <li><strong>Прозорість щодо використання файлів cookie:</strong> Платформа повинна надавати користувачам чітку інформацію щодо використання файлів cookie, які можуть зберігати дані авторизації або використовуватися для персоналізації послуг. Користувачі повинні бути інформовані про типи файлів cookie, їхні функції та мету використання, а також мати можливість налаштувати параметри cookie відповідно до власних вподобань.</li>
      </ul>
      <h2>Українське законодавство</h2>
      <p>
```

Необхідно враховувати специфіку персональних послуг, де часто обробляється чутлива інформація (наприклад, місце перебування, особисті вподобання). Згода на обробку таких даних має бути чіткою та усвідомленою.

```
            </p>
            <hr>
        `;
    } else if (siteType === 'services' && language === 'english') {
        detailedPolicy = `
            <h3>Personal Services Websites</h3>
            <ul>
```

Consent for Data Processing: Users registering on personal services websites must provide consent for the processing of their personal data. This may include information such as their name, contact details, address, service request details, and other necessary information required to provide the services. Without user consent, this data cannot be collected or used. Clear terms regarding data processing must be provided to users before they confirm their consent.

Data Minimization: The platform should only collect data that is absolutely necessary for fulfilling service requests or orders. For example, only the name, contact information, and order details may be required for booking or arranging services. Collecting unnecessary data that is not directly critical for service delivery should be avoided, minimizing risks to user privacy and security.

Protection of Personal Data: The personal data of users who order services on these platforms must be safeguarded through proper security measures such as data encryption to prevent unauthorized access or misuse. Platforms should employ robust protection mechanisms to ensure that user information remains secure and that potential data breaches are prevented.

Right to Delete Data: After the completion of the services, users have the right to request the full deletion of their personal data from the platform. This includes deleting their accounts and all associated order information. The platform should provide an easy and accessible mechanism for users to request the deletion of their data, which aligns with privacy protection principles and GDPR regulations.

Transparency Regarding Cookie Usage: The platform should provide clear information to users about the use of cookies, which may store authorization data or be used for service personalization. Users should be informed about the types of cookies, their functions, and purposes, and they should have the option to adjust their cookie preferences according to their needs.

```
            </ul>
            <h2>Ukrainian legislation</h2>
```

```
            <p>
            Due to the potentially sensitive nature of the data (e.g., location, personal preferences), explicit and informed consent is required for data processing. Special care must be taken to safeguard this information.
            </p>
            <hr>
        `;
    }

    let generatedText = baseInfo + detailedPolicy;
    if (surveyData.hasFinancialOperations  === 'yes') {
        if (language === 'ukrainian') {
            generatedText += financialNoteUa;
        } else if (language === 'english') {
            generatedText += financialNoteEn;
        }
    }

    if (surveyData.dataTransferLevel === 'medium') {
        generatedText += language === 'ukrainian' ? dataTransferEuUa : dataTransferEuEn;
    } else if (surveyData.dataTransferLevel === 'high') {
        generatedText += language === 'ukrainian' ? dataTransferNonEuUa : dataTransferNonEuEn;
    }

    document.getElementById('generated-text').innerHTML = generatedText;
    document.getElementById('generated-text-container').style.display = 'block';

}
</script>
```

```
<script>
  document.getElementById("download-button").addEventListener("click", function() {
    alert("To download the pdf* file contact our support centre support@gmail.com");
  });
</script>


<div id="generated-text-container" style="display: none;">
  <div id="generated-text">
    <h3>Інтернет-магазини (E-commerce Sites)</h3>
    <ul>
```

Прозорість обробки даних: Інтернет-магазин повинен чітко інформувати користувачів про те, які саме персональні дані збираються під час використання платформи. Це включає в себе дані, необхідні для обробки замовлень, оплат, доставки, а також для поліпшення користувацького досвіду. Важливо, щоб користувачі розуміли, як їхні дані будуть використовуватися, на який термін вони будуть зберігатися, і хто саме буде мати до них доступ. Усі етапи збору та обробки повинні бути прозорими та зрозумілими для кінцевих користувачів.

Згода на обробку платіжних даних: При здійсненні платіжних операцій користувачі повинні надавати явну згоду на обробку своїх платіжних даних, таких як банківські реквізити, платіжні картки та інші фінансові дані. Ці дані мають бути використані виключно для виконання конкретного замовлення або для надання певних послуг, і не можуть бути використані для інших цілей без додаткової згоди. Всі платіжні операції повинні бути захищені на всіх етапах процесу з використанням надійних механізмів шифрування.

Право на забуття: Користувачі Інтернет-магазинів повинні мати можливість безперешкодно вимагати видалення своїх персональних даних, включаючи історію покупок, платіжні реквізити та іншу інформацію, що була зібрана під час взаємодії з сайтом. Це право, яке гарантує користувачам, що їхні дані не зберігатимуться без їхньої згоди після завершення покупки або іншої операції, для якої ці дані були надані.

Шифрування даних: Для забезпечення безпеки персональних даних, зокрема платіжної інформації, всі транзакції та дані користувачів повинні бути захищені за допомогою сучасних методів шифрування під час їхньої передачі через Інтернет. Це гарантує, що дані користувачів не будуть доступні третім особам, і допомагає зберігати довіру клієнтів до платформи.

Мінімізація збору даних: Інтернет-магазин має дотримуватись принципу мінімізації збору даних, що означає збір тільки тих даних, які

необхідні для виконання конкретних операцій, наприклад, адреса доставки, платіжні реквізити та контактна інформація. Збір додаткових або зайвих даних повинен бути обмежений або взагалі виключений.

Cookies та інші технології відстеження: Інтернет-магазини повинні отримувати явну згоду користувачів на використання файлів cookie або інших технологій відстеження для збору даних про поведінку користувача на сайті. Якщо ці технології не є критично необхідними для роботи платформи, їх використання повинно бути чітко роз'яснене, і користувачі повинні мати можливість налаштувати або відмовитися від їх використання.

</body>

</html>

Додаток В

ІЛЮСТРАТИВНА ЧАСТИНА

«Засіб для формування політики захисту даних вебсайту відповідно до GDPR»

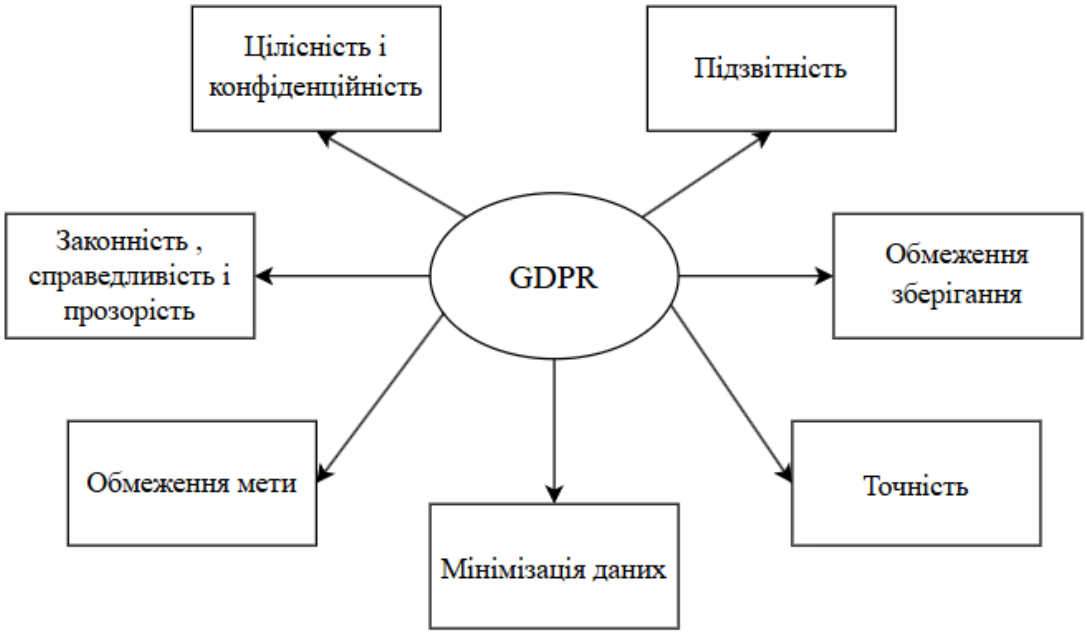
Виконала студентка 4 курсу групи 1БС-21б
спеціальності 125 – Кібербезпека

_____ Дарина МАЛЬЦЕВА
_____ 2025р.

Керівник: к. т. н., доцент каф. ЗІ

_____ Олеся ВОЙТОВИЧ
_____ 2025р.

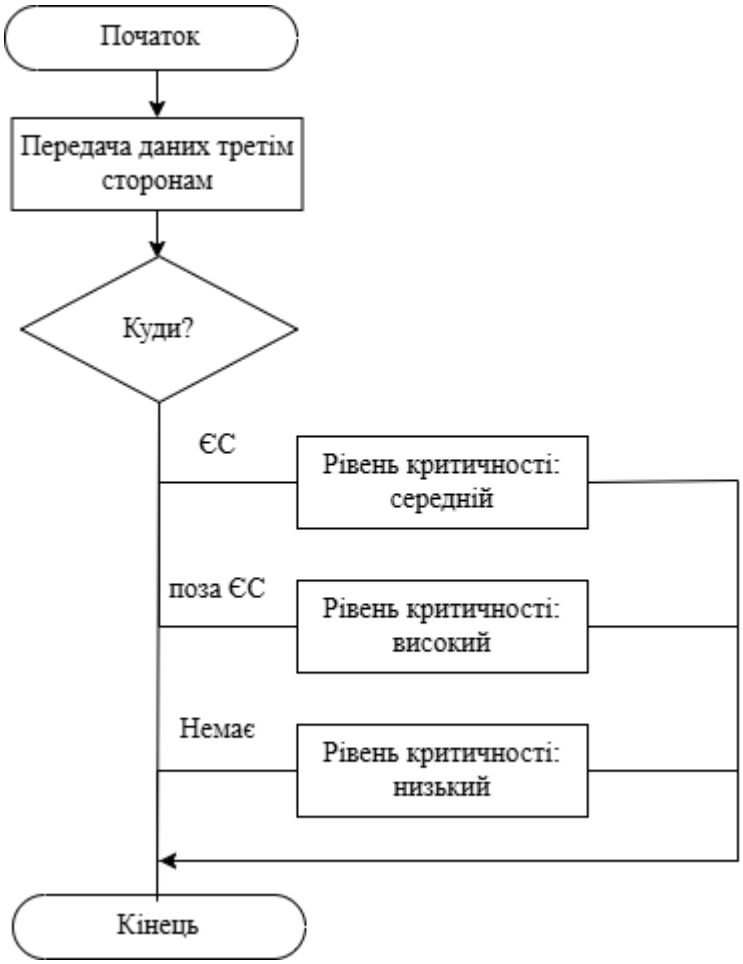
ОСНОВНІ ПРНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ GDPR



АЛГОРИТМ РОБОТИ ЗАСОБУ ДЛЯ ГЕНЕРУВАННЯ ОСНОВНИХ ПОЛОЖЕНЬ GDPR

ВИЗНАЧЕННЯ РІВНЯ КРИТИЧНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

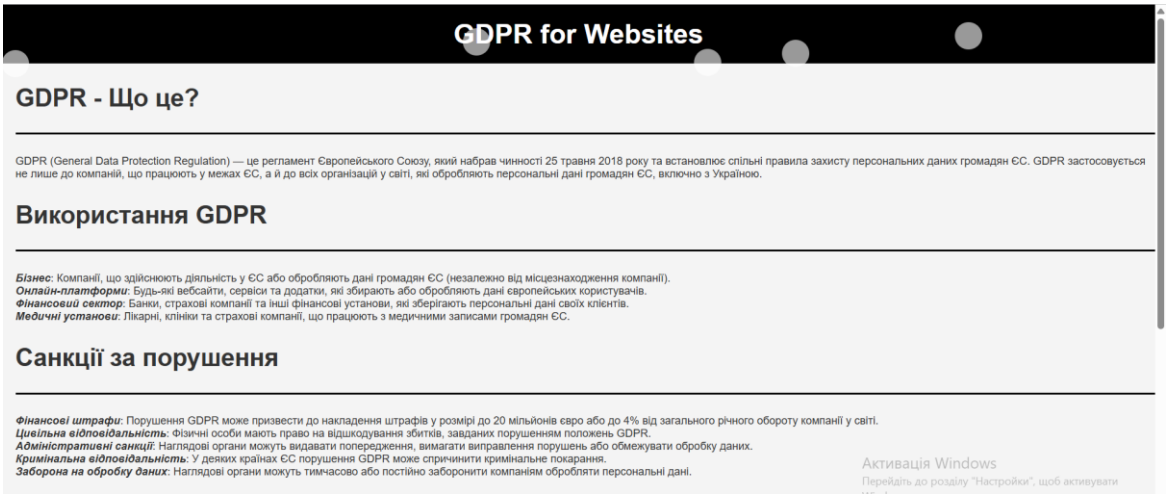
ВИЗНАЧЕННЯ РІВНЯ КРИТИЧНОСТІ ПЕРЕДАЧІ ОСОБИСТИХ ДАНИХ ТРЕТІМ СТОРОНАМ



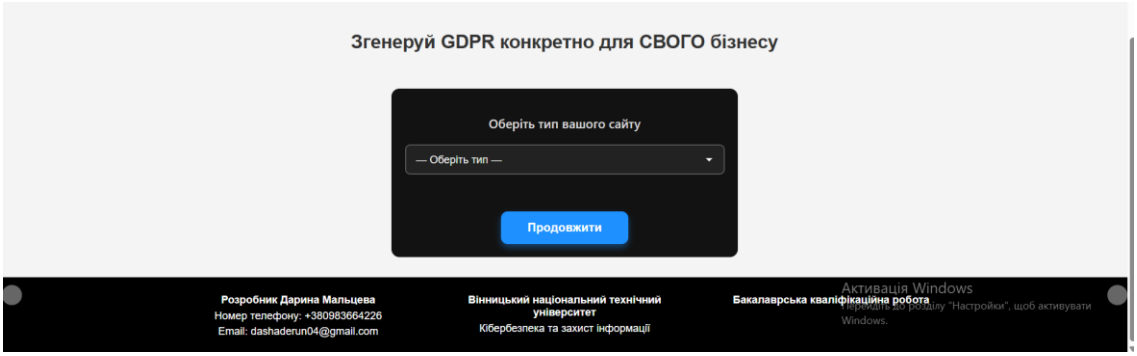
СТРУКТУРА ЗАСТОСУНКУ

АЛГОРИТМ ГЕНЕРАЦІЇ ОСНОВНИХ ПОЛОЖЕНЬ GDPR

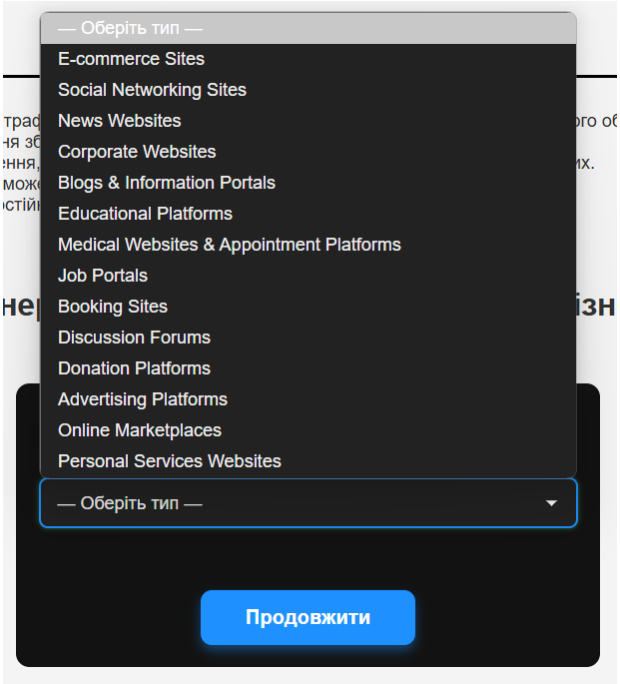
ПРИКЛАД РОБОТИ ЗАСТОСУНКУ



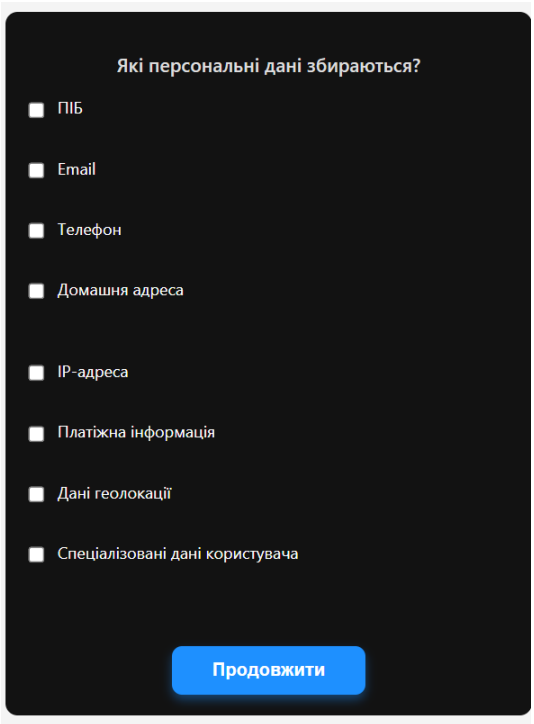
Вигляд створеного застосунку, 1 частина



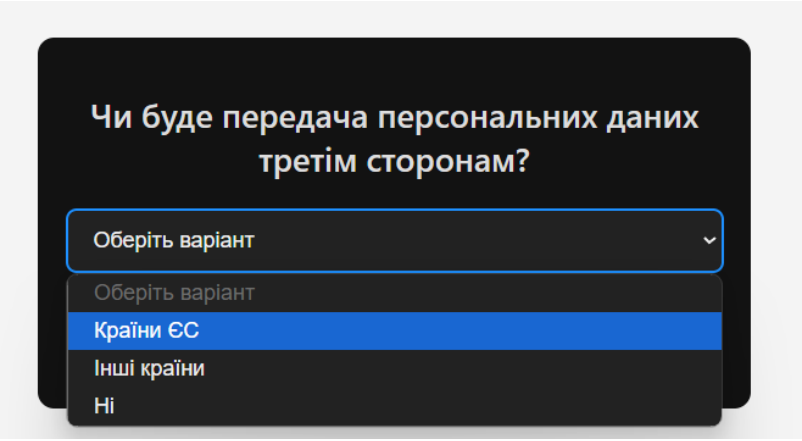
Вигляд створеного застосунку, 2 частина



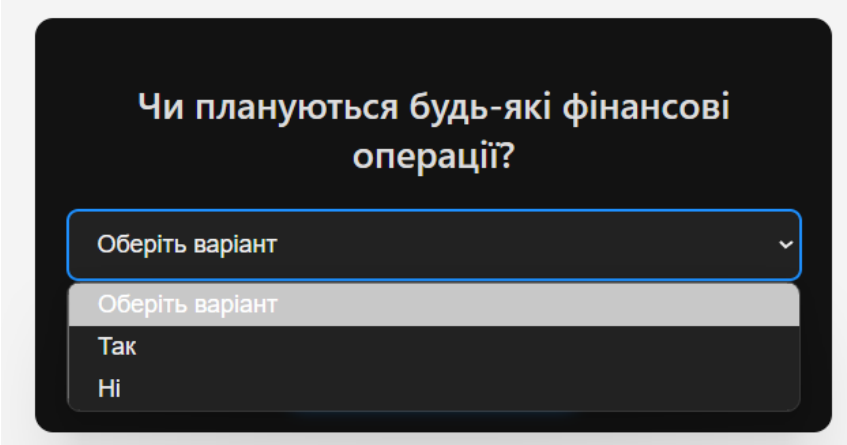
Випадаючий список для вибору типу вебсайту



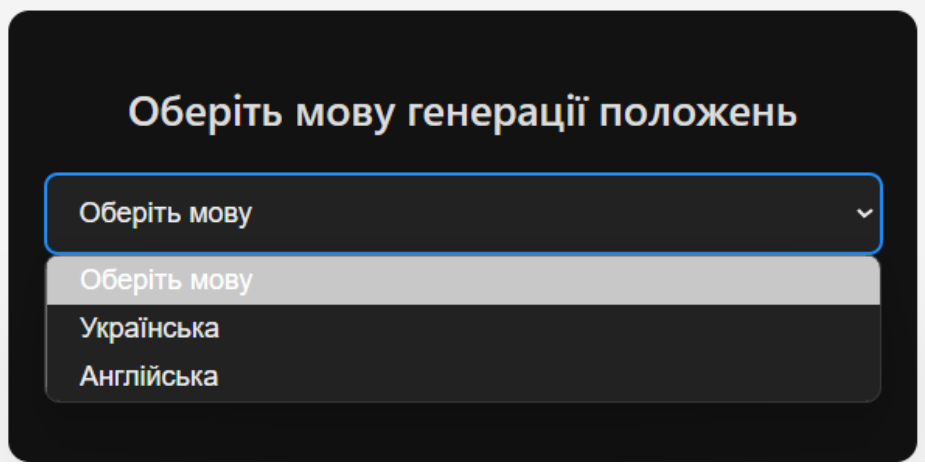
Вибір типів персональних даних клієнта



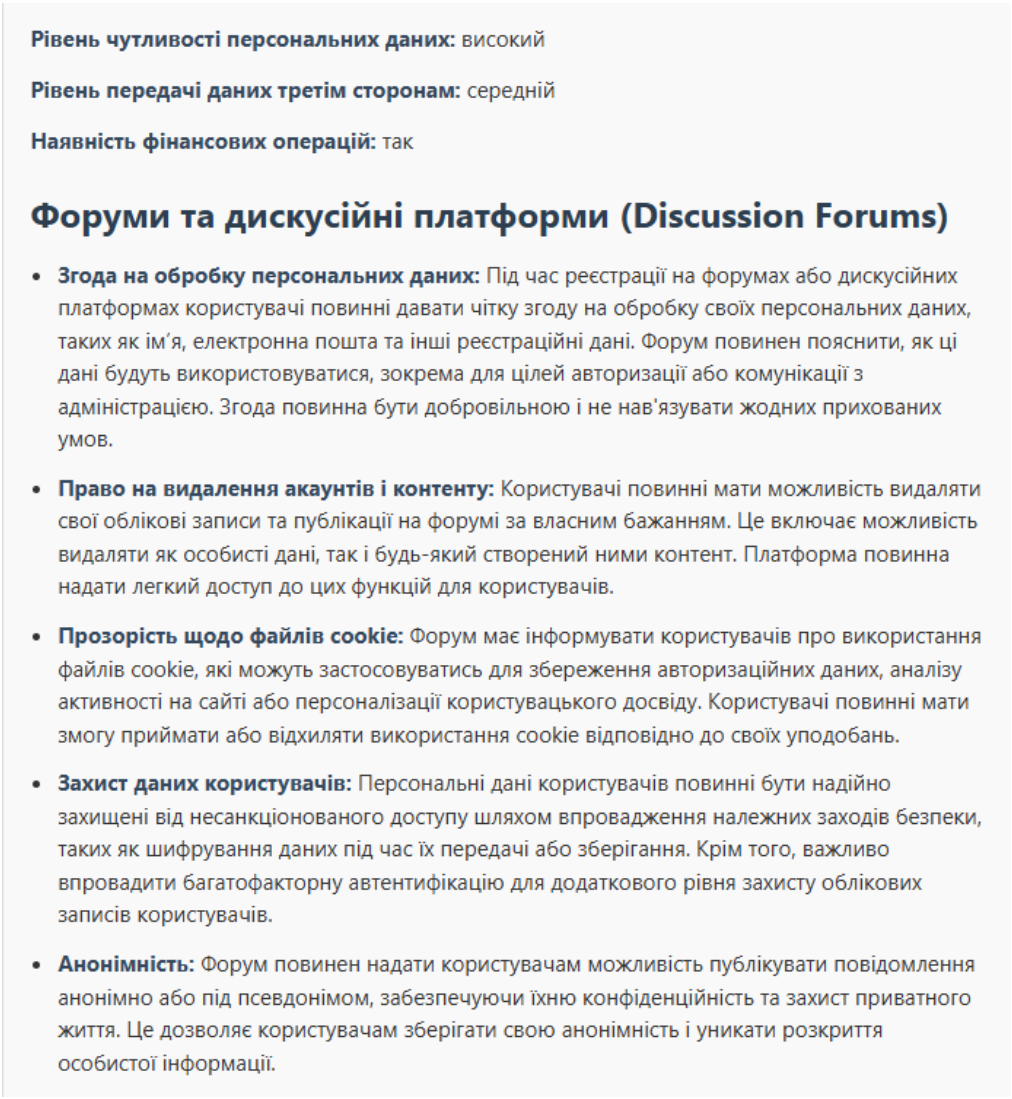
Запит про передачу персональних даних третім сторонам



Опитування про наявність будь-яких фінансових операцій



Вибір мови для генерації основних положень GDPR



Рівень чутливості персональних даних: високий

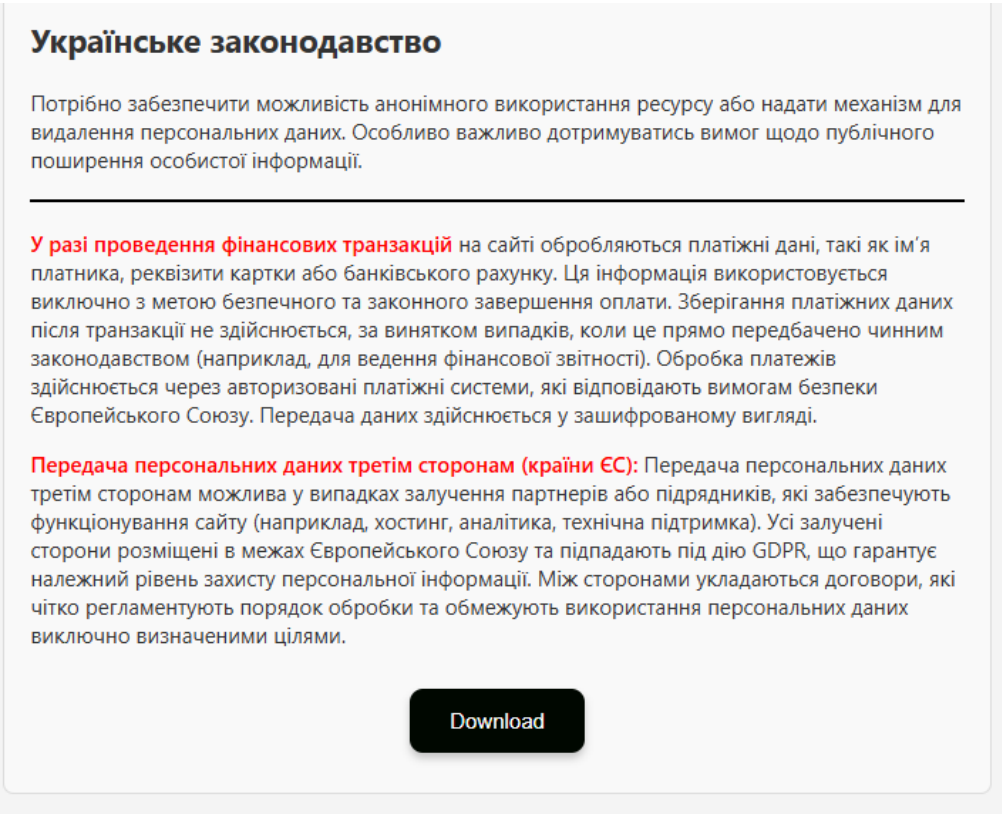
Рівень передачі даних третім сторонам: середній

Наявність фінансових операцій: так

Форуми та дискусійні платформи (Discussion Forums)

- **Згода на обробку персональних даних:** Під час реєстрації на форумах або дискусійних платформах користувачі повинні давати чітку згоду на обробку своїх персональних даних, таких як ім'я, електронна пошта та інші реєстраційні дані. Форум повинен пояснити, як ці дані будуть використовуватися, зокрема для цілей авторизації або комунікації з адміністрацією. Згода повинна бути добровільною і не нав'язувати жодних прихованих умов.
- **Право на видалення акаунтів і контенту:** Користувачі повинні мати можливість видаляти свої облікові записи та публікації на форумі за власним бажанням. Це включає можливість видаляти як особисті дані, так і будь-який створений ними контент. Платформа повинна надати легкий доступ до цих функцій для користувачів.
- **Прозорість щодо файлів cookie:** Форум має інформувати користувачів про використання файлів cookie, які можуть застосовуватись для збереження авторизаційних даних, аналізу активності на сайті або персоналізації користувацького досвіду. Користувачі повинні мати змогу приймати або відхиляти використання cookie відповідно до своїх уподобань.
- **Захист даних користувачів:** Персональні дані користувачів повинні бути надійно захищені від несанкціонованого доступу шляхом впровадження належних заходів безпеки, таких як шифрування даних під час їх передачі або зберігання. Крім того, важливо впровадити багатофакторну автентифікацію для додаткового рівня захисту облікових записів користувачів.
- **Анонімність:** Форум повинен надати користувачам можливість публікувати повідомлення анонімно або під псевдонімом, забезпечуючи їхню конфіденційність та захист приватного життя. Це дозволяє користувачам зберігати свою анонімність і уникати розкриття особистої інформації.

Основні положення GDPR для «Форуми та дискусійні платформи» (частина 1)



Основні положення GDPR для «Форуми та дискусійні платформи» (частина 2)