ЗАТВЕРДЖЕНО
Рішенням Правління АПУ
від 29 квітня 2025 р.

_____

Президент
Стеценко М.В.

Положення

про обробку та захист персональних даних Всеукраїнської громадської організації «Асоціація правників України»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. **Мета Положення**

Це Положення встановлює політику обробки та захисту персональних даних у Всеукраїнській громадській організації «Асоціація правників України» (далі – АПУ, Асоціація). Документ відповідає вимогам Закону України «Про захист персональних даних» та узгоджується з кращими практиками Регламенту (ЄС) 2016/679 (GDPR). Метою Положення є забезпечення належного, прозорого, підзвітного й правомірного поводження з персональними даними у межах усіх напрямів діяльності АПУ.

1.2. **Визначення термінів**

Терміни вживаються у значеннях, визначених у Законі України «Про захист персональних даних», GDPR, та тлумачаться відповідно до офіційних роз'яснень Європейської ради із захисту даних (EDPB). Зокрема:

Персональні дані – будь-яка інформація, що прямо або опосередковано стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи.

Обробка персональних даних – будь-яка дія або сукупність дій, що здійснюються з персональними даними, включаючи, але не обмежуючись: збирання, реєстрація, накопичення, зберігання, адаптація, зміна, поновлення, використання, поширення, передача, знеособлення, знищення.

Суб'єкт персональних даних – фізична особа, щодо якої здійснюється обробка її персональних даних.

Володілець персональних даних (контролер) – фізична або юридична особа, яка самостійно або спільно з іншими визначає мету та засоби обробки персональних даних.

Розпорядник персональних даних (обробник) – особа, яка здійснює обробку персональних даних від імені володільця згідно з договором або письмовим дорученням.

Уповноважена особа з питань захисту персональних даних (DPO) – працівник або залучений консультант, відповідальний за моніторинг дотримання законодавства про персональні дані та координацію процесів захисту в організації.

Згода на обробку персональних даних – добровільне, конкретне, інформоване та однозначне волевиявлення суб'єкта персональних даних, яке виражається шляхом заяви або активної дії.

Порушення безпеки персональних даних – випадкове або незаконне знищення, втрата, зміна, несанкціоноване розголошення чи доступ до персональних даних.

Cookies – невеликі текстові файли, які зберігаються в браузері користувача з метою ідентифікації сеансу або налаштувань.

DPIA (Data Protection Impact Assessment) – процедура оцінки впливу запланованої обробки персональних даних на права і свободи фізичних осіб з метою запобігання ризикам.

1.3. **Сфера застосування**

Це Положення застосовується до всіх форм обробки персональних даних, які здійснює АПУ у межах своєї діяльності, включаючи, але не обмежуючись:

- ведення реєстру членів АПУ;
- участь у заходах, організованих або підтриманих АПУ;
- адміністрування вебресурсів, включаючи сайт, онлайн-платформи та облікові системи;
- професійна та внутрішня комунікація;
- розсилки, маркетингові та PR-кампанії;
- співпраця з донорами, партнерами, підрядниками, державними органами.

1.4. **Принципи обробки персональних даних**

АПУ зобов'язується дотримуватись таких принципів:

- **Законність** - обробка відбувається лише на законних підставах;
- **Справедливість і прозорість** - особа має право знати, які її дані обробляються, як і з якою метою;
- **Цільове обмеження** - дані обробляються для чітко визначеної, законної мети;
- **Мінімізація** - обробляється лише той обсяг даних, який необхідний для мети;
- **Точність** - дані повинні бути актуальними, застарілі — оновлюються або видаляються;
- **Обмеження зберігання** - дані не зберігаються довше, ніж це потрібно для цілі;
- **Цілісність і конфіденційність** - впроваджено заходи для захисту від несанкціонованого доступу, втрати, пошкодження;
- **Підзвітність** - АПУ документує всі процеси та рішення щодо обробки персональних даних, зокрема веде Реєстр операцій обробки.

1.5. Роль АПУ у системі обробки даних

Асоціація правників України (АПУ) виступає **володільцем персональних даних** (відповідно до Закону України «Про захист персональних даних») та **контролером** (controller) згідно з GDPR. У разі передачі обробки третім особам – АПУ укладає договір про обробку даних (Data Processing Agreement, DPA), залишаючись відповідальною за дотримання прав суб'єктів.

1.6. Розміщення серверів та хостинг

Обробка та зберігання персональних даних може здійснюватися з використанням хмарних сервісів, розміщених в Україні, Європейському Союзі або інших країнах, які забезпечують належний рівень захисту.

1.7. Конфіденційність за задумом та за замовчуванням

АПУ впроваджує принципи конфіденційності за задумом (privacy by design) і за замовчуванням (privacy by default) , що означає впровадження технічних та організаційних заходів на всіх етапах життєвого циклу даних, зокрема:

- мінімізація обсягу персональних даних (data minimisation);
- обмеження доступу за принципом найменших прав (least privilege);
- технічна ізоляція, шифрування, псевдонімізація;
- аудит доступів, логування дій, автоматичне видалення після завершення цілей обробки.

1.8. Спільне володіння персональними даними

У випадках, коли АПУ спільно з іншим суб'єктом визначає мету та засоби обробки персональних даних (наприклад, співорганізація заходів або спільні проєкти), сторони діють як **спільні володільці персональних даних**.

У таких випадках укладається письмова угода, що визначає:

- обсяг відповідальності кожної сторони;
- порядок реалізації прав суб'єктів даних;
- точку контакту для запитів;
- дотримання принципу прозорості та відповідальності.

АПУ забезпечує інформування суб'єктів про спільне володіння через сайт та банери при реєстрації.

2. ПРАВОВІ ПІДСТАВИ ТА ЦІЛІ ОБРОБКИ

2.1. **Правові підстави обробки**

АПУ здійснює обробку персональних даних виключно на законних підставах, які включають:

- **Згода** — добровільне, інформоване волевиявлення суб'єкта, надане шляхом підпису або через активну дію (наприклад, реєстрація, позначка у вебформі);
- **Укладення або виконання договору** — коли обробка є необхідною для виконання договірних зобов'язань або для дій до його укладення;
- **Юридичний обов'язок** — коли АПУ зобов'язана обробляти дані для дотримання законодавства (наприклад, ведення бухгалтерського обліку);
- **Законний інтерес** — наприклад, адміністрування системи членства, захист від шахрайства, розвиток діяльності;
- **Життєво важливі інтереси** — обробка необхідна для захисту життя чи здоров'я суб'єкта чи іншої особи.

2.2. **Цілі обробки персональних даних**

Обробка даних здійснюється виключно у межах наступних цілей:

- забезпечення членства в АПУ, адміністрування бази членів;
- організація заходів, конкурсів, конференцій, семінарів, онлайн-курсів;
- комунікація з членами, учасниками, експертами, спікерами та партнерами;

- ведення фінансового та юридичного обліку, статистичної звітності;
- здійснення контактної взаємодії (email, телефон, месенджери);
- підготовка та поширення інформаційних та маркетингових матеріалів (включно з фото/відео);
- забезпечення безпеки цифрової інфраструктури, реєстрація запитів та інцидентів;
- виконання вимог чинного українського та міжнародного законодавства;
- інформування громадськості про діяльність АПУ та її представників.

3. КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. **Загальні категорії персональних даних**

АПУ може збирати та обробляти наступні категорії даних:

- Прізвище, ім'я, по батькові;
- Дата народження;
- Місце роботи, посада, професійна належність;
- Заклад вищої освіти та рік його закінчення;
- Контактні дані: номер телефону, адреса електронної пошти, поштова адреса;
- Дані про членство в АПУ, історія участі у заходах, участь у голосуваннях та опитуваннях;
- Платіжна інформація (лише в частині, що не порушує банківську таємницю, наприклад: факт оплати, сума, дата);
- Відомості, які суб'єкт самостійно надає у комунікації (email, анкети, звернення).

3.3. **Журнал взаємодії з суб'єктами даних** DPO АПУ веде **реєстр запитів та взаємодії із суб'єктами персональних даних**, який містить:

- дату запиту;
- суть звернення;
- особу, що подала запит (верифіковано);
- строк та спосіб відповіді;
- вжиті заходи (внесення змін, видалення, надання копії даних).

Цей журнал є частиною системи доказів підзвітності та доступний для внутрішніх і регуляторних перевірок.

3.4. Технічні та автоматично зібрані дані

Під час користування сайтом АПУ автоматично обробляються такі дані:

- IP-адреса;
- Тип браузера, операційна система;
- Геолокація (якщо дозволено користувачем);

- Cookies — за згодою користувача через банер;

- Поведінкові дані: сторінки, час перебування, джерело переходу.

Ці дані використовуються виключно для статистики, захисту системи, аналізу ефективності й не ідентифікують особу напряму без додаткових заходів.

3.4. **Джерела отримання персональних даних**

Персональні дані, що обробляються АПУ, можуть бути отримані:

- безпосередньо від суб'єкта даних (реєстраційні форми, анкети, звернення);

- з відкритих джерел (публічні реєстри, професійні бази, офіційні сайти);

- із соціальних мереж (LinkedIn, Facebook, X, Instagram) та Telegram каналу АПУ - лише з публічно доступного профілю або за згодою;

- з CRM-платформ, email-маркетингових інструментів (Mailchimp, Bitrix24, Sendpulse тощо);10

- через веб-аналітику (Google Analytics, Hotjar, Matomo);

- від партнерів/співорганізаторів заходів – за умови дотримання законних підстав та обов'язку інформування.

3.5. **Профіль ризику обробки персональних даних**

АПУ запроваджує системний підхід до аналізу ризиків, що супроводжують обробку персональних даних. Перед впровадженням нової категорії обробки проводиться оцінка за такими критеріями:

- обсяг і масштаб даних;

- категорії суб'єктів (зокрема, вразливі групи);

- наявність спеціальних або біометричних даних;

- ризик автоматизованого прийняття рішень або профілювання;

- транскордонна передача даних.

Ризики класифікуються як:

- **низькі** — базові операції з даними (наприклад, облік учасників заходів);

- **помірні** — регулярна комунікація з членами, обробка внесків;

- **високі** — медіаархіви, аналітика поведінки, нові цифрові сервіси.

Для обробки з високим ризиком обов'язково проводиться оцінка DPIA, результати якої фіксуються DPO.

3.6. **Строки зберігання персональних даних**

Категорія даних	**Строк зберігання**	**Уточнення**

Дані членів АПУ	строк членства + 5 років	для юридичних зобов'язань та архівування
Дані учасників заходів	до 3 років після події	або до відкликання згоди
Платіжні реквізити	згідно з політиками банків, що задіяні в транзакції	згідно з бухгалтерськими вимогами
Фото/відео матеріали	до 10 років або відкликання згоди	для комунікацій та архіву
Cookies/аналітика	до 12 місяців	анонімізовано або за згодою

4. ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

4.1. **Основні права**

- Кожен суб'єкт персональних даних має такі права:
- **Право на поінформованість** — бути повідомленим про обробку даних, її мету, обсяг, підстави, отримувачів та строки зберігання;
- **Право на доступ** — отримати підтвердження факту обробки, копію своїх даних та інформацію про джерело їх надходження;
- **Право на виправлення** — вимагати внесення змін у разі неточності або неповноти даних;
- **Право на видалення («право бути забутим»)** — видалення персональних даних, якщо:
    - дані більше не потрібні;
    - суб'єкт відкликає згоду;
    - обробка була незаконною;
    - існує юридичний обов'язок;
- **Право на обмеження обробки** — у випадках спору щодо точності, правомірності або потреби в обробці;
- **Право на перенесення даних** — отримати свої дані в структурованому, машиночитаному форматі та передати іншому контролеру;
- **Право на заперечення проти обробки** — у разі обробки на основі законного інтересу або для маркетингових цілей;
- **Право не бути об'єктом виключно автоматизованого рішення** — якщо таке рішення має юридичні наслідки або значно впливає на особу.

4.2. **Порядок реалізації прав**

Суб'єкт може звернутись із письмовим або електронним запитом на адресу АПУ чи на email: members@uba.ua.

Запит має містити:

- прізвище, ім'я, контактні дані заявника;
- суть запиту або вимоги;
- підтвердження особи (копія документа або електронний цифровий підпис).

4.3. **Строки та механізм реагування**

- АПУ реагує протягом 30 календарних днів з моменту отримання запиту.
- За потреби продовження строку - надається обґрунтоване повідомлення не пізніше ніж через 30 днів.

4.4. **Верифікація особи**

АПУ має право перевірити ідентичність особи, яка подає запит, з метою запобігання несанкціонованого доступу до персональних даних третіх осіб.

4.5. **Обмеження реалізації прав** У виняткових випадках реалізація прав може бути обмежена, якщо це прямо передбачено законом або необхідне:

- для захисту державної безпеки чи громадського порядку;
- для запобігання злочину;
- для забезпечення прав і свобод інших осіб.

4.6. **Право на звернення до наглядового органу**

Суб'єкт має право подати скаргу до:

- Уповноваженого Верховної Ради України з прав людини;
- Наглядового органу ЄС (якщо обробка підпадає під юрисдикцію GDPR).

5. COOKIES, АВТОМАТИЗОВАНА ОБРОБКА ТА МАРКЕТИНГ

5.1. **Cookies та аналітика**

Під час відвідування офіційного сайту АПУ можуть використовуватись файли cookie — невеликі фрагменти даних, що зберігаються у браузері користувача. Cookies поділяються на:

- **Технічно необхідні** — забезпечують базову функціональність сайту (наприклад, навігація);
- **Аналітичні** — дозволяють вимірювати ефективність сайту та взаємодії (Google Analytics);
- **Маркетингові** — використовуються для персоналізації контенту чи аналізу аудиторії (тільки за згодою).

Перед встановленням non-essential cookies запитуємо згоду користувача через банер. Налаштування cookie можуть бути змінені в будь-який час у браузері користувача. Докладніше — в окремій **Політиці використання cookies (Додаток 1)**.

5.2. **Автоматизоване прийняття рішень та профілювання**

АПУ не здійснює прийняття рішень, що базуються виключно на автоматизованій обробці, які могли б спричинити юридичні наслідки для суб'єкта даних. Якщо в майбутньому така обробка буде застосовуватись (наприклад, у CRM-системах), суб'єкт буде окремо поінформований, а обробка здійснюватиметься лише:

- на підставі явної згоди;
- якщо це необхідно для виконання договору;
- якщо це дозволено законом з відповідними гарантіями прав.

5.3. **Обробка даних з маркетинговою метою**

АПУ може використовувати персональні дані для надсилання інформаційних листів, запрошень, новин та повідомлень про заходи. Всі такі розсилки здійснюються:

- виключно за наявності згоди (opt-in);
- з можливістю у будь-який момент відмовитись від отримання (opt-out) шляхом натискання на відповідне посилання або звернення на email: members@uba.ua.

5.4. **Передача даних обробникам (процесорам)** У випадках, коли АПУ залучає підрядників для надання технічних, комунікаційних чи інших послуг, що передбачають доступ до персональних даних, з такими особами укладається **договір про обробку даних (DPA)**, який включає:

- обмеження цілей обробки;
- вимоги до захисту та збереження даних;
- обов'язок не передавати дані третім сторонам без дозволу АПУ;
- право АПУ здійснювати аудит та контроль виконання обов'язків.

Обробники діють виключно на підставі письмового договору і під наглядом DPO.

6. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ НЕПОВНОЛІТНІХ

6.1. **Загальні правила**

АПУ не здійснює цілеспрямованого збору персональних даних осіб, які не досягли 18-річного віку. У разі, якщо обробка таких даних є необхідною (наприклад, участь неповнолітніх у конкурсах, заходах, програмах), вона допускається лише за умови надання **письмової згоди одного з батьків або законного представника**.

6.2. **Перевірка віку**

При підозрі, що особа є неповнолітньою, АПУ залишає за собою право запросити додаткові документи для перевірки віку та надання підтвердження батьківської згоди.

6.3. **Особливий захист**

Усі дані неповнолітніх підлягають підвищеному рівню захисту. Вони:

- не передаються третім особам без окремої згоди;
- не використовуються для маркетингу, профілювання чи автоматизованих рішень;
- зберігаються окремо від інших даних та видаляються одразу після досягнення мети.

6.4. **Право на видалення**

На вимогу батьків або законного представника, персональні дані неповнолітньої особи підлягають негайному видаленню, якщо обробка не базується на юридичному обов'язку.

7. УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

7.1. **Призначення**

Уповноважена особа з питань захисту персональних даних (Data Protection Officer, DPO) призначається розпорядчим актом Виконавчого директора Асоціації або залучається як консультант за цивільно-правовим договором. Призначення, права та функції регулюються цим Положенням, контрактом або внутрішнім розпорядженням.

7.2. **Основні обов'язки DPO**

- моніторинг дотримання вимог GDPR, Закону України та внутрішніх політик;
- ведення реєстрів згод, запитів, інцидентів, DPIA;
- розгляд звернень суб'єктів персональних даних;
- участь у розробці внутрішніх процедур та аудитів;
- інформування та навчання працівників;
- співпраця з Уповноваженим ВРУ та наглядовими органами ЄС.

7.3. **Повноваження**

- доступ до всієї документації, IT-систем, баз даних, серверних приміщень;
- право без попереднього погодження проводити аудит і перевірку процесів обробки персональних даних;
- ініціювання дисциплінарних заходів при порушеннях вимог політики або законодавства;
- безпосереднє інформування керівництва про ризики та порушення.

7.4. **Гарантії незалежності**

- DPO діє незалежно, не отримуючи вказівок щодо змісту діяльності;
- не підлягає звільненню або покаранню за добросовісне виконання функцій;
- має пряме право звернення до Президента та Правління АПУ.

7.5. **Контактна інформація** DPO АПУ може бути досяжний за електронною адресою: members@uba.ua .

8. DPIA — ОЦІНКА ВПЛИВУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

8.1. **Що таке DPIA**

Оцінка впливу на захист персональних даних (Data Protection Impact Assessment, DPIA) — це процес виявлення, аналізу й мінімізації ризиків для прав і свобод фізичних осіб у випадках, коли запланована обробка даних може створювати високі ризики.

8.2. **Коли обов'язкова DPIA:**

- при масовому або систематичному моніторингу поведінки;

- обробка даних спеціальних категорій (здоров'я, біометрія, політичні погляди тощо);
- використання нових технологій (наприклад, штучний інтелект);
- коли обробка охоплює велику кількість суб'єктів;
- обробка з можливим суттєвим впливом на права осіб.

8.3. **Ключові етапи DPIA:**

- опис передбачуваних процесів обробки, обсягів та категорій даних;
- визначення законних підстав і мети обробки;
- аналіз потенційних ризиків для суб'єктів даних (конфіденційність, свобода, безпека);
- опис заходів захисту, технічних та організаційних рішень;
- підготовка висновку з рекомендаціями.

8.4. **Роль DPO в DPIA**

Уповноважена особа з питань захисту персональних даних (DPO):

- консультує щодо обов'язковості DPIA;
- бере участь у плануванні обробки та виборі механізмів захисту;
- документує проведення DPIA та її результати;
- веде реєстр DPIA як додаток до основного Реєстру операцій обробки.

8.5. **DPO має право:**

- ініціювати та проводити аудит внутрішніх процесів з обробки персональних даних;
- безперешкодно відвідувати всі фізичні приміщення, де обробляються персональні дані (в т.ч. серверні кімнати, архіви, робочі місця);
- копіювати та фіксувати зміст документів, журналів, системних логів і баз даних, якщо це необхідно для перевірки відповідності або розслідування порушення.

8.5. **Зовнішнє погодження**

Якщо за результатами DPIA ризики залишаються високими і не можуть бути знижені, АПУ звертається до наглядового органу за попередньою консультацією (ст. 36 GDPR).

9. ІНЦИДЕНТИ ТА РЕАГУВАННЯ НА ПОРУШЕННЯ

9.1. **Визначення порушення**

Порушенням безпеки персональних даних вважається будь-яка подія, що призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розголошення чи доступу до персональних даних (ст. 4(12) GDPR).

9.2. **Класифікація інцидентів**

- **Технічні**: збій програмного забезпечення, злом, вірусні атаки;
- **Організаційні**: несанкціонований доступ, відправлення інформації не тому адресату;

- **Фізичні**: втрата носія, крадіжка документації.

9.3. **Дії у разі виявлення порушення**

- негайне повідомлення Уповноваженої особи (DPO);
- реєстрація інциденту в журналі безпеки;
- технічний аналіз джерела, масштабів і наслідків;
- впровадження невідкладних заходів захисту (блокування доступу, ізоляція тощо).

9.4. **Повідомлення наглядовому органу**

DPO забезпечує повідомлення Уповноваженого Верховної Ради України з прав людини:

- **не пізніше 48 годин** після виявлення порушення (Закон України);
- **не пізніше 72 годин** — якщо підпадає під дію GDPR.

Повідомлення включає:

- характер порушення;
- ймовірні наслідки;
- категорії уражених даних і суб'єктів;
- заходи, яких вжито або планується вжити;
- контактні дані DPO.

9.5. **Повідомлення суб'єкта даних**

Якщо порушення може створити високий ризик для прав і свобод фізичної особи, її має бути **негайно поінформовано** про порушення з роз'ясненням:

- суті інциденту;
- наслідків;
- рекомендованих заходів захисту.

9.6. **Ведення реєстру порушень**

АПУ веде внутрішній **Реєстр порушень персональних даних**, у якому фіксуються всі випадки з:

- датою, типом, описом інциденту;
- оцінкою ризиків;
- рішенням щодо повідомлення;
- подальшими діями.

10. ОЦІНКА КОНТРАГЕНТІВ — ПРОТОКОЛ ПЕРЕВІРКИ

Усі зовнішні підрядники, які залучаються АПУ для обробки персональних даних (у тому числі CRM-платформи, email-сервіси, організатори заходів), проходять попередню оцінку відповідності. DPO АПУ здійснює перевірку за такими критеріями:

- юрисдикція постачальника та відповідність вимогам GDPR або Закону України;
- сертифікація безпеки (ISO 27001, SOC 2 тощо);
- політики конфіденційності, шифрування, реагування на інциденти;
- практики ведення журналів та реагування на запити суб'єктів;
- наявність підписаного договору про обробку даних (DPA).

11. ЗОВНІШНІ ЗАПИТИ ТА ПОРЯДОК НАДАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

АПУ діє виключно в межах законодавства при отриманні запитів від правоохоронних, контролюючих, судових органів або третіх осіб.

Перед передачею будь-яких персональних даних зовнішнім заявникам, АПУ:

- перевіряє повноваження запитувача (офіційний лист, судове рішення);
- фіксує запит у журналі взаємодії з суб'єктами даних;
- погоджує передачу з DPO;
- інформує суб'єкта даних (якщо це не заборонено законом);
- забезпечує передання лише мінімально необхідного обсягу даних.

Відповіді без належного правового обґрунтування не надаються. Інструкція щодо дій при надходженні запитів є обов'язковою для персоналу.

12. ІНСТРУКЦІЯ ДЛЯ ВІДДІЛЕНЬ АПУ

Особи, які представляють АПУ у регіонах (Голови відділень та члени Рад відділень, а також Секретаріат) та мають доступ до персональних даних під час проведення заходів, комунікацій або збору інформації, зобов'язані:

- діяти виключно відповідно до цього Положення та під наглядом DPO;
- забезпечити збирання згод на обробку даних при кожному заході (онлайн чи офлайн);
- інформувати суб'єктів про політику;
- не зберігати персональні дані на особистих пристроях без належного захисту;
- не публікувати фото/відео осіб без згоди, крім явно публічних подій;
- передавати зібрані дані в АПУ через захищені канали;
- повідомляти DPO про будь-які інциденти або запити, пов'язані з персональними даними.

13. ОНОВЛЕННЯ ПОЛІТИКИ, РЕЄСТРИ ТА ЗАТВЕРДЖЕННЯ

13.1. **Перегляд та оновлення**

Це Положення:

- переглядається на необхідність приведення до відповідності чинному законодавству щонайменше один раз на рік;

- оновлюється у випадку змін законодавства, регуляторних вимог, технологій або підходів до обробки даних;
- затверджується Правлінням АПУ, з публікацією актуальної версії на офіційному вебсайті.

DPO ініціює перегляд, здійснює аудит відповідності, готує пропозиції до змін.

13.2. **Ведення обліку та реєстрів** АПУ веде:

- **Реєстр операцій з обробки персональних даних**;
- **Реєстр згод** (із фіксацією дати, обсягу, способу надання);
- **Реєстр запитів суб'єктів** (із результатами обробки);
- **Реєстр DPIA** та **Журнал інцидентів**.

13.3. **Затвердження**

Це Положення набирає чинності з моменту його затвердження Правлінням ВГО «Асоціація правників України» та є обов'язковим для Секретаріату, волонтерів, підрядників і партнерів Асоціації.

ДОДАТКИ:

- Додаток 1. Політика використання cookies;
- Додаток 2. Шаблон згоди на обробку персональних даних;
- Додаток 3. Форма запиту на доступ/виправлення/видалення даних;
- Додаток 4. Шаблон DPIA (оцінка впливу);
- Додаток 5. Інструкція для Секретаріату щодо безпечної обробки даних.

ДОДАТОК 1.

ПОЛІТИКА ВИКОРИСТАННЯ COOKIES

Ця Політика пояснює, як Асоціація правників України (АПУ) використовує файли cookies під час відвідування сайту www.uba.ua .

1. **Що таке cookies** Cookies — це невеликі текстові файли, які зберігаються на пристрої користувача при відвідуванні вебсайтів. Вони допомагають сайту запам'ятати налаштування та покращують користувацький досвід.

2. **Типи cookies, які ми використовуємо**

   - **Сесійні cookies** — зберігаються тимчасово і видаляються після завершення сеансу;

   - **Постійні cookies** — зберігаються протягом заданого періоду часу або до їх видалення;

   - **Аналітичні cookies** — збирають інформацію про взаємодію користувача з сайтом (наприклад, Google Analytics);

   - **Функціональні cookies** — дозволяють сайту запам'ятовувати вибір користувача (мова, регіон);

   - **Маркетингові cookies** — використовуються для персоналізації контенту (встановлюються тільки після отримання згоди).

3. **Правові підстави використання cookies** Використання cookies здійснюється відповідно до законного інтересу АПУ (функціональні, безпечні cookies) або **за згодою користувача** (аналітичні, маркетингові cookies), яку можна надати або відкликати через банер згоди.

4. **Як керувати cookies** Користувач може:

   - налаштувати свій браузер на блокування cookies або повідомлення про їх використання;

   - змінити або відкликати свою згоду через банер cookies на сайті;

   - видалити cookies з історії браузера у будь-який момент.

5. **Контакти** З усіх питань щодо cookies звертайтесь на members@uba.ua .

ДОДАТОК 2.

ШАБЛОН ЗГОДИ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Я, _____, (ПІБ повністю)

ідентифікаційний код/паспортні дані: _____

контактні дані (телефон, e-mail): _____

надаю свою добровільну, однозначну, поінформовану згоду Всеукраїнській громадській організації «Асоціація правників України» (далі – АПУ) на обробку моїх персональних даних з метою:

- участі у заходах, організованих АПУ;
- отримання інформаційних та рекламних матеріалів;
- ведення внутрішньої бази даних членів і партнерів;
- виконання зобов'язань згідно з чинним законодавством України.

Обсяг персональних даних, які підлягають обробці:

- ПІБ;
- контактні дані (телефон, e-mail, адреса);
- місце роботи, посада;
- участь у заходах АПУ та історія взаємодії;
- інші дані, добровільно надані мною АПУ.

Ця згода надається строком на 10 (десять) років або до моменту її відкликання мною шляхом письмового звернення.

Я ознайомлений(а) з:

- правами суб'єкта персональних даних;
- метою обробки даних;
- політикою конфіденційності АПУ;
- правом відкликати згоду у будь-який момент.

Дата: «_**»** _____ **20**__ р.

Підпис: _____

ДОДАТОК 3.

ФОРМА ЗАПИТУ НА ДОСТУП / ВИПРАВЛЕННЯ / ВИДАЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

До: Уповноваженої особи з питань захисту персональних даних Всеукраїнської громадської організації «Асоціація правників України» e-mail: members@uba.ua

Від: _____ (ПІБ повністю)

Ідентифікаційний код / серія та номер паспорта: _____

Контактні дані: _____

ЗАПИТ

На підставі Закону України «Про захист персональних даних» та ст. 15–21 GDPR прошу:

☐ Надати доступ до моїх персональних даних, які обробляє АПУ;

☐ Надати копію всіх персональних даних, які зберігаються;

☐ Внести наступні зміни / уточнення: _____

☐ Видалити мої персональні дані (право на забуття);

☐ Обмежити обробку даних у зв'язку з: _____

☐ Надати інформацію про отримувачів або категорії отримувачів моїх персональних даних;

☐ Інше: _____

Підтвердження особи додається:

☐ Копія паспорта / ID-картки або інший документ, що посвідчує особу;

☐ Повірений документ (якщо запит подається представником).

Дата: «_**»** _____ **20**__ р.

Підпис: _____

ДОДАТОК 4.

ШАБЛОН DPIA (ОЦІНКА ВПЛИВУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ)

1. **Назва проєкту/процесу:**

---

2. **Опис операцій обробки даних:**

---

3. **Мета обробки:**

---

4. **Категорії суб'єктів даних:**

---

5. **Категорії персональних даних:**

---

6. **Обсяг даних та строки зберігання:**

---

7. **Передбачувані ризики для прав і свобод суб'єктів:**
   -
   -
   -

8. **Заходи для зниження ризиків:**
   - Технічні (шифрування, доступ за паролем, тощо): _____
   - Організаційні (інструктажі, політики, аудит): _____
9. **Участь DPO (коментарі, рекомендації):**

---

10. **Висновок DPIA:** ☐ Ризики прийнятні без погодження з регулятором; ☐ Необхідна консультація з наглядовим органом (ст. 36 GDPR).

Дата складання: «_» _____ 20____ р.

Особа, відповідальна за DPIA: _____

ДОДАТОК 5.

ІНСТРУКЦІЯ ДЛЯ СЕКРЕТАРІАТУ ЩОДО БЕЗПЕЧНОЇ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

1. **Доступ до персональних даних**

- Доступ надається лише тим з Секретаріату, які мають відповідні повноваження чи функціональні обов'язки.
- Заборонено передавати логіни та паролі третім особам.

2. **Захист робочого простору**

- Завжди блокувати комп'ютер у період його невикористання
- Документи з персональними даними не повинні зберігатися на столі або в загальнодоступних місцях.

3. **Передача даних**

- Дані передаються лише через захищені канали;
- Email із персональними даними має бути захищений паролем або вкладеним архівом із паролем, який передається окремо.

4. **Знищення та утилізація**

- Документи, що містять персональні дані, підлягають знищенню шредером або іншим безпечним способом після завершення строку зберігання.

5. **Флешки та зовнішні носії**

- Заборонено використовувати незашифровані USB-накопичувачі;
- Всі знімні носії мають бути зареєстровані в IT-службі.

6. **Поведінка в інтернеті**

- Заборонено завантажувати файли з ненадійних джерел;
- Не слід відкривати посилання з підозрілих листів або месенджерів.

7. **Повідомлення про інциденти**

- У разі підозри на порушення конфіденційності даних негайно повідомити DPO (members@uba.ua);

- Не вживати самостійних дій до консультації з DPO.

8. **Відповідальність**

- Порушення цієї Інструкції може спричинити відповідальність згідно з законодавством.

9. **Підтвердження ознайомлення**

- Кожен із Секретаріату зобов'язаний підписати цю Інструкцію перед початком роботи або після внесення змін.

Дата ознайомлення: «_**»** _____ 20____ р.

ПІБ: _____

Підпис: _____