Уповноважений
Верховної Ради України
з прав людини

РЕКОМЕНДАЦІЇ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ДИСТАНЦІЙНОГО НАДАННЯ ОСВІТНІХ ПОСЛУГ

Київ
2021

Уповноважений
Верховної Ради України
з прав людини

*Рекомендації розроблено за участі **Інни Берназюк**, представника Уповноваженого у сфері захисту персональних даних; **Марії Колосової**, начальника відділу взаємодії із суб'єктами обробки персональних даних Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого; **Олени Гунько**, завідувача сектору упровадження міжнародних стандартів у сфері захисту персональних даних Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого, та із урахуванням експертних консультацій, наданих у рамках Спільного проєкту Європейського Союзу та Ради Європи "Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини".*

Co-funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of Europe

Дизайн розроблено з використанням платформи графічного дизайну Canva.

ЗМІСТ

Передмова

Від початку пандемії, спричиненої поширенням гострої респіраторної хвороби COVID-19 набрало обертів використання різноманітних онлайн-платформ, месенджерів і чатів під час дистанційного надання освітніх послуг.

Застосування цифрових технологій з метою організації освітнього процесу значно розширило можливості надавачів освітніх послуг. Проте застосування таких методів, технологій та інструментів тісно пов'язано з безпекою в роботі та має вплив на використання і обробку персональних даних здобувачів освіти.

В ході здійснення Уповноваженим Верховної Ради України з прав людини аналізу стану забезпечення права на приватність під час дистанційного надання освітніх послуг виявлено необхідність надання рекомендацій, що допоможуть суб'єктам освітньої діяльності розібратися із практичними аспектами застосування норм законодавства у сфері захисту персональних даних та уніфікувати практику з метою запобігання порушенням, що виникають у зв'язку із застосуванням інформаційно-комунікаційних технологій і систем у сфері освіти.

Рекомендації сприятимуть кращому розумінню, як захистити персональні дані під час дистанційного навчання, та напрацюванню якісних нормативно-правових актів, що регулюватимуть порядок обробки та захисту персональних даних у освіті цій сфері.

І. Нормами яких законодавчих актів необхідно керуватися під час обробки персональних даних?

В Україні наразі немає чітко визначеної нормативно-правової бази, яка регулювала б питання безпеки суб'єктів освітньої діяльності під час дистанційного навчання, у тому числі безпеки роботи з персональними даними.

Проте є загальні норми законодавства, якими необхідно керуватися суб'єктам освітньої діяльності:

- Конституцією України, зокрема, статтями 8, 9, 22–24, 26, 31, 32, 52, 53,
- Конвенцією про захист прав людини і основоположних свобод (стаття 8),
- Конвенцією про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108),
- Конвенцією ООН про права дитини,
- Законом України «Про інформацію»,
- Законом України «Про захист персональних даних»,
- Типовим порядком обробки персональних даних та Порядком повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, затвердженими Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14,
- а також іншими законами і підзаконними нормативно-правовими актами України, які регулюють суспільні відносини у галузі освіти. Зокрема, йдеться про: Сімейний кодекс України, Цивільний кодекс України, закони України «Про освіту», «Про повну загальну середню освіту», «Про вищу освіту», постанову Кабінету Міністрів України від 13.07.2011 № 752 «Про створення Єдиної державної електронної бази з питань освіти», наказ Міністерства освіти і науки, молоді та спорту України від 10.05.2011 № 423 «Про затвердження єдиних зразків обов'язкової ділової документації у загальноосвітніх навчальних закладах усіх типів і форм власності».

Також необхідно звернути увагу на Керівні принципи щодо захисту даних дітей в освітньому середовищі, схвалені 20.11.2020 Консультативним комітетом Конвенції 108 та на рекомендації, розроблені Міжнародним союзом електрозв'язку «Захист дітей у цифровому середовищі: рекомендації для батьків та освітян».

Варто пам'ятати, якщо міжнародним договором, згода на який надана Верховною Радою України, передбачено інше правило, ніж у нормах законодавчих актів України, застосовуються правила, передбачені у відповідних міжнародних договорах.

II. Вимоги до обробки персональних даних та алгоритм дій закладів освіти для забезпечення безпеки персональних даних під час дистанційного навчання

Загальні вимоги до обробки персональних даних, в тому числі захисту персональних даних, визначені в Законі України «Про захист персональних даних» (далі – Закон).

Ураховуючи положення цього Закону та організовуючи обробку персональних даних учасників освітнього процесу під час дистанційного навчання, перш ніж обрати освітню платформу, необхідно визначитися з:

- правовою підставою для обробки персональних даних;
- складом та змістом персональних даних, що будуть оброблятися;
- метою обробки персональних даних;
- порядком обробки персональних даних.

Слід розглянути детальніше кожний з пунктів.

Правова підстава для обробки персональних даних учасників освітнього процесу

Відповідно до частини п’ятої статті 6 Закону обробка персональних даних відбувається лише на підставі згоди суб’єкта персональних даних або закону.

Зокрема, у статті 11 Закону передбачено 6 підстав для обробки персональних даних. Умовно їх можна поділити на дві групи залежно від того, чи вони ґрунтуються на підставі згоди суб’єкта персональних даних чи закону.

При цьому необхідно враховувати, якщо обробка персональних даних здійснюється на підставі закону, додатково вимагати згоду на обробку персональних даних не потрібно.

Обробка персональних даних закладами освіти під час освітньої діяльності здійснюється відповідно до законодавства про освіту, зокрема, відповідно до Закону України «Про освіту», Положення про дистанційну форму здобуття повної загальної середньої освіти, затвердженого наказом Міністерства освіти і науки України від 08.09.2020 № 1115, тобто підставою для обробки персональних даних є закон, а точніше пункти 2, 5 частини першої статті 11 Закону.

Водночас у разі зміни мети обробки персональних даних здобувачів освіти та/або їхніх законних представників заклад освіти або інший суб’єкт освітньої діяльності, який виконує обов’язки володільця, зобов’язаний отримати згоду на обробку персональних даних відповідно до зміненої мети.

Згода на обробку персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

З огляду на зміст визначення згода на обробку персональних даних має відповідати таким вимогам:

- ✓ **добровільність** – означає відсутність прямого або опосередкованого примусу при її наданні;
- ✓ **поінформованість** – означає, що перед наданням згоди суб'єкт повинен отримати достовірну інформацію про те, ким, з якою метою будуть оброблятися його персональні дані, кому будуть передаватися, які саме дані, а також про права, визначені Законом);
- ✓ **форма надання згоди може бути будь-якою** – означає, що умови згоди на обробку персональних даних можуть бути викладені у формі єдиного письмового документа, викладеного доступною для суб'єкта персональних даних мовою, що підписується ним особисто або його законним представником, у електронній формі проставивши відмітку про надання згоди, або ж навіть усно. При цьому надана згода не повинна викликати сумнівів в її однозначності і володілець повинен мати змогу підтвердити її наявність упродовж усього часу здійснення обробки персональних даних.

Суб'єкт персональних даних також має право відмовитись від надання згоди на обробку персональних даних, відкликати згоду на обробку персональних даних, яка була надана такою особою раніше, вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди, пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними, заперечувати проти обробки своїх персональних даних.

Відкликання або заперечення проти наданої згоди на обробку персональних даних у разі, якщо єдиною підставою для обробки є згода суб'єкта персональних даних, має наслідком припинення володільцем обробки таких персональних даних. Видалення або знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних.

Приклад

Адміністратором освітньої платформи обробка персональних даних учнів/студентів/вихованців здійснюється на підставі закону і вимагати у суб'єктів освітньої діяльності окремої згоди на обробку їх персональних даних під час реєстрації на освітній платформі не потрібно.

Водночас до сфери діяльності адміністратора такої освітньої платформи входить також надання рекламних послуг. Ураховуючи категорію користувачів освітньої платформи, адміністратор має на меті здійснювати рекламну розсилку повідомлень зареєстрованим користувачам освітньої платформи.

Оскільки такі дії не відповідають визначеній меті обробки персональних даних, тобто наданню освітніх послуг, то потребують надання окремої згоди на обробку персональних даних відповідно до зміненої мети (здійснення рекламної

розсилки). При цьому відмова від надання такої згоди не може впливати на обмеження прав учнів/студентів/вихованців на отримання освітніх послуг, а надана згода може бути відкликана в будь-який момент.

Склад та зміст персональних даних учасників освітнього процесу, що будуть оброблятися

Відповідно до статті 6 Закону склад та зміст персональних даних, що їх обробляють організатори освітнього процесу, організовуючи дистанційне навчання, мають відповідати легітимній меті їх обробки, бути відповідними, адекватними та ненадмірними щодо такої мети. Тобто, бути пропорційними.

Оброблятися повинні лише ті дані, обробка яких необхідна для досягнення мети. Водночас слід розуміти, що якщо певні дані використовуються для досягнення відповідної мети, проте цієї мети можна досягти і не здійснюючи обробки вказаних даних, то така обробка не відповідатиме Закону.

Зазвичай обробка повинна відбуватися із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки. Отже, не лише склад даних, а й спосіб їх обробки повинен відповідати критерієві пропорційності. Принцип пропорційності має охоплювати весь процес будь-якої обробки персональних даних.

Приклад

Для забезпечення освітнього процесу в школах батьки учнів надають доволі широкий обсяг інформації про себе та своїх дітей. Проте для реєстрації на освітній платформі для здійснення дистанційного навчання достатнім обсягом персональних даних буде ПІБ, адреса електронної пошти чи номер мобільного телефону та клас, в якому навчається дитина.

Мета обробки персональних даних учасників освітнього процесу

Ураховуючи положення частини першої статті 6 Закону щодо здобувачів освіти, мета обробки їхніх персональних даних може визначатися в актах національного законодавства України, нормами яких врегульовані особливості окремих видів освітньої діяльності, а за їх відсутності, статутами або положеннями закладів освіти, які здійснюють обов'язки володільців персональних даних здобувачів освіти.

Мета обробки персональних даних – це ті цілі, для досягнення яких володільцем здійснюється обробка персональних даних.

Загальні вимоги до мети обробки персональних даних визначено у підпунктах 2.4 та 2.5 пункту 2 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 (далі – Порядок). Згідно з цими вимогами мета обробки персональних даних, має бути чіткою і законною, а також визначеною до початку їх збору.

Конкретність формулювання цілей – основний крок для гарантування законності обробки персональних даних, оскільки, знаючи для чого потрібно

обробляти персональні дані, суб'єкти освітніх послуг зможуть дійти висновку, чи дійсно такий обсяг персональних даних потрібен, впродовж якого часу буде здійснюватися така обробка тощо.

Тому при визначенні мети обробки персональних даних здобувачів освіти, закладам освіти необхідно обов'язково враховувати характер:

- ✓ освітніх послуг,
- ✓ освітній рівень, на якому здобувач (суб'єкт персональних даних) здобуває освіту,
- ✓ форму навчання,
- ✓ види інформаційно-комунікаційних технологій, що застосовуватимуться для надання освітніх послуг,
- ✓ форму власності навчального закладу,
- ✓ інші питання, які можуть впливати на зміст і обсяг персональних даних здобувачів освіти та/або їх законних представників.

Порядок обробки персональних даних учасників освітнього процесу

Загальні вимоги до обробки та захисту персональних даних суб'єктів персональних даних, що обробляються повністю чи частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки із застосуванням неавтоматизованих засобів, також визначаються Порядком.

За загальним правилом володільці, розпорядники персональних даних самостійно визначають порядок обробки персональних даних, ураховуючи специфіку обробки персональних даних у різних сферах відповідно до вимог, визначених Законом і Порядком.

Організація порядку обробки персональних даних полягає у визначенні таких критеріїв:

- ✓ способу збору, накопичення персональних даних;
- ✓ строку та умови зберігання персональних даних;
- ✓ умови та процедури зміни, видалення або знищення персональних даних;
- ✓ умови та процедури передачі персональних даних та переліку третіх осіб, яким можуть передаватися персональні дані;
- ✓ порядку доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних;
- ✓ заходів забезпечення захисту персональних даних;
- ✓ процедури збереження інформації про операції, пов'язані з обробкою персональних даних і доступом до них.

При цьому процедури обробки, строк обробки і склад персональних даних повинні бути пропорційними меті такої обробки.

Окремо необхідно наголосити, що надавачі освітніх послуг мають вживати заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних і технічних заходів. Зокрема, вони самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних та інформаційної безпеки.

Захист персональних даних насамперед передбачає заходи, спрямовані на запобігання їх випадковій втраті або знищенню, незаконній обробці, у тому числі незаконному знищенню чи доступу до персональних даних, що охоплюють:

- ✓ визначення порядку доступу до персональних даних працівників володільця/розпорядника;
- ✓ визначення порядку ведення обліку операцій, пов'язаних із обробкою персональних даних суб'єкта та доступом до них;
- ✓ розроблення плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- ✓ систематичне навчання працівників, які працюють із персональними даними.

Відповідно надавачі освітніх послуг повинні вести облік працівників, які мають доступ до персональних даних суб'єктів (здобувачів освіти). А також визначати рівень доступу зазначених працівників до персональних даних суб'єктів. При цьому кожен із цих працівників повинен користуватися доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків.

Ведення обліку операцій, пов'язаних із обробкою персональних даних суб'єкта та доступом до них, полягає у зберіганні інформації про:

- ✓ дату, час та джерело збирання персональних даних суб'єкта;
- ✓ зміну персональних даних;
- ✓ перегляд персональних даних;
- ✓ будь-яку передачу (копіювання) персональних даних суб'єкта;
- ✓ дату та час видалення або знищення персональних даних;
- ✓ працівника, який здійснив одну із вказаних операцій;
- ✓ мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

При цьому надавачі освітніх послуг як володільці/розпорядники персональних даних самостійно визначають процедуру збереження інформації про операції, пов’язані з обробкою персональних даних суб’єкта та доступом до них.

У разі обробки персональних даних за допомогою автоматизованої системи, зафіксована нею інформація має зберігатися упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції (якщо інше не передбачено законодавством України).

Необхідно наголосити, що персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

З метою безпечної обробки персональних даних надавачами освітніх послуг мають вживатися спеціальні технічні заходи захисту та приділятися увага захисту програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

III. Яким критеріям повинні відповідати цифрові сервіси, застосунки, освітні онлайн-платформи, інші інформаційні ресурси для забезпечення належного захисту прав здобувачів освіти як суб'єктів персональних даних

Загальні вимоги, яким мають відповідати інформаційно-телекомунікаційні системи, технології і сервіси, що можуть застосовуватися закладами освіти та органами управління у галузі освіти, закріплені у статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Якщо персональні дані здобувачів освіти та їхніх законних представників обробляються в державних реєстрах, інформаційно-телекомунікаційних системах, вимога про створення яких передбачена законом, наприклад, статтею 74 Закону України «Про освіту», обробка повинна здійснюватися з використанням комплексної системи захисту інформації з підтвердженою відповідністю.

Усі інші інформаційно-телекомунікаційні системи та технології, що використовуються у галузі освіти, можуть застосовуватися без приєднання до комплексної системи захисту інформації за умови відповідності таким **обов'язковим критеріям**:

1.Підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

2.Використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

3. Якщо жоден з елементів інформаційно-телекомунікаційної системи, технології, освітнього сервісу не розташований на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами.

При цьому інформаційно-телекомунікаційні системи і технології, які використовуються закладами освіти, повинні забезпечувати можливість виконання вимог, встановлених для обробки різних категорій персональних даних, наприклад відкритої та конфіденційної інформації.

Зокрема, **біометричні дані** не повинні оброблятися у закладах освіти на постійній основі. Використання біометричних даних у закладах освіти дозволяється за виняткових обставин, наприклад для ідентифікації особи, включаючи дистанційний нагляд за вихованцями, учнями, студентами і дозволяється тільки в тих випадках, коли жоден метод, що передбачає менше втручання в особисте життя, не дозволяє досягти визначеної мети.

Упроваджуючи застосування цифрових освітніх платформ, сервісів, мобільних застосунків, законом має бути заборонено! використання програмних продуктів, що допускають автоматичне цифрове профілювання вихованців, учнів, студентів. Це будь-яка форма автоматизованої обробки персональних даних, яка полягає у застосуванні «профілю» до дитини, зокрема для прийняття рішень щодо дитини або для аналізу чи передбачення її особистих уподобань, поведінки, ставлення. За виняткових обставин таке обмеження може бути зняте, якщо воно відповідає найкращим інтересам дитини, або якщо існують вагоміші інтереси суспільства, за умови, що відповідні гарантії передбачені законом.

Діти не повинні піддаватися довільному або незаконному втручанню в їхню конфіденційність у цифровому середовищі. Заходи, що обмежують право дітей на недоторканність приватного життя, повинні здійснюватися відповідно до закону, мати законну мету, бути необхідними в демократичному суспільстві та пропорційними легітимній меті. Зокрема, заходи спостереження або перехоплення повинні відповідати цим умовам, і вони мають підлягати ефективному, незалежному та неупередженому нагляду.

З метою вироблення більш ґрунтовного підходу до вибору цифрових інструментів надання освітніх послуг рекомендується також ознайомитися з Керівними принципами щодо захисту даних дітей у освітньому середовищі, які наразі доступні українською мовою на офіційному веб-сайті Уповноваженого.

IV. Захист приватності під час впровадження інноваційних технологій. Можливі ризики

Використання електронних сервісів, мобільних додатків несуть певні ризики для персональних даних осіб, які користуються такими ресурсами. Тож при впровадженні інноваційних рішень необхідно здійснювати попередню оцінку впливу на приватність до початку введення таких технологій в експлуатацію і мінімізувати можливі ризики. Проте наразі, на жаль, ми стикаємося з ситуацією, коли питання захисту приватності починає аналізуватись лише тоді, коли обробка даних вже певний час здійснюється.

Зокрема, не варто недооцінювати конфіденційність даних учнів, студентів та інших учасників освітнього процесу. Тому, зважаючи на необхідність дистанційного надання освітніх послуг із використанням онлайн-платформ, месенджерів, чатів тощо, їх функціонування має відповідати законодавству про захист персональних даних.

У зв’язку з чим постає низка питань, що потребують вирішення:

1) доцільність створення онлайн-платформи для висвітлення порядку організації освітнього процесу в кожному закладі освіти;

2) необхідність законодавчого затвердження чітких вимог до освітніх програмних продуктів, онлайн-платформ, месенджерів, чатів тощо, які використовуються під час дистанційного надання освітніх послуг із урахуванням передбачених законодавством вимог до обробки персональних даних;

3) розроблення і затвердження окремого розпорядчого документа, яким буде врегульовано порядок обробки персональних даних під час дистанційного надання освітніх послуг, зокрема:

- впорядкування питань, пов’язаних із правовими підставами обробки персональних даних (згода/правочин/закон) та затвердження граничного обсягу персональних даних, які підлягають обробці з метою надання освітніх послуг;
- визначення відповідальної особи, що організовує роботу, пов’язану з обробкою та захистом персональних даних під час дистанційного надання освітніх послуг;
- визначення порядку доступу працівників освіти до персональних даних здобувачів освіти під час дистанційного надання освітніх послуг;
- визначення порядку ведення обліку операцій, пов’язаних із персональними даними здобувачів освіти під час дистанційного надання освітніх послуг;

4) розроблення плану дій на випадок несанкціонованого доступу до персональних даних здобувачів освіти, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

5) розроблення плану підвищення рівня знань щодо захисту персональних даних працівників освіти;

6) доцільність запровадження в навчальній програмі базового освітнього курсу для дітей з метою підвищення усвідомлення важливості захисту власних

персональних даних у процесі дистанційної освіти та під час користування мережею Інтернет й мобільними застосунками.

При цьому при закупівлі інструментів і послуг, що здійснюють обробку даних про дітей, необхідно забезпечувати повагу до прав дітей як суб'єктів даних і прав їхніх законних представників, а також реалізацію їхніх розумних очікувань щодо участі у процесі прийняття рішень про впровадження будь-якого продукту програмного забезпечення.

В якості передової практики та відповідно до національного законодавства і міжнародного права потрібно забезпечити, щоб думки, висловлені дітьми, їх законними представниками, були частиною будь-якої оцінки впливу на їхні права, що здійснюється з метою врахування думки дітей щодо обробки їхніх даних.

Ураховуючи викладене, варто виділити такі основні ризики, пов'язані із використанням електронних сервісів:

- *щодо поінформованості суб'єкта персональних даних та повідомлення про обробку персональних даних*

Зокрема, одним із прав суб'єкта персональних даних, закріплених у частині другій статті 8 Закону, є право знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних.

Проте у більшості випадків системним порушенням є відсутність відповідного повідомлення. Не знаючи необхідної інформації, особа позбавлена можливості ретельно проаналізувати для себе усі можливі ризики від такої обробки та прийняти рішення, чи надавати володільцю або розпоряднику свої данні з метою отримання певних послуг, чи ні.

Окремо варто зауважити про застосування технологій Cookies. Ураховуючи, що використання цих технологій передбачає обробку персональних даних, така обробка має здійснюватися з дотриманням вимог чинного законодавства про захист персональних даних.

Як вже зазначалось, суб'єкт персональних даних має повідомлятися про володільця персональних даних, склад та зміст зібраних персональних даних, власні права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані, у разі, якщо персональні дані збираються у такого суб'єкта, **у момент збору персональних даних**. Проте зазначена вимога більшістю володільців не реалізується або технічно реалізується на етапах, коли дані вже зібрані.

У зв'язку з цим, доцільно до моменту ознайомлення з такою інформацією (зокрема шляхом проставлення відповідної відмітки) використовувати щодо суб'єктів персональних даних тільки такі файли Cookies, що є необхідними для коректного функціонування сайту, онлайн-платформи чи інших програмних продуктів.

Крім того, суб'єкт персональних даних повинен мати можливість обирати, які типи файлів Cookies щодо нього може використовувати такий програмний продукт (окрім тих, які є необхідними для його коректного функціонування).

- *щодо цільового обмеження та обмеження у часі*

Згідно зі статтею 8 Конвенції про захист прав людини та основоположних свобод органи державної влади не можуть втручатись у здійснення права на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Відповідно до міжнародного принципу обмеженого зберігання персональні дані можуть зберігатися у формі, що дозволяє ідентифікацію суб'єктів не довше, ніж це є необхідним для цілей їхнього опрацювання.

Водночас згідно з принципом мінімізації та цільового обмеження даних їх обсяг обмежується необхідністю в них для досягнення чітко визначених цілей.

У зв'язку з цим строк обробки персональних даних в електронних сервісах необхідно встановити пропорційно до мети обробки таких даних, після чого персональні дані окремої особи підлягають знищенню або ж знеособленню.

При цьому поряд зі знеособленням або знищенням персональних даних користувачів, які збираються за допомогою електронних сервісів або мобільних додатків, **мають також знищуватися системні дані щодо них, які зберігаються у реєстраційних файлах (logfiles) серверів**, і у поєднанні з обліковими даними становлять ризик подальшої ідентифікації та/або профілювання.

Проте наразі у більшості випадків в організаційних документах володільців не встановлено чіткого алгоритму дій щодо знищення або знеособлення персональних даних після спливу строку необхідності в їх обробці.

- *щодо надмірності даних, які збираються електронними сервісами та мобільними додатками*

Під час обробки даних склад та зміст персональних даних, що обробляються володільцем, а також спосіб їх обробки повинні відповідати легітимній меті обробки. Тобто обробка має здійснюватись лише щодо тих даних, які необхідні для досягнення поставленої мети.

Проте більшість володільців збирають багато додаткових даних, які не є необхідними для кінцевої мети обробки, посилаючись на припущену ними необхідність у майбутньому. Окрім цього, в деяких випадках суб'єкт не повідомляється, що електронний сервіс може додатково збирати про нього інформацію або мати доступ до його даних, а саме:

- до камери (для здійснення фото/відео);
- геолокації (доступ до місця знаходження через навігаційні дані телефону та на основі веж стільникового зв'язку і точок доступу Wi-Fi, що фактично передбачає можливість збору даних щодо провайдера);

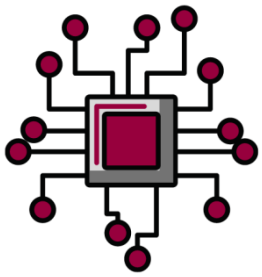
- телефонного зв’язку (безпосередньо дзвонити на номери телефонів);
- сховища пам’яті телефону (зокрема можливості читати вміст картки пам’яті телефону користувача, пересилати дані та знеособлювати або видаляти її вміст);
- телефонної книжки (копіювати всі номери, збереженні на девайсі);
- та іншого (повний доступ до мережі, доступ до використання біометричного сканера у мобільному телефоні, перегляду мережевих з’єднань, використання сканера відбитків пальців у мобільному телефоні, отримання даних з мережі Інтернет тощо).

Іноді зазначену інформацію можна віднайти в окремих вкладках «Інформація щодо додатка або сервісу», проте часто вона викладена виключно англійською мовою (що виключає поінформованість кожного українського користувача).

При цьому необмежений доступ та ризик обробки такого широкого обсягу персональних даних користувачів фактично порушує вимоги Закону. Тому така ситуація може призвести до негативних наслідків у вигляді необмеженого втручання у приватне життя користувачів державою або володільців приватного сектору.

- *щодо захисту суб’єкта персональних даних від автоматизованого рішення, що має для нього правові наслідки*

Відповідно до чинного законодавства у сфері захисту персональних даних кожен суб’єкт персональних даних має право на захист від автоматизованого рішення, що має для нього правові наслідки.



Однак усе частіше застосовується автоматизована обробка даних за допомогою різних ресурсів та/або сервісів і зазвичай охоплює великий масив даних. Це може призвести до того, що дані, отримані у законний спосіб, об’єднуються, аналізуються і за допомогою певних алгоритмів поступово формують додаткові дані, які мають іншу мету обробки. Проте зазначене не можна вважати порушенням у разі якщо така інформація є знеособленою, наприклад для формування статистичних даних.

Водночас будь-яка обробка персональних даних за допомогою автоматизованих засобів, наприклад комп’ютера, електронного сервісу, мобільного додатка, має здійснюватись із дотриманням вимог національного законодавства України, частиною якого є ратифіковані міжнародні договори.

Відповідно до європейських стандартів автоматизована обробка передбачає, що між такими автоматизованими операціями може виникати необхідність у застосуванні ручної обробки персональних даних.

Тому формуючи політику інтеграції штучного інтелекту в сучасне життя, необхідно пам’ятати, що важливо гарантувати право кожного на перегляд автоматизованих рішень щодо них людиною. Тобто має бути забезпечено гарантії для оскарження рішень, прийнятих за допомогою технологій, а володільці персональних даних повинні мати можливість пояснити алгоритм прийняття рішень штучним інтелектом.

Приватність не має бути платою за комфортне життя. Застосовуючи інновації, необхідно першочергово пам’ятати про безпеку та право на приватність.

V. Права здобувачів освіти та/або їх законних представників як суб'єктів персональних даних та механізми їх захисту

Права суб'єктів персональних даних визначено у статті 8 Закону. Цей перелік є вичерпним.

У разі виявлення здобувачами освіти та/або їх законними представниками порушення їх права на захист персональних даних, вони насамперед можуть звернутися до володільця, розпорядника персональних даних з метою поновлення права на приватність. При цьому суб'єкти освітньої діяльності, до яких надійшло таке звернення/вимога мають відповідально реагувати на такі повідомлення і вживати заходи, необхідні для поновлення порушеного права на приватність.

Необхідно зауважити, що контроль за додержанням законодавства про захист персональних даних, зокрема у галузі освіти, здійснюється Уповноваженим Верховної Ради України з прав людини та судами.

Не погоджуючись із діями чи бездіяльністю володільця чи розпорядника персональних даних, здобувачі освіти та/або їх законні представники можуть звернутися за захистом своїх прав до Уповноваженого.

Водночас суб'єкти освітньої діяльності як володільці та розпорядники персональних даних у разі виникнення труднощів із самостійним визначенням необхідних заходів захисту, організації обробки персональних даних можуть звернутися за додатковими роз'ясненнями щодо кожної окремої ситуації до Уповноваженого Верховної Ради України з прав людини.

Відповідно до статті 27 Закону України «Про захист персональних даних» професійні, самоврядні та інші громадські об'єднання чи юридичні особи можуть розробляти кодекси поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних, додержання законодавства про захист персональних даних з урахуванням специфіки обробки персональних даних у різних сферах.

При розробленні такого кодексу поведінки або внесенні змін до нього відповідне об'єднання чи юридична особа може звернутися за висновком до Уповноваженого Верховної Ради України з прав людини.

VI. Що потрібно враховувати при підготовці відповідей на запити учасників освітнього процесу та третіх осіб?

Реалізовуючи своє законне право на отримання інформації, кожен учасник освітнього процесу може звернутися до суб'єкта освітньої діяльності.

При цьому категорії запитуваної інформації можуть бути різними. Батьки можуть звернутися за інформацією про своїх малолітніх дітей, студенти можуть звернутися за інформацією про себе, треті особи можуть звернутися з метою отримання персональних даних вихованців, учнів, студентів тощо.

Розглядаючи такі запити, володільцем/розпорядником персональних даних в кожному конкретному випадку окремо, керуючись нормами Закону, необхідно прийняти рішення про задоволення такого запиту чи відмову в наданні запитуваної інформації.

На що потрібно звернути увагу? Передусім необхідно проаналізувати, ким запитується інформація, характер запитуваної інформації та правові підстави запитувача на її отримання.

Доступ до персональних даних врегульовано у статті 16 Закону.

Якщо запит на інформацію стосується отримання інформації про себе необхідно врахувати положення частини 6 зазначеної статті, в якій визначено, що суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації про прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит.

У випадку відповідності запиту зазначеним вимогам він має бути задоволений не пізніш як за тридцять календарних днів з дня надходження такого запиту.

Якщо йдеться про отримання відомостей про особу її законним представником, він повинен підтвердити наявність у нього таких повноважень. Відповідно до статті 42 Цивільного процесуального кодексу України повноваження законних представників мають бути посвідчені, серед іншого, свідоцтвом про народження дитини.

Отже, для отримання батьками інформації про своїх малолітніх дітей у своєму запиті їм необхідно вказати реквізити документа, що посвідчує особу, а також підтвердити наявність повноважень на отримання запитуваної інформації свідоцтвом про народження дитини.

Щодо розгляду запитів на доступ до персональних даних третіх осіб (запити правоохоронних органів, соціальних служб, закладів охорони здоров'я, інших юридичних чи фізичних осіб) необхідно враховувати, що доступ до персональних даних визначається умовами згоди суб'єкта запитуваних персональних даних, наданої володільцю персональних даних, або відповідно до вимог закону.

У такому запиті зазначаються:

1) прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи-заявника);

2) найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім’я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи-заявника);

3) прізвище, ім’я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

4) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

5) перелік персональних даних, що запитуються;

6) мета та/або правові підстави для запиту.

Строк вивчення запиту на предмет його задоволення **не може перевищувати десяти робочих днів з дня його надходження**.

Протягом цього строку володілець персональних даних доводить до відома запитувача, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом. При цьому головним критерієм при прийнятті рішення щодо задоволення такого запиту чи відмови у його задоволенні є саме мета та/або правові підстави для отримання запитуваної інформації. Тобто запит має бути законним та достатньо обґрунтованим.

Якщо у володільця персональних даних виникає обґрунтований сумнів щодо легітимності запиту третьої особи про доступ до персональних даних, у наданні інформації має бути відмовлено із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Окрім того, доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов’язання щодо забезпечення виконання вимог Закону України «Про захист персональних даних» або неспроможна їх забезпечити.

VII. Правила поведінки в чатах месенджерів, що використовуються для комунікації суб'єктів освітньої діяльності

Завдяки різноманітним месенджерам комунікація між суб'єктами освітньої діяльності стала зручнішою та доступнішою. Вихователями у дитячих садочках, класними керівниками в школах та старостами груп у вищих навчальних закладах створюються загальні чати для спілкування з метою донесення загальної інформації, що стосується усіх учасників спілкування.

Проте адміністраторами таких груп і решті її учасників потрібно контролювати характер та обсяг інформації, що в них публікується.

Необхідно пам'ятати про повагу до приватного життя та не допускати розголошення конфіденційної інформації. Повідомлення в таких загальних чатах мають бути інформативними, узагальненими та не можуть слугувати інструментом психологічного тиску, погроз, цькування, приниження честі та гідності та дискримінації за будь-якою ознакою.

Повідомлення особистого характеру мають бути адресовані в індивідуальному порядку.

Не варто забувати, що порушення законодавства у сфері захисту персональних даних, в тому числі за недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, частиною четвертою статті 188-39 Кодексу України про адміністративні правопорушення передбачена адміністративна відповідальність.

Особи, що допустили неправомірне поширення персональних даних в таких чатах загального спілкування підлягають притягненню до адміністративної відповідальності.