20 листопада 2020 року T-PD(2019)06BISrev5

КОНСУЛЬТАТИВНИЙ КОМІТЕТ КОНВЕНЦІЇ ПРО ЗАХИСТ ОСІБ У ЗВ'ЯЗКУ З АВТОМАТИЗОВАНОЮ ОБРОБКОЮ ПЕРСОНАЛЬНИХ ДАНИХ

Конвенція №108

Захист даних дітей в освітньому середовищі

Керівні принципи

Генеральний директорат з прав людини та верховенства права

Зміст

1. Вступ

Цифрове середовище по-різному формує життя дітей, створюючи можливості та ризики для їхнього добробуту і здійснення прав людини. Деякі цифрові інструменти дозволяють передавати важливу інформацію, об'єднуючи шкільні спільноти за межами класу. Інші надають можливість обміну освітніми матеріалами або пропонують важливі альтернативні засоби та способи отримання освіти за допомогою асистивних технологій та вдосконалених засобів зв'язку.

Ці керівні принципи[1] повинні допомагати організаціям і окремим особам в контексті освіти у дотриманні, захисті та здійсненні права дитини на захист даних в цифровому середовищі в рамках статті 3 модернізованої Конвенції №108 (часто іменованої «Конвенція №108+»)[2] і відповідно до документів РЄ, включно з Рекомендацією CM/Rec(2018)7[3] «Про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі»

Комітет Конвенції ООН про права дитини у 2001 році постановив, що

> *«Діти не втрачають своїх прав людини після того, як пройшли крізь двері школи. Освіта повинна надаватися таким чином, щоб шанувалася властива дитині гідність і щоб дитина могла вільно висловлювати свої погляди …»*

Впровадження цифрових інструментів в класі, по суті, відкриває двері школи для широкого кола різноманітних зацікавлених сторін, які взаємодіють з дітьми в повсякденній діяльності. Більшість пристроїв і застосунків, програмного забезпечення і навчальних платформ, що застосовуються в навчальних закладах, розробляються приватними комерційними організаціями.

Зацікавлені сторони повинні співпрацювати з метою створення середовища, в якому поважаються права людини, заради дотримання статті 8 Європейської конвенції про права людини і захисту людської гідності та основоположних свобод кожної людини в сфері захисту даних.

Значна частина комерційного програмного забезпечення в галузі освіти відома як «вільно розповсюджуване ПЗ», тобто таке, що пропонується освітнім установам без прямих фінансових витрат. Відповідно до Директиви ЄС про електронну комерцію (стаття 1.1) це, як правило, підпадає під визначення послуги інформаційного суспільства[4], «що надається за винагороду».

---

[1] Керівні принципи розроблені на основі доповіді «Захист даних дітей в системах освіти. Виклики та можливі шляхи їх подолання», підготовленої Джен Перссон, директоркою «defenddigitalme», що доступна за посиланням: https://rm.coe.int/t-pd-2019-06rev- eng-report-children-data-protection-in-educational-sys/168098d309

[2] Конвенція №108+: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, модернізована Протоколом про внесення поправок CETS 223, розміщена за посиланням: https://rm.coe.int/convention-108-convention-for-the- protection-of-individuals-with-regar/16808b36f1

[3] Керівні принципи Ради Європи щодо дітей в цифровому середовищі, Рекомендація CM/Rec(2018)7 Комітету міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[4] Для з'ясування сфери застосування визначення «послуга інформаційного суспільства» у Загальному регламенті про захист даних, наприклад, у Статті 4(25) цього Регламенту є посилання на Директиву 2015/1535. Див. Керівні принципи 05/2020 Європейської ради із захисту даних про згоду згідно з Регламентом 2016/679 (пункт 128).

Поширення освітніх технологій може означати, що доступ недержавних суб'єктів до особових справ дітей не лише у приватних, але й у державних школах є звичайною справою. Цифрова інфраструктура для надання державної освіти часто є комерційною власністю. У зв'язку з цим можуть поставати нові запитання про те, хто контролює виконання навчального плану у випадках, коли тип вмісту навчальних матеріалів та їх викладення визначається технологічною платформою, а також інші запитання щодо безпеки та цілісності.

Таким чином, компанії мають змогу блокувати можливості шкіл щодо використання власного програмного забезпечення. Школи повинні усвідомлювати потенційні наслідки цього для функціональної сумісності, доступу до даних та їх повторного використання, а також бюджетні та екологічні наслідки морального старіння, наприклад, коли компанія вирішує припинити оновлення технічних засобів або програмного забезпечення. На момент підготовки цього документу малі компанії зазвичай розвиваються за сприяння венчурних інвесторів, а потім викуповуються іншими більшими компаніями. Як наслідок, у процесі здобуття дитиною освіти права щодо контролю і зберігання її персональних даних можуть багаторазово передаватися внаслідок правочинів з придбання контролю над компаніями.

Зростання хмарних і транскордонних потоків даних в освітніх інформаційних системах означає, що заходи із забезпечення безпеки вимагають особливої уваги відповідно до статті 7 Конвенції №108+.

Діти не можуть бачити або розуміти, наскільки великим став їхній цифровий слід або як далеко він сягає, розповсюджуючись серед тисяч третіх осіб в освітньому середовищі або поза ним протягом усього їхнього життя. Хоча усвідомлення себе як суб'єкта вибору має життєво важливе значення для дітей і вони мають бути краще поінформовані про те, як збираються та обробляються їхні власні персональні дані, проте існує консенсус стосовно того, що не можна очікувати від дітей розуміння дуже складного інтернет середовища і того, що вони будуть вчиняти відповідні дії самостійно.

Вивчення ринку продуктів або послуг закладами освіти, необхідне до проведення закупівель, може бути складним навіть для дорослих у контексті повного розуміння програмних засобів та їх обслуговування, включаючи порівняльну оцінку наслідків використання відкритих інформаційно-комунікаційних технологій (ІКТ) або ІКТ, що є комерційною таємницею, платних послуг або вільно розповсюджуваного програмного забезпечення, проведення адекватної оцінки ризику, а також отримання і надання відповідної інформації суб'єкту даних. Це призводить до того, що важко бути достатньо кваліфікованим для дотримання і захисту прав користувачів.

Визнаючи, що законодавство про освіту та інші норми національного і міжнародного права впливають на застосування норм щодо захисту даних, зокрема про права суб'єктів даних, навчальні заклади потребують міцної законодавчої бази та кодексів професійної етики для розширення можливостей персоналу, а також для того, аби при обробці даних дітей в контексті освітньої діяльності компанії знали, що дозволено, а що ні, створюючи справедливе ігрове поле для всіх.

Особи, відповідальні за формування політики, а також практики, зокрема суб'єкти нормотворення, наглядові органи відповідно до статті 15 (2) (e) Конвенції №108+, органи у сфері освіти та суб'єкти індустрії освітніх послуг мають дотримуватися цих керівних

принципів і пропагувати їх, а також вживати заходів для виконання зобов'язань щодо захисту даних і забезпечення недоторканості приватного життя.

У закладах освіти діти позбавлені прав щодо взаємодії з державними органами, вважаються уразливими в силу недостатнього розуміння і здібностей, що лише розвиваються, а також через знаходження в процесі формування дорослої людини. Зі статичної точки зору, дитина − це особа, яка ще не досягла фізичної та психологічної зрілості. З динамічної точки зору, дитина перебуває в процесі розвитку, щоб стати дорослою людиною (Робоча група з реалізації статті 29, 2009 рік).[5] Діти також є активними користувачами прав та суб'єктами, які потребують не лише захисту, але й інформації, навчання і наставництва.

Діти та їх представники також повинні бути забезпечені такими матеріалами, як інформаційні довідники та документи щодо коректної обробки, викладені в зручній і доступній для них формі.

Слід визнати різноманітність персональних даних, які підлягають обробці, їх широке використання, зокрема у навчальних та позанавчальних цілях, в управлінських та викладацьких цілях і для поведінкової терапії, їхню конфіденційність, а також довічні ризики для недоторканості приватного життя, які можуть виникнути в результаті обробки як нецифрованих, так і цифрованих документів в освітньому середовищі.

Ці керівні принципи повинні також застосовуватися в усіх випадках, коли після зарахування дитини до освітньої установи застосовуються рішення і послуги, пов'язані з дистанційним електронним навчанням. Вони також застосовуються за межами освітнього середовища, наприклад, для виконання домашніх завдань або дистанційного навчання. Інструменти та ресурси дистанційного навчання повинні знаходитися під жорстким контролем щодо якості викладання, безпеки і дотримання стандартів захисту даних, наприклад, у частині налаштування параметрів за умовчанням, щоб використання застосунків і програмного забезпечення не обмежувало права суб'єктів даних (захист даних за умовчанням). Обробка не повинна охоплювати більше даних, ніж необхідно для досягнення законної мети. Це особливо важливо в тих випадках, коли згода не може бути надана вільно, оскільки вибір полягає у використанні продукту та отриманні інструкції або відмові від цього продукту.

Коли школа вимагає використання засобів електронного навчання, згода на обробку персональних даних, надана школою або третьою стороною-розпорядником, не вважатиметься чинною, адже така згода має бути надана однозначно та вільно[6] з можливістю її відкликання без будь-якої шкоди.[7]

---

[5] Робоча група з реалізації статті 29, Думка 2/2009 щодо захисту персональних даних дітей (Загальні керівні принципи та окремі роз'яснення щодо шкіл), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

[6] Відповідно до статті 5 (2) Конвенції №108+ і в даному контексті варто також взяти до уваги пункт 43 Преамбули до Загального регламенту про захист даних, згідно з яким: «щоб забезпечити добровільність надання згоди, остання не повинна передбачати необхідність застосування дійсних законних підстав опрацювання персональних даних у спеціальному випадку, коли існує *помітний дисбаланс між суб'єктом даних і контролером*, зокрема коли контролер є органом державної влади і, тому, малоймовірно, що згоду було надано добровільно за усіх обставин такої спеціальної ситуації»; а також що становище дітей в освітньому середовищі є типовим прикладом ситуації, коли існує дисбаланс між суб'єктом даних і контролером і потрібно застосувати іншу юридичну підставу.

[7] Як зазначено в пункті 42 Пояснювальної записки до Конвенції №108+, не можна здійснювати жодний неправомірний вплив або тиск (економічного чи іншого характеру), прямий або непрямий, на суб'єкта даних; і згода не повинна розглядатися як така, що надана вільно, в тих випадках, коли суб'єкт даних не має реального або вільного вибору, а також не може відмовитися від згоди або відкликати її без шкоди для своїх прав.

Важливо пам'ятати, що норми стосовно захисту даних не застосовуються окремо від законодавства про освіту або законів про рівноправ'я, зайнятість, недоторканність приватного життя та інших відповідних національних законів.

Ці керівні принципи повинні застосовуватися разом з принципами захисту даних, викладеними в четвертому розділі, включаючи принцип мінімізації даних.

Дорослі повинні забезпечити, щоб гарантії захисту, надані дітям, діяли не лише у період дитинства, але й враховували їхні майбутні інтереси. Ми зобов'язані сприяти безперешкодному досягненню дітьми зрілості та їх всебічному і вільному розвитку, повному розкриттю свого потенціалу і розквіту людської особистості.

2. Сфера застосування і мета

2.1. Ці керівні принципи покликані допомогти у роз'ясненні принципів захисту даних, викладених в Конвенції №108+, для розв'язання проблем у сфері захисту персональних даних, що виникають у зв'язку із застосуванням нових технологій та практичних методів, зберігаючи нейтральні з технологічної точки зору положення.

2.2. Керівні принципи спрямовані на те, щоб забезпечити дотримання всього комплексу прав дитини у сфері захисту даних під час взаємодії з освітнім середовищем, зокрема права на інформацію, на представництво її інтересів, на участь і на недоторканність приватного життя. Всі суб'єкти повинні повною мірою поважати ці права і належним чином їх враховувати при оцінюванні рівня зрілості та розуміння дитини.

2.3. Жодне положення цих керівних принципів не повинне тлумачитися таким чином, щоб унеможливлювати застосування або обмежувати дію положень Європейської конвенції про права людини та Конвенції №108[8]. Ці керівні принципи також враховують нові гарантії, передбачені Конвенцією №108+.

2.4. Керівні принципи залишаються документом високого рівня. Наглядові органи можуть виявити бажання реалізувати практичні пропозиції для закладів освіти, зокрема розробити контрольні списки для тих, хто прагне інтегрувати цифрові технології у свої процеси, як складову кодексів професійної етики та практичних посібників, пристосованих до вимог законодавства держав-учасниць Конвенції. Кодекси професійної етики можна також подавати (на затвердження) наглядовим органам (крім уповноважених органів). Держави повинні розробити стандарти на основі фактичних даних і керівні вказівки для шкіл та інших органів, відповідальних за закупівлю та використання освітніх технологій і матеріалів, щоб останні приносили користь навчальному процесу, яку можна довести, та забезпечували дотримання всього комплексу прав дітей.

3. Визначення для цілей даних керівних принципів

[8] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ETS 108, розміщена за посиланням: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

a. «дитина» − кожна людина у віці до 18 років, за винятком випадків, коли відповідно до національного законодавства особа досягає повноліття раніше.

b. «аналіз даних» означає персональні дані, що використовуються в обчислювальних технологіях, які аналізують великі обсяги даних для виявлення прихованих закономірностей, тенденцій і взаємозв'язків, а також стосується всього життєвого циклу управління даними, який полягає в зборі, впорядкуванні та аналізі даних для виявлення закономірностей, логічного виведення ситуацій або станів, прогнозування і розуміння поведінки.

c. «цифрове середовище» включає в себе інформаційно-комунікаційні технології (ІКТ), зокрема, Інтернет, мобільні та пов'язані з ними технології й пристрої, а також цифрові мережі, бази даних, застосунки та послуги.

d. «безпосереднє піклування та освіта» означає діяльність у сфері навчання, управління учбовим процесом або соціальної допомоги, пов'язану з безпосереднім викладанням й управлінням цим процесом або безпосереднім доглядом за визначеною особою, що, як правило, підпадає під визначені законом завдання держави у галузі освіти та обробки даних, виконання яких дитина і її законні представники обґрунтовано вважають складовою частиною навчання в школі. Безпосереднє піклування відрізняється від вторинного використання даних, яке полягає у будь-якому іншому *непрямому* використанні персональних даних, зібраних або логічно виведених щодо особи в рамках часу, проведеного під опікою навчального закладу, який діяв замість батьків (in loco parentis); невичерпний перелік прикладів охоплює аналіз навчального процесу, прогнозування ризиків, дослідження суспільного інтересу, для обробки в пресі або соціальних мережах, а також в маркетингових цілях.

e. «освітнє середовище» означає середовище для надання освіти дитині, яка знаходиться під юрисдикцією держав-учасниць в приватному і державному секторах, за виключенням діяльності окремої особи, що здійснюється виключно в домашніх умовах.

f. «електронне навчання» може в широкому сенсі включати в себе навчання з використанням інформаційно-комунікаційних технологій (ІКТ), особливо для передачі або доступу до змісту, дистанційне навчання або навчання через мережу інтернет (зокрема інструменти, що використовуються в режимі онлайн і без підключення до інтернету). Електронне навчання може проходити без будь-якого прямого підключення до мережі або інтернету, але часто вимагає такого доступу як складової послуги.

g. «законні представники» − особи, які вважаються такими, що наділені батьківськими обов'язками стосовно дитини відповідно до національного законодавства і мають сукупність обов'язків, прав і повноважень, спрямованих на просування і забезпечення прав і добробуту дитини відповідно до її здібностей, які розвиваються.

h. «аналітику навчального процесу» можна визначити як оцінку, збір, аналіз і звітування по даним про учнів та їхні ситуації в цілях розуміння та оптимізації навчання і середовища, в якому воно відбувається.[9]

i. «обробка» означає будь-яку операцію або комплекс операцій, що здійснюються з персональними даними, зокрема (але не лише) збір, зберігання, збереження, зміна, вилучення, розкриття, надання, стирання або знищення, а також здійснення логічних та/або арифметичних операцій з такими даними.

j. «профіль» означає набір характеристик, притаманних індивіду, що характеризують категорію осіб або призначені для застосування до особи.

k. «профілювання» стосується будь-якої форми автоматизованої обробки персональних даних, зокрема використання систем машинного навчання, що включає використання персональних або знеособлених даних для оцінки певних аспектів особистого характеру людини, зокрема, для аналізу чи прогнозування показників, пов'язаних з результативністю роботи такої особи, її економічним станом, станом здоров'я, особистими уподобаннями, інтересами, надійністю, поведінкою, місцем проживання або переміщеннями.

l. «особлива категорія даних» має таке ж значення як і в статті 6 Конвенції №108+.

m. «наглядові органи» − органи, визначені відповідальними за забезпечення дотримання положень Глави IV Конвенції №108+.

4. Принципи обробки даних

Конвенція №108+ визначає принципи, зобов'язання та права, що застосовуються до будь-якої обробки персональних даних, і тому їх застосування в освітньому середовищі є вкрай важливим.

4.1. Законність обробки, а також принципи правомірності, неупередженості, необхідності, пропорційності, цільового обмеження, точності, обмеженості часу зберігання у персоналізованій формі, прозорості та мінімізації даних, а також забезпечення того, щоб персональні дані були достатніми, актуальними та не надмірними з точки зору відповідності цілям, для яких вони обробляються згідно зі статтею 5 Конвенції №108+.

4.2. Обережний підхід і посилений захист конфіденційних даних особливих категорій, включаючи генетичні та біометричні дані, а також даних про етнічне походження, сексуальну орієнтацію або правопорушення, з визнанням додаткової вразливості дітей (стаття 6 Конвенції №108+).

4.3. Переконлива прозорість обробки даних із визнанням важливості забезпечення їх доступності шляхом використання, у разі необхідності, чітких формулювань, зручного та

[9] Аналіз навчальних та академічних даних (Learning and Academic Analytics), Siemens, G., 5 серпня 2011 року https://www.researchgate.net/publication/254462827_Learning_analytics_and_educational_data_mining_Towards_communication_and_collaboration

зрозумілого для дітей формату в процесі комунікації, в онлайн режимі та без підключення до мережі інтернет, а також на будь-якому пристрої, відповідно до статті 8 Конвенції №108+.

4.4. Підзвітність контролерів і обробників даних повинна бути чітко зазначена в будь-яких договірних механізмах в залежності від характеру обробки, відповідно до статті 10 (1) Конвенції №108+.

4.5. На практиці повинні застосовуватися принципи недоторканності приватного життя і захисту даних за умовчанням, а також вживатися відповідні організаційні та технічні заходи (стаття 10 (2) Конвенції №108+).

4.6. Оцінка можливого впливу запланованої обробки на права і свободи суб'єкта даних до початку будь-якого процесу обробки даних, на початковому етапі та протягом усього циклу такої обробки. Особливу увагу на початковому етапі слід приділяти механізму забезпечення комунікації з питань обробки даних між контролером даних і дитиною або її законним представником після залишення дитиною освітнього середовища.

4.7. Заходи безпеки[10] є необхідними для запобігання та захисту від ризиків, зокрема випадкового або несанкціонованого доступу, знищення, втрати, неналежного використання, змін, нападів програм-вимагачів або розголошення персональних даних.

4.8. Особливістю освітнього середовища є обов'язок контролерів даних визнавати права законних представників діяти від імені та у найкращих інтересах дитини відповідно до національного законодавства і міжнародного права, а також відповідно до статті 9 Конвенції №108+. Слід докладати максимальних зусиль для залучення дитини до процесу прийняття рішень щодо неї та, в разі необхідності, надавати відповідну інформацію сім'ям.

5. Основоположні принципи прав дитини в освітньому середовищі

Ці керівні принципи засновані на принципах, закріплених в Конвенції №108+, Стратегії Ради Європи з прав дитини на 2016–2021 рр.[11] і практиці Європейського суду з прав людини. Кожна дитина має право користуватися повним спектром прав людини, гарантованих Європейською конвенцією з прав людини, Конвенцією Організації Об'єднаних Націй про права дитини (КПД ООН) та іншими міжнародними документами у галузі прав людини. Ці керівні принципи заохочують держави-учасниці Конвенції №108 визнати ці права в контексті захисту даних дітей в сфері освіти. З метою забезпечення найкращих інтересів дитини при здійсненні всіх заходів, що її стосуються, держави-учасниці можуть розглянути питання про запровадження оцінки впливу на дітей, а також про підвищення її якості та ефективності відповідно до Стратегії Ради Європи з прав дитини на 2016–2021 рр.

[10] Рекомендована довідкова інформація про безпеку персональних даних під час дистанційного навчання — Посібник для шкіл, підготовлений Управлінням із захисту персональних даних (UODO) https://uodo.gov.pl/en/553/1118

[11] Стратегія Ради Європи з прав дитини на 2016–2021 рр. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8

5.1. Найкращі інтереси дитини

5.1.1. Найкращі інтереси дитини мають бути у центрі уваги, коли йдеться про будь-які дії, що стосуються дитини в цифровому середовищі.

5.1.2. Під час оцінки найкращих інтересів дитини держави повинні докладати всіх зусиль для забезпечення балансу та узгодження права дитини на захист з іншими правами, зокрема на свободу вираження поглядів та інформацію, на участь, а також з правом бути вислуханим.

5.1.3. Особливої уваги може потребувати визначення найкращих інтересів найбільш вразливих дітей в системі освіти, зокрема дітей без батьків, дітей-мігрантів, дітей-біженців та дітей-пошукачів притулку, дітей без супроводу, дітей з інвалідністю, безпритульних дітей, дітей-ромів і дітей, що знаходяться в інтернатних, медичних установах або установах для неповнолітніх правопорушників.

5.2. Здібності дитини, що розвиваються

5.2.1. Здібності дитини розвиваються з моменту народження до 18 років. Кожна дитина досягає відповідних ступенів зрілості в різному віці.

5.2.2. Як зазначено в керівних принципах щодо дотримання, захисту та реалізації прав дитини в цифровому середовищі[12], всі зацікавлені сторони повинні визнати факт розвитку здібностей дітей, в тому числі дітей з інвалідністю або дітей, які перебувають в уразливому становищі, і забезпечити прийняття політики та вжиття відповідних заходів, спрямованих на задоволення відповідних дитячих потреб в рамках цифрового середовища.

5.3. Право бути вислуханим

5.3.1. Діти мають право вільно висловлювати свою думку з усіх питань, що їх стосуються, та їхнім поглядам слід приділяти належну увагу з урахуванням їхнього віку і зрілості. Держави повинні забезпечити поінформованість дітей про їхні права в цифровому середовищі в зручній для них, прозорій, зрозумілій і доступній формі. Кожен учасник системи освіти повинен забезпечити дітям доступ до механізмів здійснення їхніх прав.

5.3.2. Персонал закладів освіти повинен розробити стандартну належну практику стосовно залучення за умовчанням законних представників і дітей, відповідно до стану розвитку їхніх здібностей, до консультацій щодо майбутніх рішень про впровадження нових технологій, пов'язаних з обробкою персональних даних дітей, для забезпечення справедливого балансу інтересів усіх причетних сторін відповідно до статті 5 (1) Конвенції №108+. Держави повинні також забезпечити, щоб консультаційні процеси охоплювали дітей, які не мають вдома доступу до цих технологій[13].

5.3.3. Відповідно до статті 5 (4) (a) Конвенції №108+ законні представники та діти повинні бути чітко поінформовані про обробку даних, якщо тільки поширення такої інформації не створює ризиків для найкращих інтересів дитини, з належним урахуванням положень статті

[12] Керівні принципи Ради Європи щодо дітей в цифровому середовищі, Рекомендація CM/Rec(2018)7 Комітету Міністрів: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[13] Комітет Організації Об'єднаних Націй з захисту прав дитини, проєкт Зауваження загального порядку щодо прав дітей у цифровому середовищі, серпень 2020 р. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

11 (b) Конвенції, або якщо дієздатна дитина не заперечує проти участі одного або декількох законних представників.

5.3.4. Відповідно до законодавства держав-учасниць, зокрема з урахуванням будь-яких вікових обмежень, встановлених законом для отримання згоди на обробку даних надавачами послуг інформаційного суспільства (ПІС), у випадках застосування визначення ПІС в освітньому середовищі, а також для підтримки дитини як суб'єкта даних законним представникам відповідно до статті 9 (1) (b) Конвенції №108+ має бути дозволено здійснювати права в галузі освіти від імені дитини, якщо вона не заперечує проти цього, з урахуванням рівня розвитку її здібностей і найкращих інтересів.

5.3.5. Механізм обробки даних на підставі згоди може не працювати, якщо існує дисбаланс повноважень, зокрема у відносинах між державним органом і особою, що завдає шкоди добровільному характеру згоди. Цей дисбаланс є більш суттєвим, коли суб'єктом даних є дитина. Тому для повсякденної діяльності з обробки даних інша підстава, вірогідно, виявиться прийнятною, але такий механізм обробки даних повинен бути закріплений в законі.

5.3.6. Шляхом надання інформації про обробку даних у зручній, прозорій, вичерпній та доступній для дитини формі потрібно забезпечити дітям можливість давати згоду на обробку даних або утримуватися від її надання в тих випадках, коли вони здатні зрозуміти наслідки свого рішення, а обробка даних слугує їхнім власним інтересам і узгоджується з будь-якими вимогами щодо віку дитини, закріпленими у національному законодавстві та міжнародному праві.

5.3.7. Діти повинні мати право доступу до належних, зрозумілих, незалежних і ефективних механізмів подання скарг і реалізовувати свої права.

5.4. Право на недискримінацію

5.4.1. Права дитини застосовуються до всіх дітей без будь-якої дискримінації. Ми маємо докладати зусиль для дотримання, захисту та реалізації прав кожної дитини в освітньому середовищі, проте може виникнути потреба у цілеспрямованих заходах для задоволення конкретних потреб. Це пов'язано з тим, що цифрове середовище здатне як підвищити вразливість дітей, так і розширити їхні можливості, захистити та підтримати їх.

6. Рекомендації для законодавців і осіб, відповідальних за розробку політики

Використання цифрових технологій в освітніх цілях призводить до обробки персональних даних дітей різними суб'єктами (від національних урядів, державних і приватних закладів освіти до приватних осіб, зокрема постачальників продуктів або послуг і розробників програмного забезпечення, а також інших осіб, зокрема вчителів, законних представників та однолітків). Дані, що підлягають обробці, надаються не лише дітьми, батьками або педагогами. Йдеться також про дані, які генеруються як побічний продукт участі користувачів, або логічно виведені дані (наприклад, на основі профілювання). Заклади освіти все частіше збирають дуже конфіденційні дані, зокрема біометричні. Збір таких даних може мати наслідки для дітей протягом усього їхнього життя. Оскільки виникають ситуації, коли різні органи влади за законом зобов'язані співпрацювати, перед збором всіх

персональних даних необхідно проводити перевірку для з'ясування суворої необхідності та пропорційності збору відповідних даних, аби забезпечити їх мінімізацію та гарантувати, що будь-яке їх використання відповідатиме розумним очікуванням дитини та принципам цільового обмеження, а також обмеженням щодо зберігання та збереження. Необхідно визнати, що коли йдеться про освіту і цифрові технології, впливу зазнає не лише право дитини на захист даних. Забезпечення права на недоторканність приватного життя і захист даних створює умови, коли виникає потреба у подальшому захисті інших прав і самої дитини. Під загрозою може опинитися також право на недискримінацію, право на розвиток, право на свободу вираження поглядів, право на дозвілля і право на захист від економічної експлуатації. Законодавці та посадові особи, відповідальні за розробку політики, повинні забезпечити, щоб увесь комплекс прав був гарантований іншими документами, протоколами та керівними принципами, в яких будуть враховані наслідки обробки даних про дітей у сфері освіти.

6.1. Перегляд законодавства, політики та практики

6.1.1. Забезпечити дотримання цих принципів і керівних вказівок, а також сприяти їх реалізації при обробці всіх даних під час входу в освітнє середовище, перебування в ньому, а також після його залишення протягом життєвого циклу даних.

6.1.2. Встановити високі критерії для конфігурацій вбудованих алгоритмів конфіденційності в стандартах щодо технічних вимог до послуг, які закуповуються.

6.1.3. Підтримувати або створити систему, зокрема, в разі необхідності, незалежні механізми, з метою просування та відстеження виконання цих керівних принципів відповідно до національних освітніх, наглядових і адміністративних систем.

6.2. Запропонувати належне сприяння реалізації права дітей бути вислуханими

6.2.1. Забезпечити наглядові органи достатніми ресурсами для того, щоб закони про захист даних належним чином виконувалися в освітньому середовищі, а використання відповідних технологій було узгодженим.

6.2.2. Забезпечити і посилити можливості представництва дітей-суб'єктів даних в наглядових органах (стаття 18) третіми сторонами. Відповідно до статті 13 держави-учасниці можуть передбачити у своєму законодавстві більш широкі гарантії захисту. Слід передбачити можливість для будь-якого органу, організації або об'єднання, незалежно від мандату суб'єкта даних, право подати скаргу в уповноважений наглядовий орган цієї держави-учасниці, коли це дозволено законом, якщо такий орган, організація або об'єднання вважає, що права суб'єкта даних були порушені в результаті обробки.

6.2.3. Встановити процедури, що дозволять дітям висловлювати свої думки та доводити їх до відома відповідних суб'єктів у зв'язку зі здійсненням дітьми права на недоторканність свого приватного життя у закладах освіти, а також забезпечити врахування їхніх думок.

6.2.4. Полегшити доступ дітей до засобів правового захисту в разі порушення положень Конвенції відповідно до статті 12, а також в дусі керівних принципів Ради Європи щодо

дружнього до дітей правосуддя[14] усунути будь-які перешкоди, що заважають дітям отримати доступ до суду, створивши підстави для належної співпраці та взаємної допомоги між наглядовими органами (статті 15, 16 і 17 (3) у питаннях, що стосуються захисту даних в освітньому середовищі.

6.2.5. Визнаючи потребу у приділенні особливої уваги правам дітей та інших вразливих осіб на захист даних, заклади освіти повинні забезпечити підготовку свого персоналу з тим, щоб працівники розуміли свою роль стосовно забезпечення належної обачності та враховували право дитини бути вислуханою.

6.3. Визнавати та враховувати права дитини

6.3.1. Дотримуватися і виконувати обов'язки та зобов'язання в рамках чинних стандартів Ради Європи та Організації Об'єднаних Націй у сфері прав дитини[15]. Ці керівні принципи застосовуються до всіх дітей з метою здійснення ними права на освіту без дискримінації та на підставі рівних можливостей.

6.3.2. Дотримуватися, захищати та реалізувати права дитини в цифровому середовищі, в освітньому середовищі відповідно до керівних принципів щодо дітей в цифровому середовищі[16].

6.3.3. Дотримуватися вимог зауважень загального порядку ООН №16 (2013) про зобов'язання держави щодо впливу підприємницького сектора на права дітей.[17] Держави повинні вживати заходів для забезпечення того, щоб договори на державні закупівлі укладалися з учасниками торгів, які зобов'язуються поважати права дітей. Держави також не повинні інвестувати державні кошти та інші ресурси в підприємницьку діяльність, якою порушуються права дітей. Держави мають вживати відповідних заходів для запобігання, моніторингу та розслідування порушень у галузі освіти та в цифровому середовищі з боку комерційних підприємств.

6.3.4. Визнавати зобов'язання, закріплені в статті 24 Конвенції про права осіб з інвалідністю, стосовно права на освіту, інклюзивності та залучення до процесу прийняття рішень з питань застосування технологій, забезпечувати загальну доступність за умовчанням і заохочувати рівноправність під час надання послуг.

---

[14] Керівні принципи щодо правосуддя дружнього до дітей, прийняті Комітетом міністрів Ради Європи 17 листопада 2010 р. Див. також Резолюцію 2010 (2014) Парламентської асамблеї «Ювенальна юстиція, дружня до дітей: від риторики до реальності», а також інструкції Європейського комітету з питань правового співробітництва стосовно просування і сприяння виконанню Керівних принципів щодо правосуддя дружнього до дітей (CDCJ(2014)15).

[15] КПД ООН, Стаття 29, п. 1: «Держави-учасниці погоджуються щодо того, що освіта дитини має бути спрямована на: a) розвиток особи, талантів, розумових і фізичних здібностей дитини в найповнішому обсязі; b) виховання поваги до прав людини та основних свобод, а також принципів, проголошених у Статуті Організації Об'єднаних Націй»: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx і Принцип 7 Декларації прав дитини (1959 р.) (Прийнята резолюцією 1386 (XIV) Генеральної Асамблеї ООН, A/RES/14/1386, 20 листопада 1959 р.).

[16] Керівні принципи щодо дітей в цифровому середовищі, Рекомендація CM/Rec(2018)7 Комітету Міністрів РЄ: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.

[17] Зауваження загального порядку № 16 (2013 рік) Комітету з прав дитини про зобов'язання держави щодо впливу підприємницького сектора на права дітей https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf
Для деяких дітей використання адаптивних технологій може бути небажаною ознакою їх інвалідності.

7. Рекомендації для контролерів даних

У ланцюжку обробки даних існує багато учасників, які можуть бути контролерами даних; не тільки навчальні заклади та державні органи, а й постачальники платформ, пристроїв, програм і застосунків. Ці комерційні суб'єкти також можуть бути повноправними контролерами даних у випадках, коли вони самостійно або спільно з іншими суб'єктами визначають характер обробки, як це визначено в статті 2 Конвенції №108+. Тому необхідно з особливою увагою ставитися до розуміння того, що характер обробки, а не лише те, що викладено в умовах договору, визначає кожну з ролей. В результаті обов'язки контролерів даних не завжди можуть покладатися виключно на суб'єктів освітнього середовища. Для забезпечення дотримання всіх відповідних принципів захисту даних, включаючи їх точність, необхідність і безпеку, заклади освіти повинні заохочувати таку культуру управління даними, що передбачає загальне дотримання правил, і за якої при оцінці ризиків завбачливо враховуються права і свободи в рамках будь-якого процесу обробки або закупівлі; при цьому якість даних перебуває під оперативним контролем та ефективним управлінням за допомогою організації ведення записів, що підкріплюється професійною підготовкою і відповідними політиками.

7.1. Законність і законна підстава

7.1.1. Відповідно до частини 1 статті 10 Конвенції №108+, обов'язок контролера полягає в тому, щоб забезпечити належний захист даних і мати змогу продемонструвати, що обробка даних здійснюється відповідно до вимог чинного законодавства.

7.1.2. Всі сторони, які беруть участь в обробці даних у закладах освіти, повинні уточнити питання щодо розподілу відповідальності та підзвітності між суб'єктами з метою визначення юридичних підстав та їхніх обов'язків щодо обробки даних. Це стосується також укладання договорів з постачальниками та третіми сторонами-обробниками даних.

7.1.3. Особлива категорія даних про дітей, як визначено в статті 6, вимагає посиленого захисту при обробці, починаючи з відповідної правової підстави для обробки. Якщо немає іншої законної підстави для обробки, у законного представника необхідно отримати інформовану та добровільну згоду на обробку медичних та інших особливих категорій даних; ця згода повинна бути зафіксована як належна гарантія для дитини згідно зі статтею 6 (1), коли така обробка даних відповідає найкращим інтересам дитини. До таких особливих категорій даних може бути наданий спільний доступ в цілях, що виходять за рамки безпосереднього піклування про дитину та її освіти, лише за наявності добровільної, конкретної, інформованої та чітко висловленої згоди суб'єкта даних або його законного представника.

7.1.4. Згоду на будь-яку обробку даних, включаючи, серед іншого, особливу категорію даних про дитину, надану від імені законних представників або дітей, в жодному разі не можна вважати такою, що легітимізує обробку даних третіми сторонами-постачальниками.

7.1.5. Контролери даних повинні визнати, що діти та законні представники не можуть надати чинну згоду на використання даних третіми сторонами-обробниками даних, якщо від такої згоди не можна відмовитися вільно і без шкоди для своїх прав.

7.1.6. Повноваження законного представника щодо здійснення прав від імені дитини як суб'єкта даних закінчуються після досягнення дієздатною дитиною встановленого законом віку зрілості. Суб'єкт даних (дитина) повинен бути поінформований про будь-яку поточну обробку даних про нього, на яку дав згоду законний представник, щоб мати змогу здійснювати права суб'єкта даних як доросла людина.

7.1.7. Не слід очікувати, що діти укладатимуть договір з третіми сторонами, наприклад, з постачальником послуг з електронного навчання, або із застосунком, уповноваженими закладом освіти. Заклад освіти має обробляти дані про дітей на підставі письмового договору, укладеного між ним і третьою стороною. Обробка персональних даних такими службами повинна здійснюватися на законних підставах, визначених законодавством.

7.1.8. Договори між третіми сторонами та постачальниками освітніх послуг повинні виключати можливість внесення будь-яких змін до умов, які впливають на основоположні права і свободи суб'єкта даних. Будь-які зміни до договорів між третіми сторонами та постачальниками освітніх послуг за умовчанням вимагають перегляду договору і повідомлення суб'єкта даних (або, в разі необхідності, його законних представників) з чітким і безпосереднім поясненням запропонованих змін.

7.1.9. Для виконання зобов'язань щодо забезпечення прав дитини на освіту заклади повинні запропонувати альтернативний спосіб надання освіти належного рівня без шкоди для дитини, якщо родини або дитина реалізують своє право на відмову від обробки даних за допомогою цифрових технологій, як засіб правового захисту відповідно до статті 9 (1) (f) Конвенції №108+.

7.1.10. Відповідно до статті 9 (1) (d) реклама не повинна вважатися законною підставою або прийнятною метою відповідно до вимог статті 5 (4) (b), яка має пріоритет над найкращими інтересами дитини або його основоположними правами та свободами.

7.1.11. Аналіз даних і розробка продуктів з використанням персональних даних не повинні вважатися законним і прийнятним використанням для подальшої обробки, яке має пріоритет над найкращими інтересами або правами та основоположними свободами дитини, чи розумними очікуваннями суб'єктів даних відповідно до пункту 49 пояснювальної записки до Конвенції №108+.

7.1.12. Контролери та обробники не повинні передавати персональні дані дітей, зібрані в процесі їх навчання, іншим особам для отримання фінансової вигоди або повторної обробки з метою продажу знеособлених або деідентифікованих даних, наприклад, брокерам даних.

7.1.13. Подальша обробка персональних даних, про яку йдеться в статті 5 (4) (b), для архівування в інтересах суспільства, для наукових чи історичних досліджень або у статистичних цілях є прийнятною, якщо її цілі відповідають цілям, визначеним в пункті 50 пояснювальної записки до Конвенції №108+.

7.1.14. Відповідно до національного законодавства держав-учасниць кодекси професійної етики повинні містити керівні вказівки щодо ситуацій, коли працівники закладів або діти отримують доступ до систем програмного забезпечення освітнього процесу, баз даних або інших продуктів третіх сторін за допомогою особистих електронних пристроїв або з дому, і

змішують персональні дані, включаючи метадані, про своє приватне і сімейне життя з даними своїх особових справ, створених в цілях професійної діяльності або навчання.

7.2. Сумлінність

7.2.1. Відповідно до статті 5 (4) (a) дані повинні оброблятися з дотриманням принципів сумлінності та прозорості. Стаття 8 (1) (a)-(e) Конвенції №108+ визначає, що потрібно зробити задля виконання вимоги стосовно прозорості та повноти обробки даних. Відповідно до пункту 68 пояснювальної записки до Конвенції, формат обробки може бути будь-яким, але забезпечувати сумлінне та ефективне надання інформації суб'єкту даних. Це передбачає, зокрема, врахування стану розвитку здібностей дитини, використання доступної для дитини форми та зрозумілої мови, а також забезпечення доступу до альтернативних форм подання інформації, зокрема лише текстової версії. У контексті освіти даний принцип слід тлумачити як необхідність забезпечення того, щоб інформація була зрозумілою для дієздатної дитини або, якщо йдеться про дітей молодшого віку, для їхніх законних представників, або щоб викладення інформації відповідало стану розвитку здібностей дитини.

7.2.2. Для виконання зобов'язань щодо забезпечення прозорості необхідно забезпечити завчасне (до початку процесу збору даних) надання суб'єкту даних, зокрема дитині та її законному представнику, інформації про повний комплекс прав, якими вони наділені, у доступній для них формі. Як правило, інформація має бути отримана безпосередньо дитиною та її законними представниками. Надання інформації законному представникові не повинно вважатися альтернативою повідомлення інформації дитині у формі, що відповідає стану розвитку її здібностей.

7.2.3. Заклади освіти повинні вести та оприлюднювати реєстр своєї діяльності з обробки даних, список партнерів, зокрема постачальників і субпідрядників, оцінку впливу захисту даних, повідомлення про конфіденційність, а також інформацію про будь-які зміни правил та умов, які відбуваються з часом.

7.2.4. Заклади освіти повинні звітувати перед наглядовими органами згідно з вимогами Конвенції №108+, перед самими суб'єктами даних, у разі вчинення порушень відповідно до статті 7 (2) Конвенції, а також ділитися з третіми сторонами аудиторськими звітами, щоб довести свою підзвітність і прозорість при обробці даних.

7.2.5. Заяви про обробку персональних даних повинні надаватися за запитом у рамках реалізації суб'єктом своїх прав на доступ до цієї інформації. Належною практикою може вважатися надання такої інформації за допомогою інструментів самообслуговування, безоплатних для дитини як суб'єкта даних.

7.2.6. Суб'єкт даних і його законні представники мають бути завчасно поінформовані про початок транскордонних потоків персональних даних, які можуть відбутися за умови забезпечення відповідного рівня захисту згідно з вимогами статей 14 (3) і (4).

7.3. Оцінка ризику

7.3.1. Контролери повинні оцінити можливий вплив запланованої обробки даних на права та основоположні свободи дитини до початку обробки даних відповідно до статті 10 (2)

Конвенції 108+. Вони мають організувати обробку даних у такий спосіб, щоб запобігти або звести до мінімуму ризик порушення цих прав і основоположних свобод відповідно до вимог статті 10 (3) Конвенції №108+ та всіх інших принципів, що в ній закріплені.

7.3.2. 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, зокрема комерційного або так званого «вільно розповсюджуваного програмного забезпечення».

7.3.3. У тих випадках, коли закони про свободу інформації застосовуються до державних органів, їхні кодекси професійної етики могли б містити, як приклад передової практики, положення про доступність оцінок впливу захисту даних в рамках звичайного порядку оприлюднення з метою забезпечення всебічної прозорості та підзвітності.

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

7.4. Збереження

7.4.1. У той час, коли дитина залишає систему освіти, збереженню підлягає лише мінімально необхідний обсяг даних про неї, які дозволяють ідентифікувати її особу, з урахуванням найкращих інтересів цієї дитини, щоб продемонструвати досягнення цілей здобуття освіти, захистити майбутні права на доступ та виконати передбачені законом зобов'язання.

7.4.2. Персональні дані, які залишаються у закладі освіти, не повинні зберігатися у формі, що допускає ідентифікацію дитини протягом більш тривалого часу, ніж це необхідно відповідно
до вимог статті 5 (4) (e).

7.4.3. Заклади освіти не повинні зберігати персональні дані у формі, що дозволяє ідентифікувати дитину протягом більш тривалого часу, ніж це необхідно, і з належним урахуванням положень статей 5 (4), 7 (2), 8 (1) і 9 Конвенції №108+. Винятки можуть застосовуватися у випадках, коли забезпечено дотримання суті прав та основоположних свобод дитини, та коли вони є пропорційною мірою, необхідною в демократичному суспільстві для цілей статті 11 Конвенції №108+.

7.4.4. Після закінчення кожного етапу обов'язкової освіти або при зміні закладу (в будь-якому віці, в дитячому садку, в початковій, середній школі, на етапі подальшої, зокрема вищої освіти), найкращою практикою вважається отримання дітьми повної копії своєї особової справи, включаючи інформацію про збереження та знищення персональних даних. Йдеться про інформацію щодо того, які персональні дані про дитину після того, як вона залишила заклад, продовжують зберігатися та оброблятися, ким і з якою метою. У будь-якому випадку, контролери даних повинні підтримувати механізми, що дозволяють їм виконувати будь-які поточні зобов'язання перед суб'єктом даних.

7.4.5. Оскільки належне знеособлення даних є доволі складним, найкраща практика полягатиме у забороні повторної ідентифікації та вимозі до третіх сторін не здійснювати спроб повторної ідентифікації та не дозволяли іншим особам здійснювати це після отримання знеособлених даних. Визнати, в тих випадках, коли це можливо відповідно до національного законодавства деяких держав-учасниць, що повторна ідентифікація вважається злочином.

7.5. Захист персональних даних у закладах освіти

Заклади освіти можуть залучатися до широкомасштабної обробки даних про дітей протягом тривалих періодів часу. Застосування належних заходів безпеки щодо цих даних та умов їх обробки як в стані спокою, так і під час передачі, має вкрай важливе значення для забезпечення захисту даних дітей відповідно до найвищих стандартів. Як зазначено в Конвенції, заходи безпеки повинні враховувати сучасні методи і засоби забезпечення безпеки даних в галузі обробки даних. Їх вартість повинна бути співмірна рівню та ймовірності потенційних ризиків. Безпека даних передбачає додаткові зобов'язання, а заходи контролю, перераховані нижче, є особливо актуальними для обробки даних у закладах освіти.

7.5.1. Заходи захисту, що застосовуються до персональних даних, повинні ґрунтуватися на оцінці ризиків відповідно до галузевих стандартів і передового досвіду, з використанням загальноприйнятих технічних рекомендацій (зокрема серія стандартів ISO 27000 та інші, за потреби).

7.5.2. Заходи повинні відповідати конкретним обставинам обробки та ризикам, що існують для дітей, чиї дані обробляються, і бути спрямованими на забезпечення конфіденційності, цілісності, доступності, автентичності даних про дітей незалежно від контексту, в якому вони обробляються, а також стабільності систем і служб обробки.

7.5.3. Таким чином, оцінка ризиків повинна мати за мету досягнення результатів, орієнтованих на досягнення високих стандартів безпеки впродовж всього процесу обробки, беручи до уваги її характер, масштаби, контекст і цілі, а також ризики, які вона породжує. Така оцінка повинна ґрунтуватися на міркуваннях необхідності та пропорційності, а також на основоположних принципах захисту даних:

- врахування всього спектру ризиків, включаючи фізичну доступність;
- мережевий доступ до пристроїв і даних;
- резервне копіювання та архівування даних.

7.5.4. Фізична доступність (зокрема, до пристроїв і даних в освітньому середовищі) охоплює дані, зібрані або збережені, принаймні у таких умовах:

- навчальний клас/електронне навчання (зокрема дистанційне навчання за межами приміщення школи);
- шкільна адміністрація;
- приміщення (фізичний доступ, системи відеоспостереження, в тому числі на шкільних транспортних засобах, біометричні зчитувачі).

7.5.5. Необхідно розглянути питання про те, як діти-користувачі повинні проходити перевірку дійсності (автентифікацію) в системах, зокрема, чи вимагається така перевірка у процесі обробки даних. При оцінці ризиків слід врахувати методи перевірки дійсності, які можуть знадобитися при будь-якому використанні, приділяючи належну увагу альтернативним підходам, у разі їх доступності, а також забезпечити збереження

конфіденційності користувачів, зокрема систем ідентифікаторів і паролів з можливістю повної ідентифікації, на противагу пристроям ідентифікації та контролю доступу на основі атрибутів. Автентифікація повинна бути надійною і здатною забезпечити захист даних. Принципи цільового обмеження і мінімізації даних також повинні бути частиною оцінки будь-якої системи автентифікації.

7.5.6. Коли йдеться про доступ до даних у мережі, автентифікація, певно, є потрібною і бажаною для запобігання несанкціонованому доступу. Тут постають ті самі питання, що й у випадку локального доступу: яка технологія автентифікації є найбільш прийнятною і чи надається доступ на підставі особистих даних (ім'я, прізвище) або атрибута («учень цієї школи»).

7.5.7. Оцінка ризиків перед обробкою повинна також передбачати оцінку захищеності даних від несанкціонованого доступу, зміни та видалення/знищення. Коли дані обробляються поза межами школи (наприклад, третіми особами-постачальниками послуг), постачальники освітніх послуг, як контролери даних, повинні усвідомлювати свої поточні обов'язки. Потрібно провести ретельну перевірку на предмет здатності третьої сторони забезпечити належний захист персональних даних, в тому числі їхні конфіденційність, цілісність і доступність.

7.5.8. Аналогічні запитання потрібно піднімати також щодо цифрових даних, які зберігаються для цілей резервного копіювання та/або архівування, особливо якщо ці послуги надаються третіми сторонами, як явно (наприклад, архівною службою, залученою на підставі договору), так і неявно, у контексті захисту доступності даних, запропонованого в рамках електронного навчання, адміністративних послуг.

7.5.9. Держави-учасниці не повинні забороняти у своєму законодавстві або правозастосовній практиці використання технологій шифрування по відношенню до дітей.[18] Якщо шифрування не інтегроване у застосунок або послугу, бажано було б шифрувати дані «вручну» в якості самостійного засобу захисту.

7.5.10. Численні рівні захисту можуть застосовуватися і навіть поєднуватися. Управління зашифрованими даними має здійснюватися так само, як і резервне копіювання/архівування даних, тобто процес відновлення даних (із зашифрованого стану, з резервної копії або архіву) повинен регулярно перевірятися. Слід передбачити процедури нейтралізації несправності для тих випадків, коли особа, яка несе основну відповідальність, не може виконати це завдання.

7.5.11. Ефективність будь-яких вжитих заходів повинна регулярно перевірятися, як це передбачено в статті 7 Конвенції №108+, з ураховуванням методів та засобів забезпечення безпеки даних і ризиків, що змінюються, а також регулярно переглядатися і, за необхідності, оновлюватися.

[18] Рекомендація CM/Rec(2018)7 Комітету міністрів державам-членам «Про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі».

7.6. Автоматизовані рішення і профілювання

7.6.1. Кожна особа має право не бути суб'єктом рішення, що істотно впливає на її життя, яке приймається виключно на підставі автоматизованої обробки даних без урахування точки зору цієї особи відповідно до статей 9 (1) (a) та 9 (1) (c) Конвенції №108+. Інформація про міркування, що лежать в основі обробки даних у тих випадках, коли її результати зачіпають інтереси суб'єкта даних, повинні бути доступними для цієї особи без будь-яких перешкод.

7.6.2. Профілювання по відношенню до дітей має бути заборонене законом. За виняткових обставин держави можуть зняти це обмеження, якщо воно відповідає найкращим інтересам дитини, або якщо існують більш важливі інтереси суспільства, за умови, що законом передбачені відповідні гарантії (відповідно до пункту 37 керівних принципів про дитину в цифровому середовищі).

7.6.3. Результати навчання та досягнень дітей не повинні систематично профілюватися з метою оцінки функціонування систем, наприклад, для визначення ефективності роботи школи або вчителя, на підставі того, що таке профілювання не виправдане пріоритетними інтересами суспільства.

7.6.4. Заклади освіти повинні дотримуватися керівних принципів щодо штучного інтелекту і захисту даних[19] у тому, що стосується автоматичної обробки персональних даних, для забезпечення того, щоб застосування штучного інтелекту не завдавало шкоди людській гідності, правам людини та основоположним свободам кожної дитини, як узятої окремо, так і в рамках спільноти, зокрема праву дитини на недискримінацію.

7.6.5. Визнання прав дитини як суб'єкта даних і його законних представників є необхідним як у ситуаціях алгоритмічного прийняття рішень, пов'язаних з обробкою персональних даних із використанням штучного інтелекту, так і під час інформованої обробки (див. керівні принципи щодо штучного інтелекту і захисту даних).[20]

7.6.6. Контролери даних зобов'язані проводити оцінки впливу на захист даних і недоторканність приватного життя. Такі оцінки повинні окремо враховувати вплив на права дітей[21] і демонструвати, що результати застосування алгоритмів відповідають найкращим інтересам дитини, а також забезпечувати, щоб на розвиток дитини не здійснювався надмірний вплив у непрозорий спосіб.

7.6.7. Персоналізація контенту може (але не завжди) бути невід'ємним і очікуваним елементом деяких онлайн послуг, і тому в певних випадках може вважатися необхідною для виконання договору між постачальником послуг і закладом освіти, але тільки не по відношенню до дітей, оскільки вони не можуть укладати договори[22] навіть за наполяганням закладу освіти.

---

[19] Керівні принципи щодо штучного інтелекту і захисту даних, документ T-PD(2019)01, доступний за посиланням: https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

[20] Той самий документ.

[21] Комітет з прав дитини, Зауваження загального порядку № 16 (2013) про зобов'язання держави щодо впливу підприємницького сектора на права дітей, пп. 77–81 https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

[22] Персоналізація контенту може (але не завжди) бути невід'ємним і очікуваним елементом деяких онлайн послуг, і тому в певних випадках може вважатися необхідною для виконання договору з користувачем послуг.

7.6.8. Прогнози щодо груп або осіб із загальними характеристиками, засновані на аналізі великих масивів персональних даних, тим не менше вважаються обробкою персональних даних, навіть коли відсутній намір, щоб така обробка призвела до втручання в життя конкретної особи.

7.6.9. Поширення і використання програмного забезпечення або використання послуг, призначених для спостереження і моніторингу діяльності користувача в терміналі або в комунікаційній мережі зі створенням профілю поведінки, не повинно допускатися, якщо це прямо не передбачено національним законодавством і не супроводжується відповідними гарантіями, як зазначено в Принципі 3.8 Рекомендації Ради Європи CM/Rec(2010)13 та Пояснювальній записці[23], щодо захисту осіб у зв'язку з автоматизованою обробкою персональних даних в контексті профілювання.

7.7. Біометричні дані

7.7.1. Біометричні дані не повинні на постійній основі оброблятися у закладах освіти. Використання біометричних даних у закладах освіти за виняткових обставин, зокрема для перевірки особистості, включаючи дистанційний нагляд за студентами, дозволяється тільки в тих випадках, коли жодний метод, що передбачає менше втручання в особисте життя, не може досягти такої самої мети. Це має відбуватися відповідно до принципу суворої необхідності, після проведення оцінки впливу на захист даних і за наявності відповідних гарантій, закріплених законом, згідно з вимогами статті 6 (1) Конвенції №108+. Ці гарантії мають включати належне врахування ризиків стосовно обробки конфіденційних даних для прав і основоположних свобод дитини, зокрема дискримінацію протягом усього життя. Альтернативні методи повинні пропонуватися без шкоди для інтересів дитини.

7.7.2. Винятки щодо використання біометричних даних в цілях підтримки дітей і педагогічного персоналу з особливими потребами щодо доступу, наприклад, у вигляді ідентифікації по очах за допомогою екрану, для їхньої безпосередньої вигоди та без дискримінації[24], повинні застосовуватися із наданням належних гарантій, закріплених в законі.

7.7.3. Підтверджуючи, що визначення біометричних даних, яке міститься в статті 6 Конвенції, призначене виключно для ідентифікації особи, органи влади повинні також проявляти пильність щодо конфіденційності обробки даних, пов'язаних з тілом і поведінкою дитини, які не можуть використовуватися для перевірки особи. Натомість мета обробки таких даних може полягати у впливі на фізичний або психічний досвід дитини, наприклад, у віртуальній реальності з повним зануренням. Обробка таких характеристик як голос, рух очей і хода; соціальне, емоційне та психічне здоров'я і настрій; реакції на нейростимуляцію з метою впливу на поведінку дитини або спостереження за нею повинна здійснюватися на основі принципу обережності, а ці дані мають розглядатися як біометричні відповідно до Конвенції №108+, навіть якщо їх обробка не має за мету виключно ідентифікацію особи.

(Європейська рада із захисту даних, Керівні принципи 2/2019)

[23] Рекомендація Ради Європи CM/Rec(2010)13 та пояснювальна записка (2011 рік) https://rm.coe.int/16807096c3

[24] Доповідь про дітей з інвалідністю в цифровому середовищі «Два кліки вперед і один клік назад» (2019 р.), Рада Європи, (стор. 5) «Для деяких дітей використання адаптивних технологій може бути небажаною ознакою їх інвалідності», https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f

7.7.4. Заклади освіти повинні приділяти особливу увагу тим випадкам, коли використання ними тієї чи іншої послуги є договірним зобов'язанням, наприклад, при використанні програмного забезпечення для відео конференцій в рамках здійснення програм дистанційного навчання, згідно з якими персонал може погоджуватися на певні умови для отримання послуг, що включають обробку і запис контенту, зокрема зображень і голосових даних дітей. Персонал повинен забезпечити, щоб у випадках, коли обробка даних здійснюється на підставі згоди, остання не могла бути наданою закладом освіти від імені дитини. Натомість ця згода має бути інформованою та однозначно і вільно висловленою дитиною − суб'єктом даних з урахуванням стану розвитку її здібностей, або її законним представником з дотриманням усіх інших принципів захисту даних, включаючи цільове обмеження.

8. Рекомендації для індустрії освітніх послуг

Наглядові органи, які розробляють кодекси професійної етики на підставі цих керівних принципів, повинні під час цього процесу забезпечити співробітництво з широким колом розробників та представників індустрії, педагогів-практиків, науковців, організацій, що представляють вчителів і родини учнів/студентів, а також з громадянським суспільством і самими дітьми. Стандарти можуть включати мінімальні критерії або чіткі вказівки для процесу закупівель певних товарів або послуг, пов'язаних з обробкою даних про дітей, в тому числі продуктів або послуг, якими пропонується користуватися безоплатно або за низьку плату, а також для будь-якої продукції та дослідницьких випробувань.

8.1. Стандарти

8.1.1. Оскільки діти заслуговують на особливий захист, очікувані стандарти обробки їхніх даних у галузі освіти повинні встановлювати високу планку стосовно налаштування параметрів за умовчанням, щоб відповідати належним стандартам якості та правовладдя, а також захисту даних за умовчанням.

8.1.2. Стандарти можуть бути викладені в кодексах професійної етики та у вигляді сертифікації, які повинні розроблятися у співпраці з широким колом розробників та представників індустрії, педагогів-практиків, науковців, організацій, що представляють вчителів і родини учнів/студентів, а також з громадянським суспільством і самими дітьми.

8.1.3. Положення договорів про обробку даних, укладених на підставі закону з відповідними організаціями, які були узгоджені на момент закупівлі послуг, повинні продовжувати застосовуватися і після того, як згадані організації були придбані іншими підприємствами, відбулося їх злиття, або перехід права власності на них стався іншим чином. Потрібно передбачати розумний строк, упродовж якого можна повідомити про будь-яку зміну умов, реалізувати своє право на зміну або заперечення проти нових умов, на припинення контракту і відкликання даних про учня за запитом.

8.2. Прозорість

8.2.1. Розробники повинні забезпечити, щоб їхнє власне розуміння всіх функціональних можливостей продукції, яку вони створюють, було викладене у достатньо зрозумілій формі, щоб відповідати нормативним і законним вимогам, а також за умовчанням уникнути

створення тягаря з вивчення запропонованої продукції, що був би надмірним для персоналу у закладах освіти та дітей.

8.2.2. Інформація про конфіденційність та інші опубліковані положення та умови, правила і стандарти відповідної спільноти повинні бути короткими та викладеними зрозумілою для дітей мовою. Методи комунікації, дружні до дітей, не повинні призводити до того, щоб пояснення, необхідні для правомірної обробки даних, були нечіткими. Натомість вони не повинні бути надмірними та мають бути відокремлені від юридичних і договірних умов, призначених для законних представників і вчителів. Окремі повідомлення про конфіденційність для різних категорій осіб могли б допомогти задовольнити потребу в повній і одночасно доцільній інформації.

8.3. Особливості розробки з точки зору захисту даних і наслідків для конфіденційності

8.3.1. Очікування щодо дотримання принципів захисту даних при розробці продукту й за умовчанням повинні перешкоджати обранню продуктів, які містять функції, що можуть спонукати дітей надавати зайві персональні дані або знизити рівень налаштувань конфіденційності.

8.3.2. Існує сувора необхідність в обробці персональних даних в цілях покращення якості та безпеки послуг. Така обробка має здійснюватися в рамках надання основних послуг, а також розумними є очікування щодо її здійснення у контексті надання користувачам послуг, передбачених контрактом.

8.3.3. Аналітична обробка даних[25], заснована на персональних даних та відстеженні користувачів, не повинна вважатися формою покращення якості послуг або підвищення безпеки та не є необхідною для виконання контракту.

8.3.4. Заходи з удосконалення продукту, наприклад ті, що спрямовані на додавання нових функцій до застосунку або поліпшення його продуктивності, вимагають окремого прийняття цих нових умов або надання на них згоди, а також надання явної згоди перед їх установкою. У тих випадках, коли замість договору використовуються інші законні підстави, суб'єкт даних повинен бути завчасно поінформований про заплановане оновлення програми або застосунку відповідно до цих законних підстав.

8.3.5. Особливу увагу слід приділити статті 14 Конвенції, аби гарантувати, що транскордонні потоки персональних даних в освітніх цілях відповідають умовам цієї статті для обмеження транскордонних потоків персональних даних в освітніх цілях і забезпечення того, щоб ці потоки відбувалися в рамках загальновизнаних норм щодо захисту даних.

8.3.6. Відстеження геолокації з метою визначення місця використання пристрою, місцезнаходження користувача, для активації функціональних можливостей застосунку або профілювання має застосовуватися лише у разі потреби та за наявності належної правової підстави. Послуги повинні передбачати наявність індикатора активації функції з відстеження місцезнаходження, а також дозволяти легко відключати таку функцію без

[25] Керівні принципи щодо захисту осіб у зв'язку з обробкою персональних даних у світі великих даних (2017), T- PD(2017)01

втрати основних функціональних можливостей застосунку. Такі профілі та історія повинні легко видалятися після закінчення сесії.

8.3.7. Дані про дітей, зібрані за допомогою інструментів програмного забезпечення у сфері освіти, не повинні оброблятися для використання у поведінковій рекламі, для аукціонів рекламних оголошень у режимі реального часу або для реклами в застосунку, у маркетингових цілях щодо товарів/послуг для дітей або родин з дітьми, для оновлення продуктів або для розробки додаткових продуктів в інтересах постачальника.