

## **ЗАХИСТ ТА ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ ОСВІТИ**

**ШЕВЧУК Олександр Олександрович** - кандидат юридичних наук, асистент кафедри міжнародного права Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

**ORCID: 0009-0009-7697-2950**

**ДЕРКАЧЕНКО Юлія Вікторівна** - кандидат юридичних наук, доцент кафедри мовних та гуманітарних дисциплін факультету автоматизації виробництва та цифрових технологій ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»

**ORCID: 0000-0002-3019-9730**

**БАНТУШ Вікторія Вікторівна** - доктор юридичних наук, професор кафедри права, Північноукраїнський інститут імені Героїв Крут

**ORCID: 0009-0001-5594-8275**

**DOI: <https://doi.org/10.71404/EP.2025.3.7>**

---

*Стаття присвячена питанню захисту та обробки персональних даних у системі освіти. За результатами дослідження визначено основні проблемні питання пов'язані з захистом та обробкою персональних даних під час здійснення освітньої діяльності. На основі цього запропоновано практичні механізми підвищення рівня захисту персональних даних у системі освіти.*

*Метою цієї статті є дослідження європейського та національного досвіду в питаннях обробки та захисту персональних даних у системі освіти.*

*Методологічна основа дослідження базується переважно на загальнонаукових і спеціально-юридичних методах, підходах, принципах дослідження. Зокрема, використано діалектичний, феноменологічний, аксіологічний, порівняльно-правовий, формально-логічний, формально-юридичний, модельний, прогностичний та інші методи.*

*У результаті сформовано низку наукових положень.*

*Цифрова трансформація у сфері освіти і науки є важливим елементом реформи цієї галузі в Україні. Особливо враховуючи виклики, які постали перед галуззю освіти і науки в період пандемії і війни. Проте, важ-*

*ливо пам'ятати, що при побудові будь-якого освітнього застосунку, бази даних чи реєстру потрібно забезпечити, у першу чергу, належний рівень захисту персональних даних при обробці персональних даних у цих системах. Впровадження принципів data protection by default (захист даних за замовчуванням) та data protection by design (захист даних за призначенням) мають стати основою при проектуванні будь-якої інформаційної системи у сфері освіти. Тільки так, ми зможемо зберегти баланс між цифровізацією і приватністю. Особливо, коли мова заходить про забезпечення права на приватність дітей.*

*Ключові слова: освіта, захист персональних даних, обробка персональних даних, захист даних за замовчуванням, захист даних за призначенням, порядок обробки персональних даних.*

### **Постановка проблеми**

Проблема обробки та захисту персональних даних завжди турбує керівників закладів освіти та учасників освітнього процесу. Особливо вона актуалізувалася під час пандемії, коли українська освіта вперше вимушена була перейти на дистанційну форму навчання з використанням різнома-

нітних державних та приватних електронних систем і платформ.

Дистанційна взаємодія педагогічного працівника зі здобувачами освіти спровокувала в учасників освітнього процесу багато нових запитань, зокрема щодо здійснення та оприлюднення відеозаписів занять, оприлюднення оцінок, передачі даних платформам, необхідним для навчання. Після повномасштабного вторгнення частина закладів освіти продовжують здійснювати дистанційне або змішане навчання.

Повномасштабне вторгнення загострило питання безпеки висвітлення інформації про роботу закладів освіти, учасників освітнього процесу, зокрема дітей військовослужбовців, питання шифрування даних на тимчасово окупованих територіях тощо.

Запровадження дистанційного формату навчання під час пандемії та його продовження після початку повномасштабної війни були вимушеними та вкрай важливими кроками, які допомогли нам зберегти систему освіти. Зараз майже 1 млн дітей навчається онлайн: приблизно 600 тисяч в Україні, ще майже 400 тисяч за кордоном. Дистанційне навчання — один із найбільших викликів для держави [1].

#### **Аналіз останніх досліджень і публікацій**

Теоретичною основою для цієї статті є наукові розробки вітчизняних та зарубіжних учених. З поміж робіт вітчизняних науковців, які досліджували питання обробки та захисту персональних даних у системі освіти в Україні слід виділити праці таких учених: Ольга Шпакович, Лілія Олексюк, Маркіян Бем, Іван Городиський, Володимир Венгер, Олег Заярний та інші.

Серед зарубіжних учених, які акцентують свою увагу на питаннях обробки та захисту персональних даних у системі освіти в ЄС слід згадати таких дослідників, як: Д. Шинкуєне, Д. Перссон, Л. Патерсон, Л. Грант та інші.

**Метою цієї статті** є дослідження європейського та національного досвіду в питаннях обробки та захисту персональних даних у системі освіти.

#### **Виклад основного матеріалу**

Навчальні заклади (дитсадки, школи, коледжі, університети тощо) збирають та у подальшому обробляють персональні дані фізичних осіб (суб'єктів даних): учнів, студентів (у тому числі тих, які закінчили навчання у закладі), батьків та законних представників, працівників тощо. Діти та працівники вважаються вразливими категоріями суб'єктів даних, тому під час обробки їхніх даних слід приділяти особливу увагу захисту їхніх прав і свобод.

Під час організації процесу обробки персональних даних навчальні заклади повинні здійснити такі дії [5]:

- розробити, підтримувати та періодично переглядати внутрішні документи, спрямовані на забезпечення впровадження принципів захисту даних;
- запровадити ефективні внутрішні процеси та процедури для забезпечення обробки персональних даних відповідно до внутрішніх документів;
- підтримувати ефективне управління ризиками (виявлення, оцінювання, мінімізацію різноманітних внутрішніх і зовнішніх ризиків);
- вести облік операцій обробки персональних даних, щоб мати можливість продемонструвати дотримання вимог щодо захисту даних;
- проводити періодичний огляд усіх впроваджених засобів захисту персональних даних (правил, процедур тощо).

Щоб забезпечити законність обробки персональних даних, навчальні заклади повинні переконатися, що операція обробки здійснюється на законній підставі. Перш ніж прийняти рішення щодо правової підстави для обробки персональних даних, навчальний заклад повинен розглянути такі елементи [2]:

- мета операції з обробки персональних даних повинна бути чітко визначена перед вибором правової підстави для обробки;
- пропорційність обробки: якщо обробка персональних даних не є необхідною (мета може бути в належному обсязі досягнута без обробки), обробка персо-

нальних даних не може бути підкріплена жодною правовою підставою;

- правова підстава обробки повинна бути визначена до початку обробки персональних даних;

- якщо мета обробки змінюється, але нова мета сумісна з початковою, можна продовжити процес обробки у відповідності до первинної правової підстави. Якщо нова мета не сумісна з початковою, обробку можна здійснювати, якщо воно оснований на згоді суб'єкта даних або на вимогах законодавства;

- усі правові підстави є рівними, і жодна не переважає над іншими, тому необхідно розглянути найбільш відповідну з урахуванням конкретного випадку обробки даних.

#### **Внутрішні документи навчальних закладів**

Важливою частиною процесу обробки персональних даних у навчальних закладах є внутрішні документи, що регламентують питання обробки персональних даних та пов'язані з ним різноманітні процедури та процеси. Ці документи допомагають забезпечити належне впровадження принципів і вимог у сфері захисту персональних даних і є одним з елементів принципу підзвітності, що дозволяє продемонструвати відповідність застосовним правовим вимогам.

Внутрішній документ може мати різні цілі та сферу застосування — він може регулювати загальні аспекти обробки персональних даних, окремі процедури, операції обробки або містити зразки та шаблони.

Порядок обробки персональних даних є внутрішнім документом загального характеру, який описує підхід та зобов'язання навчального закладу у сфері захисту персональних даних, надає загальний огляд процесів щодо обробки та захисту персональних даних і робить їх відповідними до вимог законодавства про захист персональних даних.

Порядок обробки персональних даних може охоплювати: зобов'язання щодо реалізації принципів захисту даних, загальні зобов'язання персоналу, якому доручено обробляти персональні дані, права

суб'єктів даних, алгоритм дій у зв'язку з порушеннями безпеки персональних даних, відносини з операторами персональних даних, розкриття даних третім особам, управління ризиками та безпека даних, навчання персоналу, процедури перегляду Порядку.

Інші внутрішні документи, додаються до Порядку обробки персональних даних:

- документи, що детально регламентують певні процедури та процеси, зокрема: збереження/видалення даних; реалізація прав суб'єктів даних; ведення протоколів обробки даних; алгоритм дій у зв'язку з порушеннями безпеки персональних даних; оцінка впливу на захист даних; оцінка ризиків та впровадження організаційно-технічних заходів щодо захисту персональних даних;

- шаблони та форми документів, розроблені з метою виконання конкретних вимог, зокрема: згода суб'єкта даних; зобов'язання щодо конфіденційності для працівників та інших осіб, яким довірено обробку персональних даних; заява про конфіденційність; договір про надання послуг з обробки даних; реєстр порушень безпеки персональних даних; шаблон повідомлення про порушення безпеки персональних даних для наглядового органу/суб'єкта даних; шаблон протоколу обробки персональних даних тощо.

Шаблони та форми допомагають співробітникам уникнути помилок під час виконання обов'язків у сфері обробки персональних даних. Навчальний заклад також має встановити для персоналу конкретні обов'язки, щоб забезпечити використання — заповнення та ведення — шаблонів і форм у повсякденній діяльності.

#### **Обов'язки щодо захисту персональних даних у навчальних закладах**

Залежно від посади та статусу конкретного працівника навчального закладу в нього можуть бути різні ролі та обов'язки, пов'язані із забезпеченням виконання вимог щодо захисту персональних даних.

Керівник (директор тощо) навчального закладу відповідає за:

- розуміння принципів захисту персональних даних та інших зобов'язань,

пов'язаних з навчальним закладом, який діє як контролер персональних даних;

- прийняття рішення щодо фінансових та інших ресурсів, необхідних для належного виконання вимог захисту персональних даних; встановлення та затвердження Порядку обробки персональних даних та відповідної документації;

- прийняття рішення про те, які саме технології використовувати для обробки персональних даних; прийняття рішення про те, які дані будуть передані, підписання договорів з операторами персональних даних і третіми особами;

- отримання консультацій від співробітника з питань захисту даних, якщо це необхідно; забезпечення проведення тренінгів з питань захисту персональних даних для персоналу не рідше одного разу на рік.

Усі співробітники несуть відповідальність за:

- участь у підготовці та розуміння того, що таке персональні дані, що означає обробку персональних даних, а також принципи обробки персональних даних;

- їхні обов'язки щодо виявлення та внутрішнього звітування про порушення безпеки персональних даних;

- розуміння та дотримання прав суб'єктів персональних даних; дотримання зобов'язань щодо конфіденційності та розуміння ризиків, пов'язаних із незаконним розкриттям персональних даних; ознайомлення з Порядком обробки персональних даних та відповідними внутрішніми документами.

Співробітники, які безпосередньо беруть участь в операціях з обробки персональних даних (збір, зберігання, введення даних у програмне забезпечення/реєстри/бази даних/інформаційні системи тощо), повинні виконувати додаткові зобов'язання, а саме:

- бути ознайомленими з процесами обробки персональних даних та їхньою роллю та відповідними обов'язками;

- забезпечити наявність правових підстав для збору та подальшої обробки персональних даних, а також відповідність

обробки персональних даних внутрішнім документам навчального закладу, які регламентують питання обробки персональних даних;

- бути в змозі ідентифікувати всі ризики, пов'язані із обробкою та захистом персональних даних; розуміти та вміти виконувати інші спеціальні завдання, передбачені внутрішніми документами та інструкціями.

#### **Інформація про освітню діяльність на вебсайтах та в соціальних мережах навчальних закладів**

Багато навчальних закладів мають власні вебсайти, призначені для інформування громадськості про свою діяльність. Вони також використовують різні канали комунікації (зокрема, соціальні мережі тощо), як інструменти внутрішньої/зовнішньої комунікації. Персональні дані, які обробляються в межах такої комунікації, стосуються учнів та/або членів їхніх сімей.

Навчальні заклади повинні пам'ятати, що розповсюдження зображень, відеозаписів та відповідних персональних даних повинно здійснюватися відповідно до принципів захисту персональних даних, зокрема законності, чесності та прозорості, мінімізації та пропорційності даних, обмеження зберігання персональних даних у часі. Особливу увагу слід звернути на ризики, пов'язані з оприлюдненням персональних даних (втрата контролю над подальшим використанням даних невизначеною кількістю невідомих третіх осіб, реалізація прав суб'єктів даних тощо). З метою захисту персональних даних дітей навчальним закладам можна надати такі рекомендації:

- при виборі каналів зовнішньої комунікації слід віддавати перевагу тим, які повністю контролюються навчальним закладом, а не третіми особами (наприклад, вебсайт закладу, а не платформам соціальних мереж);

- для внутрішньої комунікації всередині спільноти навчального закладу настійно рекомендується використовувати механізми обмеженого доступу (наприклад, вхід за допомогою логіна користувача та пароля); якщо продукт/додаток ІКТ, наданий третіми особами, призначений для вико-

ристання, навчальний заклад повинен дотримуватися рекомендацій щодо використання приватних систем;

- під час публікації фотографій та відповідних персональних даних дітей в Інтернеті завжди слід оцінювати тип фотографії, доречність її публікації та її цільове призначення; слід оцінити ризики, пов'язані з використанням персональних даних дітей невизначеною кількістю невідомих третіх осіб для будь-яких цілей, у тому числі передачу до третіх країн, що не забезпечують належного рівня захисту, і вжити відповідних заходів безпеки;

- принцип мінімізації даних повинен бути реалізований з урахуванням мети публікації (наприклад, оприлюднення фотографій без даних, які дають змогу безпосередньо ідентифікувати дитину, зокрема імені, прізвища тощо);

- розміщення індивідуальних фотографій ідентифікованих дітей, а також публікація будь-яких персональних даних дітей у соціальних мережах або іншим чином в Інтернеті завжди має здійснюватися за згодою (законних представників або дитини, залежно від віку). Необхідно отримати згоду для кожного окремого каналу (наприклад, вебсайту навчального закладу, соціальних мереж тощо). Право дитини бути почутою є надзвичайно важливим, тому перш ніж запитувати згоду, батькам слід порадити обговорити це зі своїми дітьми. Завжди потрібно враховувати заперечення дитини;

- у разі колективних фотографій, що представляють діяльність навчального закладу (наприклад, шкільні заходи), і відповідно до національного законодавства, яке може відрізнятися залежно від країни, попередня згода батьків може не вимагатися, якщо фотографії не дають змогу легко ідентифікувати учнів. У таких випадках навчальний заклад повинен повідомити дітей, батьків чи інших законних представників про фотографування та подальше використання фотографій та надати можливість заперечити (відмовитися від фотозйомки);

- навчальні заклади мають запроваджувати принцип обмеження зберігання персональних даних у часі, встановлюючи

часові рамки для видалення або періодичного перегляду необхідності оприлюднення персональних даних;

- обробка персональних даних на вебсайті навчального закладу, платформі соціальних мереж тощо повинна бути описана в політиці конфіденційності навчального закладу і доведена до відома дітей та їхніх законних представників.

#### **Обробки персональних даних, отриманих під час відеоспостереження**

Відеоспостереження все ширше використовується в навчальних закладах. Відеоспостереження відноситься до засобів контролю, які можуть бути особливо нав'язливими. Здатність технологій відеоспостереження впливати на права та свободи учнів та співробітників означає, що їхнє встановлення потребує особливої уваги та оцінки.

Не можна порекомендувати якое одне рішення, яке б діяло для всіх аспектів діяльності навчального закладу та для всіх частин території та приміщень. Одне з головних правил, якого слід дотримуватися, полягає в тому, що камери відеоспостереження слід встановлювати лише в разі необхідності та якщо недоступні інші засоби досягнення тієї ж мети, які забезпечують менше втручання в приватне життя.

Впровадженню відеоспостереження завжди має передувати ретельне обговорення між усіма, хто присутній у навчальному закладі: вчителями, батьками чи іншими законними представниками, а також дітьми, враховуючи поставлені цілі та достатність запропонованих засобів.

Застосування відеоспостереження може бути виправданим з метою безпеки, однак слід брати до уваги його допоміжний характер та ретельно розглядати його в поєднанні з іншими заходами, які слід також застосовувати (контроль доступу до приміщень тощо). Наприклад, відеоспостереження може бути легше виправдати на вході та виході, а також в інших місцях, де перебувають люди (не лише учні та співробітники навчального закладу, а й інші люди, які з будь-якої причини відвідують приміщення), і безпека має першочергове значення.

У більшості інших частин навчального закладу, особливо в класах, право дітей (а також вчителів та інших працівників) на приватне життя, свободу навчання та свободи слова, а також суттєву свободу викладання переважають над необхідністю постійного відеоспостереження. Те саме стосується зон відпочинку, спортзалів та роздягалень.

Робоча група із захисту даних за статтею 29 у Висновку 2/2009 щодо захисту персональних даних дітей (Загальні рекомендації та особливий випадок шкіл) (WP 160), ухваленому 11 лютого 2009 року, підкреслила важливість дотримання права на розвиток особистості, яким володіють усі діти, а також шкоду, яка може бути нанесена дітям, які тільки розвивають уявлення про власну свободу, якщо вони з раннього дитинства припускають, що те, щоб за ними стежили пристрої відеоспостереження, є нормою. [3] Вебкамери чи подібні пристрої не можна використовувати для дистанційного спостереження за дітьми під час навчання.

Принцип мінімізації даних вимагає, щоб обробка завжди була релевантною, здійснювалася в належний спосіб і в обсязі, що не є надмірним щодо його мети. Це можна реалізувати шляхом правильного вибору розташування та налаштувань камер відеоспостереження. Наприклад, проведення відеоспостереження в неробочий час школи можна вважати належним з міркувань безпеки. З іншого боку, використання запису голосу та інших функцій, які дозволяють обробляти додаткові дані та/або впливати на поведінку дітей, не є сумісним із вимогами захисту персональних даних.

З метою дотримання принципу прозорості діти, їхні законні опікуни, інші суб'єкти даних повинні бути проінформовані про здійснення відеоспостереження та його цілі, особу контролера даних, а також отримати іншу інформацію, передбачену статтею 13(1) та (2) GDPR. [1]

Відповідно до Рекомендацій Європейської ради із захисту даних 3/2019 щодо обробки персональних даних за допомо-

гою відеопристроїв, прийнятих 29 січня 2020 року [4], беручи до уваги обсяг інформації, який необхідно надати суб'єкту даних, контролерами даних може застосовуватися багаторівневий підхід.

Найважливіша інформація повинна міститися власне на попереджувальному знаку (перший рівень), а додаткові обов'язкові відомості можуть надаватися в інші способи (другий рівень).

Перший рівень має містити відомості про цілі обробки, особу контролера та наявність прав суб'єкта даних, а також інформацію про найважливіші наслідки обробки. Перший рівень також має посилатися на більш детальний другий рівень інформації, а також де і як її знайти. Інформація першого рівня може посилатися на цифрове джерело (наприклад, QR-код або адресу вебсайту) другого рівня. Іншим відповідним засобом може бути номер телефону, на який можна зателефонувати.

Інформація другого рівня також має бути доступною в нецифровому вигляді, у місці, легко доступному для суб'єкта даних, як-от заповнений інформаційний лист, доступний у центральному місці (наприклад, інформаційний стенд), або представлена на легкодоступному плакаті. Повинна бути можливість отримати доступ до інформації другого рівня, не входячи в зону відеоспостереження, особливо якщо інформація надається в цифровому вигляді.

Якщо відеоспостереження здійснюється відповідно до законних інтересів згідно з підпунктом (f) статті 6(1) GDPR, навчальний заклад повинен підготувати та задокументувати тест балансу інтересів. Варто пам'ятати, що особливу увагу потрібно приділяти інтересам, основним правам і свободам дітей, як зазначено вище.

Враховуючи нові можливості технологій і характер відеоспостереження, що втручається в приватне життя, усі ризики для прав і свобод дітей повинні бути ретельно оцінені та мінімізовані, тому перед обробкою рекомендується провести оцінювання впливу на захист даних.

### **Висновок**

#### **Внутрішньо-розпорядчі документи закладів освіти**

Внутрішньо-розпорядчі документи відіграють ключову роль у виконанні навчальним закладом принципу підзвітності і доведенню виконання обов'язків, покладених на них положеннями законодавства.

#### **Підвищення рівня професійної підготовки працівників закладів освіти**

Існує необхідність підготовки методичних матеріалів та проведення роз'яснювальної роботи із закладами освіти щодо підстав для обробки персональних даних та відповідних повноважень володільців та розпорядників таких даних.

Систематичне проведення семінарів, тренінгів, лекцій, практикумів для працівників закладів освіти, присвячених теоретичним та практичним аспектам захисту персональних даних, сприятиме підвищенню їх кваліфікації і рівня знань при виконанні їх посадових обов'язків, пов'язаних з обробкою персональних даних.

#### **Висвітлення інформації про освітню діяльність на вебсайтах та в соціальних мережах закладу освіти**

Навчальні заклади повинні пам'ятати, що розповсюдження зображень, відеозаписів та відповідних персональних даних повинно здійснюватися відповідно до принципів захисту даних, зокрема законності, чесності та прозорості, мінімізації та пропорційності даних, обмеження зберігання. Особливу увагу слід звернути на ризики, пов'язані з оприлюдненням персональних даних (втрата контролю над подальшим використанням даних невизначеною кількістю невідомих третіх осіб, реалізація прав суб'єктів даних тощо).

#### **Збереження та використання персональних даних, які отримані під час відеофіксації та відеоспостереження**

Застосування відеоспостереження може бути виправданим з метою безпеки, однак слід брати до уваги його допоміжний характер та ретельно розглядати його в поєднанні з іншими заходами, які слід також застосовувати. Враховуючи нові можливості технологій і характер відеоспостереження, що втручається в приватне життя, усі ри-

зики для прав і свобод дітей повинні бути ретельно оцінені та мінімізовані, тому перед обробленням рекомендується провести оцінювання впливу на захист даних. Порядок обробки персональних даних засобами відеоспостереження має бути частиною політики захисту даних навчального закладу.

### **Література**

1. Міністерство освіти і науки України ««Школа офлайн»: як держава планує повернути 300 тисяч дітей до очного навчання». URL: <https://mon.gov.ua/news/shkola-offlain-iak-derzhava-planuie-povernuty-300-tysiach-ditei-do-ochnoho-navchannia>
2. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
3. Article 29 Data Protection Working Party “Opinion 2/2009 on the protection of children’s personal data (General Guidelines and the special case of schools)”. URL: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf)
4. European Data Protection Board “Guidelines 3/2019 on processing of personal data through video devices”. URL: [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201903\\_video\\_devices\\_en\\_0.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf)
5. Діана Шинкунене та Олександр Шевчук дослідження «Аналіз захисту та обробки персональних даних у системі освіти в Україні». URL: <https://rm.coe.int/report-dp-2024-2web/1680b25a5f>

### **PROTECTION AND PROCESSING OF PERSONAL DATA IN THE EDUCATION SYSTEM**

Article on the processing and protection of personal data in the education system is devoted to the structural analysis of the functioning of the Ukrainian education system and its compliance with the data protection standards.

The analysis bases and reflects the Council of Europe and other international standards in the field of data protection, in particular Convention 108+.

Effective protection of personal data in Ukraine requires enhanced and detailed rights of data subjects, in particular persons who are responsible for processing of personal data in the area of education. Educational institution must respect, protect and fulfil children's right to privacy and data protection. They should ensure that those who process personal data, parents and educators, as well as children themselves, are made aware of children's right to privacy and data protection.

The use of digital technologies for educational purposes leads to the processing of personal data of children by a variety of actors (including national governments, public and private educational establishments, commercial enterprises such as providers of

products or services, software developers and individuals such as teachers, legal guardians and peers). The data that are processed are not only provided by children, parents or educators but are also created as a by-product of user engagement or can be data that are inferred (for instance on the basis of profiling). Highly sensitive data, such as biometric data, are increasingly collected by educational institutions. Such data collection may have lifelong implications for children. It is essential to acknowledge that it is not only the child's right to data protection that is affected when it comes to education and digital technologies but also that the right to privacy and data protection are enabling rights for the protection of further rights and of the child.

**Keywords:** education, personal data protection, personal data processing, data protection by default, data protection by design.

