АНАЛІЗ ЗАХИСТУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ ОСВІТИ В УКРАЇНІ

Проєкт Ради Європи
«Підтримка впровадження європейських стандартів захисту прав людини в Україні»

Діана Шинкунєне
Олександр Шевчук

2024

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

АНАЛІЗ ЗАХИСТУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ ОСВІТИ В УКРАЇНІ

Звіт підготували
Діана Шинкунєне, Олександр Шевчук

КИЇВ, 2024

Аналіз підготували Діана Шинкунєне,
Олександр Шевчук.

Ця публікація розроблена за фінансової підтримки Ради Європи. Погляди, викладені в цьому документі, є відповідальністю його автора і можуть не співпадати з офіційною політикою Ради Європи.

Дозволяється відтворення уривків публікації (до 500 слів) за умови некомерційного використання, збереження цілісності тексту, контексту та надання повної інформації, яка не повинна жодним чином вводити читача в оману щодо характеру, обсягу чи змісту тексту. Необхідно обов'язково зазначати джерело тексту: «© Рада Європи, рік видання». Усі інші запити щодо відтворення або перекладу цієї публікації або будь-якої її частини повинні адресуватися Директорату комунікацій Ради Європи (F-67075 Strasbourg Cedex або publishing@coe.int).

Уся інша кореспонденція щодо цієї публікації повинна направлятися до Головного Директорату з прав людини та верховенства права.

Верстка, дизайн обкладинки та друк: «K.I.C.»

Фото: © Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
(http://book.coe.int)

© Рада Європи, 2024

ЗМІСТ

АВТОРИ ДОСЛІДЖЕННЯ

Автори цього звіту — експерти Ради Європи Діана Шинкунєне та Олександр Шевчук.

Діана Шинкунєне

Діана Шинкунєне — випускниця факультету права Вільнюського університету. З лютого 2023 року обіймає посаду Директора інспекції із захисту персональних даних Литовської республіки. З 2001 по 2018 роки вона була заступником директора Державної інспекції із захисту персональних даних, на якій, поміж іншим, відповідала за аналіз законопроєктів та чинного законодавства Литовської Республіки, зокрема надання пропозицій стосовно формулювання, внесення змін і скасування норм щодо захисту персональних даних і недоторканості приватного життя. У 2017–2018 роках пані Шинкунєне брала участь у підготовці до здійснення на державному рівні реформи у сфері захисту персональних даних у Європейському Союзі — була керівником робочої групи, відповідальної за підготовку змін до Закону про захист персональних даних у контексті Регламенту (ЄС) 2016/679, брала участь у нарадах із зацікавленими сторонами, заходах з інформування громадськості. Діана Шинкунєне активно залучена до заходів, спрямованих на посилення інституційних спроможностей наглядових органів у сфері захисту персональних даних, зокрема на посадах експерта і головного експерта у рамках партнерського проєкту ЄС-UA/47b «Впровадження кращого європейського досвіду з метою посилення інституційного потенціалу Секретаріату Уповноваженого Верховної Ради з прав людини для захисту прав і свобод людини» та експерта Ради Європи в питаннях експертизи проєктів нового законодавства України щодо захисту персональних даних та створення незалежного органу у цій сфері. Пані Шинкунєне також є викладачем курсу з технологій конфіденційності та безпеки в Університеті Миколаса Ромеріса (Вільнюс, Литва).

Олександр Шевчук

Олександр Шевчук — випускник факультету міжнародного права Інституту міжнародних відносин Київського Національного університету імені Тараса Шевченка 2015 року. З 2016 по 2019 роки обіймав посаду експерта з наближення законодавства в рамках проєкту ЄС «Підтримка впровадження Угоди про асоціацію між Україною та ЄС». Виконував обов'язки в Урядовому офісі координації європейської та євроатлантичної інтеграції, де, зокрема, відповідав за порівняльний аналіз законодавства України та ЄС. У 2019 році здобув ступінь кандидата юридичних наук, захистивши дисертацію на тему «Правове регулювання охорони персональних даних в Європейському Союзі». У 2019–2020 роках обіймав посаду національного експерта з електронного правосуддя за напрямком удосконалення захисту персональних даних у рамках проєкту ЄС «Право-Justice». Брав участь в оцінюванні концепцій і практичних заходів з підготування та ухвалення нового законодавства щодо захисту персональних даних. Наразі він національний консультант у сфері захисту персональних даних у рамках спільного проєкту ЄС та Ради Європи з посилення спроможностей Омбудсмана для захисту прав людини. Працював над розробкою навчального онлайн-курсу «Захист персональних даних». У 2019–2021 роках брав участь у підготуванні реформи системи захисту персональних даних в Україні. Входить до складу робочої групи з реформування національного законодавства у сфері обробки і захисту персональних даних. Олександр Шевчук — один з авторів проєкту закону «Про захист персональних даних» та проєкту закону «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації».

ПРОБЛЕМАТИКА ДОСЛІДЖЕННЯ

Насамперед вважаємо за потрібне окреслити ряд проблемних питань, пов'язаних із захистом та обробкою персональних даних під час ведення освітньої діяльності, які стануть предметом нашого дослідження.

1. Визначення правових підстав для обробки персональних даних з метою ведення освітньої діяльності

У керівників закладів освіти та учасників освітнього процесу виникають питання, коли освітній заклад має брати згоду на обробку персональних даних дитини, а коли персональні дані дитини обробляють без такої згоди на підставі закону та повноважень закладу освіти.

2. Використання приватних інформаційних систем, різних додатків, електронних журналів і щоденників в освіті

Частина батьків не погоджується надавати дозвіл на обробку персональних даних дітей у приватних платформах, електронних журналах, щоденниках, бо вважає, що це порушує їхнє право на приватне життя, а також вони не впевнені в надійності збереження персональних даних дитини третіми особами. Натомість заклади, управління освіти чинять тиск на батьків з приводу використання приватних систем під час освітнього процесу.

Водночас трапляється, що батьки вимагають видалити інформацію про дитину або не дають згоди на збереження персональних даних дітей у державних інформаційних системах ПАК «АІКОМ», «ЄДЕБО», що призводить до порушення прав дитини на освіту й унеможливлює отримання документа про здобуття освіти. Керівники закладів освіти іноді не розуміють, як діяти в таких ситуаціях, бо нема системного документа з правовими підставами та алгоритмом дій у такій ситуації.

3. Обробка та захист персональних даних на тимчасово окупованих територіях під час доступу до української освіти

Діти, що залишаються на ТОТ, мають змогу навчатися за українською програмою дистанційно, але здебільшого таке навчання небезпечне для життя та здоров'я через загрози із боку окупантів, тому більшість дітей, які перебувають на ТОТ, мають проблеми з доступом до української освіти.

Водночас існує проблема збереження персональних даних під час дистанційного навчання, бо на ТОТ є лише російський інтернет, який щільно контролюють спецслужби окупантів: ФСБ, російська військова розвідка, самопризначені колаборантські «органи влади». Тому під час дистанційного навчання педагогічні працівники намагаються зашифровувати справжні прізвища, імена, по батькові учнів під різними нікнеймами.

4. Висвітлення інформації про освітню діяльність на вебсайтах та в соціальних мережах закладу освіти

Питання фото- і відеознімання та використання фото дітей окремо законодавством України не врегульоване. Загальне трактування таке, що, з урахуванням Закону України «Про інформацію», згоду на фото- чи відеознімання неповнолітнього, мають надавати батьки.

В умовах воєнного стану розповсюдження конфіденційної інформації про особу може становити загрозу для її життя і здоров'я та життя і здоров'я її родини.

5. Збереження та використання персональних даних, які отримані під час відеофіксації та відеоспостереження

У суспільстві неодноразово порушувалося питання щодо можливості відеофіксації та відеоспостереження в закладах освіти як необов'язкового, але важливого компонента дотримання прав та безпеки учасників освітнього процесу.

6. Облік дітей, що перебувають за кордоном

Наразі в освітньому законодавстві немає норми, що зобов'язувала б батьків повідомляти заклад освіти про місце перебування (проживання дітей). Частина батьків цікавиться, чи правомірно вчитель щомісяця збирає дані про місце перебування дитини та чи правомірно це повідомляти. З цим питанням звертаються і педагоги, бо не знають, де перебуває дитина, адже батьки не повідомляють заклад освіти, що ускладнює облік дітей на рівні закладу освіти та громади. Постає питання, чи потрібно зобов'язати батьків повідомляти заклад освіти про місце перебування (проживання) дитини?

На цих основних питаннях ми зосередимо увагу під час проведення нашого дослідження, оцінення поточної ситуації із захистом персональних даних у системі освіти України та надання рекомендацій, як правомірно вчинити в тій чи іншій ситуації учасникам освітнього процесу, коли мова заходить про обробку та захист персональних даних з метою ведення освітньої діяльності**.**

ВСТУП

20 листопада 2020 року Консультативний комітет Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних опублікував Керівні принципи щодо захисту даних дітей в освітньому середовищі, які базуються на доповіді Джен Перссон, директорки «DefendDigitalMe», «Захист даних дітей в системах освіти. Виклики та можливі засоби їх розв'язання».

«Не варто недооцінювати конфіденційність цифрових даних учнів та студентів … Потенційна шкода від неналежного використання звичайних цифрових освітніх записів може здатися незначною проти складніших технологій, які вже використовуються в освіті. Але якщо оцінити масштаби учнівських баз даних, що містять сотні одиниць персональних даних про поіменно названих осіб у мільйонах різних записів на національному рівні, то ризики для людей, а також інституційні та репутаційні ризики втрати навіть найпростіших даних можуть стати очевиднішими» — йдеться в доповіді Джен Перссон.

«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, щоб в обробці даних дітей в контексті освітньої діяльності компанії знали, що дозволено, а що ні, створюючи справедливе ігрове поле для всіх» — підкреслюється в Керівних принципах щодо захисту даних дітей в освітньому середовищі[1].

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 різноманітних державних та приватних електронних систем і платформ.

Дистанційна взаємодія педагогічного працівника зі здобувачами освіти викликала в учасників освітнього процесу багато нових запитань, зокрема щодо ведення та оприлюднення відеозаписів занять, оприлюднення оцінок, передання 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. Тепер майже 1 млн дітей навчається онлайн: приблизно 600 тисяч в Україні, ще майже 400 тисяч за кордоном. Дистанційне навчання — один із найбільших викликів

1. https://www.coe.int/uk/web/kyiv/-/children-s-data-protection-in-an-education-setting-joint-eu-council-of-europe-project-provided-translation-of-guidelines.

для держави, Сьогодні маємо різні категорії учнів із різними потребами, як-от діти на ТОТ чи діти за кордоном. Водночас дистанційна освіта — це також питання безпеки персональних даних дітей. Особливо це питання стосується дітей, які проживають на ТОТ і продовжують дистанційне навчання за українською програмою. В таких випадках порушення безпеки персональних даних може мати наслідком не тільки втручання в приватне життя дитини і її батьків, але і спричинити загрозу для її фізичної безпеки і навіть становити загрозу її життю[2].

Відсутність на державному рівні чітких рекомендацій, інструкцій для володільця та розпорядників персональних даних, а також для учасників освітнього процесу щодо особливостей обробки та захисту персональних даних у сфері освіти ускладнює роботу закладів освіти та комунікацію учасників освітнього процесу, які потребують просвітницької та роз'яснювальної роботи.

2. https://mon.gov.ua/news/shkola-oflain-iak-derzhava-planuie-povernuty-300-tysiach-ditei-do-ochnoho-navchannia.

ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ ОСВІТИ УКРАЇНИ

Закон України «Про захист персональних даних» — це правова основа для регулювання відносин, що стосується передання та обробки персональних даних, і забезпечення водночас захисту прав суб'єкта персональних даних.

Мета захисту персональних даних — забезпечення за допомогою законодавчих, регуляторних та організаційних заходів, гарантії захисту прав та інтересів суб'єкта даних (учасників освітнього процесу) під час передання та обробки його персональних даних.

Зміст ключових термінів у сфері захисту персональних даних

Означення поняття «персональні дані» закріплено в статті 2 Закону України «Про захист персональних даних».

Поняття «персональні дані»

Персональні дані

- це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Фізична особа, яку можна ідентифікувати, —

така особа, яку можна ідентифікувати прямо чи опосередковано, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи кількома факторами, визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

Що таке обробка персональних даних?

Обробка персональних даних — будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передання), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Обробка біометричних даних учасників освітнього процесу

Біометричні дані — персональні дані, які стосуються фізичних, фізіологічних чи поведінкових характеристик фізичної особи, які внаслідок спеціальної технічної обробки дають можливість ідентифікувати або верифікувати фізичну особу[3].

Біометричні дані не повинні на постійній основі оброблятися в закладах освіти. Використання біометричних даних у закладах освіти за виняткових обставин, зокрема для перевірки особистості, як-от дистанційного нагляду за студентами, дозволяється тільки тоді, 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 оцінення впливу на захист даних і за наявності відповідних гарантій, закріплених законом. Ці гарантії мають охоплювати 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.

Винятки з використання біометричних даних з метою підтримки дітей і педагогічного персоналу з особливими потребами щодо доступу, наприклад у вигляді ідентифікації по очах за допомогою екрана, для їхньої безпосередньої вигоди та без дискримінації, повинні застосовуватися з наданням належних гарантій, закріплених в законі[4].

Усі учасники освітнього процесу — суб'єкти персональних даних.

Відповідно до частини першої статті 19 Закону України «Про повну загальну середню освіту» до учасників освітнього процесу в закладах освіти належать: учні, педагогічні працівники, інші працівники закладу освіти, батьки учнів, асистенти дітей.

Заклад освіти і кожен педагогічний працівник як його представник несе відповідальність за збереження тих персональних даних учнів, батьків, педагогічних працівників, обробку яких він здійснює.

Принципи обробки персональних даних

Важливо розуміти, що будь-яка обробка персональних даних учасників освітнього процесу має здійснюватися з дотриманням основоположних принципів обробки персональних даних, закріплених у національному і міжнародному законодавстві.

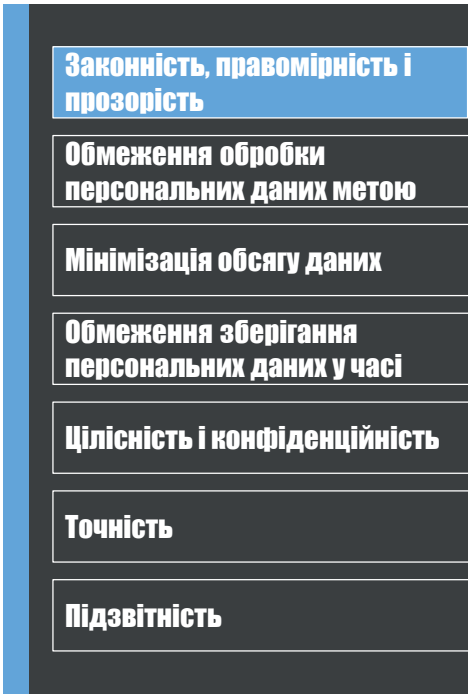
В обробці персональних даних слід обов'язково дотримуватися основних принципів щодо конфіденційності і захисту персональних даних[5].

3. https://itd.rada.gov.ua/billInfo/Bills/Card/40707.
4. https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-ua-f/1680a2addc.
5. Лілія Олексюк та Андрій Ніколаєв. «Принципи захисту персональних даних та ризики їх порушення при використанні технології зв'язку 5G». URL: http://perspectives.pp.ua/index.php/vp/article/view/807/809.

Принцип перший: «законність, правомірність і прозорість»

Персональні дані повинні оброблятися законним, правомірним і прозорим способом стосовно суб'єкта даних («законність, правомірність і прозорість»). Будь-яка обробка персональних даних має бути законною та справедливою. До фізичної особи має бути прозоро донесено те, що її персональні дані збирають, використовують, переглядають або іншим чином обробляють, а також те, яким обсягом персональні дані обробляють і будуть обробляти.

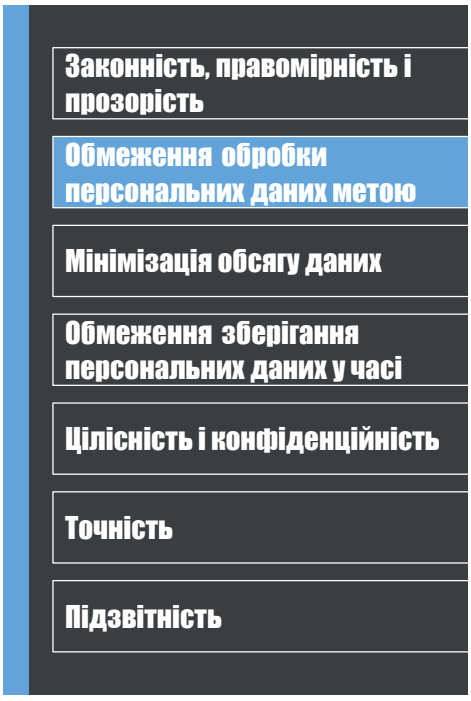
Також передбачається необхідність інформування суб'єктів персональних даних про особу володільця, про цілі (мету) обробки персональних даних і додаткове інформування для забезпечення справедливої та прозорої обробки в частині, що стосується відповідних фізичних осіб і права на отримання підтвердження та відомостей про ті персональні дані, які обробляють на їх основі.



Принцип другий: «обмеження обробки персональних даних метою»

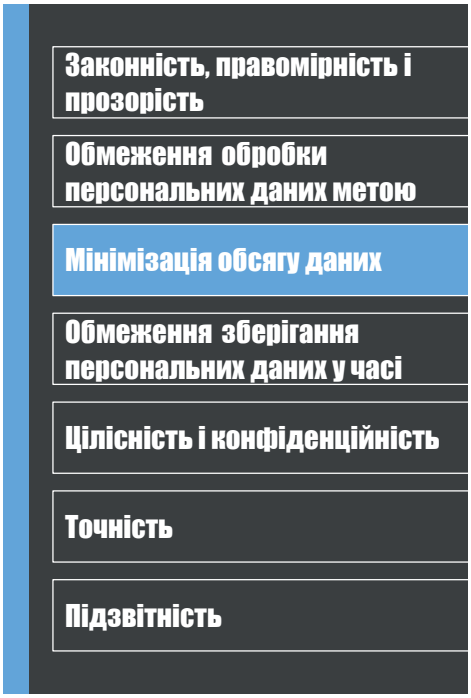
Персональні дані можуть збирати лише для конкретних, чітких і законних цілей, і їх не повинні обробляти в подальшому способом, несумісним із визначеними цілями («конкретність цілей»). Мета обробки обов'язково має бути чітко визначеною до початку обробки. Також необхідно переконатися, що дії, які планується виконувати з персональними даними, цілком законні. Також мета має бути задокументована, тобто прописана у відповідних документах, які регламентують обробку (порядок обробки, політика конфіденційності тощо).

Можна обробляти персональні дані з іншою метою, тільки якщо вона сумісна з початковою метою, або отримано згоду суб'єкта на обробку з новою метою, або обробка необхідна для виконання зобов'язання встановленого законом, або обробка ведеться для реалізації повноважень встановлених законом.



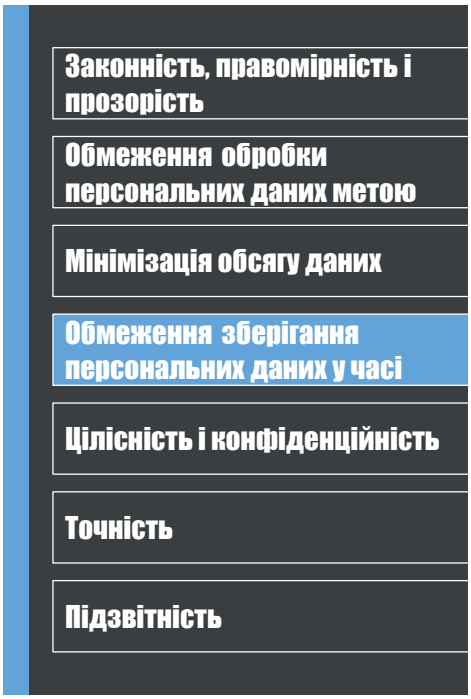
Принцип третій: «мінімізація обсягу даних»

Персональні дані повинні бути адекватними, відповідними та ненадмірними й обмежуватися тим, що необхідно для мети, з якою їх обробляють («мінімізація персональних даних»). Можна виділити такі показники: дані адекватні, якщо вони достатні для досягнення мети обробки; дані відповідні, якщо вони мають раціональний зв'язок із метою обробки та сприяють її досягненню; дані ненадмірні, якщо їх обсяг не більший, ніж це необхідно для досягнення мети обробки; не можна збирати дані «про всяк випадок».



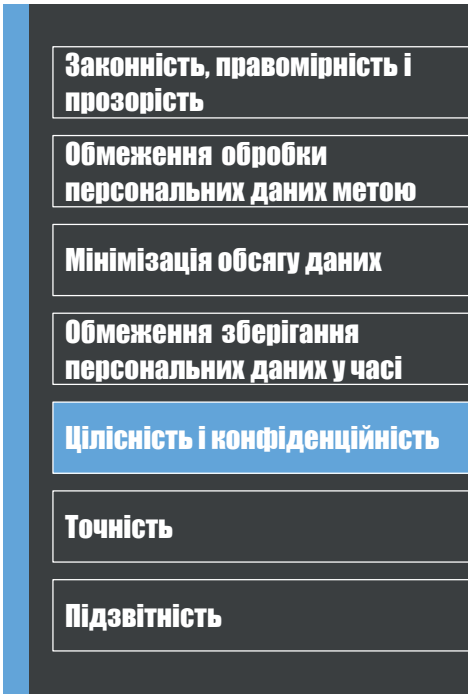
Принцип четвертий: «обмеження зберігання персональних даних у часі»

Персональні дані не повинні зберігатися довше ніж вони потрібні для цілей, для яких ці дані обробляють («обмеження строків зберігання»). Після того як мета досягнута, персональні дані повинні бути знищені або знеособлені. Знеособлені персональні дані — це дані, зі складу яких вилучили всі відомості, та які вже не дають змоги будь-яким чином ідентифікувати конкретну особу— суб'єкта персональних даних. Персональні дані можуть зберігатися протягом тривалішого часу винятково для досягнення цілей суспільних інтересів, наукового чи історичного дослідження або статистичних цілей, за умов вжиття відповідних технічних і організаційних заходів, передбачених законодавством, для гарантування прав і свобод суб'єкта даних.



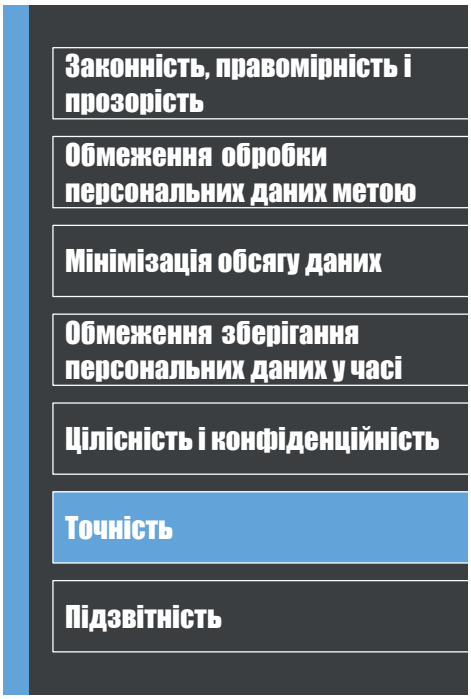
Принцип п'ятий: «цілісність та конфіденційність»

Персональні дані повинні оброблятися так, щоб забезпечити їх цілісність та конфіденційність. Персональні дані повинні оброблятися так, щоб забезпечити належний рівень безпеки та конфіденційності цих персональних даних, зокрема для запобігання несанкціонованому доступові або несанкціонованому використанню персональних даних та обладнання, що використовується для обробки. Володільці та розпорядники зобов'язані вживати технічних та організаційних заходів безпеки на рівні, що відповідає законодавчим вимогам.



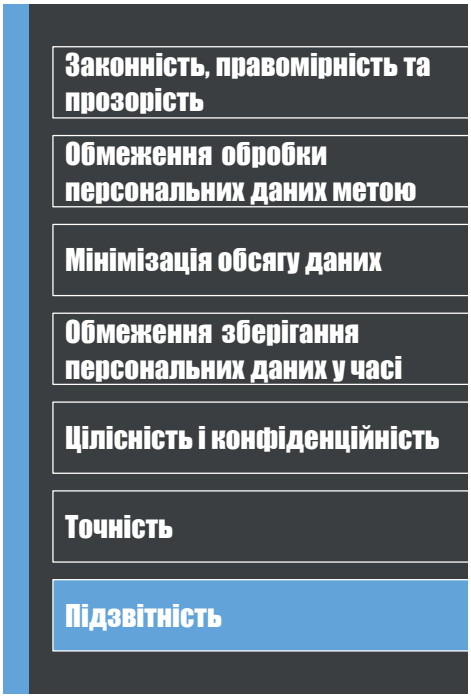
Принцип шостий: «точність»

Персональні дані мають бути точними, вірогідними та оновлюваними, якщо це необхідно для мети їх обробки («точність»). Необхідно вживати всіх раціональних заходів, щоб забезпечити точність персональних даних, які обробляються, а також усіх відповідних заходів для того, щоб неточні персональні дані були негайно видалені або виправлені.



Принцип сьомий: «підзвітність»

Володілець несе відповідальність за дотримання принципів обробки персональних даних та має бути здатним це довести («підзвітність»). Обов'язок доведення дотримання цих принципів покладається на володільця.



Права суб'єктів персональних даних — учасників освітнього процесу

Відповідно до статті 8 Закону України «Про захист персональних даних» суб'єкт персональних даних (учасник освітнього процесу) має право:

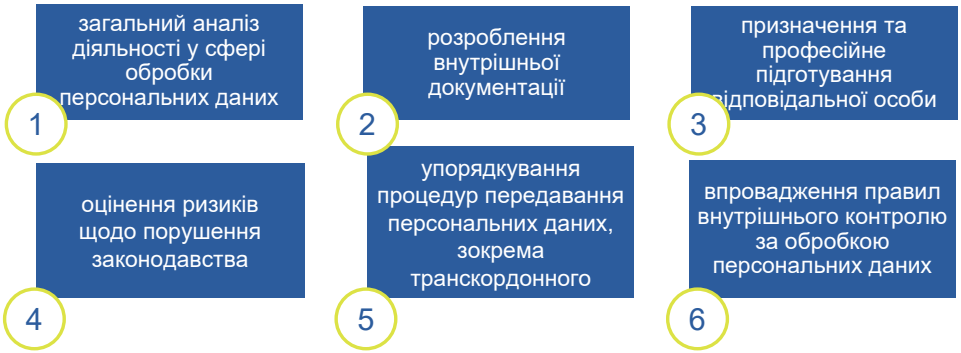
- отримувати інформацію про джерела збору та місце збереження своїх персональних даних, мету їх обробки;
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються персональні дані;
- отримувати не пізніше ніж за тридцять календарних днів з дня надходження запиту (крім випадків, передбачених Законом України «Про захист персональних даних») інформацію щодо обробки та використання персональних даних;
- пред'являти вмотивовану вимогу володільцеві персональних даних із запереченням щодо обробки персональних даних;
- відкликати згоду на обробку персональних даних;
- звертатися зі скаргами щодо обробки персональних даних володільцем чи розпорядником персональних даних до Уповноваженого Верховної ради України з прав людини або до суду;
- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.

Порядок організації процесу обробки персональних даних

Проводячи обробку персональних даних, володільцеві персональних даних (закладам освіти, адміністраторам освітніх електронних інформаційних систем) необхідно забезпечити захист персональних даних від випадкових втрати або знищення, від незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних. Володілець персональних даних

вживає заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, зокрема за допомогою організаційних та технічних заходів.

До основних організаційних заходів можна віднести:



З метою убезпечення обробки персональних даних вживають технічних заходів захисту, зокрема щодо виключення несанкціонованого доступу до персональних даних, що обробляються, та роботи технічного і програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

Для того щоб контролювати цей процес та здійснювати обробку персональних даних законно й прозоро, потрібно упорядкувати цю роботу за допомогою відповідних внутрішньорозпорядчих документів[6].

До переліку внутрішньорозпорядчих документів можна віднести:

1. Порядок обробки персональних даних
2. Загальна внутрішня інструкція роботи з персональними даними, де визначені чіткі вимоги до персоналу, залежно від їхніх повноважень щодо роботи з даними
3. Правила внутрішнього контролю за процесами обробки даних
4. Правила роботи зі знеособленими даними
5. Перелік місць зберігання матеріальних носіїв персональних даних
6. Посадові інструкції осіб, відповідальних за організацію обробки даних, де буде також міститися зобов'язання про нерозголошення персональних даних
7. Правила щодо передачі персональних даних третім особам або їх поширення

6. Захист персональних даних: роз'яснення для суб'єктів владних повноважень від Уповноваженого Верховної Ради України з прав людини. URL: https://ombudsman.gov.ua/storage/app/media/27012023/37676120-9a08-47d9-a376-b498dd07ede5.pdf.

Вагому роль в забезпеченні захисту персональних даних відводиться обов'язкові володільця вести облік операцій (реєстр операцій), пов'язаних з обробкою персональних даних. Згідно з Типовим порядком обробки персональних даних з цією метою володілець / розпорядник зберігає інформацію про дату, час та джерело збирання персональних даних суб'єкта.

Реєстр повинен містити інформація про:

1. Правові підстави та джерела збору даних
2. Цілі обробки даних
3. Види та категорії персональних даних, що збираються
4. Перелік осіб, які мають доступ до даних та беруть участь в їх обробці
5. Перелік третіх осіб, кому були або будуть розкриті дані, зокрема треті країни або міжнародні організації, а також законні підстави та цілі надання інформації
6. Строки зберігання та видалення даних
7. Організаційні заходи безпеки даних

Порядок ведення контролю за додержанням законодавства про захист персональних даних

У роз'ясненні освітнього омбудсмена зазначено алгоритм дій у разі порушення безпеки персональних даних учасників освітнього процесу: «Якщо батьки побачили, що захист персональних даних їхніх дітей з боку конкретного вчителя або закладу освіти порушується — зверніться до вчителя або закладу освіти з проханням забезпечити конфіденційність персональних даних. Якщо вчитель постраждав від розголосу його персональних даних з боку учня або батьків — зверніться до батьків із проханням видалити інформацію, що містить персональні дані. Якщо ситуацію не було вирішено, і батьки, і педагогічні працівники можуть звернутися до Уповноваженого Верховної Ради України з прав людини»[7].

Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, покладено на Уповноваженого Верховної Ради України з прав людини.

Контроль полягає в установленні відповідності процесу обробки персональних даних до вимог Конституції України, Закону України «Про захист персональних даних», Типового порядку обробки персональних даних, а також чинних міжнародних договорів України у сфері захисту персональних даних, згоду на обов'язковість яких надала Верховна Рада України.

Контроль Уповноваженим Верховної Ради України з прав людини у сфері захисту персональних даних здійснюється шляхом проведення перевірок фізичних осіб, фізичних осіб — підприємців, підприємств, установ і організацій усіх форм власності, органів державної влади та місцевого

7. https://info.eo.gov.ua/kudy-zvertatysya-uchasnykam-osvitnogo-proczesu-yakshho-porushuyetsya-zahyst-personalnyh-danyh/.

самоврядування — володільців та/або розпорядників персональних даних. Перевірки можуть бути планові, позапланові, виїзні та безвиїзні[8].

За результатами перевірок складають акти перевірки додержання вимог законодавства про захист персональних даних, на підставі яких у разі виявлення порушень складають припис про їх усунення або протокол про адміністративне правопорушення.

Важливо зазначити, що порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом. Зокрема, у разі виявлення під час перевірки передбаченого статтею 188-39 чи статтею 188-40 Кодексу України про адміністративні правопорушення адміністративного правопорушення на суб'єкта перевірки в установленому законом порядку може накладатися штраф від ста до двох тисяч неоподатковуваних мінімумів доходів громадян.

У разі виявлення під час перевірки ознак кримінального правопорушення Уповноважений направляє необхідні матеріали до правоохоронних органів.

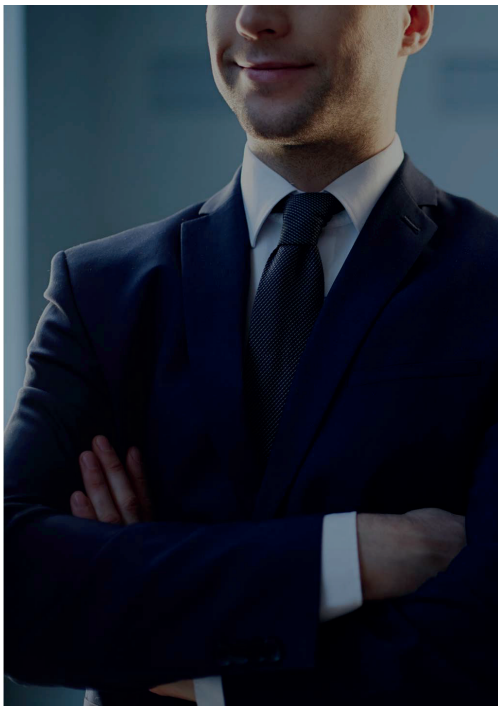
Підвищення рівня професійного підготування учасників освітнього процесу

Важливі є навчання і професійне підготування працівників закладу освіти щодо обробки персональних даних учасників освітнього процесу.

Які обов'язки в посадових осіб, які проводять обробку персональних даних?

Зокрема вони повинні бути спроможні:

- роз'ясняти суб'єктові персональних даних його права в цій сфері;
- вживати заходів щодо забезпечення вірогідності оброблюваних персональних даних. У разі необхідності вносити зміни до персональних даних, які неповні, застарілі або неточні;
- вести контроль за терміном обробки даних відповідно до заявлених цілей. Припиняти обробку, а також забезпечувати видалення або блокування, якщо нема правових підстав для подальшої роботи з даними;
- надавати доступ, передавати або поширювати персональні дані лише за наявності відповідної правової підстави;
- забезпечувати доступ до персональних даних у встановленому порядку, вести облік (реєстр) у разі передання персональних даних третім особам.



Питання, які повинні розглядатися в рамках професійного підготування[9]:

- роз'яснення положень національного законодавства та міжнародних стандартів у сфері захисту персональних даних;
- аналіз діяльності та оцінення ризиків під час обробки персональних даних;
- права суб'єкта персональних даних;
- повноваження, законна підстава та порядок доступу до інформації з боку третіх осіб;

8. https://ombudsman.gov.ua/uk/kontrol-za-doderzhannyam-vimog-zakonodavstva-zpd.
9. https://ombudsman.gov.ua/storage/app/media/27012023/37676120-9a08-47d9-a376-b498dd07ede5.pdf.

- розроблення внутрішньої документації (зміст, процедури та заходи);
- операції з обробки персональних даних, що можуть становити особливий ризик для прав і свобод людини;
- використання інформаційних систем: *ведення реєстрів, терміни зберігання, порядок доступу третіх осіб, інформування суб'єктів даних;*
- видалення або знищення персональних даних;
- правила внутрішнього контролю та відповідальність.

ОРГАНІЗАЦІЯ ПРОЦЕСУ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОСВІТИ В ЄС / ДЕРЖАВАХ — ЧЛЕНАХ ЄС

Порядок організації процесу обробки персональних даних у сфері освіти

Навчальні заклади (дитсадки, школи, коледжі, університети тощо) збирають та в подальшому обробляють персональні дані фізичних осіб (суб'єктів даних): учнів, студентів (зокрема тих, які закінчили навчання в закладі), батьків та законних представників, працівників тощо, а також виступають як контролери даних, як це визначено Конвенцією 108+ та Загальним регламентом захисту даних (ЄС) 2016/679 (надалі — GDPR). 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 обробки персональних даних навчальні заклади Литви також зобов'язані дотримуватися різноманітних національних нормативно-правових актів, а саме: Закону про захист персональних даних, Закону про освіту, Закону про вищу освіту та науково-дослідницьку діяльність, Закону про фізичне виховання та спорт, Закону про керування державними інформаційними ресурсами, постанов уряду, що регулюють питання обробки даних, зокрема діяльність державного реєстру / інформаційної системи та інші аспекти обробки даних, накази міністра освіти, культури та спорту.

З метою реалізації основних принципів захисту персональних даних, викладених у статті 5 Конвенції 108+, і дотримуючись принципу підзвітності, як того вимагає стаття 5(2) GDPR, під час організації процесу обробки персональних даних навчальні заклади повинні виконати такі дії:

- розробити, підтримувати та періодично переглядати внутрішні документи, спрямовані на забезпечення впровадження принципів захисту даних, встановлених Конвенцією 108+ та GDPR;
- запровадити ефективні внутрішні процеси та процедури для забезпечення обробки персональних даних відповідно до зазначених вище внутрішніх документів;
- підтримувати ефективне керування ризиками (виявляти, оцінювати, мінімізувати різноманітні внутрішні і зовнішні ризики);
- 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).

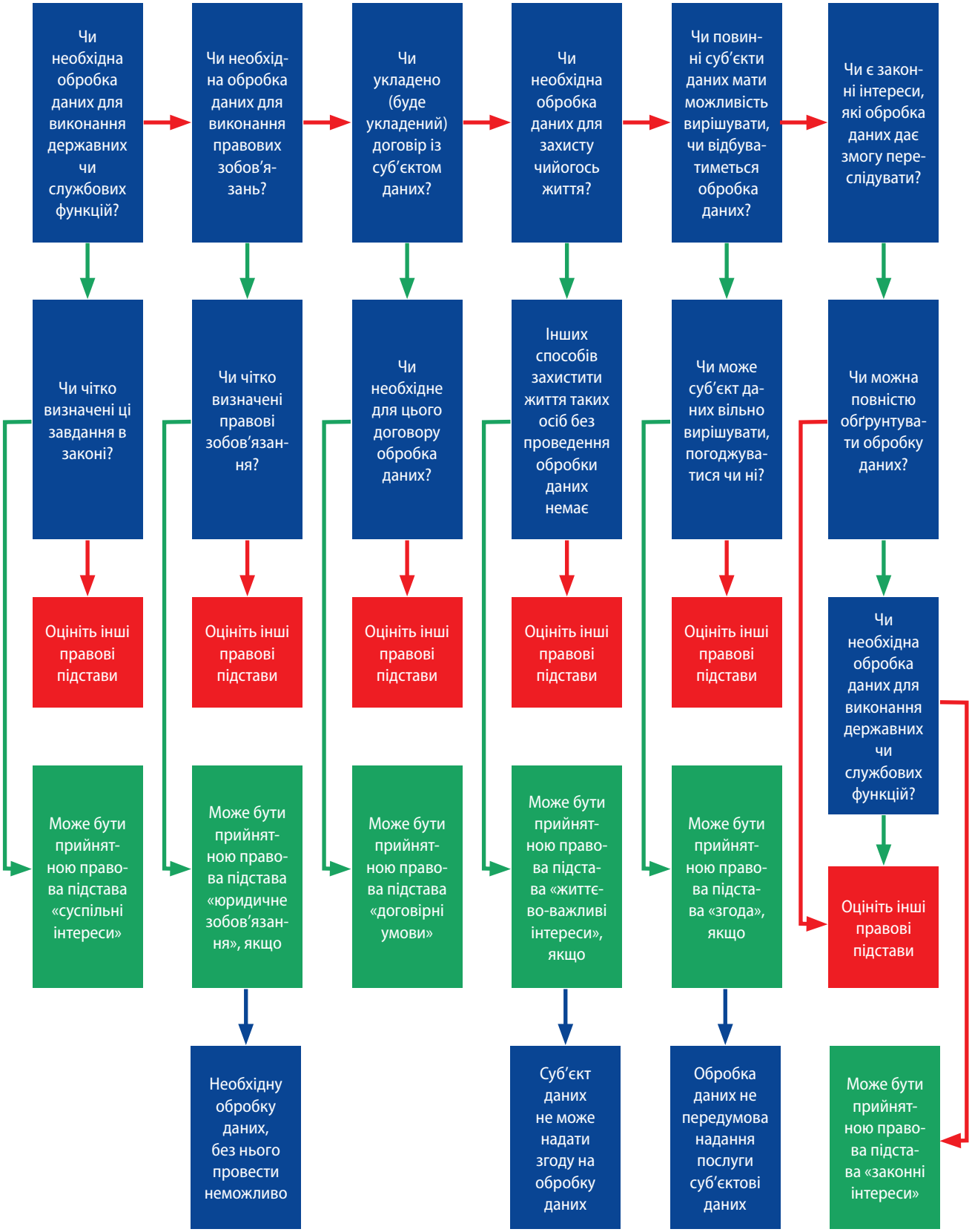
Законність обробки персональних даних

Щоб забезпечити законність обробки персональних даних, навчальні заклади повинні переконатися, що операція обробки здійснюється на законній підставі, встановленій пунктом 1 статті 6 GDPR, або, у разі обробки спеціальних категорій даних, покладається на винятки, передбачені пунктом 2 статті 9 GDPR. А що законність обробки тісно пов'язана з іншими принципами, встановленими пунктом 1 статті 5 GDPR, то перш ніж ухвалити рішення щодо правової підстави для обробки персональних даних, навчальний заклад повинен розглянути такі елементи:

- **мета операції з обробки персональних даних повинна бути чітко визначена** перед вибором правової підстави для обробки;
- **пропорційність обробки**: якщо обробка персональних даних не необхідність (мета може бути належним обсягом досягнута без обробки), обробка персональних 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[10], можна продовжити процес обробки відповідно до первинної правової підстави. Якщо нова мета не сумісна з початковою, обробку можна здійснювати, якщо вона основана на згоді суб'єкта даних або на вимогах законодавства[11];
- **усі правові підстави рівні**, і жодна не переважає інші, тому необхідно розглянути найбільш відповідну з урахуванням конкретного випадку обробки даних.

Наведений нижче алгоритм[12] може стати у пригоді під час вибору відповідної правової підстави для обробки даних[13]:

10. Згідно з пунктом 4 статті 6 GDPR, щоб переконатися у сумісності цілей, слід брати до уваги такі обставини: будь-який зв'язок між цілями, для яких збирають персональні дані, і цілями запланованої подальшої обробки; контекст збирання персональних даних, зокрема, щодо взаємозв'язку між суб'єктами даних і контролера; специфіку персональних даних (зокрема, питання обробки спеціальних категорій персональних даних згідно зі статтею 9 або обробки персональних даних про судимості і кримінальні злочини згідно зі статтею 10); можливі наслідки запланованого подальшої обробки для суб'єктів даних; наявність належних гарантій, що можуть передбачати шифрування чи використання псевдонімів.
11. Норма законодавства Союзу або держави-члена, яка слугує необхідним і пропорційним заходом у демократичному суспільстві для захисту цілей, зазначених у пункті 1 статті 23.
12. Розробила благодійна довірча компанія «Саус-Вест Грід фор Лернінг Траст Лтд» (South West Grid for Learning Trust Ltd), зареєстрована в Англії. Номер компанії: 5589479. Номер благодійної організації: 1120354. Реєстраційний номер платника ПДВ: GB 880. 8618 88. Посилання: https://swgfl.org.uk/assets/documents/swgfl-gdpr-lawful-basis-assessment-tool.pdf. Дата звернення: 13 серпня 2024 р.
13. Посилання: https://swgfl.org.uk/resources/gdpr-guidance-for-schools-and-colleges/part-4/. Дата звернення: 13 серпня 2024 р.



Зелені стрілки означають відповідь «так», а **червоні** — «ні». **Сині** стрілки в нижньому рядку алгоритму вказують на відповідні передумови.

Навчальні заклади повинні визначити правові підстави для обробки, задокументувати це в протоколах обробки даних[14] чи інших внутрішніх документах (правилах обробки персональних даних) і надати відповідну інформацію суб'єктам даних, дотримуючись принципу прозорості, закріпленого в статті 8 Конвенції 108+ та відповідно до статей 13 і 14 GDPR.

Внутрішні документи навчальних закладів

Важлива частина процесу обробки персональних даних у навчальних закладах — 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 вони один з елементів принципу підзвітності, що дає змогу продемонструвати відповідність до застосовних правових вимог. 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 — внутрішній документ 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 GDPR та національного 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, керування ризиками та безпека даних, навчання персоналу, процедури перегляду Порядку[15].

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; оцінення впливу на захист даних; оцінення 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[16].

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.

14. Протоколи обробки даних повинні зберігатися відповідно до вимог, зазначених у статті 30 ЗРЗД.
15. Наприклад, у Литві навчальні заклади можуть виконувати функції обробників даних щодо обробки даних у державних реєстрах та інформаційних системах.
16. Щоб зменшити адміністративне навантаження, рекомендується використовувати шаблони та форми, надані наглядовим органом з питань захисту даних.

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; ухвалення рішення щодо фінансових та інших ресурсів, необхідних для належного виконання вимог захисту персональних даних; встановлення та затвердження Порядку обробки персональних даних та відповідної документації; ухвалення рішення про те, які саме технології використовувати для обробки персональних даних; ухвалення 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[17]; забезпечення проведення тренінгів з питань захисту персональних даних для персоналу не рідше ніж один раз на рік[18].
- **Усі співробітники** несуть відповідальність за участь у підготуванні та розуміння того, що таке персональні дані, що означає обробка 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** (зборі, зберіганні, введенні 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 своєю роллю та відповідними обов'язками; забезпечити наявність правових підстав для збору та подальшої обробки персональних даних, а також відповідність обробки персональних даних до внутрішніх документів 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.

Облік дітей у навчальних закладах

Облік дітей у навчальних закладах залежить від особливостей національної системи освіти та вимог законодавства, яке регулює цей процес. У Литві особа має право обрати державну, муніципальну чи недержавну школу та змінити її. Процес обліку може бути організований способом, визначеним відповідними законодавчими вимогами. Згідно із Законом про освіту[19]:

17. Згідно з пунктом 1 статті 38 GDPR, навчальний заклад повинен забезпечити, щоб співробітника з питань захисту даних залучали, належним чином і вчасно, до всіх питань, що стосуються захисту персональних даних. У пункті 2 статті 35 встановлено обов'язок для контролера звернутися по рекомендації до співробітника з питань захисту даних у ході проведення оцінювання впливу на захист даних.
18. Проведення навчальних тренінгів один раз на рік — мінімальна вимога, встановлена в Методичних рекомендаціях щодо оцінення ризиків і заходів безпеки для контролерів і операторів даних Державної інспекції захисту даних Литовської Республіки, див. онлайн литовською мовою: https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf. Дата звернення: 16 серпня 2024 р. З огляду на роль співробітника та засоби, що використовуються для проведення обробки, може знадобитися конкретніше підготування, зокрема моделювання кібербезпеки.
19. Див. онлайн, литовською мовою: https://www.e-tar.lt/portal/lt/legalAct/TAR.9A3AD08EA5D0/asr. Дата звернення: 15 серпня 2024 р.

1) Порядок прийняття до державної та муніципальної загальноосвітньої школи для навчання за програмами дошкільної освіти, загальноосвітніми програмами, до закладу дошкільної освіти для навчання за програмою дошкільної освіти визначає заклад що реалізує права та обов'язки власника (наприклад, муніципалітет) [20] відповідно до критеріїв прийняття, затверджених міністром освіти, науки та спорту.

2) Критерії та порядок прийняття до державного та муніципального закладу дошкільної освіти для навчання за програмою дошкільної освіти та школи неформальної освіти дітей визначає установа, що реалізує права та обов'язки власника.

3) Порядок прийняття до недержавного навчального закладу, що реалізує програми формальної та/або неформальної освіти дітей, визначає власник відповідно до вимог до прийняття на відповідні програми, встановлених цим Законом.

Відповідно до пункту 1 частини другої статті 29 Закону про освіту з 1 січня 2026 року подання заяв про вступ до державних і муніципальних навчальних закладів, які реалізують програму дошкільної, початкової, основної, середньої освіти, формування черги учнів, підтвердження списків прийнятих учнів, надання відомостей про вступ до школи, запрошення до підписання договору про навчання та його підписання, **обробка даних учнів здійснюється централізовано** в порядку, встановленому міністром освіти, науки та спорту.

Прийняття на навчання за освітніми програмами (крім програм вищої освіти) здійснюється централізовано, а прийняття на навчання за скороченою програмою, програмою першого циклу з отриманням ступеня бакалавра, інтегрованою та фаховими програмами — **централізовано призначеною державною установою з використанням державної інформаційної системи, призначеної для цієї функції**. Власник цієї державної установи — держава, а права та обов'язки власника реалізовує уряд або уповноважений ним орган. Діяльність цієї державної установи фінансується коштом асигнувань державного бюджету та інших коштів, виділених Міністерству освіти, науки та спорту.

Правила прийняття до вищих навчальних закладів визначає Закон про науку та освіту. Відповідно до частини сьомої статті 59 Закону про науку та освіту[21] прийняття осіб (крім іноземців, які претендують на здобуття освіти за недержавною формою навчання), які зараховуються на навчання за скороченою програмою, програмою першого циклу з отриманням ступеня бакалавра, інтегрованою або фаховими програмами, здійснюється з використанням спеціалізованої державної інформаційної системи[22]. **Централізована координація** прийняття на навчання за скороченою програмою, програмою першого циклу з отриманням ступеня бакалавра, інтегрованою та фаховими програмами здійснюється в порядку, встановленому міністром освіти, науки і спорту.

Оперативна сумісність державних реєстрів у сфері освіти

Обробка персональних даних у державних реєстрах має здійснюватися згідно з принципами захисту персональних даних, тому всі нормативно-правові акти (їхні проєкти), що регулюють функціонування державних реєстрів та інформаційних систем, узгоджуються з Державною інспекцією із захисту даних Литовської Республіки.

20. Наприклад, муніципалітети як власники затверджують опис порядку організації прийняття дітей у групи дошкільної освіти навчальних закладів.
21. Див. онлайн литовською мовою: https://www.e-tar.lt/portal/lt/legalAct/TAR.C595FF45F869/asr. Дата звернення: 15 серпня 2024 р.
22. Загальна інформаційна система вступу, контролер даних — Асоціація вищої освіти Литви для організації спільного вступу.

Згідно зі статтею 6 Закону Литовської Республіки про керування державними інформаційними ресурсами[23], основу державних інформаційних ресурсів становлять інформаційні системи реєстрів, до яких вносяться основні об'єкти (резиденти, юридичні особи, адреси, нерухоме майно, права власності на нерухоме майно та правові акти) та за допомогою яких здійснюється керування даними цих об'єктів та їхній облік. Дані, які пройшли обробку в них, можуть використовуватися в інших інформаційних системах. Оперативна сумісність інформаційних систем — ключовий елемент їхнього функціонування. Інформаційні системи обмінюються між собою даними, необхідними для функціонування та виконання функцій суб'єктів, встановлених нормативно-правовими актами, через інтегровані інтерфейси, розроблені для забезпечення взаємодії. Законні підстави такої взаємодії визначені в нормативних актах, що регулюють роботу таких інформаційних систем, а сама взаємодія підтримується відповідно до порядку та умов, встановлених у таких нормативних актах, шляхом передавання та постійного оновлення даних, що обробляються в інформаційних системах, через електронні комунікаційні мережі. Приклади реєстрів у сфері освіти в Литві та їхня сумісність з іншими реєстрами / інформаційними системами наведені в таблиці нижче.

№	Назва реєстру	Предмет реєстру	Оперативна сумісність з іншими реєстрами / інформаційними системами
1.	Реєстр освітян	Науково-педагогічні працівники навчальних закладів	Реєстр населення Литовської Республіки Реєстр навчальних і науково-дослідницьких установ Реєстр освітньої діяльності, програм навчання та кваліфікацій Реєстр дипломів, атестацій та кваліфікаційних сертифікатів
2.	Реєстр учнів	Учні, які здобувають початкову, основну, середню освіту та/або формальну професійно-технічну освіту, неформальну дитячу освіту та освіту, що доповнює формальну освіту; навчаються за програмами дошкільної освіти, програмами литовської освіти	Реєстр населення Литовської Республіки Реєстр навчальних і науково-дослідницьких установ Реєстр освітньої діяльності, програм навчання та кваліфікацій Реєстр дипломів, атестацій та кваліфікаційних сертифікатів Реєстр ліцензій Реєстр освітян Реєстр іноземців Реєстр програм неформальної освіти Централізована інформаційна система державних іспитів
3.	Реєстр учнів та студентів	Реєстр учнів старших класів	Реєстр населення Литовської Республіки Реєстр навчальних і науково-дослідницьких установ Реєстр освітньої діяльності, програм навчання та кваліфікацій Реєстр дипломів, атестацій та кваліфікаційних сертифікатів Реєстр учнів Інформаційна система надання, адміністрування та погашення студентських кредитів Інформаційна система стипендіального та матеріального забезпечення студентів

23. Див. онлайн литовською мовою: https://www.e-tar.lt/portal/lt/legalAct/TAR.85C510BA700A/asr. Дата звернення: 15 серпня 2024 р.

4.	Реєстр дипломів, атестацій та кваліфікаційних сертифікатів	Документи, що засвідчують досягнення результатів навчання	Реєстр учнів Реєстр учнів та студентів Реєстр навчальних і науково-дослідницьких установ Реєстр освітньої діяльності, програм навчання та кваліфікацій Реєстр бланків дипломів про освіту

Надаючи адміністративні чи державні послуги в електронній формі, суб'єкти повинні використовувати лише дані, оброблені в інформаційних системах. У переданні даних до інших інформаційних систем для забезпечення їхньої сумісності використовуються ідентифікаційні коди об'єктів, якими управляє реєстр. Обмін даними здійснюється відповідно до форматів передавання даних і стандартів, встановлених компетентним органом.

Навчальні заклади обробляють (надають, отримують, передають тощо) персональні дані учнів, їхніх законних представників та педагогів згідно з нормативно-правовими актами відповідного державного реєстру / інформаційної системи.

Використання приватних інформаційних систем, додатків, електронних журналів і щоденників у навчанні

Навчальні заклади можуть використовувати інформаційні системи, прикладні програми, програмне забезпечення (надалі — продукти / ресурси / послуги ІКТ), які розробляють і підтримують приватні структури. Ухвалюючи рішення про використання для обробки даних дітей ресурсів ІКТ, які створюють, обслуговують, підтримують приватні структури, навчальні заклади повинні враховувати всі нормативні акти, рекомендації, висновки, рішення щодо окремих сфер (наприклад, електронних щоденників, дистанційного навчання тощо), видані державними органами у сфері освіти та/або наглядовими органами з питань захисту даних. Відповідно до Методичних рекомендацій T-PD(2019)06BISrev5 щодо захисту даних дітей в освітньому середовищі Комітету Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних («Конвенція 108») від 20 листопада 2020 року, обробка персональних даних системами електронного навчання та іншими службами мають здійснюватися на законних підставах відповідно до вимог законодавства[24]. Важливо зазначити, що продукт ІКТ слід оцінювати відповідно до потреб освітнього закладу, беручи до уваги такі аспекти та відповідні ризики:

- чи призначений продукт ІКТ для використання з освітньою метою та для обробки персональних даних дітей;
- яку функцію освітнього процесу підтримуватиме продукт ІКТ і чи розроблений цей продукт способом, який забезпечує обробку для визначеної, чіткої та законної мети (цілей), встановленої навчальним закладом, і чи не здійснюватиметься обробка в подальшому[25] способом, несумісним з цими цілями[26];
- чи надаються відповідні повідомлення про конфіденційність, розроблені чіткою та простою мовою, яку дитина може легко зрозуміти, суб'єктам даних (офлайн і онлайн, на будь-якому пристрої), як дитині, так і законним представникам дитини, перед початком обробки;

24. Посилання: https://rm.coe.int/t-pd-2019-06bisrev2-en-education-guidelines/16809c3c46. Станом на 16 липня 2024 р.
25. Ані постачальником продуктів ІКТ і пов'язаних послуг, ані третіми особами.
26. Реклама, аналітика даних і розроблення продуктів із використанням особистих даних, передавання чи продаж даних брокерам даних вважаються несумісним використанням для обробки в подальшому, яке не має переваги над інтересами, правами та основоположними свободами дитини.

- обробка не повинна охоплювати більше даних, ніж необхідно для досягнення мети обробки (дизайн і налаштування продукту ІКТ мають забезпечувати реалізацію принципу мінімізації даних);
- такі налаштування за замовчуванням, щоб використання продукту ІКТ не порушувало прав суб'єктів даних (принцип захисту даних за замовчуванням вимагає, щоб за замовчуванням персональні дані не були доступні для невизначеної кількості осіб без виконання відповідних дій особою);
- чи потрібна згода на обробку персональних даних, а якщо так — чи відповідатиме вона вимогам щодо добровільності, конкретності, поінформованості та однозначності, встановлених Конвенцією 108+ та GDPR, разом зі згодою дитини та особи, яка виконує батьківські зобов'язання[27]. Наприклад, якщо навчальний заклад вимагає використання продукту ІКТ для дистанційного навчання, згода як підстава для обробки персональних даних неправомірна, бо згода має бути однозначною, надаватися вільно[28], і в ній має бути можливість відмовитися чи відкликати згоду без шкоди для наявних прав суб'єкта даних;
- чи дає змогу продукт ІКТ реалізувати принцип обмеження зберігання даних в часі (зберігати персональні дані протягом визначеного навчальним закладом періоду часу та видаляти їх назавжди);
- чи будуть персональні дані передаватися до третіх країн, які не забезпечують належного рівня захисту (або чи можуть до них дістати доступ органи влади / організації), а якщо так — чи впроваджено відповідні гарантії, зокрема на подальше передавання;
- чи є чітка підзвітність, встановлена в договорі[29], що регулює відносини між навчальним закладом і постачальником продуктів ІКТ та/або постачальниками пов'язаних послуг[30] під час обробки персональних даних;
- які організаційні та технічні заходи вживає постачальник продукту ІКТ для забезпечення належного рівня безпеки, що відповідає ризикові (шифрування тощо).

Ризики, пов'язані з обробкою персональних даних дітей за допомогою продуктів ІКТ, що надають приватні структури, повинні бути ретельно оцінені та мінімізовані, тому перед обробкою[31] рекомендується оцінити вплив на захист даних та оприлюднити результати.

Інформація про освітню діяльність на вебсайтах і 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

27. Якщо для обробки немає іншої законної підстави, слід отримати інформовану та добровільно надану згоду від законного представника на обробку медичних та інших спеціальних категорій даних за умови, що вона відповідає інтересам дитини.
28. Відповідно до Методичних рекомендацій щодо захисту даних дітей в освітньому середовищі Комітету Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних («Конвенція 108»), «діти в освітньому середовищі — типовий приклад ситуації, коли спостерігається дисбаланс між суб'єктом даних і контролером і де слід застосувати іншу правову підставу» (див. примітку 6 на сторінці 5). Посилання: https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b. Станом на 16 липня 2024 року.
29. Важливо зазначити, що договір з постачальником продукту чи послуги ІКТ повинен укладати навчальний заклад, а не сама дитина.
30. Постачальник послуг може виступати як контролер даних (спільний контролер) або обробник даних. Слід зауважити, що кожна роль визначається не лише умовами угоди чи договору, але й характером обробки.
31. З практичних міркувань рекомендується провести оцінювання впливу на захист даних перед початком процедур закупівель.

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 (втрату контролю над подальшим використанням даних невизначеною кількістю невідомих третіх осіб, реалізацію прав суб'єктів даних тощо). З метою захисту персональних даних дітей навчальним закладам можна надати такі рекомендації:

- у виборі каналів зовнішньої комунікації слід віддавати перевагу тим, які повністю контролює навчальний заклад, а не треті особи (наприклад, вебсайтові 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 використання, навчальний заклад повинен дотримуватися рекомендацій щодо використання приватних систем (див. розділ 4);
- 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, зокрема передання 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 ім'я, прізвище 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 надзвичайно важливе, тому, перш ніж запитувати згоду, батькам слід порадити обговорити це зі своїми дітьми. Завжди потрібно враховувати заперечення дитини;
- у разі колективних фотографій, що подають 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 змоги 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 фотознімання);
- 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.

Обробка персональних даних, отриманих під час відеоспостереження

Відеоспостереження все ширше використовується в навчальних закладах. Відеоспостереження належить до засобів контролю, які можуть бути особливо нав'язливими. Здатність технологій відеоспостереження впливати на права та свободи учнів та співробітників означає, що їх встановлення потребує особливої уваги та оцінення. Неможливо порекомендувати якесь 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 разом 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 учителів та інших працівників) на приватне життя, свободу навчання та свободу 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 завдана дітям, які тільки розвивають уявлення про власну свободу, якщо вони з раннього дитинства припускають, що те, що за ними стежать пристрої відеоспостереження, — норма[32]. Вебкамери чи подібні пристрої не можна використовувати для дистанційного спостереження за дітьми під час навчання.

Принцип **мінімізації даних** вимагає, щоб обробка завжди була релевантна, здійснювалася належним способом і обсягом, що не надмірний для її 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 дають змогу обробляти додаткові дані та/або впливати на поведінку дітей, несумісне з вимогами захисту персональних даних.

З метою дотримання **принципу прозорості** діти, їхні законні представники, інші суб'єкти даних повинні бути поінформовані про ведення відеоспостереження та його цілі, особу контролера даних, а також отримати іншу інформацію, передбачену статтею 13(1) та (2) GDPR. Відповідно до Рекомендацій Європейської ради із захисту даних 3/2019 щодо обробки персональних даних за допомогою відеопристроїв, ухвалених 29 січня 2020 року[33], беручи до уваги обсяг інформації, який необхідно надати суб'єктові даних, контролери даних можуть застосовувати багаторівневий підхід. Найважливіша інформація повинна міститися власне на попереджувальному знаку

32. Посилання: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf. Дата звернення: 16 серпня 2024 р.
33. Посилання: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf. Дата звернення: 16 серпня 2024 р.

(перший рівень), а додаткові обов'язкові відомості можуть надаватися іншими способами (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 детальніший 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 телефона, на який можна зателефонувати. Інформація другого рівня також має бути доступною в нецифровому вигляді, у місці, легкодоступному для суб'єкта даних, як-от заповнений інформаційний лист, доступний у центральному місці (наприклад, на інформаційному стенді), 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 ведеться 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**.

Порядок обробки персональних даних засобами відеоспостереження має бути частиною політики захисту персональних даних навчального закладу та містити: визначену, чітку та законну мету відеоспостереження; правові підстави для ведення відеоспостереження; опис покриття системи відеоспостереження із зазначенням територій та приміщень; список тих, хто має доступ до записів з камер відеоспостереження та кому можуть бути надані зображення; інформацію про онлайн-моніторинг і, у разі ведення запису, як довго зберігаються дані; реалізацію прав суб'єктів даних (право доступу тощо); періоди часу, протягом яких буде вестися відеоспостереження; порядок періодичної перевірки необхідності відеоспостереження[34]; порядок видалення даних після закінчення строку зберігання; порядок надання інформації суб'єктам даних (надання інформації на місці тощо) та реалізації інших прав (право доступу тощо); осіб у навчальному закладі, відповідальних за ведення відеоспостереження та порядок отримання доступу до персональних даних; аутсорсинг операцій обробки даних і надання доступу третім особам; порядок ведення реєстру передавання та розкриття даних[35]; заходи безпеки, які використовуються для захисту системи відеоспостереження (використання захищених каналів зв'язку, захист фізичного доступу до диспетчерської, розташування моніторів, система реєстрації, яка дає змогу визначити, хто, де і коли отримував доступ до системи тощо).

34. Мета таких періодичних перевірок — переконатися, що відеоспостереження все ще найкраще рішення для досягнення цілей обробки та розв'язання поставленого завдання.
35. Цей реєстр повинен містити принаймні дату запиту, запитувача, причину запиту та обґрунтування для його задоволення.

РЕКОМЕНДАЦІЇ ЗАКЛАДАМ ОСВІТИ ЩОДО ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ З МЕТОЮ ВЕДЕННЯ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

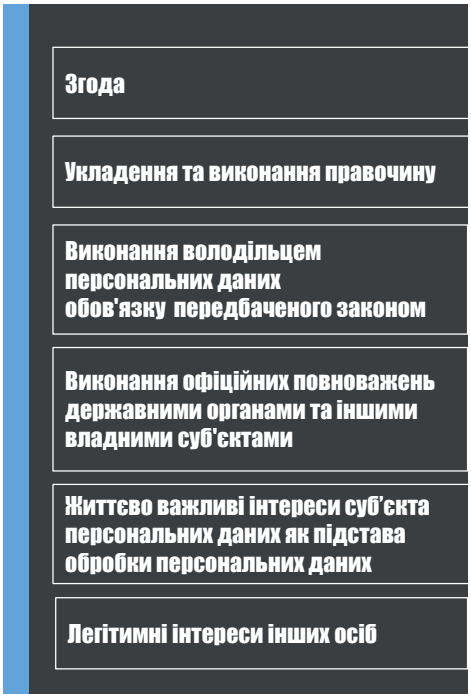
Правові підстави обробки персональних даних з метою ведення освітньої діяльності

Основні вимоги щодо обробки персональних даних визначені в Законі України «Про захист персональних даних».

Один із головних критеріїв законності обробки персональних даних — наявність правових підстав для такої обробки. Підстави - це певні передумови, у разі настання яких, можна обробляти персональні дані.

У статті 11 Законі України «Про захист персональних даних» закріплюється шість підстав для обробки персональних даних.

Правові підстави для обробки персональних даних

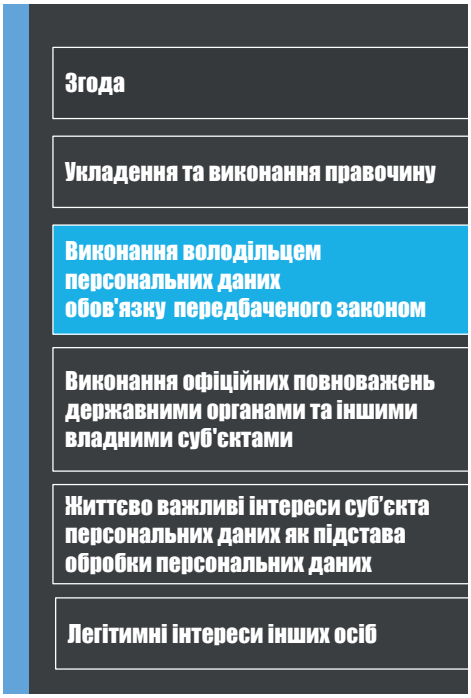


Під час обробки персональних даних заклад освіти та його працівники повинні дотримуватися положень Закону України «Про захист персональних даних».

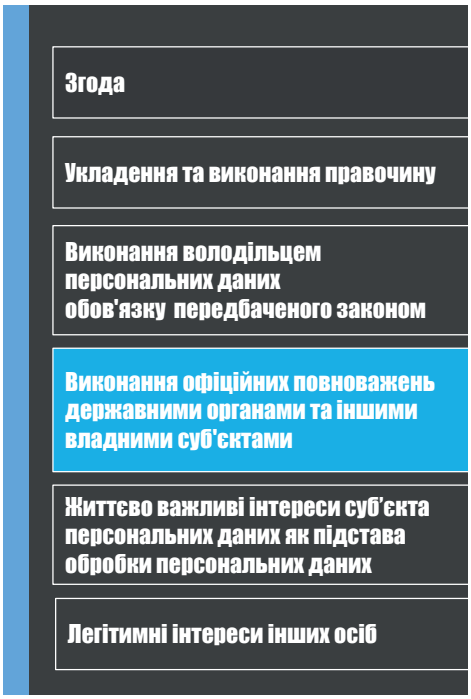
Відповідно до чинного законодавства України державні освітні електронні реєстри, які використовують у своїй діяльності заклади освіти — ЄДЕБО та АІКОМ, обов'язкові для ведення

закладами освіти з метою організації освітніх процесів та забезпечення права на освіту. Обробка персональних даних в ЄДЕБО та АІКОМ здійснюється на підставі пунктів 2 та 5 частини першої статті 11 Закону України «Про захист персональних даних»: пункти 2 та 5 частини першої статті 11 Закону (дозвіл на обробку персональних даних, наданий володільцеві персональних даних відповідно до закону лише для виконання його повноважень та необхідність виконання обов'язку володільця персональних даних, який передбачений законом).

Відповідно до вказаного положення володілець може проводити обробку лише тих персональних даних суб'єктів, які необхідні для виконання ним свого обов'язку, передбаченого законом. При цьому, за загальним правилом, володілець самостійно вирішує, виходячи з покладених на нього обов'язків, чи потребує він для їх здійснення обробки персональних даних суб'єктів.



Якщо володілець має визначені законом повноваження, реалізація яких потребує обробки персональних даних, це вже в контексті вказаного положення Закону достатня підстава для їх обробки. При цьому може бути здійснена обробка лише тих даних, які необхідні для досягнення цілі обробки, тобто виконання конкретних завдань/повноважень. Це положення Закону дозволяє обробляти персональні дані не лише у разі, коли на це є пряма вказівка закону, а й коли це об'єктивно обумовлюється повноваженнями державного органу.



Виконання офіційних повноважень державними органами та іншими владними суб'єктами

У 19 Конституції України зазначається, що посадові особи зобов'язані діяти лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією та законами України. З огляду на це положення органи влади (їх посадові особи) можуть здійснювати обробку персональних даних (будь-яку дію або сукупність дій) лише за наявності наданих повноважень, законної підстави й обґрунтованої мети та у спосіб, передбачений законом.

Тобто, не потрібно отримувати згоду суб'єкта персональних даних у тих випадках, коли збір такої інформації прямо передбачено законом та необхідний для виконання службового обов'язку чи реалізації повноважень.

Заклад загальної середньої освіти може вести облік дітей в освітньому процесі з використанням освітніх ресурсів, ведення яких передбачено законодавством про освіту для надання освітніх послуг, а саме із застосуванням засобів програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту» (далі — АІКОМ), головні завдання якого визначені частиною другою ст. 74[1] Закону України «Про освіту». Частиною третьою та четвертою статті 74[1] Закону України «Про освіту» визначено, що обробка персональних даних у АІКОМ здійснюється відповідно до конкретно визначеної мети, яка обмежується проведенням освітньої діяльності та з дотриманням вимог Закону України «Про захист персональних даних».

Чи можуть заклад освіти та його працівники використовувати згоду як підставу для оброки персональних даних учасників освітнього процесу**?**

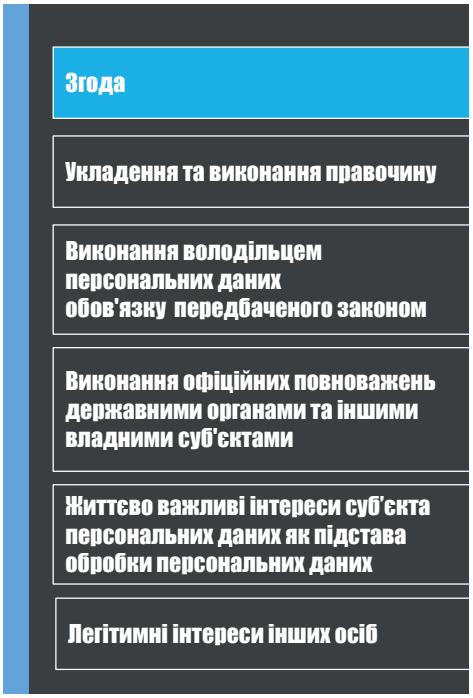
Відповідно до «Керівних принципів — Захист даних дітей в освітньому середовищі»[36] Консультативного комітету Конвенції про захисту осіб у зв'язку з автоматизованою обробкою персональних даних від 20 листопада 2020 року: «Коли школа вимагає використання засобів електронного навчання, згода на обробку персональних даних, надана школою або третьою стороною-розпорядником, не вважатиметься чинною, адже така згода має бути надана однозначно та вільною з можливістю її відкликання без будь-якої шкоди». Як зазначено в пункті 42 Пояснювальної записки до Конвенції №108+, не можна чинити жодного неправомірного впливу або тиску (економічного чи іншого характеру), прямого або непрямого, на суб'єкта даних; і згода не повинна розглядатися як така, що надана вільно, тоді, 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.

У звіті «Захист даних дітей в системах освіти. Виклики та можливі засоби їх розв'язання» Консультативного комітету Конвенції про захисту осіб у зв'язку з автоматизованою обробкою персональних даних від 15 листопада 2019 року[37] зазначається: «Освіта обов'язкова для дітей та молоді. Згода як основний чинник розширення прав і можливостей особи вкрай недосконала та майже ніколи не надається вільно у відносинах між дитиною і дорослим, між родиною і навчальним закладом».

Варто нагадати, що згода лише одна з шести законних підстав для обробки персональних даних відповідно до ЗУ «Про захист персональних даних».

36. https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-ua-f/1680a2addc.
37. https://rm.coe.int/report-children-s-data-protection-in-education-ua-fin/1680a2addb.

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



Згода

Згода повинна володіти трьома невіддільними ознаками:

- добровільність – відсутній прямий чи опосередкований примус при наданні згоди. Згоду суб'єкт може відкликати в будь-який час.

- поінформованість: перед наданням згоди на обробку персональних даних суб'єкт повинен отримати інформацію про те, хто, з якою метою буде обробляти його персональні дані, кому будуть передаватися, які саме дані (склад даних), а також про права, визначені Законом.
Така інформація повинна бути надана в доступному вигляді і володілець повинен за будь-яких умов мати можливість підтвердити факт надання такої інформації суб'єктові;

- форма надання згоди може бути фактично будь-якою. Однозначність згоди не повинна викликати сумнівів і володілець повинен мати змогу підтвердити її наявність упродовж усього часу проведення обробки персональних даних.

Проблема використання згоди на обробку персональних даних в освітньому процесі особливо гостро постає, коли йдеться про обробку персональних даних дітей в сервісах електронних журналів і щоденників, що належать комерційному суб'єктові господарювання чи громадській організації.

Обробка персональних даних в електронний системах та реєстрах без згоди суб'єкта персональних даних можлива у разі, якщо такі системи і реєстри державні та передбачені чинним законодавством, зокрема АІКОМ. У разі використання сторонніх комерційних програм і систем необхідно отримати згоду суб'єкта персональних даних на передання таких даних. Отже, отримання згоди на передання персональних даних здобувача освіти комерційним сервісам обов'язкове.

Без отримання такої згоди використання персональних даних становить порушення чинного законодавства.

У разі, якщо батьки відмовилися від обробки персональних даних дітей в сервісах електронних журналів і щоденників, що належать комерційному суб'єктові господарювання чи громадській організації, заклад освіти має застосовувати традиційні методи для контролю реалізації освітньої програми, фіксації результатів навчальних досягнень учнів, відвідування ними занять, — паперовий журнал.

Якщо обробка персональних даних здійснюється на підставі згоди суб'єкта персональних даних, можлива й реалізація закріпленого статтею 8 Закону України «Про захист персональних даних» права відкликати згоду на обробку персональних даних.

У роз'ясненні освітнього омбудсмена зазначено алгоритм дій закладу освіти у разі, якщо суб'єкт персональних даних відкликає згоду на обробку персональних даних:[38]

- прийняти заяву та зареєструвати її, повідомити батьків про вхідний номер та дату реєстрації;
- видалити персональні дані з таких систем;
- подати письмовий запит до власників таких систем та реєстрів з вимогою видалити персональні дані щодо певного здобувача освіти та батьків;
- отримати письмову відповідь від власників систем та реєстрів, де оброблялися персональні дані учасників освітнього процесу;
- надіслати письмову відповідь батькам, у якій повідомити про видалення персональних даних із систем та реєстрів, які належать комерційним суб'єктам господарювання чи громадським організаціям, і додати письмову відповідь від цих суб'єктів (за наявності).

Отже, слід наголосити, що насамперед обробка персональних даних має відбуватися на законних підставах і відповідно до вимог Закону України «Про захист персональних даних». Якщо заклад освіти не має технічної чи організаційної можливості забезпечити право суб'єкта персональних даних відкликати згоду на обробку персональних даних у разі, коли така обробка ведеться в сервісах електронних журналів і щоденників, що належать комерційному суб'єктові господарювання чи громадській організації — обробка закладом освіти має здійснюватися лише з використанням паперових журналів.

Цифрова трансформація освіти. Захист та обробка персональних даних у державних освітніх електронних інформаційних системах

МОН підготувало проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року, яка представляє комплексне системне стратегічне бачення цифрової трансформації цих сфер. Створення єдиного цифрового середовища, яке об'єднує всіх суб'єктів освітньої та наукової діяльності, що забезпечує простір для комунікації та обміну даними, значно зменшить бюрократичне навантаження системи освіти і науки та спростить управлінські процеси, які відбуваються в них[39].

Проєкт Концепції, який визначає стратегічні напрями цифрового розвитку та цифрової трансформації освіти і науки було презентовано на майданчику Всеукраїнського форуму «Україна 30. Освіта і наука». Стратегія цифрової трансформації освіти і науки націлена на те, щоб створити

38. https://eo.gov.ua/obrobka-personalnykh-danykh-v-elektronnykh-zhurnalakh-ta-shchodennykakh/2023/09/05/.
39. https://www.kmu.gov.ua/news/koncepciya-cifrovoyi-transformaciyi-osviti-i-nauki-mon-zaproshuye-do-gromadskogo-obgovorennya.

єдину освітню екосистему, яка допоможе здобувачам освіти та педагогічним працівникам розвиватись, опановувати цифрові компетентності й мати постійний доступ до якісного цифрового контенту[40].

Для ефективного формування та реалізації державної політики у сфері освіти і науки, ухвалення управлінських рішень будь-якого рівня необхідна аналітична, статистична інформація. Тому функціонування цілісної системи збору, обробки та передавання інформації — необхідна основа системного підходу до розв'язання проблем та поставлення завдань. Брак інтероперабельності державних реєстрів у сфері освіти і науки, інструментів обліку дітей на місцях призводить до дублювання даних, неефективного використання кадрових ресурсів, унеможливлення обміну даними між різними базами, зайвої бюрократизації процесів. Тож невірогідність даних у державних реєстрах унеможливлює прогнозування результатів та оцінювання ризиків впроваджуваних політик. Тому цифрова трансформація освіти і науки передбачає, зокрема, трансформацію процесів збору, обробки та передавання інформації, а також доступу до актуальних статистичних даних для всіх заінтересованих сторін[41].

Перед тим як безпосередньо розглянути питання захисту та обробки персональних даних в освітніх інформаційно-аналітичних системах Автоматизований інформаційний комплекс освітнього менеджменту (АІКОМ) та Єдина державна електронна база з питань освіти (ЄДЕБО), важливо проаналізувати загальні принципи функціонування інформаційних систем, передбачених Керівними принципами щодо реєстрації населення ОБСЄ/БДІПЛ (2009) та Посібником ЮНСІТРАЛ з основних принципів ділового реєстру.

40. https://nrat.ukrintei.ua/proyekt-strategiyi-czyfrovoyi-transformacziyi-osvity-i-nauky/.
41. https://www.kmu.gov.ua/news/koncepciya-cifrovoyi-transformaciyi-osviti-i-nauki-mon-zaproshuye-do-gromadskogo-obgovorennya.

Релевантність даних

Один з ключових елементів, про який слід пам'ятати, визначаючи, яку інформацію потрібно фіксувати, — це простота оновлення такої інформації. Для досягнення максимальної ефективності реєстр повинен містити мінімальну кількість інформації, необхідної для виконання своєї функції в суспільстві, для якого він працює (адже що більше зібраної інформації, то більше завдання щодо актуалізації такої інформації). Кожна установа, відповідальна за реєстрацію конкретної інформації, повинна забезпечити регулярне та своєчасне оновлення даних, а також їх правильність і повноту. Після внесення до національного реєстру нещодавно оновлена інформація одразу стає доступною для всіх користувачів системи, які мають право переглядати дані.

Якщо дані хибні або неповні, від відповідних органів слід вимагати виправлення та заповнення даних після отримання заяви про це від суб'єкта даних. У разі зберігання даних, які більше не потрібні для мети, для якої вони були спочатку зібрані, або дані були отримані незаконно, їх слід видалити. Реєстр може бути ефективним лише в тому разі, якщо він зберігає кількість даних, не більшу за необхідну для виконання законних цілей реєстру.

Конфіденційність

Суб'єкти даних повинні бути впевнені, що їхня особиста інформація — повністю або частково — буде використовуватися лише для цілей, передбачених законом, і без розкриття їхньої особи. Дані слід використовувати лише відповідно до мети, для якої вони були зібрані спочатку. Цей фундаментальний принцип також повинен застосовуватися, коли особисті дані передають або обмінюють державні органи. Отже, передавання даних повинно регулюватися відповідно до галузевих компетенцій та принципу розподілу обов'язків. Кожне передання даних з одного реєстру в інший сектор повинно регулюватися, виходячи з мети передання, одержувача та категорій даних, які підлягають переданню.

Основні заходи захисту даних охоплюють контроль як фізичного, так і віртуального доступу, автентифікації та авторизації, регулювання протоколів входу в систему, контроль за будь-якими завданнями, що передаються на виконання третім особам, та контроль розкриття інформації за допомогою таких технологій, як шифрування даних. Коротше кажучи, слід розглянути питання забезпечення гарантій того, що:

- вжито заходів щодо захисту даних;
- обробка даних законна;
- забезпечено безпеку даних.

Надійні адміністративні процедури, що регулюють процес

Щоб ефективно запустити систему реєстрації, необхідно розробити детальні процедури та правила, що регулюють процес реєстрації, орієнтований на послуги. Якщо зібрана інформація зберігається в електронному форматі і потім розподіляється між різними системами та реєстрами, слід звертати увагу не лише на відповідні адміністративні процедури, а й на стандарти даних та засоби електронного передавання.

Обмін інформацією, сумісність та доступність

Керування системою реєстрації вимагає створення ефективних механізмів обміну даними, а також точної координації між установами, відповідальними за реєстрацію. Коли держава

запроваджує взаємодію між різними органами влади, вона повинна вирішувати, як органи державної влади можуть обмінюватися захищеними даними, що стосуються фізичних осіб та підприємств, щоб не порушити права власників даних. Отже, держави повинні гарантувати, що обмін інформацією між органами державної влади відбувається відповідно до чинного законодавства, яке повинно встановлювати умови, за яких такий обмін дозволений[42].

Перевага даних над паперовими документами

У разі незгоди дані, які можна перевірити в реєстрі, мають перевагу над паперовими документами. Потрібно виходити з того, що правдивість даних у реєстрі гарантує держава.

Захист та обробка персональних даних у державних освітніх електронних інформаційних системах

1. Єдина державна електронна база з питань освіти (ЄДЕБО) — це автоматизована система збирання, обробки, зберігання та захисту інформації щодо здобувачів освіти, суб'єктів освітньої діяльності, яку формують (створюють) і використовують для забезпечення потреб фізичних і юридичних осіб. Вона входить до освітньої інфраструктури освіти та зазначена в статті 74 Закону України «Про освіту».

2. Автоматизований інформаційний комплекс освітнього менеджменту (АІКОМ) — це державна інформаційно-аналітична система, яку використовують суб'єкти освітньої діяльності для ефективного керування закладами освіти (крім закладів вищої освіти). Комплекс входить до освітньої інфраструктури освіти і визначений у статті 74-1 Закону України «Про освіту». Власник АІКОМ — Міністерство освіти і науки України, а технічний адміністратор — державна наукова установа «Інститут освітньої аналітики», що належить до сфери керування МОН.

3. Інші сервіси електронних журналів належать комерційним суб'єктам господарювання чи громадським організаціям.

Надалі спробуємо дати відповіді на найпоширеніші питання, які стосуються захисту та обробки персональних даних в ЄДЕБО та АІКОМ.

Чи АІКОМ обов'язковий для використання під час освітнього процесу в закладах освіти?

Частиною першою ст. 74[1] Закону України «Про освіту» визначено, що з метою забезпечення належної цифрової взаємодії в системі освіти між органами державної влади, органами місцевого самоврядування, закладами та установами освіти, їхніми структурними підрозділами, учасниками освітнього процесу та іншими юридичними і фізичними особами в Україні функціонує Автоматизований інформаційний комплекс освітнього менеджменту (далі — АІКОМ).

Абзацом четвертим частини другої ст. 74[1] Закону України «Про освіту» одне із завдань АІКОМ — забезпечення ведення в електронній формі ділової документації та подання звітності закладами освіти, ведення обліку дітей дошкільного та шкільного віку (зокрема дітей, не охоплених навчанням), учасників освітнього процесу та суб'єктів освітньої діяльності.

Постановою Кабінету Міністрів України від 05 вересня 2023 р. № 985 «Про внесення змін до постанови Кабінету Міністрів України від 13 вересня 2017 р. № 684» затверджено Порядок ведення обліку дітей дошкільного, шкільного віку, вихованців та учнів, який застосовуватиметься з 1

42. Посібник ЮНСІТРАЛ з основних принципів ділового реєстру.

липня 2024 року. Зокрема, правовими нормами цього документа передбачено, що облік ведеться за допомогою АІКОМ.

Чи є електронна інформаційна взаємодія між ЄДБЕО та АІКОМ; чи можуть бути внесені персональні дані вступників до закладів освіти / здобувачів освіти до ЄДБЕО для отримання документа про освіту без використання АІКОМ?

Відповідно до статті 74 Закону України «Про освіту» ЄДЕБО в порядку електронної взаємодії може обмінюватися інформацією з іншими юридичними особами обсягом та у випадках, визначених законом.

Підпунктом 4 пункту 5 Положення про програмно-апаратний комплекс «Автоматизований інформаційний комплекс освітнього менеджменту», затвердженого постановою Кабінету Міністрів України від 02.12.2021 № 1255, визначено, що функціональні можливості АІКОМ — забезпечення взаємодії центральної бази даних зі сторонніми інформаційними системами та державними електронними інформаційними ресурсами, зокрема з Єдиною державною електронною базою з питань освіти.

Обмін інформацією між АІКОМ та ЄДЕБО здійснюється, зокрема, через відкритий програмний інтерфейс та/або систему електронної взаємодії державних електронних інформаційних ресурсів, усі складові частини якої мають комплексну систему захисту інформації з підтвердженою відповідністю до Закону України «Про захист персональних даних».

На сьогодні з використанням ЄДЕБО серед документів ЗЗСО виготовляють тільки документи про початкову освіту. Для їх виготовлення в базу вносять інформацію про осіб, які завершують здобуття початкової освіти. Зважаючи на те, що в АІКОМ ведеться облік здобувачів загальної середньої освіти, триває робота, щоб замовлення на документи про базову середню та повну загальну середню освіту для осіб, які здобувають її в ЗЗСО, формувалося в АІКОМ та передавалося в ЄДЕБО.

Чи мають доступ до ЄДЕБО як користувачі володільці / користувачі електронних інформаційних систем приватних суб'єктів господарювання, під'єднаних до АІКОМ?

Володільці та користувачі електронних інформаційних систем приватних суб'єктів господарювання не мають доступу до ЄДЕБО. Доступ до даних в ЄДЕБО надається лише уповноваженим органам та особам відповідно до чинного законодавства.

Чи може заклад освіти вести одночасно класні журнали в паперовій та електронній формах у разі запровадження ведення ділової документації закладу освіти в електронній формі?

Заклад загальної середньої освіти може вести облік дітей в освітньому процесі з використанням освітніх ресурсів, ведення яких передбачено законодавством про освіту для надання освітніх послуг.

Відповідно до частини четвертої статті 38 Закону України «Про повну загальну середню освіту», організація освітнього процесу та діяльності закладу загальної середньої освіти загалом належить до повноважень його керівника. Отже, у рамках своєї автономії, заклади загальної середньої освіти можуть самостійно розв'язувати питання щодо використання онлайн-інструментів для цифровізації процесу управління загальною середньою освітою, обирати інформаційно-комунікаційні системи та ухвалювати рішення щодо переходу до ведення документації в електронній формі, зокрема до ведення електронних класних журналів.

Наказом МОН від 8 серпня 2022 року № 707, зареєстрованим у Міністерстві юстиції України 9 вересня 2022 за №1029/38365, затверджено Інструкцію з ведення ділової документації у закладах загальної середньої освіти в електронній формі, яка дозволяє закладам загальної середньої освіти вести електронні журнали замість паперових, а також інші документи закладу освіти в електронній формі.

Якщо батьки відмовилися від обробки персональних даних дітей в сервісах електронних журналів та щоденників, що належать комерційному суб'єктові господарювання чи громадській організації, заклад освіти має застосовувати традиційні методи для контролю реалізації освітньої програми, фіксації результатів навчальних досягнень учнів, відвідування ними занять, тобто паперовий журнал.

Облік дітей дошкільного та шкільного віку, вихованців та учнів

Облік ведеться з використанням програмно-апаратного комплексу «Автоматизований інформаційний комплекс освітнього менеджменту» шляхом внесення, накопичення, актуалізації, обробки, ведення аналізу та узагальнення інформації про дітей дошкільного та шкільного віку, вихованців і учнів, зокрема дітей, не охоплених навчанням[43].

Облік ведуть відповідальні працівники, яким доступ до автоматизованого комплексу менеджменту надав технічний адміністратор зазначеного комплексу.

Для ведення обліку в автоматизованому комплексі менеджменту опрацьовується профіль дитини, що містить інформацію про її:

- прізвище, власне ім'я та по батькові (за наявності);
- дату і місце народження;
- свідоцтво про народження (серію та номер);
- задекларованe / зареєстроване або фактичне місце проживання (перебування);
- громадянство, документ, що посвідчує особу та підтверджує громадянство України (за наявності);
- документ, що посвідчує спеціальний статус дитини, зокрема довідка про взяття на облік внутрішньо переміщеної особи, довідка про звернення по захист в Україні, посвідчення біженця (серія та номер) (за наявності);
- унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності);
- податковий номер (реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб — платників податків) (за наявності);
- місце, форму здобуття освіти (заклад освіти чи сім'я (у разі здобуття освіти за сімейною формою) та рік навчання (клас (група)).

Проблемне питання наразі — облік дітей, що перебувають за кордоном

Міністерство з питань реінтеграції тимчасово окупованих територій України розглядає можливість запровадження єдиного електронного обліку для ведення особових справ учнів[44].

43. https://zakon.rada.gov.ua/laws/show/684-2017-%D0%BF#Text.
44. https://sud.ua/uk/news/ukraine/297854-v-kabmine-rassmatrivayut-vvedenie-elektronnogo-reestra-ukrainskikh-shkolnikov-za-granitsey.

В аспекті всіх заходів із запровадження єдиного електронного обліку для ведення особових справ учнів важливе є питання забезпечення за замовчуванням обробки персональних даних способом, який гарантує особам захист прав, якими вони наділені відповідно до Закону України «Про захист персональних даних».

По суті, при запровадженні єдиного електронного обліку для ведення особових справ учнів вимагається:

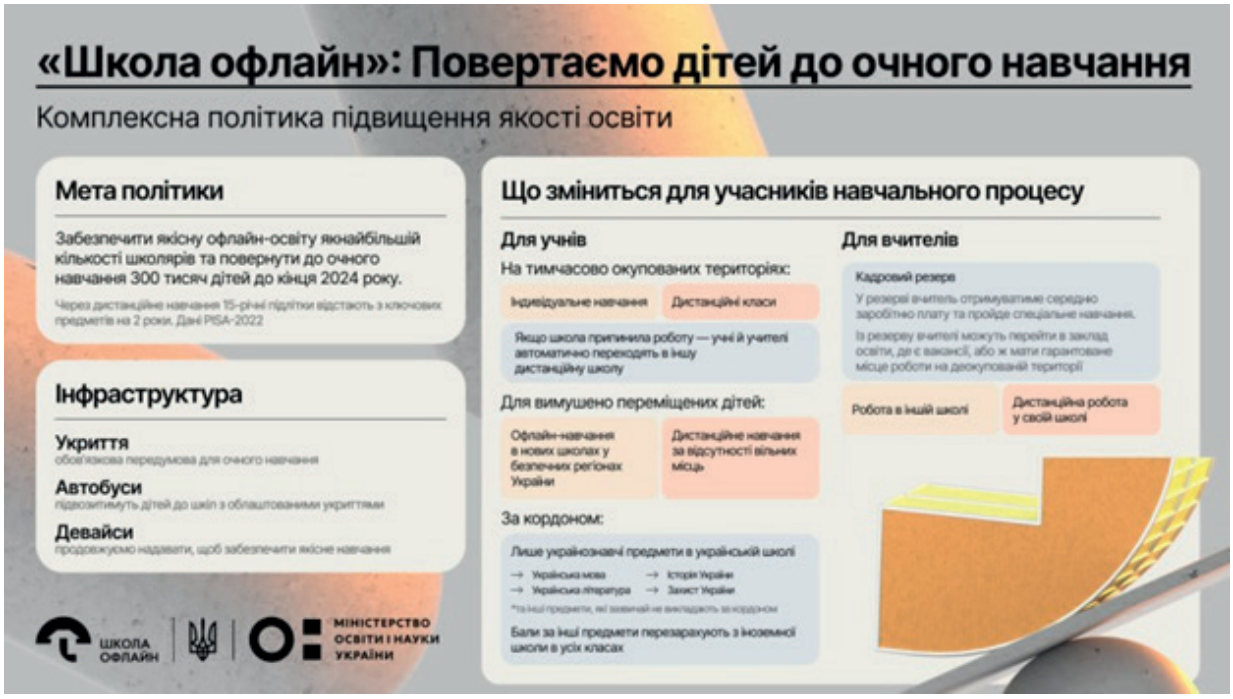
(а) у визначенні способу обробки даних і під час самої обробки вживати належних технічних і організаційних заходів (напр., псевдонімізацію) з метою забезпечення наявності необхідних запобіжників у передаванні даних; та

(б) вживати належних технічних і організаційних заходів для забезпечення за замовчуванням обробки лише тих персональних даних, які необхідні для досягнення певної мети.

Обробка та захист персональних даних під час дистанційного навчання дітей, які перебувають на тимчасово окупованих територіях

За даними Міністерства освіти та науки України, сьогодні майже 600 000 дітей здобувають освіту дистанційно в Україні, ще понад 390 000 — це ті діти, які перебувають за кордоном, але продовжують навчатися в українських школах дистанційно. Тож критично важливо покращити якість онлайн-навчання та адаптуватися під потреби кожної категорії дітей[45].

Міністерство освіти і науки оприлюднило план політики «Школа офлайн», за допомогою якого до очного навчання планують повернути 300 тисяч дітей[46].



У цьому контексті важливе питання організації навчання дітей, які проживають на перебувають на тимчасово окупованих територіях.

45. https://offlineschool.mon.gov.ua/#about.
46. https://mon.gov.ua/news/shkola-oflain-iak-derzhava-planuie-povernuty-300-tysiach-ditei-do-ochnoho-navchannia.

Для дітей, які перебувають на тимчасово окупованих територіях, вводять нові формати навчання. Зокрема, індивідуальний план навчання (педагогічний патронаж) або ж подальше навчання в дистанційному класі своєї школи, якщо безпекова ситуація дає змогу відвідувати заняття. Або ж разом з учителем перейти до іншого класу, якщо їхня школа тимчасово припиняє роботу. Для цього батьки мають написати заяву[47].

Наразі перед МОН постає завдання виробити чіткий та безпечний алгоритм дій для можливості дистанційного навчання дітей, які перебувають на тимчасово окупованих територіях при цьому впроваджуючи належні технічні та організаційні заходи для забезпечення пропорційності рівня захисту персональних даних наявним ризикам, забезпечуючи конфіденційність систем обробки персональних даних і застосування процедур з регулярної перевірки ефективності цих заходів.

47. https://mon.gov.ua/news/shkola-oflain-iak-derzhava-planuie-povernuty-300-tysiach-ditei-do-ochnoho-navchannia.

ВИСНОВКИ

1. Визначення правових підстав для обробки персональних даних з метою ведення освітньої діяльності

Обробка персональних даних в ЄДЕБО та АІКОМ здійснюється на підставі пунктів 2 та 5 частини першої статті 11 Закону України «Про захист персональних даних». У разі використання сторонніх комерційних програм і систем необхідно отримати згоду суб'єкта персональних даних на передавання таких даних. Таким чином отримання згоди на передавання персональних даних здобувача освіти комерційним сервісам є обов'язковою. Без отримання такої згоди використання персональних даних — порушення чинного законодавства.

Якщо заклад освіти не має технічної чи організаційної можливості забезпечити право суб'єкта персональних даних відкликати згоду на обробку персональних даних у разі, коли така обробка ведеться в сервісах електронних журналів і щоденників, що належать комерційному суб'єктові господарювання чи громадській організації, то обробка закладом освіти має здійснюватися з використанням паперових журналів.

2. Використання приватних інформаційних систем, різних додатків, електронних журналів і щоденників в освіті

Відкритим залишається питання обробки персональних даних під час використання електронних платформ для навчання комерційними суб'єктами господарювання чи громадськими організаціями, коли батьки або законні представники дитини відмовляються надавати дозвіл на внесення і обробку даних здобувачів освіти до відповідних систем та платформ.

Якщо батьки відмовилися від обробки персональних даних дітей в сервісах електронних журналів і щоденників, що належать комерційному суб'єктові господарювання чи громадській організації, заклад освіти має застосовувати традиційні методи для контролю реалізації освітньої програми, фіксації результатів навчальних досягнень учнів, відвідування ними занять, — паперовий журнал.

Використання сторонніх сервісів для забезпечення освітнього процесу без належної взаємної інтеграції та юридичних гарантій щодо захисту персональних даних може створювати ризики як для забезпечення конфіденційності даних, так і надмірного дублювання персональних даних.

3. Оперативна сумісність державних реєстрів у сфері освіти

Обробка персональних даних у державних реєстрах має здійснюватися з дотриманням принципів захисту персональних даних. Оперативна сумісність інформаційних систем — ключовий елемент їхнього функціонування. Інформаційні системи обмінюються між собою даними, необхідними для функціонування та виконання функцій суб'єктів, встановлених нормативно-правовими актами, через інтегровані інтерфейси, розроблені для забезпечення взаємодії. Законні підстави

такої взаємодії визначені в нормативних актах, що регулюють роботу таких інформаційних систем, а сама взаємодія підтримується відповідно до порядку та умов, встановлених у таких нормативних актах, шляхом передавання та постійного оновлення даних, що обробляються в інформаційних системах, через електронні комунікаційні мережі.

4. Обробка та захист персональних даних на тимчасово окупованих територіях під час доступу до української освіти

Для дітей, які перебувають на тимчасово окупованих територіях, вводять нові формати навчання. Зокрема, індивідуальний план навчання (педагогічний патронаж) або ж подальше навчання в дистанційному класі своєї школи, якщо безпекова ситуація дає змогу відвідувати заняття. Або ж разом з учителем перейти до іншого класу, якщо їхня школа тимчасово припиняє роботу. Для цього батьки мають написати заяву.

Наразі перед МОН постає завдання виробити чіткий та безпечний алгоритм дій для можливості дистанційного навчання дітей, які перебувають на тимчасово окупованих територіях, при цьому впроваджуючи належні технічні та організаційні заходи для забезпечення пропорційності рівня захисту персональних даних наявним ризикам, забезпечуючи конфіденційність систем обробки персональних даних і застосування процедур з регулярної перевірки ефективності цих заходів.

5. Висвітлення інформації про освітню діяльність на вебсайтах та в соціальних мережах закладу освіти

Навчальні заклади повинні пам'ятати, що розповсюдження зображень, відеозаписів і 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). Також варто звернути увагу на рекомендації наведені у відповідному розділі цього аналізу.

6. Збереження та використання персональних даних, отриманих 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 разом з іншими заходами, які слід також застосовувати. 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 обробленням рекомендується провести оцінювання впливу на захист даних. Порядок обробки персональних даних засобами відеоспостереження має бути частиною політики захисту даних навчального закладу.

7. Облік дітей, що перебувають за кордоном

Міністерство з питань реінтеграції тимчасово окупованих територій України наразі розглядає можливість запровадження єдиного електронного обліку для ведення особових справ учнів.

В аспекті всіх заходів із запровадження єдиного електронного обліку для ведення особових справ учнів важливим є забезпечення за замовчуванням обробки персональних даних способом, який

гарантує особам захист прав, якими вони наділені на підставі Закону України «Про захист персональних даних».

По суті, при запровадженні єдиного електронного обліку для ведення особових справ учнів вимагається:

(а) у визначенні способу обробки даних і під час самої обробки вживати належних технічних і організаційних заходів (напр., псевдонімізацію) з метою забезпечення наявності необхідних запобіжників у передаванні даних; та

(б) вживати належних технічних і організаційних заходів для забезпечення за замовчуванням обробки лише тих персональних даних, які необхідні для досягнення певної мети.

8. Підвищення рівня професійного підготування працівників закладів освіти

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

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

9. Розробка та впровадження внутрішніх документів навчальних закладів

Важлива частина процесу обробки персональних даних у навчальних закладах — 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 вони — один з елементів принципу підзвітності, що дає змогу продемонструвати відповідність до застосовних правових вимог. 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.

Діана ШИНКУНЄНЕ — випускниця факультету права Вільнюського університету 2000 року. З лютого 2023 року обіймає посаду Директора інспекції із захисту персональних даних Литовської республіки. З 2001 по 2018 роки вона була заступником директора Державної інспекції із захисту персональних даних Литовської Республіки. У 2017–2018 роках вона брала участь у підготуванні до здійснення на державному рівні реформи у сфері захисту персональних даних у Європейському Союзі — була керівником робочої групи, відповідальної за підготування змін до Закону про захист персональних даних у контексті Регламенту (ЄС) 2016/679. Діана Шинкунєне активно залучена до заходів, спрямованих на посилення інституційних спроможностей наглядових органів у сфері захисту персональних даних. Викладає курс з технологій конфіденційності та безпеки в Університеті Миколаса Ромеріса (Вільнюс, Литва).

Олександр ШЕВЧУК — випускник факультету міжнародного права Інституту міжнародних відносин Київського Національного університету імені Тараса Шевченка 2015 року. З 2016 по 2019 роки обіймав посаду експерта з наближення законодавства в рамках проєкту ЄС «Підтримка впровадження Угоди про асоціацію між Україною та ЄС». Виконував обов'язки в Урядовому офісі координації європейської та євроатлантичної інтеграції, де, зокрема, відповідав за порівняльний аналіз законодавства України та ЄС. У 2019 році здобув ступінь кандидата юридичних наук, захистивши дисертацію на тему «Правове регулювання охорони персональних даних в Європейському Союзі». У 2019–2020 роках обіймав посаду національного експерта з електронного правосуддя за напрямком удосконалення захисту персональних даних у рамках проєкту ЄС «Право-Justice». Наразі він національний консультант у сфері захисту персональних даних у рамках спільного проєкту ЄС та Ради Європи з посилення спроможностей Омбудсмана для захисту прав людини. У 2019–2021 роках брав участь у підготуванні реформи системи захисту персональних даних в Україні. Входить до складу робочої групи з реформування національного законодавства у сфері обробки і захисту персональних даних. Олександр Шевчук — один з авторів проєкту закону «Про захист персональних даних» та проєкту закону «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації».

UKR

www.coe.int

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 46 держав-членів, включно з усіма державами — членами Європейського Союзу. Усі держави — члени Ради Європи приєдналися до Європейської конвенції з прав людини — договору, спрямованому на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE