Project number	101085612
Project name	Data Protection in the EU
Funding Programme	ERASMUS2027
Project start date	01-10-2022

Deliverable number	1.5
Deliverable name	Teaching materials for the module “Data Protection: implementation of European Experience” (for Ph.D. in Computer Science)
Work Package number	1
Lead Beneficiary	Lviv Polytechnic National University
Type	DEM — Demonstrator, pilot, prototype R — Document, report
Dissemination level	Public
Due date (in months)	3
Description	The use cases for discovering designing of information systems, accordingly to a legal framework of EU by collaborative learning group should be created using the software for interactive cooperation. E- format, Ukrainian language
Website link	https://datapro.org.ua/portfolio-item/dataproeu_data_protection_phd/
Author(s)	Anastasiya Doroshenko

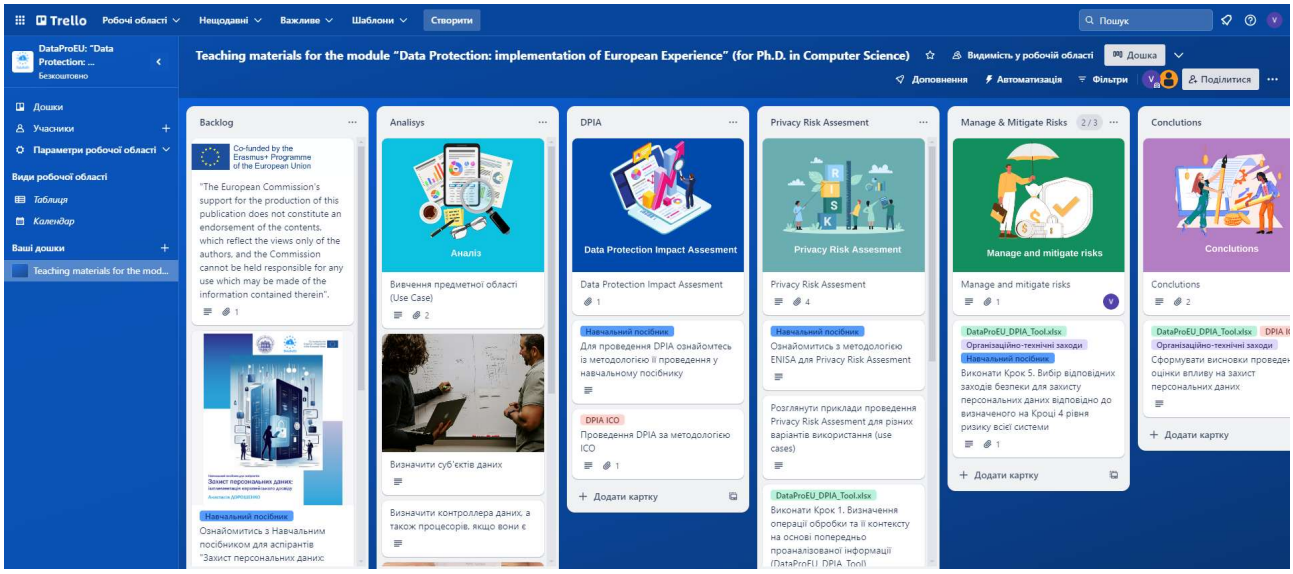
Teaching materials for the module “Data Protection: implementation of European Experience” (for Ph.D. in Computer Science)

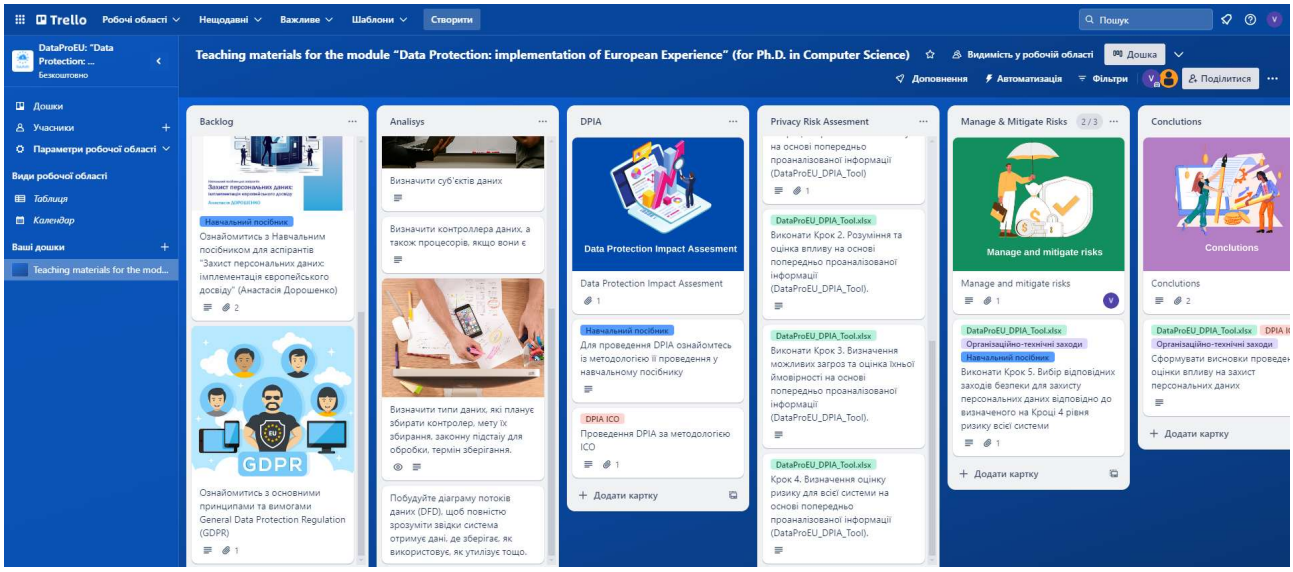
Teaching materials for the module “Data Protection: implementation of European Experience” (for Ph.D. in Computer Science) consist of 3 parts:

1. The tutorial, which highlights the current problem of assessing the risks of personal data loss in various subject areas in compliance with the requirements of modern European legislation. The legal basis for processing personal data, in particular the provisions of the EU General Data Protection Regulation (Regulation (EU) 2016/679 General Data Protection Regulation, GDPR) is considered in detail.
   The advantage of the developed manual is that it contains examples of risk assessment of personal data loss in information systems and shows examples of its use for specific use cases.

2. The second component of the developed learning materials is an interactive collaboration tool developed using Trello. (https://trello.com/b/v0scFz8u/teaching-materials-for-the-module-data-protection-implementation-of-european-experience-for-phd-in-computer-science)
   This tool allows postgraduate students to form groups and work together on the task of assessing the risk of personal data leakage for a specific subject area and a specific use case in accordance with the EU legal framework.

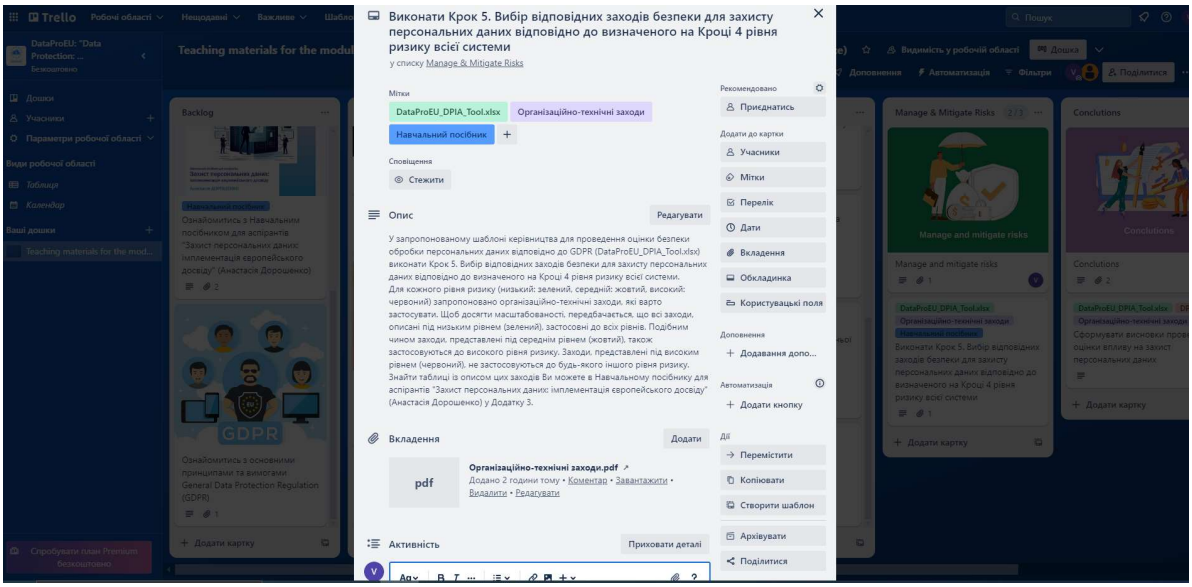
   This tool not only allows you to visualize the risk assessment process in accordance with the methodology developed in this course, but also to assign responsibility for each task, track progress and set deadlines.



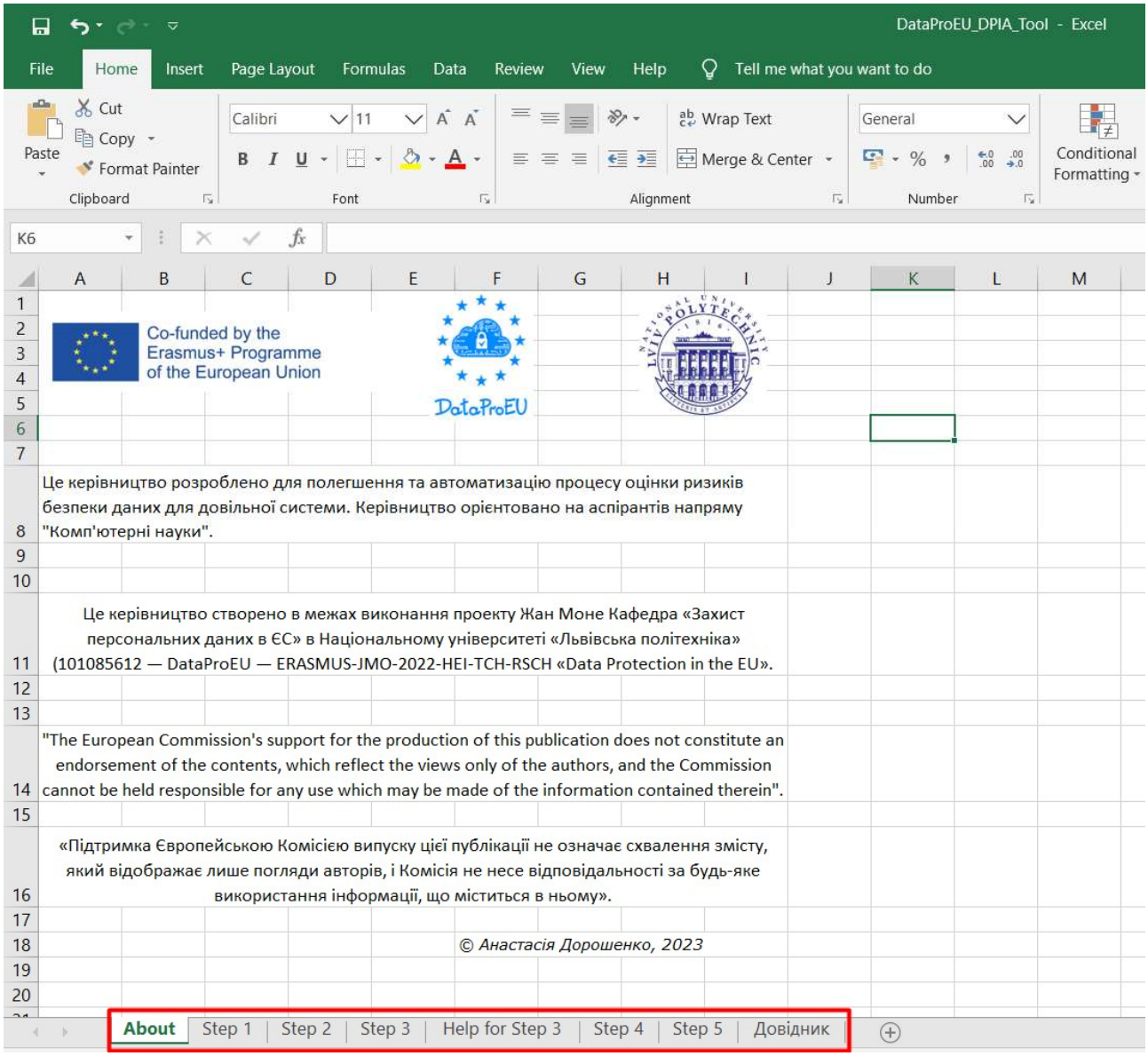


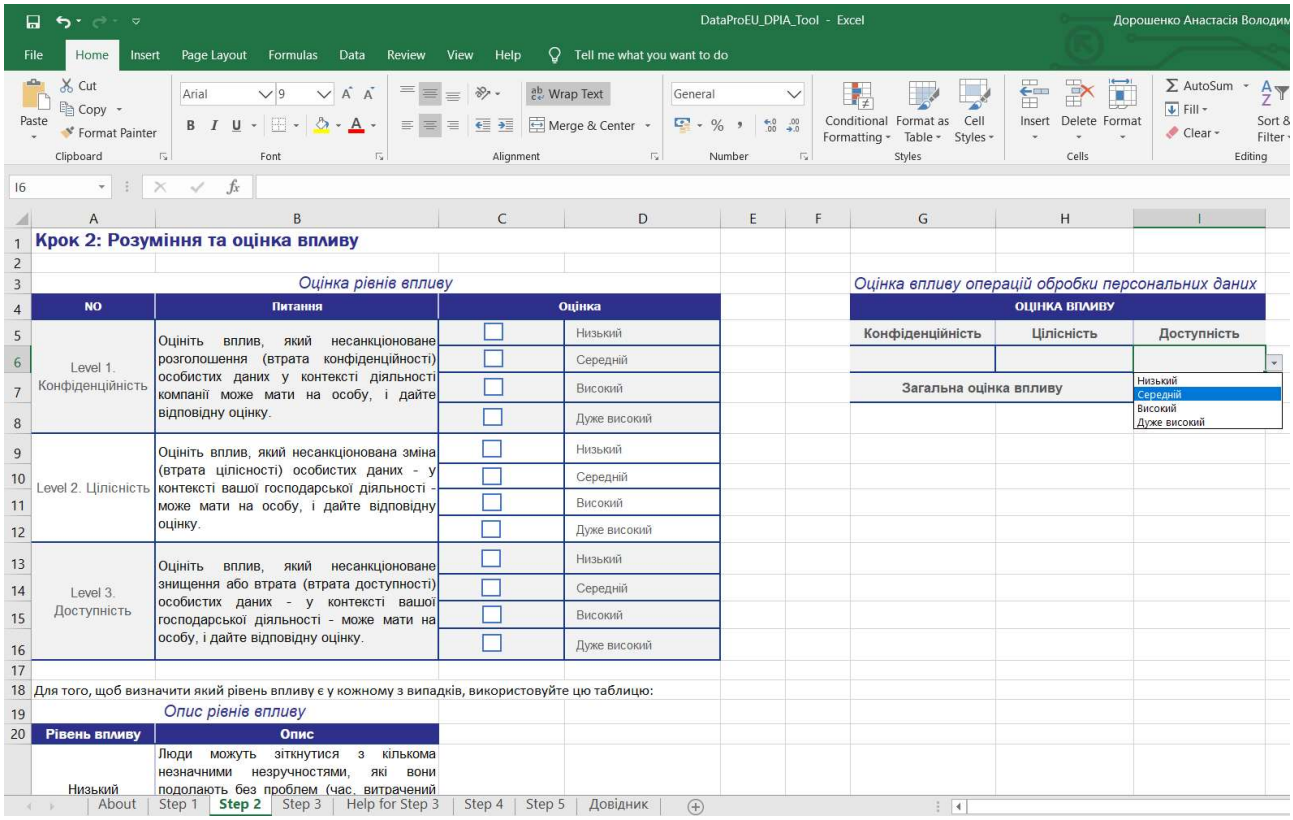
It is also very convenient to be able to store all the necessary work and training materials directly in the project, which greatly facilitates not only the work of the team, but also the teacher's check of the completed assignment.

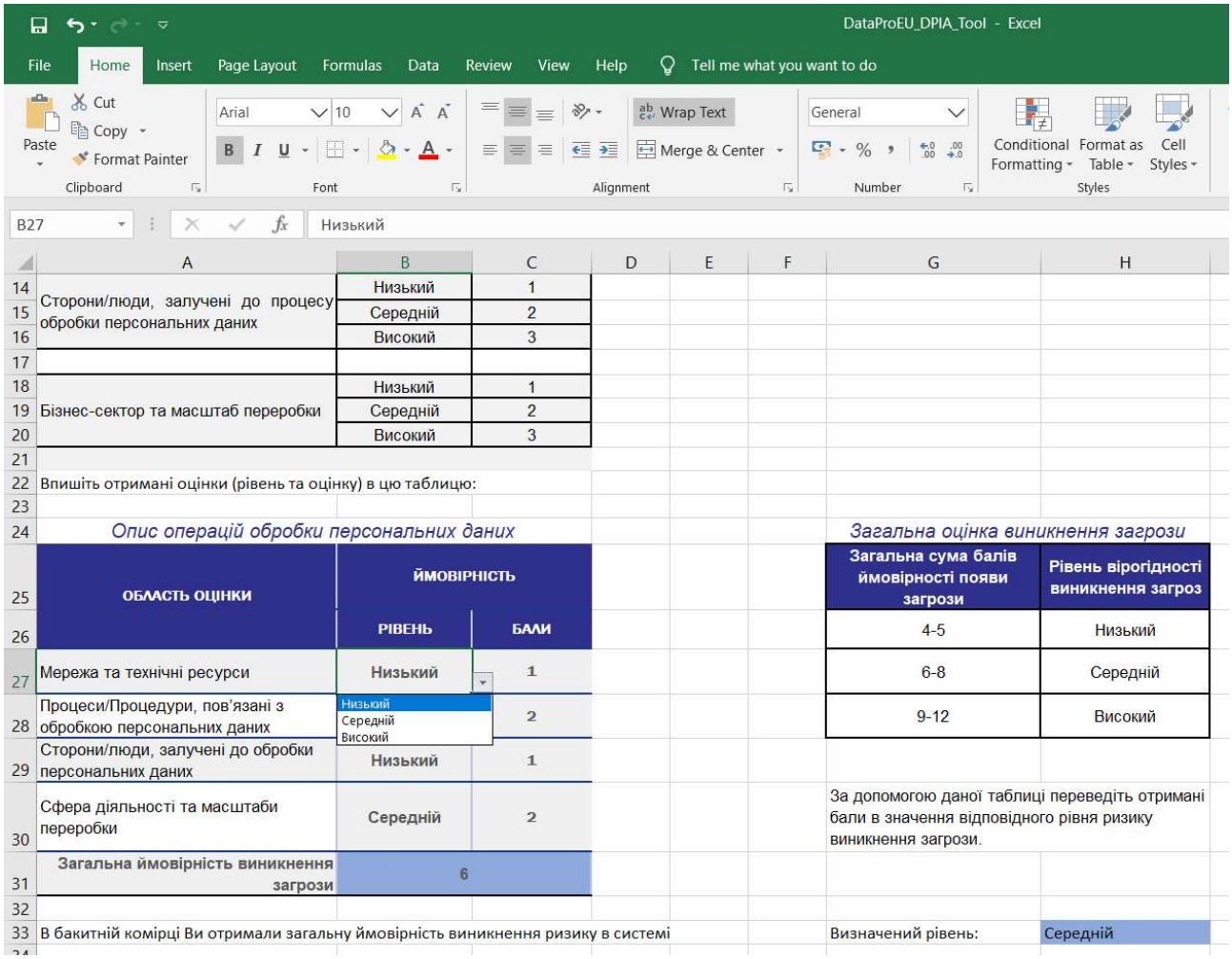
The ability to leave a comment for each step is very useful for the learning process. Accordingly, the teacher can leave a comment or recommendation for each of the completed tasks.

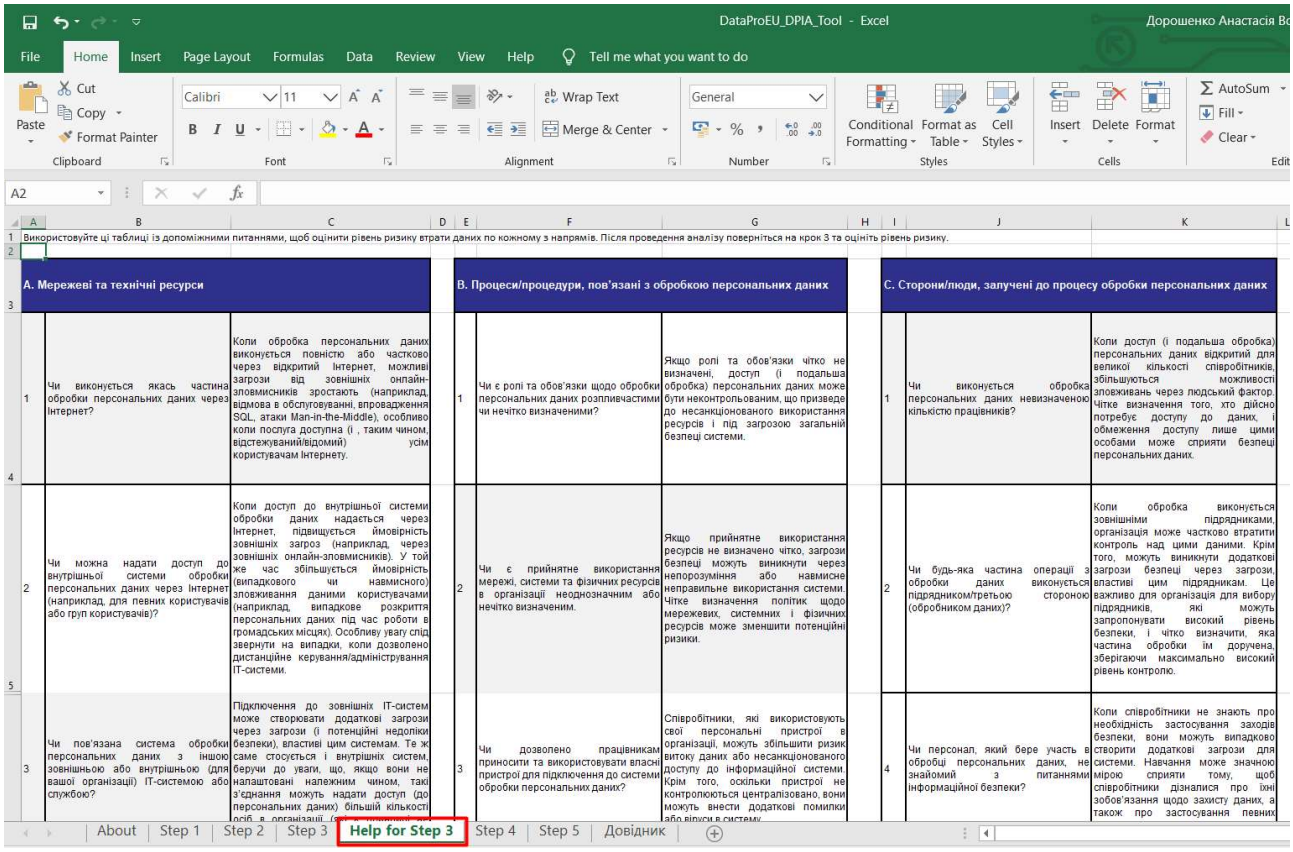


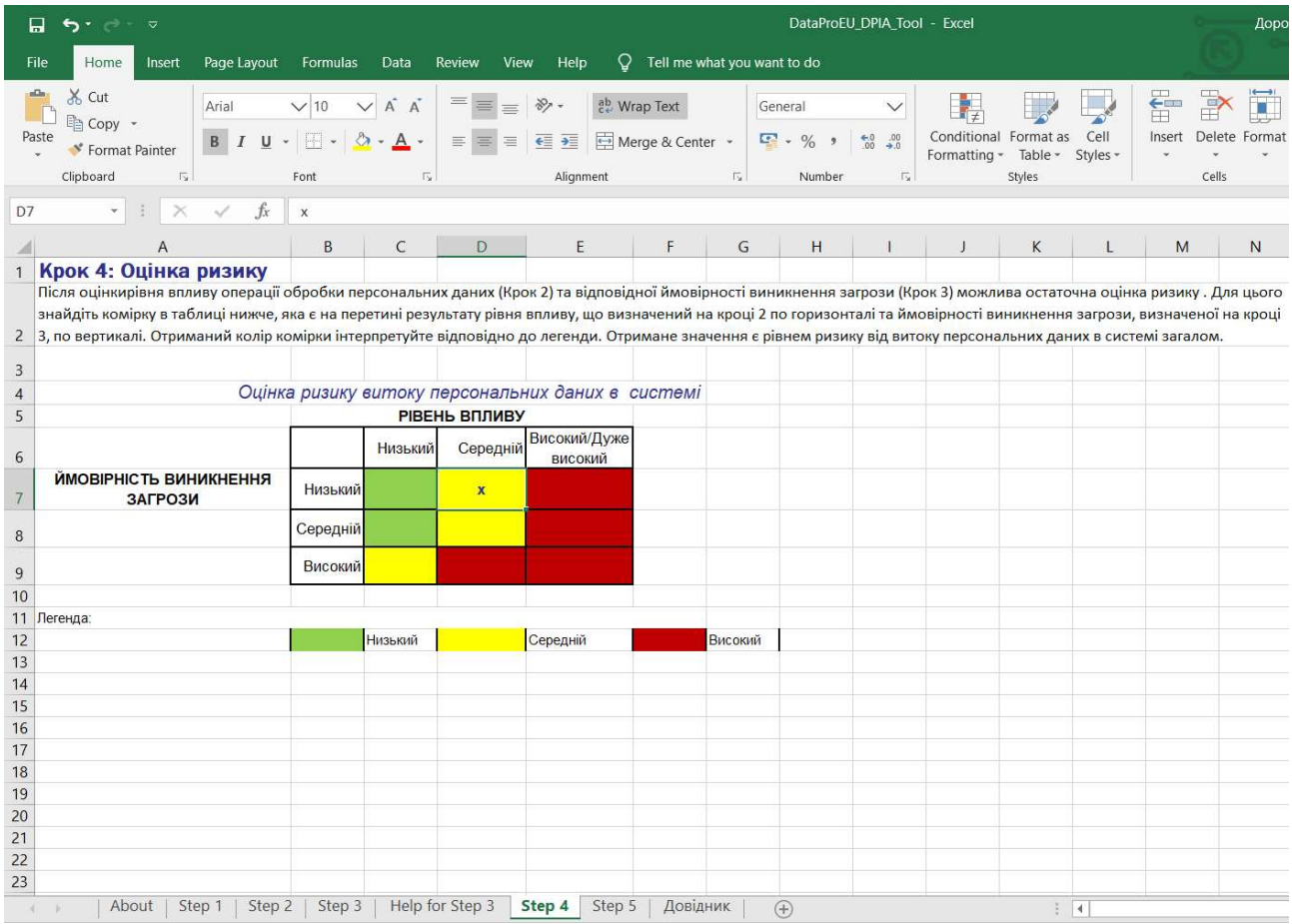
3. The third component of the developed training materials is an interactive template that provides a step-by-step methodology for assessing the risk of personal data leakage for a particular subject area.
   The use of this template greatly facilitates and accelerates the process of performing a DPIA by students, as it breaks down the process into specific steps, each of which contains specific and clear recommendations for its implementation.




DataProEU_DPIA_Tool - Excel
Дорошенко Анастасія Володим
File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do
Paste Cut Copy Format Painter
Arial 9 Wrap Text General
Merge & Center
Conditional Formatting Format as Table Cell Styles
Insert Delete Format
AutoSum Fill Clear Sort & Filter
Clipboard Font Alignment Number Styles Cells Editing
I6
Крок 2: Розуміння та оцінка впливу
Оцінка рівнів впливу
NO Питання Оцінка
Level 1. Конфіденційність
Оцініть вплив, який несанкціоноване розголошення (втрата конфіденційності) особистих даних у контексті діяльності компанії може мати на особу, і дайте відповідну оцінку.
Level 2. Цілісність
Оцініть вплив, який несанкціонована зміна (втрата цілісності) особистих даних - у контексті вашої господарської діяльності - може мати на особу, і дайте відповідну оцінку.
Level 3. Доступність
Оцініть вплив, який несанкціоноване знищення або втрата (втрата доступності) особистих даних - у контексті вашої господарської діяльності - може мати на особу, і дайте відповідну оцінку.
Низький
Середній
Високий
Дуже високий
Оцінка впливу операцій обробки персональних даних
ОЦІНКА ВПЛИВУ
Конфіденційність Цілісність Доступність
Загальна оцінка впливу
Низький
Середній
Високий
Дуже високий
Для того, щоб визначити який рівень впливу є у кожному з випадків, використовуйте цю таблицю:
Опис рівнів впливу
Рівень впливу Опис
Низький
Люди можуть зіткнутися з кількома незначними незручностями, які вони подолають без проблем (час, витрачений
About Step 1 Step 2 Step 3 Help for Step 3 Step 4 Step 5 Довідник

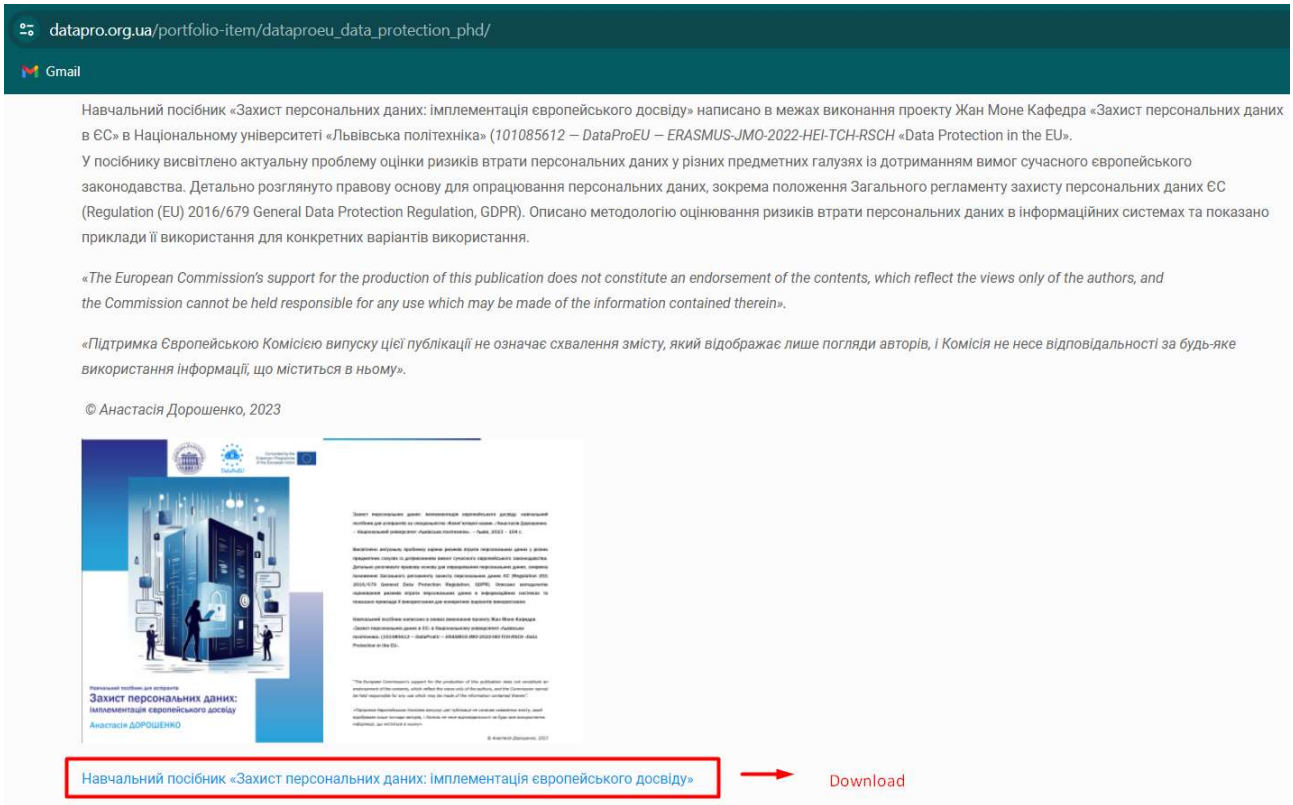

DataProEU_DPIA_Tool - Excel
File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do
Paste Cut Copy Format Painter
Arial 10 Wrap Text General
Merge & Center
Conditional Formatting Format as Table Cell Styles
Clipboard Font Alignment Number Styles
B27 Низький
Сторони/люди, залучені до процесу обробки персональних даних
Низький 1
Середній 2
Високий 3
Бізнес-сектор та масштаб переробки
Низький 1
Середній 2
Високий 3
Впишіть отримані оцінки (рівень та оцінку) в цю таблицю:
Опис операцій обробки персональних даних
ОБЛАСТЬ ОЦІНКИ
ЙМОВІРНІСТЬ
РІВЕНЬ БАЛИ
Мережа та технічні ресурси Низький 1
Процеси/Процедури, пов'язані з обробкою персональних даних 2
Сторони/люди, залучені до обробки персональних даних Низький 1
Сфера діяльності та масштаби переробки Середній 2
Загальна ймовірність виникнення загрози 6
Низький
Середній
Високий
Загальна оцінка виникнення загрози
Загальна сума балів ймовірності появи загрози
Рівень вірогідності виникнення загроз
4-5 Низький
6-8 Середній
9-12 Високий
За допомогою даної таблиці переведіть отримані бали в значення відповідного рівня ризику виникнення загрози.
В бакитній комірці Ви отримали загальну ймовірність виникнення ризику в системі
Визначений рівень: Середній

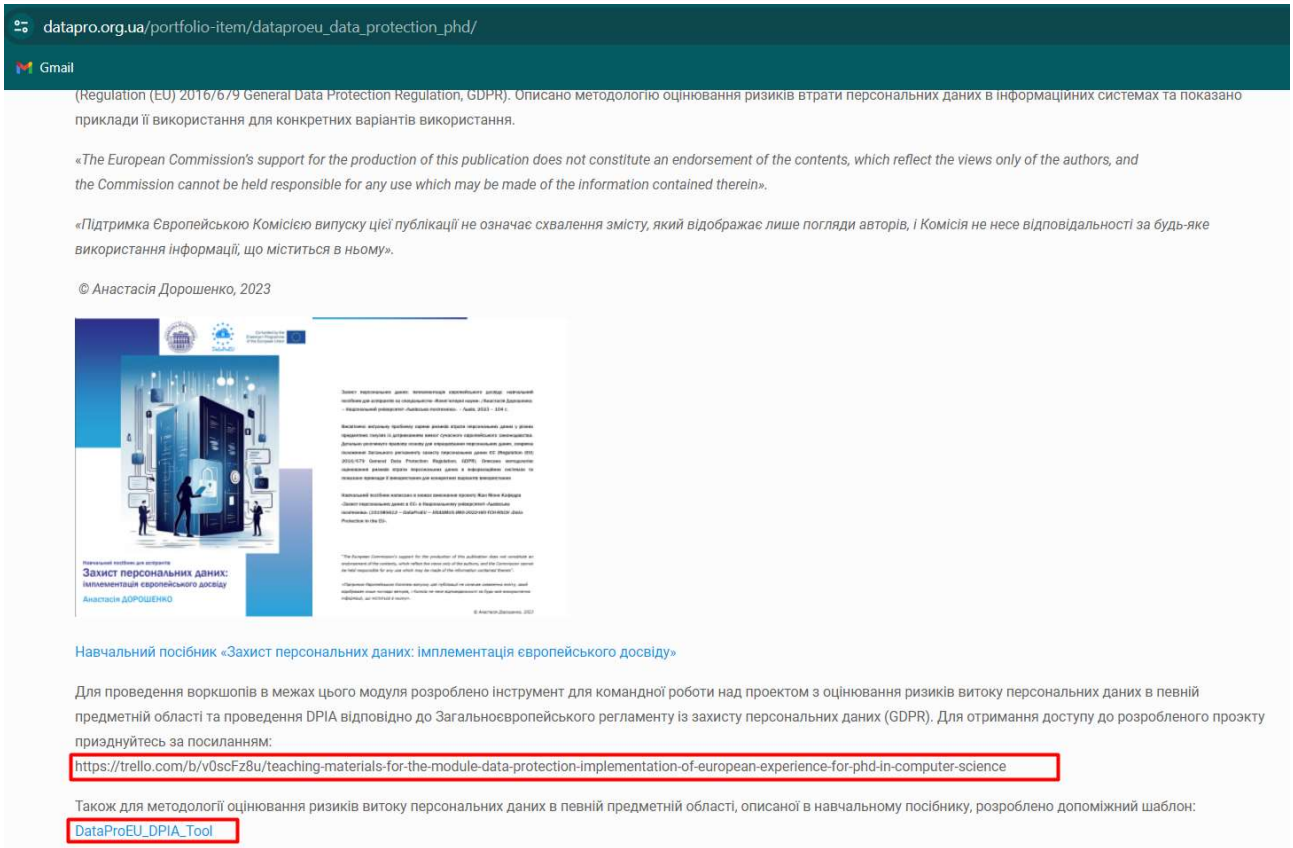




Furthermore, the public availability for unlimited download makes possible the dissemination of the course notes and developed tool to the general public interested in the aforementioned topics, thus broadening the impact of this deliverable beyond its primary target.

All materials are available for download to any visitor to the project website and can be downloaded via the link:
https://datapro.org.ua/portfolio-item/dataproeu_data_protection_phd/





Co-funded by
the European Union

Навчальний посібник для аспірантів

Захист персональних даних:
імплементація європейського досвіду

Анастасія ДОРОШЕНКО

Захист персональних даних: імплементація європейського досвіду: навчальний посібник для аспірантів за спеціальністю «Комп'ютерні науки» /Анастасія Дорошенко. – Національний університет «Львівська політехніка». – Львів, 2023 – 104 с.

Висвітлено актуальну проблему оцінки ризиків втрати персональних даних у різних предметних галузях із дотриманням вимог сучасного європейського законодавства. Детально розглянуто правову основу для опрацювання персональних даних, зокрема положення Загального регламенту захисту персональних даних ЄС (Regulation (EU) 2016/679 General Data Protection Regulation, GDPR). Описано методологію оцінювання ризиків втрати персональних даних в інформаційних системах та показано приклади її використання для конкретних варіантів використання.

Навчальний посібник написано в межах виконання проекту Жан Моне Кафедра «Захист персональних даних в ЄС» в Національному університеті «Львівська політехніка» (*101085612 — DataProEU — ERASMUS-JMO-2022-HEI-TCH-RSCH* «Data Protection in the EU».

Зміст

Вступ

Останнім часом у багатьох країнах Європи та світу запроваджуються нові або значно посилюються існуючі закони про захист даних та кібербезпеку. Ці закони істотно впливають на інформаційні системи і більшість видів діяльності у сфері IT, аналітики даних та наукових досліджень. Водночас необхідність захисту даних – або, точніше, реалізація основних прав, покладених в основу концепції захисту даних – не є абсолютною і не повинна перешкоджати здійсненню інших основоположних прав та суспільних інтересів. Тобто завданням розробників інформаційних систем та фахівців, що займаються аналізом персональних даних, є знаходження рівноваги між захистом даних відповідно до чинного законодавства та вирішенням необхідних бізнес-питань.

Тому розглянемо основні поняття та принципи концепції захисту даних відповідно як до Загальноєвропейського регламенту захисту персональних даних (General Data Protection Regulation, GDPR), так і до інших стандартів та регуляторних актів.

Після цього розглянемо основні практичні рекомендації для розробників ІС, дотримуючись яких можна задовольнити основні вимоги щодо захисту даних. Слід зазначити, що ефективний захист даних не є чимось недосяжним: він вимагає чітко визначених дій, які можна здійснити як під час розробленні, так і під час впровадження інформаційних систем. Аналогічно дотримання вимог у сфері захисту даних не вимагає особливих витрат ані з погляду людських ресурсів, ані в контексті фінансових вкладень у технології. За допомогою кількох простих для реалізації заходів будь-яка організація може значно підвищити свій рівень дотримання вимог до захисту даних.

Розглянемо історію питання захисту персональних даних, аналіз правових принципів захисту даних. Опишемо практичне застосування цих принципів та обговоримо права суб'єктів даних, оскільки саме їхні інтереси покликана захищати нормативна база. Розглянемо можливості використання даних з метою суспільної корисності та наукових інтересів, а також способи знаходження рівноваги інтересів, що зачіпаються в цьому контексті. На конкретних практичних прикладах розглянемо заходи, яких необхідно вжити для досягнення такої рівноваги, зокрема створення механізмів нагляду та розширення прав та можливостей.

1. Основні поняття захисту персональних даних

1.1. Історія регулювання захисту персональних даних

У 1890 р. американські юристи Семюел Д. Уоррен і Луїс Брендіс написали есе «Право на конфіденційність», в якому стверджували, що люди мають «право бути залишеними у спокої»: це формулювання використано як визначення конфіденційності [1]. У 1948 р. було прийнято Загальну декларацію прав людини, до якої увійшло дванадцяте основне право — декларація про недоторканність особистого життя [2]. У міру прискорення технічного прогресу розвивалася правова база у сфері захисту даних. У 1980 р. в умовах дедалі ширшого використання комп'ютерів для обробки даних та зростання їх обчислювальної потужності Організація економічного співробітництва та розвитку випустила посібник із захисту персональних даних [3]. Роком пізніше Рада Європи ухвалила Конвенцію про захист даних (Конвенцію № 108), яка стала першим документом у законодавстві європейських країн, що закріпив право на конфіденційність особистих даних [4]. Спочатку ця нормативна база мала захищати окремих громадян від зазіхань на конфіденційність їхніх особистих даних із боку держави.

Наприкінці 1983 р. Федеральний конституційний суд Німеччини прийняв принципове рішення у так званій «справі про перепис населення» [5]. Цей вердикт сприймається як історична віха у сфері захисту даних, оскільки у ньому сформульовано «право інформаційного самовизначення». Протягом наступних десятиліть це рішення суду продовжуватиме стимулювати розширення захисту даних. У 1995 р. було прийнято Європейську директиву про захист даних 95/46/ЕС, в якій було відображено технологічні досягнення та впроваджено нові поняття, включаючи, зокрема, обробку даних, конфіденційні персональні дані та згоду. Директива була покликана зокрема нівелювати зростаючу нерівність у співвідношенні правових пріоритетів між приватними корпораціями та громадянами та уточнювала, що право на інформаційне самовизначення дійсно має універсальний характер і може бути використане проти будь-кого.

У 2016 році після чотирьох років обговорення Європейський Парламент затвердив Загальний регламент захисту даних (GDPR) [6]. GDPR є основою прийняття різних законів про захист даних у всьому світі. У 2018 р. Організація Об'єднаних Націй ухвалила документ «Принципи захисту персональних даних та недоторканності особистої інформації» як основний посібник із захисту персональних даних у всіх установах Організації Об'єднаних Націй [7].

Відповідно до законів про захист даних, що діють у різних країнах світу, можна сформулювати такі уніфіковані визначення.

Персональні дані – це будь-яка інформація, що стосується фізичних осіб, які ідентифіковані або можуть бути ідентифіковані.

Ідентифікована фізична особа – це фізична особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема, за допомогою ідентифікаційного номера (наприклад, номера в системі соціального страхування) або через одну або кілька ознак, характерних для її фізичної, фізіологічної, психологічної, економічної, культурної чи соціальної ідентичності (наприклад, прізвище та ім'я, дата народження, біометричні дані, відбитки пальців тощо).

Важливим терміном у цьому визначенні є поняття «що стосується», оскільки воно передбачає і те, що такі дані не належать суб'єкту даних (як об'єкт права власності), і те, що такі дані можуть належати більше ніж одній особі. Наприклад, інформація про те, що особа страждає на дальтонізм (захворювання, на яке частіше страждають чоловіки), однаково стосується і його матері як носія відповідного гена, і батька його матері, який також був дальтоніком. Отже, обробка таких даних на основі поінформованої згоди може вимагати згоди всіх суб'єктів даних, яким належать ці дані.

Суб'єкт даних – це будь-яка особа, яка ідентифікована або може бути ідентифікована, якій належать персональні дані.

Персональні дані, які були знеособлені, зашифровані або псевдонімізовані, але все ще залишаються потенційним засобом повторної ідентифікації особи, зберігають статус персональних даних та підпадають під дію законів про захист даних.

Персональні дані, надані анонімно таким чином, що особа не ідентифікується або більше не може бути ідентифікована, не вважаються персональними даними. Щоб дані вважалися дійсно знеособленими, знеособлення має бути незворотним.

1.2. Основні принципи захисту персональних даних

Процес захисту даних побудований на дотриманні основних принципів, закріплених у таких важливих документах, як Конвенція № 108 Ради Європи, Хартія Європейського Союзу (ЄС) про основні права [8] та національні конституції багатьох країн.

Для забезпечення повного дотримання застосовних законів та нормативних актів у сфері захисту даних фізичні або юридичні особи, які опрацьовують персональні дані (процесори), повинні дотримуватись таких принципів захисту даних:

- ✓ ***Справедливість, законність та прозорість***: обробка персональних даних повинна проводитися справедливо, законно та прозоро стосовно суб'єкта даних. Зокрема, персональні дані слід обробляти лише в тому випадку, якщо це дозволено законом і коли для цього є підстави: переважаючий законний інтерес процесора або згода на те суб'єкта даних.

- ✓ ***Обмеження мети:*** персональні дані можна отримувати лише для однієї чи більше конкретних та законних цілей; обробляти їх будь-яким чином, що не сприяє досягненню цієї мети (цілей), заборонено.
- ✓ ***Точність:*** персональні дані мають бути точними, і за необхідності їх слід оновлювати.
- ✓ ***Мінімізація даних:*** персональні дані повинні бути актуальними, відповідати меті їх обробки, а також обмежуватися лише необхідним для її досягнення.
- ✓ ***Обмеження терміну зберігання:*** персональні дані, що обробляються з певною метою, не повинні зберігатися довше, ніж потрібно для досягнення цієї мети.
- ✓ ***Права суб'єктів даних:*** персональні дані повинні оброблятися з дотриманням прав суб'єктів даних, як цього вимагає законодавство в галузі захисту даних.
- ✓ ***Цілісність та конфіденційність:*** необхідно вжити відповідних фізичних, технічних, юридичних та організаційних заходів для запобігання несанкціонованій або незаконній обробці персональних даних та їх випадкової втрати, зміни або пошкодження.
- ✓ ***Передача персональних даних на міжнародному рівні:*** персональні дані не повинні передаватися до третіх країн або міжнародних організацій, якщо в цих країнах/організаціях не забезпечений відповідний рівень захисту прав і свобод суб'єктів даних у зв'язку з обробкою персональних даних [9].

Дотримання цих принципів гарантує здатність контролерів даних, таких як заклади охорони здоров'я, продемонструвати, що їхня діяльність повною мірою підзвітна, а обробка даних здійснюється справедливим і збалансованим чином, що стосується права на інформаційне самовизначення або право на конфіденційність лише тією мірою, якою це є необхідно для дотримання громадських інтересів у сфері охорони здоров'я.

Рекомендовані дії:

- ✓ Розробити комплексне розуміння принципів.
- ✓ Розробити план реалізації принципів у конкретних умовах.
- ✓ Розробити довгостроковий план систематичного дотримання цих принципів.

1.3. Законні підстави для обробки даних

Незалежно від мети обробки персональних даних така обробка не допускається за відсутності незаперечних доказів того, що контролер даних має вагомі законні підстави для подібної обробки (стаття 6 GDPR). Це положення закріплено у

першому принципі захисту даних. Для обробки даних є шість законних підстав. Жодна з цих підстав не є більш правильною чи важливою, ніж інші: вибір на користь тієї чи іншої підстави роблять залежно від мети обробки та взаємовідносин із відповідною фізичною особою. Законна підстава має бути визначена до початку обробки та належним чином задокументована згідно з типом обробки. Детальний опис цих шести категорій наведено нижче.

1. ***Згода:*** особа явно надала поінформовану згоду на обробку персональних даних для конкретного завдання.
2. ***Договір:*** обробка даних необхідна для виконання умов договору, укладеного між контролером та особою, або через те, що суб'єкт даних попросив розпочати процедуру обробки до укладення договору.
3. ***Правовий обов'язок:*** обробка необхідна для дотримання законодавства (не включаючи договірних зобов'язань).
4. ***Життєво важливі інтереси:*** обробка необхідна для захисту будь-якого життя.
5. ***Суспільний інтерес:*** обробка необхідна для виконання завдання на користь суспільства або здійснення частини офіційного завдання або функції, які мають чітку правову основу.
6. ***Законні інтереси:*** обробка необхідна для захисту законних інтересів третьої сторони і при цьому немає вагомої причини захищати персональні дані особи, яка була б більшою, ніж законні інтереси такої сторони; ця юридична підстава, однак, не застосовується у тих випадках, коли орган державної влади опрацьовує персональні дані у межах здійснення своїх офіційних завдань.

Однією з найважливіших правових підстав є поінформована згода суб'єкта даних: вона, безумовно, відіграє значну роль при здійсненні дослідницької діяльності, але також може використовуватися, наприклад, для завдань охорони громадського здоров'я, вирішити які можна лише маючи набори даних без суттєвих прогалин.

Отже, поінформована згода суб'єкта даних може не знадобитися за наявності законної підстави (наприклад, для створення онкореєстру) або явного переважаючого державного інтересу (наприклад, у разі пандемії). Концепція поінформованої згоди застосовна лише за умови, що суб'єкт даних має «реальний» вибір, а також якщо відмова дати згоду не тягне за собою негативних наслідків для суб'єкта даних [10].

На практиці поінформована згода суб'єкта даних часто неправомірно застосовується як практично універсальна правова підстава. У зв'язку з цим часто рекомендується вибирати альтернативну правову основу. Однак необхідно бути обережними, оскільки дія вимог до прозорості може бути припинена тільки у разі конкретних винятків.

Рекомендовані дії:

- ✓ Визначити конкретну правову основу обробки даних.
- ✓ Ретельно проаналізувати перспективи використання поінформованої згоди як правової основи.
- ✓ Використовувати підстави, пов'язані з життєвими інтересами, лише у виняткових випадках, коли втручання у сфері охорони здоров'я приносить безпосередню користь суб'єктам даних.
- ✓ Правильно документувати всі обговорення та будь-які прийняті рішення.

1.4. Принцип поінформованої згоди

Оскільки для будь-якої обробки даних потрібна правова підстава, дослідники часто вдаються до поінформованої згоди суб'єктів даних, зокрема для легітимізації обробки персональних даних [11]. Проте, як зазначалося вище, поінформована згода є лише однією з шести правових підстав; її необхідно використовувати у громадській охороні здоров'я лише за виконання певних умов.

- ✓ Згода передбачає, що суб'єкти даних мають реальний вибір і можливості для управління ситуацією.
- ✓ Згода вимагає позитивної відповіді суб'єкта даних, тобто чіткого вираження його волі.
- ✓ Згода має бути конкретною та детальною – зокрема щодо цілей обробки даних. У дослідницькій діяльності застосовуються винятки з цього правила: так, формулювання «згода на медичні дослідження» може виявитися достатньо конкретним, якщо суб'єкт даних здатний зрозуміти наслідки цієї згоди.
- ✓ У тому випадку, якщо інформація про суб'єкт даних надходить у розпорядження об'єктів державної інфраструктури суспільної охорони здоров'я або досліджень, також допустиме використання широкої згоди [12].

Згода може застосовуватися лише в тому випадку, якщо у суб'єкта даних є реальний вибір, і якщо суб'єкта даних ані безпосередньо, ані опосередковано не змушують дати згоду на обробку даних. Ця вимога завжди має велике значення в тих випадках, коли отримують згоду, наприклад, у медичній установі, оскільки відмова дати згоду може серйозно вплинути на рівень медичної допомоги, що надається. Аналогічним чином згоду не можна застосовувати тоді, коли контролер даних не здатний (або не має наміру) запропонувати суб'єкту реальний вибір, оскільки в такому разі процедура отримання згоди спрямована на введення в оману та несправедлива за своєю суттю.

Згода має бути задокументована належним чином, причому використовувані для цього документи повинні мати чітку структуру, доступний зміст та складатися мовою, зрозумілою суб'єкту даних. Суб'єкту даних слід дати достатньо часу для обмірковування свого вибору та за необхідності забезпечити йому доступ до додаткової інформації та консультацій. Визначення «інформоване» не менш важливе, ніж саме слово «згода»; докладно це питання розглянуто у розділі 5, присвяченому темі прозорості.

Рекомендовані дії

- ✓ Інформовану згоду не можна використовувати як засіб «спрощення» вибору правової основи: необхідно ретельно оцінити, чи правильним буде його використання у вашій ситуації, пов'язаній з обробкою даних.
- ✓ Ретельно оцінити ступінь свободи вибору суб'єкта даних.
- ✓ Чітко донести до суб'єкта даних, що в нього є реальний вибір.
- ✓ Дотримуватись принципів детальності та конкретності: за можливості уникати використання широкої чи загальної згоди.

1.5. Прозорість обробки персональних даних

Як зазначалося вище, однією з основних принципів сучасного законодавства у сфері захисту є принцип прозорості. Цей факт безпосередньо пов'язаний з історичним рішенням німецького суду у справі про перепис населення 1983 р. (див. розділ 1), у якому суд заявив: «Виходячи з поняття самовизначення, загальне право особистості включає надану окремій особі можливість самостійно приймати принципове рішення про те, чи розкривати будь-які аспекти свого особистого життя і якщо так, то якою мірою. <…> Якщо особа не здатна з достатньою впевненістю визначити, якого роду особиста інформація відома його оточенню, і навіть важко встановити, яка інформація доступна його потенційним партнерам із комунікації, це може серйозно порушити свободу здійснення самовизначення» [13].

Отже, принцип прозорості має фундаментальний та невід'ємний зв'язок із принципом справедливості. Принцип прозорості обробки даних у контексті суспільної охорони здоров'я полягає в тому, що взаємодія з суб'єктами даних має здійснюватися зрозумілим, відкритим та чесним чином; для цього необхідно, щоб заклади охорони здоров'я розкривали суть основних елементів діяльності з обробки даних [14].

Чітка та коротка інформація повинна надаватися зрозумілою суб'єкту даних мовою незалежно від того, чи отримано дані безпосередньо від суб'єкта або від третьої сторони.

Надання інформації також є дуже важливим у разі зміни мети обробки (наприклад, при вторинному використанні інформації охорони здоров'я), якщо до ситуації не застосовні конкретні винятки. Основними прикладами таких винятків є ситуації, у яких надання подібної інформації виявляється неможливим або потребує не відповідних цілям зусиль, або ситуації, у яких виняток передбачено законом.

Для забезпечення належної прозорості контролери даних можуть керуватися статтями 13 та 14 GDPR, які містять перелік інформації, що надається суб'єкту даних. Крім безпосередньої комунікації з суб'єктами даних через повідомлення про конфіденційність або умови дотримання конфіденційності, контролерам також рекомендується вести активний діалог із громадянським суспільством і регулярно звітувати перед громадськістю про свою діяльність у сфері захисту даних.

Рекомендовані дії

- ✓ Розробити політику конфіденційності та опублікувати її на веб-сайті чи іншим чином.
- ✓ Переконатися, що її написано простою мовою, доступною для розуміння непрофесіоналів.
- ✓ Забезпечити наявність каналів зв'язку із суб'єктами даних.
- ✓ Активно працювати з громадянським суспільством, доводячи до його відома використовувані концепції та процедури захисту даних.

1.6. Права суб'єктів даних відповідно до GDPR

Мета сучасних законів про захист даних полягає в тому, щоб дати громадянам можливість здійснювати свої права у світі, який дедалі більше контролюють технологічні компанії та інші сторони, які обробляють величезні обсяги даних, що належать громадянам.

Дотримання прав суб'єктів даних нерозривно пов'язано з принципом прозорості, оскільки лише поінформовані громадяни здатні відстоювати та захищати свої права. Відповідальність за дотримання прав суб'єктів даних покладено на контролера даних. Виступаючи в цій якості, контролер даних також зобов'язаний забезпечити дотримання прав суб'єктів даних будь-яким процесором (або у разі передачі даних між контролерами будь-яким одержувачем даних).

Основними правами суб'єктів даних є [14]:

- ✓ ***Право на доступ до даних*** означає: а) право суб'єкта даних знати, чи обробляються його персональні дані і б) якщо це так, то право на доступ до таких даних та отримання копії цих даних.

- ✓ ***Право на внесення виправлень*** означає, що якщо персональні дані є неточними, суб'єкт даних має право вимагати від контролера виправлення фактично неточних даних.
- ✓ ***Право на видалення*** (у деяких юрисдикціях, якщо персональні дані були оприлюднені, воно називається ***правом на забуття***) – це основне право, що дозволяє обмежити обробку даних та забезпечити дотримання термінів їх зберігання.
- ✓ ***Право на обмеження обробки*** по суті є правом громадянина обмежити обробку своїх персональних даних у тому випадку, якщо він може претендувати на переважне право такого обмеження.
- ✓ ***Право на отримання інформації*** є основним правом, яке слід сприймати як ключовий елемент прав суб'єкта даних.
  Більшість законів про захист даних, що діють у європейських та інших країнах, вимагають від контролерів інформувати суб'єктів даних щодо низки питань; як правило, інформування повинно здійснюватися заздалегідь, чітко, коротко і в доступних для розуміння неспеціаліста термінах. Це право може не застосовуватись у низці виняткових випадків, які, наприклад, стосуються досліджень у сфері медицини чи охорони здоров'я чи іншої діяльності, що стосується охорони громадського здоров'я. Проте будь-який виняток із права на отримання інформації має бути ретельно проаналізований та задокументований.
- ✓ ***Право на перенесення даних*** у багатьох юрисдикціях є відносно новим; воно пов'язане з правом на доступ до даних, оскільки передбачає право отримувати дані, що належать особі у форматі, придатному для машинного зчитування, причому, можливо, громадянин навіть може попросити контролера даних передати дані іншому контролеру. Як правило, право на перенесення даних поширюється лише на дані, отримані на підставі згоди суб'єкта даних або договору із суб'єктом даних. Воно не поширюється на обробку, що здійснюється на законних підставах, і не може застосовуватись у тих випадках, коли його дотримання може порушити важливі суспільні інтереси, включаючи охорону громадського здоров'я.
- ✓ Одним із важливих прав є ***право суб'єкта даних на заперечення***. Воно означає, що суб'єкт даних може висловити заперечення проти обробки його персональних даних. Незважаючи на те, що цьому праву відводиться важлива роль у ситуаціях прямого маркетингу або складання профілів, воно може бути обмежене, якщо орган охорони здоров'я або інший державний орган має переважну зацікавленість у обробці даних та здійснює її для загального блага. Наприклад, у ситуації пандемії громадяни можуть бути позбавлені права заперечувати проти обробки даних, якщо така обробка необхідна для відстеження та спостереження за їх діями. Проте в таких випадках застосування права на заперечення проти обробки може фактично зобов'язати державні установи забезпечити, щоб обробці

піддавався лише мінімальний обсяг даних, необхідний для виконання поставленого завдання.

- ✓ ***Право суб'єкта даних не бути об'єктом рішення, основаного виключно на автоматизованій обробці,*** включаючи складання профілю, що породжує юридичні наслідки щодо суб'єкта даних або аналогічним чином істотно впливає на нього, має такі самі обмеження, що й право на заперечення, у контексті заходів щодо охорони здоров'я. Слід зазначити, що при здійсненні діяльності на благо суспільства установи повинні забезпечувати повне дотримання суті права на інформаційне самовизначення та гарантувати, що суб'єкт даних не є об'єктом рішення, основаного виключно на автоматичній обробці [15].

Рекомендовані дії

- ✓ Чітко та ефективно інформувати суб'єктів даних про їхні права.
- ✓ Визначити процедури та платформи для подання запитів суб'єктами даних.
- ✓ Забезпечити партнерські відносини із суб'єктами даних, які є «клієнтами».
- ✓ Документувати запити суб'єктів даних та заходи для їх виконання.
- ✓ Гарантувати, що IT-системи сприяють виконанню запитів суб'єктів даних (наприклад, видалення даних).
- ✓ Розробити стратегію інформування про будь-які причини, через які відбувається відхилення запитів суб'єктів даних.

Дотримання прав суб'єктів даних має найважливіше значення, оскільки якщо компанії чи установи (як приватні, так і державні) дотримуються цих прав, то громадяни ставляться до їх діяльності з обробки даних із більшою довірою. Наприклад, якщо б під час пандемії COVID-19 додаток для відстеження контактів ігнорував права суб'єктів даних і створював можливість застосування таких даних для вторинних цілей, наприклад, для збору податків, громадяни могли б відмовлятись від використання такого додатка. В онлайновому світі довіра є найціннішою валютою; компанії практично неможливо буде повернути втрачену довіру клієнтів [16].

2. Оцінювання впливу на захист даних

Для того, щоб підвищити рівень довіри користувачів до ІС відповідно до GDPR рекомендується пройти добровільну сертифікацію на відповідність опрацювання персональних даних користувачів всім вимогам GDPR (стаття 42 (1)). Сертифікацію здійснюють органи сертифікації, вказані в статті 43, або компетентні наглядові органи, на підставі критеріїв, затверджених таким компетентним наглядовим органом згідно зі статтею 58(3) або Радою згідно зі статтею 63 GDPR.

Однак, перш ніж розпочинати процедуру сертифікації, контролеру рекомендується самостійно за участі DPO (Data Protection Officer) компанії оцінити вплив на захист даних (Data protection impact assessment DPIA) існуючої ІС. Процедура проведення DPIA визначається статтею 35 GDPR, відповідно до якої якщо тип опрацювання персональних даних, зокрема з використанням нових технологій, і зважаючи на специфіку, обсяг, контекст і цілі опрацювання, ймовірно призведе до виникнення високого ризику для прав і свобод фізичних осіб, контролер до здійснення опрацювання повинен оцінити вплив передбачених операцій опрацювання на захист персональних даних. Єдине оцінювання може стосуватися низки подібних операцій опрацювання, що становлять подібні високі ризики.

У випадку розроблення нової ІС зрозуміло, що таке оцінювання впливу на захист даних повинне бути зроблене на етапі проектування ІС, до початку її експлуатації, що відповідатиме такому принциповому підходу GDPR, як спроектована конфіденційність (Privacy by Design), визначеному у статті 25.

Різними організаціями, що займаються захистом персональних даних, розроблено різні шаблони, які дозволяють DPO спростити процедуру проведення DPIA. У цьому навчальному посібнику використовуватимемо шаблон, розроблений ICO (Information Commissioner's Office) [17], повний текст якого знаходиться у Додатку 1. Додаток 2 містить альтернативний варіант шаблону, розроблений організацією Iapp (International Association of Privacy Professionals) [18].

Розглянемо покроково процес здійснення оцінювання впливу на захист даних:

Крок 1: Визначте потребу в DPIA

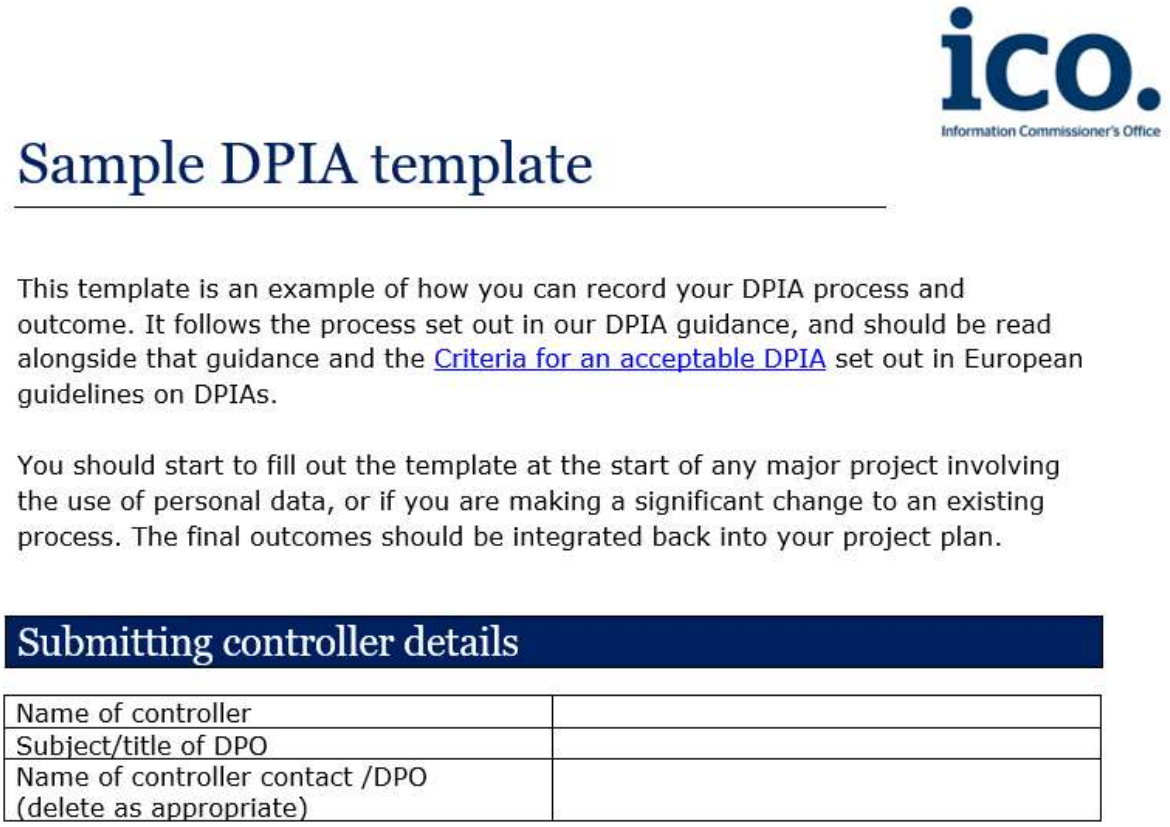
Загально поясніть, на що спрямований проект і який тип обробки він передбачає. Вам може бути корисним посилання на інші документи, такі як проектна пропозиція. Підсумуйте, чому ви визначили потребу в DPIA.

Крок 2: Опишіть обробку

2.1. Опишіть характер обробки: як ви будете збирати, використовувати, зберігати та видаляти дані? Яке джерело даних? Чи будете ви ділитися даними з кимось?

Вам може бути корисно звернутися до діаграми потоків або іншого способу опису потоків даних. Які типи обробки, визначені як високоризикові, задіяні?

2.2. Опишіть обсяг обробки: який характер даних і чи включають вони дані, що належать до особливої категорії (чутливі дані) чи про кримінальні правопорушення? Скільки даних ви будете збирати та як плануєте використовувати ці дані? Як часто? Як довго ви будете їх зберігати? Скільки осіб може постраждати у випадку витоку даних? Яку географічну територію вони охоплюють?



ico.
Information Commissioner's Office

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Рис.2.1. Фрагмент шаблону, розробленого ICO для проведення DPIA

2.3. Опишіть контекст обробки: який характер ваших стосунків з окремими особами? Наскільки вони матимуть контроль над зібраними даними? Чи очікують вони, що ви будете використовувати їхні дані таким чином? Чи включають вони дітей чи інші вразливі групи? Чи є попередні занепокоєння щодо такого типу обробки чи недоліків безпеки? Чи є така обробка даних чимось новим? Який поточний стан технологій у цій галузі? Чи є якісь поточні проблеми, що викликають занепокоєння суспільства, які ви повинні враховувати? Чи прийняли ви будь-який затверджений кодекс поведінки або схему сертифікації (якщо їх буде затверджено)?

2.4. Опишіть цілі обробки: чого ви хочете досягти? Який передбачуваний вплив на окремих людей? Які переваги обробки – для вас загалом?

Крок 3: Процес консультації

Подумайте про те, як проводити консультації з відповідними зацікавленими сторонами: опишіть, коли і як ви збираєтеся дізнатися думки окремих осіб – або обґрунтуйте, чому це робити недоцільно. Кого ще вам потрібно залучити до вашої організації? Вам потрібно попросити своїх процесорів допомогти? Чи плануєте ви консультуватися з експертами з інформаційної безпеки чи будь-якими іншими експертами?

Крок 4: Оцініть необхідність і пропорційність

Опишіть заходи відповідності та пропорційності, зокрема: яка ваша законна підстава для обробки? Чи справді обробка досягає вашої мети? Чи є інший спосіб досягти такого ж результату? Як запобігти повзучому функціонуванню? Як ви забезпечите якість даних і мінімізацію даних? Яку інформацію ви надаєте особам? Як ви допоможете відстояти їхні права? Які заходи ви вживаєте, щоб забезпечити відповідність процесорів? Як ви захищаєте міжкордонну передачу даних?

Крок 5: Визначте та оцініть ризики

Опишіть джерело ризику та характер потенційного впливу на осіб. За потреби включіть пов'язану відповідність і корпоративні ризики:

- ✓ Імовірність заподіяння шкоди (Віддалена, можлива або ймовірна)
- ✓ Тяжкість заподіяної шкоди (Мінімальна, значна або серйозна)
- ✓ Загальний ризик (Низький, середній або високий)

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Рис.2.2. Фрагмент шаблону, розробленого ICO для проведення DPIA

Крок 6: Визначте заходи для зменшення ризику

Визначте додаткові заходи, які ви можете вжити для зменшення або усунення ризиків, визначених як середній або високий ризик на кроці 5

Для кожного ризику необхідно запропонувати варіанти зменшення або усунення ризику:

- ✓ Вплив на ризик (Виключений, зменшений або прийнятий)
- ✓ Залишковий ризик (Низький, середній, високий)
- ✓ Захід затверджено (Так/ні)

Крок 7: Підпишіться та запишіть результати

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Рис.2.3. Фрагмент шаблону, розробленого ICO для проведення DPIA

Проведення такого оцінювання впливу на захист даних може відбуватись як до початку проектування та розробки системи і буде важливим елементом імплементації спроектованої конфіденційності (Privacy by Design), так і під час функціонування системи – для того, щоб переконатись, що всі процеси відбуваються відповідно до вимог GDPR.

3. Безпека обробки персональних даних відповідно до GDPR

Беручи до уваги сучасний рівень техніки, витрати на впровадження та характер, обсяг, контекст і цілі обробки, а також ризик різної ймовірності та серйозності для прав і свобод фізичних осіб, відповідно до статті 32 GDPR контролер і процесор повинні впроваджувати відповідні технічні та організаційні заходи для забезпечення рівня безпеки, відповідного ризику, включаючи, зокрема, такі випадки, як:

- ✓ псевдонімізація та шифрування персональних даних ;
- ✓ здатність забезпечити постійну конфіденційність, цілісність, доступність і стійкість систем і послуг обробки ;
- ✓ здатність своєчасно відновити доступність і доступ до персональних даних у разі фізичного чи технічного інциденту;
- ✓ процес регулярного тестування, оцінювання та оцінки ефективності технічних і організаційних заходів для забезпечення безпеки обробки .

При оцінці відповідного рівня безпеки облікового запису мають враховуватися, зокрема, ризики , пов’язані з обробкою: захист від випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних , що передаються, зберігаються або іншим чином оброблені.

Крім того, стаття передбачає, що «при оцінці відповідного рівня безпеки обліковий запис повинен враховувати, зокрема, ризики, пов’язані з обробкою даних, зокрема від випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних. передається, зберігається або обробляється іншим чином». У ньому також згадується, що дотримання затвердженого кодексу поведінки (стаття 40 GDPR) або затвердженого механізму сертифікації (стаття 41 GDPR) може використовуватися як елемент для демонстрації відповідності вимогам щодо безпеки обробки. Нарешті, в ній йдеться про те, що контролер і процесор «вживають заходів для забезпечення того, щоб будь-яка особа, яка діє під їхнім повноваженням і має доступ до персональних даних, не обробляла їх, окрім як за вказівками контролера, якщо інше не вимагається законодавством Союзу або держав-членів».

Відповідно до вищезазначених положень, у GDPR безпека рівною мірою охоплює конфіденційність, цілісність і доступність і повинна розглядатися відповідно до підходу, що ґрунтується на оцінці ризику: чим вищий ризик (для прав і свобод суб’єктів даних), тим суворіші заходи контролер або процесор повинен вживати (щоб керувати ризиком). Крім того, безпеку обробки слід розглядати в межах загальної системи підзвітності GDPR для захисту даних, яка також базується на оцінці ризику та впливу та спрямована на те, щоб відповідати конкретному операційному контексту та практикам організації.

Відповідно, як альтернативу розглянутому вище підходу до проведення DPIA, можна використати методологію оцінювання ризиків щодо захисту персональних даних, розроблену Агенцією Європейського Союзу з кібербезпеки (ENISA), та запропоновану як спрощений підхід для малих та середніх підприємств (МСП) (які виконують функції контролерів або обробників даних) для конкретних операцій обробки даних, допомагаючи їм оцінити відповідні ризики з точки зору безпеки та визначити необхідні заходи безпеки [19].

3.1. Методологія оцінки ризиків безпеки від ENISA

Рекомендації ENISA для МСП пропонують підхід до оцінки ризику, який базується на чотирьох кроках, а саме:

1. Визначення операції обробки та її контексту.
2. Розуміння та оцінка впливу.
3. Визначення можливих загроз та оцінка їх вірогідності (імовірності виникнення загрози).
4. Оцінка ризику (поєднання ймовірності виникнення загрози та впливу).

Після оцінки ризику МСП можуть прийняти технічні та організаційні заходи безпеки (із запропонованого списку), які відповідають рівню ризику.

Розглянемо детальніше як повинне відбуватись проходження кожного з кроків.

Крок 1: Визначення операції обробки та її контексту

Цей крок є відправною точкою оцінки ризику та є основним для контролера даних для визначення меж системи обробки даних (оцінюється) та її відповідного контексту. Щоб допомогти малим і середнім підприємствам визначити операцію обробки, надається набір запитань.

1. Що таке операція обробки персональних даних?
2. Які типи персональних даних обробляються?
3. Яка мета обробки?
4. Які засоби використовуються для обробки персональних даних?
5. Де відбувається обробка персональних даних?
6. Які є категорії суб’єктів даних?
7. Хто є одержувачами даних?

Відповідаючи на ці запитання, МСП має враховувати різні етапи обробки даних (збір, зберігання, використання, передача, утилізація тощо) та їхні наступні параметри.

Крок 2: Розуміння та оцінка впливу

На основі аналізу Кроку 1 контролер даних на цьому етапі повинен оцінити вплив на основні прав та свобод осіб у результаті можливої втрати безпеки персональних даних. Розглянуто чотири рівні впливу (низький, середній, високий, дуже високий), як показано в таблиці 3.1 нижче.

Таблиця 3.1

Опис рівнів впливу

Рівень впливу	Опис
Низький	Люди можуть зіткнутися з кількома незначними незручностями, які вони подолають без проблем (час, витрачений на повторне введення інформації, роздратування тощо).
Середній	Особи можуть зіткнутися зі значними незручностями, які вони зможуть подолати, незважаючи на деякі труднощі (додаткові витрати, відмова в доступі до бізнес-послуг, страх, нерозуміння, стрес, незначні фізичні нездужання тощо).
Високий	Особи можуть зіткнутися зі значними наслідками, які вони повинні бути в змозі подолати, хоча й із серйозними труднощами (привласнення коштів, занесення фінансовими установами до чорних списків, пошкодження майна, втрата роботи, виклик до суду, погіршення здоров'я тощо).
Дуже високий	Особи, які можуть зіткнутися зі значними або навіть незворотними наслідками, які вони можуть не подолати (непрацездатність, тривалі психологічні чи фізичні захворювання, смерть тощо).

Оцінка впливу є якісним процесом, і контролер даних повинен враховувати низку факторів, таких як типи персональних даних, критичність операції обробки, обсяг персональних даних, особливі характеристики контролера даних, а також як спеціальні категорії суб'єктів даних.

Щоб підтримати контролера в цьому процесі, таблицю 3.2 можна використовувати для окремої оцінки впливу від втрати конфіденційності, цілісності та доступності.

Після цієї оцінки буде отримано три різні рівні впливу (для втрати конфіденційності, цілісності та доступності). Найвищий із цих рівнів вважається остаточним результатом оцінки впливу, що стосується загальної обробки персональних даних.

Таблиця 3.2

Оцінка рівнів впливу

NO	Питання	Оцінка	
I.1.	Оцініть вплив, який несанкціоноване розголошення (втрата конфіденційності) особистих даних у контексті	☐	Низький
		☐	Середній

	діяльності компанії може мати на особу, і дайте відповідну оцінку.	☐	Високий
		☐	Дуже високий
I.2.	Оцініть вплив, який несанкціонована зміна (втрата цілісності) особистих даних - у контексті вашої господарської діяльності - може мати на особу, і дайте відповідну оцінку.	☐	Низький
		☐	Середній
		☐	Високий
		☐	Дуже високий
I.3.	Оцініть вплив, який несанкціоноване знищення або втрата (втрата доступності) особистих даних - у контексті вашої господарської діяльності - може мати на особу, і дайте відповідну оцінку.	☐	Низький
		☐	Середній
		☐	Високий
		☐	Дуже високий

Крок 3: Визначення можливих загроз та оцінка їхньої ймовірності

На цьому етапі контролер даних повинен зрозуміти загрози, пов'язані із загальним середовищем обробки персональних даних (зовнішнього чи внутрішнього), і оцінити їхню ймовірність (ймовірність виникнення загрози).

Щоб спростити цей процес, було визначено низку запитань для оцінки, які мають на меті ознайомити МСП із середовищем обробки даних (яке безпосередньо стосується загроз).

Зокрема, вони стосуються чотирьох основних вимірів цього середовища (областей оцінки), а саме:

- Мережа та технічні ресурси (апаратне та програмне забезпечення)
- Процеси/процедури, пов'язані з операцією обробки даних
- Різні сторони та люди, залучені до операції обробки
- Сфера діяльності та масштаб переробки

В таблицях 3.3-3.6 наведено уточнюючі питання, які варто використовувати для більш точної оцінки ймовірності виникнення загрози.

Таблиця 3.3

Оцінка ймовірності виникнення загрози в мережі та технічних ресурсах

A. Мережеві та технічні ресурси		
1	Чи виконується якась частина обробки персональних даних через Інтернет?	Коли обробка персональних даних виконується повністю або частково через відкритий Інтернет, можливі загрози від зовнішніх онлайн-зловмисників зростають (наприклад, відмова в обслуговуванні, впровадження SQL, атаки Man-in-the-Middle), особливо коли послуга доступна (і , таким

		чином, відстежуваний/відомий) усім користувачам Інтернету.
2	Чи можна надати доступ до внутрішньої системи обробки персональних даних через Інтернет (наприклад, для певних користувачів або груп користувачів)?	Коли доступ до внутрішньої системи обробки даних надається через Інтернет, підвищується ймовірність зовнішніх загроз (наприклад, через зовнішніх онлайн-зловмисників). У той же час збільшується ймовірність (випадкового чи навмисного) зловживання даними користувачами (наприклад, випадкове розкриття персональних даних під час роботи в громадських місцях). Особливу увагу слід звернути на випадки, коли дозволено дистанційне керування/адміністрування IT-системи.
3	Чи пов'язана система обробки персональних даних з іншою зовнішньою або внутрішньою (для вашої організації) IT-системою або службою?	Підключення до зовнішніх IT-систем може створювати додаткові загрози через загрози (і потенційні недоліки безпеки), властиві цим системам. Те ж саме стосується і внутрішніх систем, беручи до уваги, що, якщо вони не налаштовані належним чином, такі з'єднання можуть надати доступ (до персональних даних) більшій кількості осіб в організації (які в принципі не авторизовані для такого доступу).
4	Чи можуть неавторизовані особи легко отримати доступ до середовища обробки даних?	Хоча основна увага приділяється електронним системам і службам, фізичне середовище (що стосується цих систем і послуг) є важливим аспектом, який, якщо його не захистити належним чином, може серйозно поставити під загрозу безпеку (наприклад, дозволяючи неавторизованим сторонам отримати фізичний доступ до IT обладнання та мережевих компонентів або неспроможність забезпечити захист комп'ютерної кімнати у випадку фізичної катастрофи).
5	Чи система обробки персональних даних розроблена, впроваджена чи підтримується без дотримання відповідних передових практик?	Погано розроблені, реалізовані та/або обслуговуються апаратні та програмні компоненти можуть становити серйозні ризики для інформаційної безпеки. З цією метою хороші або найкращі практики накопичують досвід попередніх подій і можуть розглядатися як практичні рекомендації щодо того, як уникнути впливу та досягти певного рівня стійкості.

Таблиця 3.4

Оцінка ймовірності виникнення загрози в процесах обробки даних

В. Процеси/процедури, пов'язані з обробкою персональних даних		
1	Чи є ролі та обов'язки щодо обробки персональних даних розпливчастими чи нечітко визначеними?	Якщо ролі та обов'язки чітко не визначені, доступ (і подальша обробка) персональних даних може бути неконтрольованим, що призведе до несанкціонованого використання ресурсів і під загрозою загальній безпеці системи.
2	Чи є прийнятне використання мережі, системи та фізичних ресурсів в організації неоднозначним або нечітко визначеним.	Якщо прийнятне використання ресурсів не визначено чітко, загрози безпеці можуть виникнути через непорозуміння або навмисне неправильне використання системи. Чітке визначення політик щодо мережевих, системних і фізичних ресурсів може зменшити потенційні ризики.
3	Чи дозволено працівникам приносити та використовувати власні пристрої для підключення до системи обробки персональних даних?	Співробітники, які використовують свої персональні пристрої в організації, можуть збільшити ризик витоку даних або несанкціонованого доступу до інформаційної системи. Крім того, оскільки пристрої не контролюються централізовано, вони можуть внести додаткові помилки або віруси в систему.
4	Чи дозволено працівникам передавати, зберігати або іншим чином обробляти персональні дані поза межами організації?	Обробка персональних даних поза межами організації може запропонувати велику гнучкість, але в той же час створює додаткові ризики, пов'язані як з передачею інформації через, можливо, незахищені мережеві канали (наприклад, відкриті мережі Wi-Fi), так і з несанкціоноване використання цієї інформації.
5	Чи можна здійснювати дії з обробки персональних даних без створення лог-файлів?.	Відсутність відповідних механізмів реєстрації та моніторингу може посилити навмисне або випадкове зловживання процесами/процедурами та ресурсами, що призведе до подальшого зловживання персональними даними.

Таблиця 3.5

Оцінка ймовірності виникнення загрози , пов'язаної із сторонами/людьми, залученими до процесу обробки персональних даних

С. Сторони/люди, залучені до процесу обробки персональних даних		
1	Чи виконується обробка персональних даних невизначеною кількістю працівників?	Коли доступ (і подальша обробка) персональних даних відкритий для великої кількості співробітників, збільшуються можливості зловживань через людський фактор. Чітке визначення того, хто дійсно потребує доступу до даних, і обмеження доступу лише цими особами може сприяти безпеці персональних даних.
2	Чи будь-яка частина операції з обробки даних виконується підрядником/третьою стороною (обробником даних)?	Коли обробка виконується зовнішніми підрядниками, організація може частково втратити контроль над цими даними. Крім того, можуть виникнути додаткові загрози безпеці через загрози, властиві цим підрядникам. Це важливо для організація для вибору підрядників, які можуть запропонувати високий рівень безпеки, і чітко визначити, яка частина обробки їм доручена, зберігаючи максимально високий рівень контролю.
3	Чи є зобов'язання сторін/осіб, залучених до обробки персональних даних, неоднозначними чи нечітко визначеними?	Коли співробітники не мають чіткої інформації про свої обов'язки, загрози від випадкового зловживання (наприклад, розголошення або знищення) даних значно зростають.
4	Чи персонал, який бере участь в обробці персональних даних, не знайомий з питаннями інформаційної безпеки?	Коли співробітники не знають про необхідність застосування заходів безпеки, вони можуть випадково створити додаткові загрози для системи. Навчання може значною мірою сприяти тому, щоб співробітники дізналися про їхні зобов'язання щодо захисту даних, а також про застосування певних заходів безпеки.
5	Чи особи/сторони, залучені до операції з обробки даних, нехтують безпечним зберіганням та/або знищенням персональних даних?	Багато порушень персональних даних відбуваються через відсутність заходів фізичного захисту, таких як замки та системи безпечного знищення. Паперові файли, як правило, є частиною вхідних або вихідних даних інформаційної системи, можуть містити особисті дані, а також повинні бути захищені від несанкціонованого розкриття та повторного використання.

Таблиця 3.6

Оцінка ймовірності виникнення загрози , пов'язаної із особливістю бізнес-сектора та масштабу даних, що обробляються

D. Бізнес-сектор та масштаб даних, що обробляються		
1	Чи вважаєте ви свій бізнес-сектор схильним до кібератак?	Якщо атаки на безпеку вже відбулися в певному секторі бізнесу, є ознака того, що організації, ймовірно, потрібно буде вжити додаткових заходів, щоб уникнути подібної події.
2	Чи зазнавала ваша організація будь-якої кібератаки чи іншого типу порушення безпеки протягом останніх двох років?	Якщо організація вже була атакована або є ознаки того, що це могло статися, необхідно вжити додаткових заходів, щоб запобігти подібним подіям у майбутньому.
3	Чи отримували ви сповіщення та/або скарги щодо безпеки IT-системи (яка використовується для обробки персональних даних) протягом останнього року?	Помилки/вразливості безпеки можна використовувати для здійснення атак (кібернетичних або фізичних) на системи та служби. Слід розглянути бюлетені безпеки, що містять важливу інформацію про вразливі місця, які можуть вплинути на вищезгадані системи та служби.
4	Чи стосується операція обробки великого обсягу фізичних осіб та/або персональних даних?	Тип і обсяг персональних даних (масштаб) можуть зробити операцію обробки привабливою для зловмисників (через невід'ємну цінність цих даних).
5	Чи існують найкращі практики безпеки, характерні для вашого бізнес-сектору, яких не дотримуються належним чином?	Специфічні для сектора заходи безпеки зазвичай пристосовуються до потреб (і ризиків) конкретного сектора. Відсутність дотримання найкращих практик може свідчити про погане керування безпекою.

Дотримуючись цього підходу, рівень ймовірності виникнення загрози може бути визначений для кожної з областей оцінювання таким чином:

- Низький: загроза навряд чи реалізується.
- Середній: існує достатній шанс, що загроза матеріалізується.
- Високий: загроза, ймовірно, матеріалізується

Потім таблиці 3.7 і 3.8 можна використовувати для документування ймовірності виникнення загрози для кожної області оцінювання та відповідно обчислити її кінцеве значення.

Таблиця 3:7

Оцінка ймовірності виникнення загроз у певній сфері

Предметна область оцінки	Ймовірність	
	Рівень	Оцінка
Мережеві та технічні ресурси	Низький	1
	Середній	2
	Високий	3
Процеси/процедури, пов'язані з обробкою персональних даних	Низький	1
	Середній	2
	Високий	3
Сторони/люди, залучені до процесу обробки персональних даних	Низький	1
	Середній	2
	Високий	3
Бізнес-сектор та масштаб переробки	Низький	1
	Середній	2
	Високий	3

Відповідно, додавши кількість балів, що відповідає оцінці ризику за кожним з напрямів, отримаємо результуюче значення, що можна інтерпретувати як ймовірність появи загрози в системі загалом. Відповідно до розподілу, що наведено в таблиці 3.8. можна визначити загальну оцінку виникнення загрози в системі (низька, середня чи висока).

Таблиця 3.8

Загальна оцінка виникнення загрози

Загальна сума балів ймовірності появи загрози	Рівень вірогідності виникнення загроз
4 - 5	Низький
6 - 8	Середній
9 -12	Високий

Крок 4: Оцінка ризику

Після оцінки впливу операції обробки персональних даних та відповідної ймовірності виникнення загрози можлива остаточна оцінка ризику (табл. 3.9).

Таблиця 3.9

Оцінка ризику витоку персональних даних в системі

РІВЕНЬ ВПЛИВУ

ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ		Низький	Середній	Високий/Дуже високий
	Низький			
	Середній			
	Високий			

Легенда:

Низький | Середній | Високий

Незалежно від результату цієї дії, МСП може коригувати отриманий рівень ризику, беручи до уваги специфічні характеристики операції обробки даних (які, можливо, були упущені під час процесу оцінки) та надаючи належне обґрунтування для цього коригування.

Крок 5: Заходи безпеки

Після оцінки рівня ризику МСП може приступити до вибору відповідних заходів безпеки для захисту персональних даних.

Рекомендації ENISA розглядають дві великі категорії заходів (організаційні та технічні), які додатково поділяються на спеціальні підкатегорії. У кожній підкатегорії представлено заходи для рівня ризику (низький - зелений, середній - жовтий, високий - червоний). Щоб досягти масштабованості, передбачається, що всі заходи, описані під низьким рівнем (зелений), застосовні до всіх рівнів. Подібним чином заходи, представлені під середнім рівнем (жовтий), також застосовуються до високого рівня ризику. Заходи, представлені під високим рівнем (червоний), не застосовуються до будь-якого іншого рівня ризику (Додаток 3) [19].

4. Оцінка ризиків опрацювання персональних даних для конкретних варіантів використання (Use Cases)

4.1. Use Case: Процеси у відділі кадрів підприємства

Типове МСП оброблятиме персональні дані своїх працівників у межах діяльності відділу кадрів (HR) та бухгалтерії.

Залежно від характеру ділової діяльності, розміру та внутрішньої організації малого та середнього підприємства, діяльність відділу людських ресурсів може стосуватися додаткових процедур, обробляти більшу чи меншу кількість персональних даних або для інших цілей [20]. Зокрема, управління заробітною платою, управління відпустками та відсутністю, влаштування на роботу нових працівників, оцінка персоналу. Інші операції можуть включати дані про здоров'я персоналу (наприклад, щорічні медичні огляди, які вимагає роботодавець, навчання персоналу тощо) [21]. Кожна з цих задач має власні особливості з точки зору опрацювання персональних дані, які визначаються типом даних, що опрацьовуються, метою їх обробки та аудиторії, чиї персональні дані збираються.

Розглянемо детальніше оцінювання ризиків при роботі із персональними даними відповідно до описаної раніше методології ENISA для різного типу завдань відділу кадрів та бухгалтерії.

4.1.1. Управління заробітною платою

В межах цього сценарію використання ми розглядаємо як приклад роздрібне МСП, яке обробляє персональні дані своїх працівників для нарахування та виплати зарплат, пільг і соціального забезпечення. Особисті дані, які підлягають обробці, це: контактна інформація (така як прізвище та ім'я, адреса, номери телефонів), номер соціального страхування, ідентифікаційний номер, дата працевлаштування, інформація про посаду та зарплату. Операція обробки полегшується IT-системою відділу кадрів, яка розгорнута в приміщенні МСП, і нею керує спеціаліст відділу кадрів. Існує спеціальна політика використання. Однак немає жодних спеціальних правил щодо збереження та знищення даних. Обробка персональних даних обмежена приміщеннями компанії. Ближче до кінця кожного місяця спеціаліст з кадрів подає до фінансових установ та інституту соціального

захисту звіти про всіх працівників. Незважаючи на те, що співробітник відділу кадрів підписав застереження про конфіденційність, нещодавно для працівників SME не було проведено жодних тренінгів із безпеки чи захисту даних.

1) Визначення операції обробки та її контексту

Конкретну операцію обробки даних можна деталізувати таким чином:

Таблиця 4.1

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	УПРАВЛІННЯ ЗАРОБІТНОЮ ПЛАТНЕЮ СПІВРОБІТНИКІВ	
Персональні дані обробляються	Контактна інформація (прізвище та ім'я, адреса, номер телефону), номер соціального страхування, податковий ідентифікатор, дата роботи, інформація про зарплату	
Мета обробки	Розрахунок заробітної плати (виплата заробітної плати, допомоги та внесків на соціальне страхування)	
Суб'єкт даних	Співробітники	
Засоби обробки	IT-система людських ресурсів	
Одержувачі даних	Зовнішні	Фінансові установи
	Зовнішні	Система соціального страхування
Персональні дані обробляються	Власний (без процесора даних)	

2) Оцінка впливу

Дотримуючись підходу, описаного в розділі 3, можна зробити наступний аналіз:

✓ Втрата конфіденційності

У межах операції з обробки заробітної плати співробітників, як описано вище, вплив втрати конфіденційності в основному пов’язаний з можливим ненавмисним розголошенням доходів (та інших відповідних даних) третім сторонам [22]. Це може наразити суб’єкта даних на наслідки, починаючи від дискомфорту, що виникає через публічне знання власних особистих даних, і навіть, в окремих випадках, до потенційного ризику цілеспрямованих атак з боку крадіжок або шукачів грошей. Це може бути більше, ніж просто роздратування, і, таким чином, вплив втрати конфіденційності можна встановити на СЕРЕДНИЙ.

✓ Втрата цілісності та доступності

Втрата цілісності та/або доступності загалом може вважатися НИЗЬКОЮ, оскільки очікується, що суб’єкти даних зіткнуться з незручностями (наприклад, необхідно буде повторно надіслати інформацію або не зможуть вчасно отримати щомісячний платіж), але проблеми можна швидко подолати. Більш серйозні наслідки від втрати конфіденційності можуть бути встановлені на СЕРЕДНІЙ, якщо наслідки для суб’єктів даних є більш стійкими з часом (наприклад,

неодноразова затримка виплати зарплати); однак це не вважається загальним випадком у нашому прикладі [23].

В таблиці 4.2. узагальнено результати описаного вище аналізу.

Таблиця 4.2

Оцінка впливу операцій обробки персональних даних

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Середня	**Низька**	**Низька**
	Загальна оцінка впливу	**СЕРЕДНЯ**

Загальний результат оцінки впливу є найвищим визначеним. Тому загальний вплив у цьому конкретному випадку оцінюється як СЕРЕДНІЙ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може бути вищим від обчисленого вище.

Прикладом такого випадку може бути систематична обробка конкретних даних про здоров'я/інвалідність (наприклад, через особливі привілеї/робочі умови, такі як додаткові надбавки для працівників із вадами чи знедоленими працівниками). У такому випадку контролер даних повинен розглянути, чи встановлено рівень впливу на ВИСОКИЙ.

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в Розділі 3, можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання:

- ***Мережа та технічні ресурси:*** ймовірність виникнення загрози НИЗЬКА, оскільки система не підключена до Інтернету та не дозволяє отримати доступ з Інтернету до внутрішніх ресурсів та інших IT-систем. Для цього варіанту використання передбачається, що захист від несанкціонованого доступу здійснюється відповідно до найкращих практик безпеки ІКТ.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози НИЗЬКА, якщо припустити, що ролі та обов'язки співробітника відділу кадрів чітко визначені відповідно до прийнятної політики використання, обробка персональних даних обмежена приміщеннями організації та файли журналу створюються для будь-якої обробки.
- ***Сторони/люди, які беруть участь в обробці персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки співробітники відділу кадрів не пройшли відповідної підготовки з інформаційної безпеки, і немає впевненості, що персональні дані

завжди безпечно обробляються та/або знищуються (через відсутність відповідних політики – див. опис варіантів використання).

- ***Бізнес-сектор і масштаби обробки:*** ймовірність виникнення загрози НИЗЬКА, оскільки бізнес-сектор МСП загалом не вважається схильним до кібератак. Передбачається, що в минулому не було відомо про порушення персональних даних, і операція обробки обмежена лише працівниками SME.

Таблиця 4.3

Опис операцій обробки персональних даних

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Низький	1
Процеси/Процедури, пов'язані з обробкою персональних даних	Низький	1
Сторони/люди, залучені до обробки персональних даних	Середній	2
Сфера діяльності та масштаби переробки	Низький	1
Загальна ймовірність виникнення загрози	Низький (5)	

Після вищезгаданої оцінки загальна ймовірність виникнення загрози розраховується як НИЗЬКА.

4) Оцінка ризику та прийняття заходів безпеки.

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 3.4.

Таблиця 4.4

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	Середній	Високий/Дуже високий
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	Низький		X	
	Середній			
	Високий			

Загальний ризик для цього конкретного випадку зазвичай вважається СЕРЕДНІМ. Додаток 3: (A.1 і A.2) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути іншим (вищим) за особливих умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози.

4.1.2. Набір персоналу

У цьому варіанті використання ми знову розглянемо МСП, описане у розділі 4.1. Підбір персоналу – це процес, яким управляє відділ кадрів, і складається з численних організаційних заходів, спрямованих на підбір людей, які мають певні навички або здатні виконувати певні завдання. Після публікації оголошення про вакансію кандидатам пропонується подати заявку в електронному вигляді разом із докладною навчальною програмою, вказавши академічну освіту та кваліфікацію, досвід роботи, додаткову професійну чи академічну підготовку, сімейний стан та особисті дані, такі як ім'я та прізвище. адреса, телефони, дата народження. Приймальна комісія розглядає та оцінює заявки та складає список кандидатів, яких запросять на співбесіду. Під час співбесіди члени відбіркової комісії записують результати роботи кандидата і наприкінці складають докладний звіт, який надається вищому керівництву. Обробку полегшує IT-система, яка підтримує подання заяв, складання короткого списку кандидатів та звіти про співбесіди та керується співробітником відділу кадрів.

1) Визначення операції обробки та її контексту

Відповідно до методології, описаної в розділі 3 (крок 1), для конкретної предметної області та конкретної задачі, в якій відбувається обробка даних, необхідно визначити типи персональних даних, що обробляються, мету такої обробки, суб'єктів та одержувачів даних. Ця інформація структурована у таблиці 4.5.

Таблиця 4.5

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	УПРАВЛІННЯ ЗАРОБІТНОЮ ПЛАТНЕЮ СПІВРОБІТНИКІВ	
Персональні дані обробляються	Академічна освіта та кваліфікація, досвід роботи, подальша професійна або академічна підготовка, сімейний стан, ім'я та прізвище, адреса, номери телефонів, дата народження, записи/звіт про співбесіду	
Мета обробки	Управління відбором кандидатів на роботу	
Суб'єкт даних	Кандидати на роботу	
Засоби обробки	Рекрутингова IT платформа	
Одержувачі даних	Внутрішні	Вище керівництво
Персональні дані обробляються	Власний (без процесора даних)	

2) Оцінка впливу

Дотримуючись підходу, представленого в розділі 3 (крок 2), необхідно провести зробити такий аналіз:

✓ **Втрата конфіденційності**

В межах операції з найму співробітників, як описано вище, втрата конфіденційності може призвести до розголошення даних кандидатів, що потенційно призведе до дискримінації або наклепу. Це в основному пов'язано з результатами оцінювання, які можуть дати оцінку професійного досвіду та спроможності кандидата, а також інших особистих якостей (наприклад, здатність добре спілкуватися або чітко висловлюватись) [24]. Для цілей цього варіанту використання ми припускаємо, що рекрутингова платформа передбачає структуровану оцінку кандидатів на основі конкретних професійних критеріїв і не включає інші типи оцінок особистості чи характеристик кандидата (наприклад, психологічний профіль) . Відповідно до вищезазначеного опису очікується, що суб'єкт даних зіткнеться з незначними чи серйозними незручностями через втрату конфіденційності, що в деяких випадках може вплинути на його здатність працевлаштуватися. Таким чином, рівень впливу для цього випадку загалом можна вважати СЕРЕДНІМ.

✓ **Втрата цілісності**

Рівень впливу, спричинений втратою цілісності, вважається СЕРЕДНІМ, оскільки несанкціонована зміна персональних даних, що обробляються, може або перешкодити успішному виконанню процедури найму, або внести зміни до звіту про відповідність вимогам/співбесіди кандидата (і, таким чином, його можливості отримати найнятий).

✓ **Втрата доступності**

Рівень впливу внаслідок втрати цілісності вважається НИЗЬКИМ, оскільки очікується, що суб'єкти даних зіткнуться з незначними незручностями через затримку процесу, яка, однак, не буде визнана недійсною. В таблиці 4.6. узагальнено результати проведеного аналізу.

Таблиця 4.6

Визначення загальної оцінки впливу

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Середня	**Середня**	**Низька**
	Загальна оцінка впливу	**СЕРЕДНЯ**

Отже, загальний результат оцінки впливу є найвищим визначеним, тому загальний оцінений вплив є СЕРЕДНІМ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може бути вищим від обчисленого вище. Наприклад, це може бути випадок процесу оцінювання, що включає психологічні тести або специфічні поведінкові характеристики кандидатів. Інший випадок може бути, якщо також обробляються персональні дані, пов'язані з інвалідністю, етнічним походженням тощо.

3) Імовірність виникнення загрози

На основі відповідей на запитання, які було розглянуто у розділі 3 (крок 3), зробимо оцінку для кожного виміру середовища операцій обробки:

- ***Мережа та технічні ресурси:*** ймовірність виникнення загрози НИЗЬКА, оскільки обробка не виконується через Інтернет, а платформа оцінки є спеціальною системою, яка не пов'язана з іншими IT-системами МСП. Як і в попередніх випадках, передбачається, що передові практики застосовуються для запобігання несанкціонованому доступу та, відповідно, захисту даних.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози НИЗЬКА, якщо припустити, що ролі та обов'язки залучених працівників чітко визначені разом із прийнятною політикою використання, обробка персональних даних обмежена приміщеннями організації та файли журналу створюються для будь-якої обробки.
- ***Сторони/люди, які беруть участь в обробці персональних даних:*** ймовірність виникнення загрози є СЕРЕДНЬОЮ, оскільки включає велику кількість працівників, залучених до обробки (спеціалісти з персоналу, комісія з відбору, вище керівництво), і передбачається, що не всі працівники, залучені до обробки пройшли відповідне навчання з інформаційної безпеки.
- ***Бізнес-сектор і масштаби обробки:*** ймовірність виникнення загрози НИЗЬКА, оскільки бізнес-сектор малого та середнього бізнесу загалом не вважається схильним до кібератак, і не відомо, що в минулому не було порушень персональних даних. Операція обробки обмежена лише працівниками МСП.

Після проведеної оцінки (таблиця 4.7) загальна ймовірність виникнення загрози розраховується як НИЗЬКА.

Таблиця 4.7

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Низький	1
Процеси/Процедури, пов'язані з обробкою персональних даних	Низький	1
Сторони/люди, залучені до обробки персональних даних	Середній	2
Сфера діяльності та масштаби переробки	Низький	1
Загальна ймовірність виникнення загрози	**Низький (5)**	

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 3 (крок 4).

Таблиця 4.8

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	Середній	Високий/Дуже високий
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	Низький		X	
	Середній			
	Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається СЕРЕДНІМ. Додаток А: (А.1 і А.2) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Слід зауважити, що ризик може бути іншим (вищим) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози [25]. Наприклад, якщо кандидати мають доступ до своїх звітів про оцінку безпосередньо через IT-платформу найму, ймовірність виникнення загрози, ймовірно, збільшиться до ВИСОКОЇ. Див. також відповідні міркування в розділі 3.3.2 щодо оцінки впливу.

4.1.3. Оцінка співробітників

У межах цього варіанту використання розглянемо МСП, що спеціалізується на IT-продуктах і відповідних консультаційних послугах. Щороку кожен співробітник оцінюється лінійним керівником за попередньо визначеними та попередньо узгодженими критеріями, пов'язаними з його/її продуктивністю та професійними характеристиками, які

включають надійність, орієнтацію на користувачів/клієнтів, організованість, навички міжособистісного спілкування, гнучкість, автономію, навички письмового та усного спілкування та командний дух. Обробка виконується співробітником відділу кадрів і лінійними керівниками за допомогою електронних інструментів і паперової документації. Лінійний керівник складає першу версію звіту на папері та обговорює результати зі співробітником. Остаточна версія звіту належним чином підписується та подається в електронному вигляді до відділу кадрів, а резюме та висновки/результати звіту також подаються в електронному вигляді [26].

1) Визначення операції обробки та її контексту

Відповідно до методології, описаної в розділі 3 (крок 1), для даної предметної області та конкретної задачі, в якій відбувається обробка даних, необхідно визначити типи персональних даних, що обробляються, мету такої обробки, суб'єктів та одержувачів даних. Ця інформація структурована у таблиці 4.9.

Таблиця 4.9

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	УПРАВЛІННЯ ЗАРОБІТНОЮ ПЛАТНЕЮ СПІВРОБІТНИКІВ	
Персональні дані обробляються	Ім'я та прізвище, посада в МСП, дата працевлаштування, трудова історія, технічні навики, знання та поведінка (звіти про оцінку ефективності роботи)	
Мета обробки	Оцінка результативності та професійних характеристик, що виникають при виконанні роботи	
Суб'єкт даних	Працівники	
Засоби обробки	ІТ-система людських ресурсів	
Одержувачі даних	Внутрішні	Лінійні менеджери
Персональні дані обробляються	Власний (без процесора даних)	

2) Оцінка впливу

Дотримуючись підходу, представленого в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності

У рамках цієї операції обробки слід брати до уваги, що оцінка персоналу надає детальний професійний профіль працівника шляхом приписування кількісних і якісних значень її продуктивності на роботі. Хоча оцінка може бути обмежена продуктивністю роботи, у ході вправи можуть з'явитися характеристики інших осіб, створюючи незначний ризик того, що інформація, що стосується поведінки

та особистості працівників, також буде оброблена. Втрата конфіденційності цих даних може варіюватися від простого дискомфорту до ганьби чи навіть обмежень для працівника, напр. при пошуку нової роботи. Тому вплив втрати конфіденційності вважається СЕРЕДНІМ.

✓ **Втрата цілісності**

Втрату цілісності загалом можна вважати СЕРЕДНЬОЮ, оскільки очікується, що суб'єкти даних зіткнуться зі значними незручностями, включаючи неналежну оцінку або відсутність або затримки в отриманні переваг від результатів оцінки.

✓ **Втрата доступності**

Загалом втрату доступності можна вважати НИЗЬКОЮ, оскільки очікується, що суб'єкти даних зіткнуться з незначними незручностями через затримку процесу, яка, однак, не буде визнана недійсною. Наступна таблиця підсумовує вищезгаданий аналіз [27].

Таблиця 4.10

Визначення загальної оцінки впливу

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Середня	**Середня**	**Низька**
	Загальна оцінка впливу	**СЕРЕДНЯ**

Загальний результат оцінки впливу є найвищим визначеним, тому загальний оцінений вплив є СЕРЕДНІМ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може бути вищим від обчисленого вище. Прикладом такого випадку може бути, коли: специфічний робочий контекст вимагає оцінки психологічних характеристик співробітників або коли під час процесу оцінки включені конфіденційні дані (наприклад, стосовно осіб з обмеженими можливостями) [28].

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в Розділі 2.1.3, можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання:

- ***Мережа та технічні ресурси:*** ймовірність виникнення загрози НИЗЬКА, оскільки система не підключена до Інтернету та не дозволяє отримати доступ з Інтернету до внутрішніх ресурсів та інших IT-систем. Для цього випадку використання передбачається, що несанкціонований доступ запобігається на основі відповідних передових практик.

- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ, якщо припустити, що політика використання чітко не визначена, а обробка інформації не обов'язково обмежується приміщеннями організації (паперовий процес) [29].
- ***Сторони/люди, які беруть участь в обробці персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки припускається (з опису випадку), що немає спеціальних правил щодо безпечного зберігання та видалення даних (особливо, коли частина процесу здійснюється на паперових носіях).
- ***Бізнес-сектор і масштаби обробки:*** ймовірність виникнення загрози НИЗЬКА, оскільки бізнес-сектор малого та середнього бізнесу загалом не вважається схильним до кібератак, і передбачається, що раніше не було порушень персональних даних. Операція обробки обмежена лише працівниками МСП.

Таблиця 4.11

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Низький	1
Процеси/Процедури, пов'язані з обробкою персональних даних	Низький	2
Сторони/люди, залучені до обробки персональних даних	Середній	2
Сфера діяльності та масштаби переробки	Низький	1
Загальна ймовірність виникнення загрози	**СЕРЕДНІЙ (6)**	

Після вищезгаданої оцінки загальна ймовірність виникнення загрози розраховується як СЕРЕДНІЙ.

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 3 (крок 4).

Таблиця 4.12

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	Середній	Високий/Дуже високий
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	Низький			
	Середній		X	
	Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається СЕРЕДНІМ. Додаток А: (А.1 і А.2) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути іншим (вищим) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози (див. також відповідні міркування в розділі 3.3.2).

4.2. Use Case: Управління клієнтами, маркетинг і постачальники

Типове МСП оброблятиме персональні дані своїх клієнтів і здійснюватиме маркетингову діяльність, щоб залучити нових клієнтів. Він також може обробляти персональні дані щодо своїх постачальників. Залежно від характеру господарської діяльності, характеру та обсягу портфеля продуктів і послуг, а також цільового ринку, діяльність може диференціюватись і включати обробку різних типів персональних даних у різних масштабах та/або для різних цілей [30].

4.2.1. Замовлення та доставка товару

Розглянемо роздрібне МСП, яке пропонує товари через спеціальний електронний магазин. Клієнти можуть переглядати доступні товари, додавати їх у кошик і оформляти замовлення. Щоб оформити замовлення, клієнт повинен зареєструватися на платформі електронного магазину (якщо ще не зареєстрований) і надати свої контактні дані (ім'я та прізвище, адреса доставки, номер телефону та адреса електронної пошти). Під час оформлення замовлення зареєстрованим користувачам також пропонується надати платіжні реквізити в окремій формі, яка надається постачальником платіжних послуг. Після успішного розміщення замовлення та підтвердження від постачальника платіжних послуг деталі замовлення передаються до системи планування ресурсів підприємства (ERP), до системи керування відносинами з клієнтами (CRM) і до постачальника послуг доставки. Що стосується використання системи, існує конкретна політика використання, а передові практики впроваджуються та підтримуються. Однак немає конкретних правил щодо збереження та знищення даних, і не всі залучені працівники пройшли відповідне навчання з інформаційної безпеки.

1) Визначення операції обробки та її контексту

Конкретну операцію обробки даних можна деталізувати таким чином, як зображено в таблиці 4.13.

Таблиця 4.13

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	ЗАМОВЛЕННЯ ТА ДОСТАВКА ТОВАРУ	
Персональні дані обробляються	Контактна інформація (прізвище та ім'я, адреса, номер телефону) платіжні дані (кредитна картка, реквізити банківського рахунку)	
Мета обробки	Замовлення та доставка товару	
Суб'єкт даних	Клієнти	
Засоби обробки	Система управління замовленнями	
Одержувачі даних	Зовнішні	постачальник платіжних послуг
	Зовнішні	постачальник послуг доставки
	Внутрішні	система управління взаємовідносинами з клієнтами (CRM).
	Внутрішні	Система планування ресурсів підприємства (ERP).
Персональні дані обробляються	Внутрішні та зовнішні сторони	

2) Оцінка впливу

Дотримуючись підходу, представленого в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності та цілісності

У межах конкретної операції обробки, як описано раніше, вплив від втрати конфіденційності та/або цілісності вважається СЕРЕДНІМ, оскільки несанкціоноване розкриття та/або зміна оброблених персональних даних, у тому числі фінансових даних, може призвести до значних незручностей для суб'єкт даних (який можна відновити, доклавши певних зусиль).

✓ Втрата доступності

Рівень впливу внаслідок втрати доступності вважається НИЗЬКИМ, оскільки очікується, що недоступність персональних даних, що обробляються, призведе лише до незначних незручностей для суб'єкта даних, які можна легко подолати, напр. затримка доставки товару.

Таблиця 4.14

Визначення загальної оцінки впливу

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Середня	**Середня**	**Низька**
	Загальна оцінка впливу	**СЕРЕДНЯ**

Таким чином, загальний результат оцінки впливу є СЕРЕДНІМ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може відрізнятися (вищим) від обчисленого вище. Прикладом може бути випадок, коли товари, доступні для замовлення, можуть розкривати конфіденційні дані про особу, напр. щодо її здоров'я, сексуальних або політичних і релігійних уподобань.

3) Імовірність виникнення загрози

На основі питань і підходу, наведених в розділі 3 (крок 3), можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання. Результати оцінки зведено в таблицю 4.15.

Таблиця 4.15

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Середній	2
Процеси/Процедури, пов'язані з обробкою персональних даних	Низький	1
Сторони/люди, залучені до обробки персональних даних	Середній	2
Сфера діяльності та масштаби переробки	Середній	2
Загальна ймовірність виникнення загрози	**СЕРЕДНІЙ (7)**	

- ***Мережа та технічні ресурси:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки частина обробки персональних даних виконується через Інтернет, а система обробки взаємопов'язана з іншими внутрішніми та зовнішніми ІТ-системами. Для цього випадку використання передбачається, що несанкціонований доступ до особистих даних запобігає на основі відповідних передових практик.
- ***Процеси/процедури, пов'язані з обробкою персональних даних***: ймовірність виникнення загрози НИЗЬКА, оскільки припускається, що ролі та обов'язки співробітників чітко визначені відповідно до прийнятної політики використання, обробка персональних даних обмежена приміщеннями організація та файли журналу створюються для будь-якої виконаної обробки.
- ***Сторони/люди, які беруть участь в обробці персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки не всі співробітники пройшли відповідне навчання з інформаційної безпеки, і не гарантується, що персональні дані завжди безпечно обробляються та/або знищуються.
- ***Бізнес-сектор і масштаб обробки***: ймовірність виникнення загрози СЕРЕДНЯ, оскільки бізнес-сектор, як бізнес-сектор МСП (електронний

магазин), загалом можна вважати схильним до кібератак, а операція обробки стосується великої кількості фізичних осіб. Однак для конкретного випадку передбачається, що порушення персональних даних уже мало місце в минулому.

Після вищезгаданої оцінки загальна ймовірність виникнення загрози розраховується як СЕРЕДНЯ.

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 2.1.4.

Таблиця 4.16

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	**Середній**	**Високий/Дуже високий**
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	**Низький**			
	Середній		X	
	Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається СЕРЕДНІМ. Додаток А: (А.1 і А.2) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути іншим (вищим) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози (див. також відповідні міркування в розділі 3.3.2).

4.2.2. Постачальники послуг і товарів

Розглянемо роздрібне МСП, описане в 4.2, яке купує послуги та товари, необхідні як для повсякденної роботи, так і для продажу товарів. У певних випадках ці процедури можуть включати обробку персональних даних, наприклад, контактних даних конкретних працівників, які працюють на постачальників, або контактних і фінансових даних осіб, які мають прямий договір із МСП (тобто безпосередньо діють як постачальники товарів чи послуг) [31].

Операція обробки підтримується IT-системою, підключеною до системи планування ресурсів підприємства (ERP) і системи бухгалтерського обліку. Оброблені персональні дані включають назву компанії та контактні дані, фінансові дані (податковий номер, банківський рахунок), фотографії

співробітників та облікові дані доступу (для персоналу, який працює в приміщеннях) [32].

Усі ділові відносини між МСП і постачальниками відбуваються за допомогою CRM через екстранет, безпосередньо на платформах постачальників. Оплата здійснюється за допомогою дистанційного банківського обслуговування. Існує офлайн-платформа, де рахунки за доставку та рахунки-фактури завантажуються протягом ночі партіями. Адміністративне спілкування з постачальниками відбувається через звичайну електронну пошту.

1) Визначення операції обробки та її контексту

Конкретну операцію обробки даних можна деталізувати таким чином, як зображено в таблиці 4.17.

Таблиця 4.17

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	ПОСТАЧАЛЬНИКИ ПОСЛУГ І ТОВАРІВ	
Персональні дані обробляються	Ім'я та прізвище, контактна інформація, податкова та банківська інформація (для постачальника), фото та облікові дані (для персоналу, який працює на території).	
Мета обробки	Управління постачанням	
Суб'єкт даних	Співробітники, які працюють на постачальників товарів і послуг	
Засоби обробки	IT-система	
Одержувачі даних	Зовнішні	постачальник платіжних послуг
	Зовнішні	CRM постачальники
	Внутрішні	система управління взаємовідносинами з клієнтами (CRM).
	Внутрішні	Система планування ресурсів підприємства (ERP).
Персональні дані обробляються	Внутрішні та зовнішні сторони	

2) Оцінка впливу

Дотримуючись підходу, описаного в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності

У межах конкретної операції обробки вплив від втрати конфіденційності вважається НИЗЬКИМ, оскільки в деяких випадках особи можуть зіткнутися з

незначними проблемами через те, що треті сторони отримують доступ до їхніх оброблених персональних даних невідомим чином.

✓ **Втрата цілісності та доступності**

Вплив від втрати цілісності та/або доступності вважається НИЗЬКИМ, оскільки окремі особи можуть зіткнутися з незручностями, пов'язаними із затримкою досягнення ділових відносин між компаніями, або можуть перенаправити замовлені товари на неправильну адресу або взагалі не бути доставленими, але це може можна подолати з обмеженими зусиллями.

Таблиця 4.18

Визначення загальної оцінки впливу операцій обробки персональних даних

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Низька	**Низька**	**Низька**
	Загальна оцінка впливу	**НИЗЬКА**

Загальний результат оцінки впливу НИЗЬКИЙ.

Додатково до припущень, зроблених у цьому випадку використання, можуть бути випадки, коли загальний вплив може відрізнятися (вищий) від обчисленого вище. Прикладом такого випадку може бути ситуація, коли компанія працює в «делікатному» середовищі, і, таким чином, розголошення імен співробітників може поставити їх під загрозу (наприклад, у військовому середовищі).

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в розділі 3 (крок 3), можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому варіанті використання:

- ***Мережа та технічні ресурси:*** Імовірність виникнення загрози СЕРЕДНЯ, оскільки система підключена до Інтернету та є можливість надати доступ до внутрішньої системи обробки персональних даних через Інтернет. Однак для запобігання несанкціонованому доступу використовуються найкращі методи.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози НИЗЬКА, оскільки передбачається, що ролі та обов'язки персоналу чітко визначені відповідно до прийнятної політики використання, працівникам заборонено приносити власні пристрої та зберігати , передавати або іншим чином обробляти персональні дані за межами приміщень організації, а файли журналів створюються для будь-якої обробки, що виконується.
- ***Сторони/люди, залучені до обробки персональних даних:*** ймовірність виникнення загрози для НИЗЬКА, оскільки працівники не

можуть передавати, зберігати чи іншим чином обробляти персональні дані за межами приміщень організації за прийнятного використання мережі, системи та фізичних ресурсів. всередині організації чітко визначено, а працівники, задіяні в операції обробки даних, безпечно зберігають і знищують персональні дані.

- ***Бізнес-сектор і масштаб обробки:*** ймовірність виникнення загрози НИЗЬКА, оскільки бізнес-сектор малого та середнього бізнесу загалом не вважається схильним до кібератак, інциденту порушення безпеки або скарги не надходили протягом останніх двох років, а операція обробки не стосується великої кількості осіб.

Таблиця 4.19

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Середній	2
Процеси/Процедури, пов'язані з обробкою персональних даних	Низький	1
Сторони/люди, залучені до обробки персональних даних	Низький	1
Сфера діяльності та масштаби переробки	Низький	1
Загальна ймовірність виникнення загрози	**Низький (5)**	

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 2.1.4.

Таблиця 4.20

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	Середній	Високий/Дуже високий
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	Низький	X		
	Середній			
	Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається НИЗЬКИМ. Додаток А (А.1) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути різним (середній або навіть високий) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних (див. також відповідні міркування в розділі 4.3.2).

4.3. Use Case: Безпека та захист

У межах цього сценарію використання розглянемо консалтингову компанію (SME), яка обробляє персональні дані своїх співробітників і відвідувачів для контролю фізичного доступу в свої приміщення, щоб гарантувати, що лише уповноважені особи мають доступ до та поза конкретними областями.

4.3.1. Управління доступом

Розгорнута система контролю доступу складається з зчитувачів RFID-карт, встановлених у заздалегідь визначених точках, RFID-карт і платформи керування контролем доступу [33].

Кожен співробітник, приступаючи до виконання своїх обов'язків, реєструється на платформі управління контролем доступу та отримує унікальне буквено-цифрове значення, яке зберігається на картці RFID. Особисті дані, які використовуються під час реєстрації, включають ім'я та прізвище, дату працевлаштування, посаду в організації, закінчення роботи (якщо це передбачено договором) та фотографію профілю. RFID-картка кожного співробітника персоналізована, оскільки на картці друкуються ім'я працівника та його фотографія профілю [34].

Для кожного типу посади в організації (адміністрація, керівник, підтримка секретаріату тощо) визначені спеціальні права доступу [35]. Щоразу, коли працівник проводить свою картку проти зчитувача, платформа перевіряє права та відповідно надає доступ до приміщення. Кожна спроба реєструється на платформі, і в разі спроби несанкціонованого доступу офіцер служби безпеки повідомляється. Відвідувачам також видаються відповідні анонімні RFID-карти відвідувачів, які попередньо налаштовані на доступ лише до кімнат для переговорів.

Після прибуття відвідувача офіцер безпеки реєструє на платформі ім'я та прізвище відвідувача, ім'я та прізвище супроводжуючого працівника та очікувану тривалість візиту та тимчасово призначає відвідувачу RFID-картку. Після від'їзду або закінчення терміну візиту картка анулюється та повертається офіцеру служби безпеки. Співробітники служби безпеки, які керують платформою, пройшли спеціальну підготовку щодо функцій платформи та їхніх обов'язків, і передбачається дотримання найкращих практик.

1) Визначення операції обробки та її контексту

Операцію обробки персональних даних для цієї задачі можна деталізувати таким чином, як зображено в таблиці 4.21.

Таблиця 4.21

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	УПРАВЛІННЯ ДОСТУПОМ	
Персональні дані обробляються	Для співробітників: ім'я та прізвище, дата працевлаштування, посада в організації, закінчення роботи, фото профілю.	
Мета обробки	Для відвідувачів: ім'я та прізвище, дата і час візиту, очікуваний час від'їзду.	
Суб'єкт даних	Безпека контролю фізичного та логічного доступу	
Засоби обробки	Співробітники, відвідувачі	
Одержувачі даних	Внутрішні	Офіцер безпеки
Персональні дані обробляються	Власний (без процесора даних)	

2) Оцінка впливу

Дотримуючись підходу, описаного в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності, цілісності та доступності

У межах конкретної операції обробки вплив від втрати конфіденційності, та/або цілісності та/або доступності вважається НИЗЬКИМ, оскільки очікується, що люди зіткнуться з незначними незручностями, які вони зможуть подолати, доклавши обмежених зусиль. Наприклад, працівники можуть не мати доступу до певних приміщень SME та виконувати свої завдання (втрата цілісності або доступності) або присутність відвідувача в приміщеннях SME може бути розголошена (втрата конфіденційності).

Таблиця 4.22

Визначення загальної оцінки впливу операцій обробки персональних даних

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Низька	**Низька**	**Низька**
	Загальна оцінка впливу	**НИЗЬКА**

Тому загальний результат оцінки впливу НИЗЬКИЙ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може відрізнятися (вищим) від обчисленого вище. Прикладом такого випадку є випадки, коли відвідування приміщень МСП може виявити конкретну конфіденційну інформацію, напр. щодо стану здоров'я, релігійних переконань, політичних чи сексуальних уподобань.

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в Розділі 2.1.3, можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання:

- ***Мережа та технічні ресурси:*** ймовірність виникнення загрози НИЗЬКА, оскільки система не підключена до Інтернету, вона не дає доступу з Інтернету до внутрішніх ресурсів і підключення до інших IT-систем, і передбачається, що найкращі практики використовуються для запобігання несанкціонований доступ до системи.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози НИЗЬКА, оскільки передбачається, що ролі та обов'язки співробітника служби безпеки чітко визначені відповідно до прийнятної політики використання, а файли журналів створюються для будь-якої обробки, що виконується .
- ***Сторони/люди, які беруть участь в обробці персональних даних***: ймовірність виникнення загрози НИЗЬКА, оскільки офіцер служби безпеки не може передавати, зберігати чи іншим чином обробляти персональні дані за межами приміщень організації за прийнятного використання мережі, системи та фізичні ресурси в межах МСП чітко визначені.
- ***Бізнес-сектор і масштаб обробки:*** ймовірність виникнення загрози НИЗЬКА, оскільки бізнес-сектор МСП загалом не вважається схильним до кібератак, порушення персональних даних не відбувалося в минулому, а операція обробки не стосується великої кількості фізичних осіб.

Таблиця 4.23

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Низький	1
Процеси/Процедури, пов'язані з обробкою персональних даних	Низький	1
Сторони/люди, залучені до обробки персональних даних	Низький	1
Сфера діяльності та масштаби переробки	Низький	1
Загальна ймовірність виникнення загрози	**Низький (4)**	

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 3 (крок 4).

Таблиця 4.24

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	Середній	Високий/Дуже високий
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	Низький	X		
	Середній			
	Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається НИЗЬКИМ. Додаток А (А.1) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути іншим (середнім або навіть високим) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози. Наприклад, ймовірність виникнення загрози може бути вищою, якщо МСП працює в «чутливому» середовищі, напр. лабораторія даних про здоров'я (таким чином, збільшуються можливості зловмисних спроб несанкціонованого доступу до приміщень).

Крім того, в цілому Варто зазначити той факт, що контроль доступу є невід'ємним заходом для запобігання несанкціонованому доступу до приміщень і, таким чином, безпосередньо пов'язаний із безпекою та безпекою людей і товарів. Таким чином, знову ж таки залежно від характеру організації, МСП може розглянути можливість підвищення загального ризику до СЕРЕДНЬОГО або навіть ВИСОКОГО.

4.4. Use Case: Сектор охорони здоров'я

В межах цього сценарію використання ми розглядаємо МСП у сфері охорони здоров'я (невелику клініку), яка обробляє персональні дані для надання медичних послуг.

4.4.1. Надання медичних послуг

Для кожного пацієнта, який відвідує клініку для огляду або консультації, створюється (або оновлюється) електронний запис, який містить контактні дані пацієнтів, номер соціального страхування, результати медичних оглядів, патології, алергії, схеми діагнозу та лікування (медичні

інформація) [34]. Завдяки цьому запису лікарі та медсестри мають огляд історії та стану здоров'я пацієнтів і можуть отримати до нього доступ, якщо необхідно, із заздалегідь визначених терміналів у приміщеннях клініки. Перед медичним оглядом або візитом для консультації право пацієнта на таке обстеження або лікування без покриття його вартості підтверджується відповідно до записів системи громадського здоров'я [36]. Якщо пацієнт або обстеження не відповідають вимогам, вартість повідомляється IT-системі бухгалтерського обліку, яка виставляє відповідний рахунок. Після кожного огляду або консультації лікар або медсестра оновлюють записи пацієнтів останніми даними шляхом сканування паперових документів або вручну вставляючи схеми діагностики та лікування.

IT-платформа, що підтримує цю операцію обробки, розміщена на території МСП і недоступна через Інтернет. Для цілей сценарію використання передбачається, що передові практики використовуються для запобігання несанкціонованому доступу до платформи та що періодично організовуються тренінги з підвищення обізнаності щодо безпеки. Проте права доступу до медичних записів пацієнтів чітко не визначені на рівні деталізації, оскільки медсестри та лікарі повинні мати можливість отримати доступ до файлів у будь-який час, а система не підтримує відповідну деталізацію. SME планує мати більш спеціалізовану систему обліку пацієнтів протягом наступних років.

1) Визначення операції обробки та її контексту

Відповідно до методології, описаної в розділі 3 (крок 1), для конкретної предметної області та конкретної задачі, в якій відбувається обробка даних, необхідно визначити типи персональних даних, що обробляються, мету такої обробки, суб'єктів та одержувачів даних.

Додатково варто нагадати, що частина персональних даних, що опрацьовується в сфері охорони здоров'я відповідно до GDPR належить до категорії чутливих даних (результати аналізів, медичних оглядів, біометричні та генетичні дані тощо). Відповідно це накладає додаткові вимоги до процедур їх збереження та обробки, а також значно підвищує ризики, які можуть виникнути у випадку витоку таких персональних даних пацієнтів.

Ця інформація структурована у таблиці 4.25.

Таблиця 4.25

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	НАДАННЯ МЕДИЧНИХ ПОСЛУГ	
Персональні дані обробляються	Контактна інформація (прізвище та ім'я, адреса, номер телефону), номер соціального страхування, результати медичного огляду, патології, алергії, схеми діагностики та лікування (медична інформація), адміністративна та фінансова інформація (рахунки-фактури, документи про госпіталізацію тощо).	
Мета обробки	Надання медичних послуг (діагностика, лікування, госпіталізація)	
Суб'єкт даних	Пацієнти	
Засоби обробки	Медична ІТ система	
Одержувачі даних	Внутрішні	Лікуючі лікарі та медсестри
	Внутрішні	ІТ-система адміністрування та обліку
	Зовнішні	Система охорони здоров'я
Персональні дані обробляються	Власний (без процесора даних)	

2) Оцінка впливу

Дотримуючись підходу, описаного в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності, цілісності та доступності

У межах конкретної операції обробки вплив від втрати конфіденційності вважається ВИСОКИМ, оскільки очікується, що люди зіткнуться із серйозними несприятливими наслідками через несанкціонований доступ до даних, пов'язаних зі здоров'ям. Не менш важливою (ВИСОКА) може бути втрата цілісності, оскільки неправильна медична інформація може навіть поставити під загрозу життя людини. Те ж саме (ВИСОКИЙ) можна стверджувати і щодо втрати доступності, оскільки навіть тимчасова недоступність ІТ-системи клініки може перешкоджати її роботі, таким чином піддаючи пацієнтів серйозному ризику [37].

Таблиця 4.26

Визначення загальної оцінки впливу операцій обробки персональних даних

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Високий	**Високий**	**Високий**
	Загальна оцінка впливу	**ВИСОКИЙ**

Тому загальний результат оцінки впливу є ВИСОКИМ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив можна навіть вважати ДУЖЕ ВИСОКИМ, наприклад, у випадках уразливих категорій суб'єктів даних або неповнолітніх.

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в Розділі 2.1.3, можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання:

- ***Мережа та технічні ресурси:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки система взаємопов'язана з іншими зовнішніми та внутрішніми системами. Однак до даних неможливо отримати доступ через Інтернет, і, згідно з описом варіанту використання, найкращі методи безпеки були застосовані для запобігання несанкціонованому доступу до системи.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози НИЗЬКА, оскільки ролі та обов'язки персоналу чітко визначені разом із прийнятною політикою використання, обробка даних обмежена в приміщеннях SME та файлах журналів створюються для будь-якої обробки, що виконується [38].
- ***Сторони/люди, залучені до обробки персональних даних:*** ймовірність виникнення загрози ВИСОКА, оскільки обробка персональних даних виконується невизначеною кількістю співробітників і немає чіткої політики щодо детального доступу до медичних записів. Однак обов'язки всіх сторін, залучених до обробки, чітко визначені, а семінари для підвищення обізнаності організовуються періодично.
- ***Бізнес-сектор і масштаб обробки:*** ймовірність виникнення загрози ВИСОКА, оскільки бізнес-сектор МСП (охорона здоров'я) загалом вважається схильним до кібератак, а операція обробки стосується великої кількості осіб. Однак припускається, що порушення персональних даних раніше не було.

Таблиця 4.27

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ		ЙМОВІРНІСТЬ	
		РІВЕНЬ	БАЛИ
Мережа та технічні ресурси		Середній	2
Процеси/Процедури, пов'язані з обробкою персональних даних		Низький	1
Сторони/люди, залучені до обробки персональних даних		Високий	3
Сфера діяльності та масштаби переробки		Високий	3
Загальна ймовірність виникнення загрози		**ВИСОКИЙ (9)**	

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 3 (крок 4).

Таблиця 4.28

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	**Середній**	**Високий/Дуже високий**
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	**Низький**			
	Середній			
	Високий			X

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається ВИСОКИМ. Додаток А (А.1, А.2, А.3) можна використовувати для вжиття заходів, що відповідають наявному ризику.

4.5. Use Case: Сектор освіти

В межах цього випадку використання ми розглядаємо.

4.5.1. Комунікаційна платформа для школи раннього розвитку

Розглянемо діяльність дошкільного навчального закладу (дитячого садочку або школи раннього розвитку), яка використовує веб-платформу для взаємодії з батьками. Веб-платформа, що розглядається, використовується для підтримки повсякденної фізичної, інтелектуальної, мовної, емоційної та соціальної діяльності неповнолітніх між школою та батьками. Крім того, платформа може також містити інформацію про стан здоров'я, апетит і характер дітей (надається батьками). Батьки також можуть спілкуватися з вихователем і шукати поради та підтримки щодо того, як виховувати та краще підтримувати когнітивний та соціально-емоційний розвиток своєї дитини.

Платформа розміщена у хостинг-провайдера в ЄС і керується викладачами. Кожен викладач керує та оновлює інформацію про дітей, закріплених за його чи її класом, тоді як загальне адміністрування платформи виконує секретаріат школи. Батьки реєструються на платформі секретаріатом і можуть лише переглядати та оновлювати дані своєї дитини. Передбачається, що для запобігання несанкціонованому доступу використовуються найкращі практики, ролі та обов'язки залучених працівників чітко визначені та

повідомлені, а для всіх дій з обробки даних створюються файли журналів. Платформа обробляє такі дані: ім'я та прізвище, дата народження, домашня адреса, щоденна інформація про продуктивність дитини (включно з харчуванням, заняттями тощо), дані про здоров'я, алергію, непереносимість харчових продуктів, ім'я та останнє ім'я батьків ПІБ, номер телефону батьків (батьків), номер екстреного зв'язку.

1) Визначення операції обробки та її контексту

Відповідно до методології, описаної в розділі 3 (крок 1), для конкретної предметної області та конкретної задачі, в якій відбувається обробка даних, необхідно визначити типи персональних даних, що обробляються, мету такої обробки, суб'єктів та одержувачів даних [39].

Цей варіант використання є цікавим та особливим через те, що в системі зберігаються та опрацьовуються дитячі персональні дані. Нагадаємо, що відповідно до статті 8 GDPR до досягнення дитиною граничного віку (не менше 13 років) згоду на обробку її персональних даних повинні надавати батьки.

Додатково варто нагадати, що частина персональних даних, що опрацьовується в цій системі описують стан здоров'я дитини і відповідно до GDPR належать до категорії чутливих даних [40]. Відповідно це накладає додаткові вимоги до процедур їх збереження та обробки, а також значно підвищує ризики, які можуть виникнути у випадку витоку таких персональних даних пацієнтів.

Ця інформація структурована у таблиці 4.29.

Таблиця 4.29

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	КОМУНІКАЦІЙНА ПЛАТФОРМА ДЛЯ ДИТЯЧОГО САДОЧКА	
Персональні дані обробляються	Ім'я та прізвище, дата народження, домашня адреса, щоденна інформація про успішність дитини (включаючи харчування, заняття тощо), дані про здоров'я, алергію, непереносимість харчових продуктів, ім'я та прізвище батьків (батьків), телефон батьків (батьків). номер, номер екстреного зв'язку	
Мета обробки	Надання освітніх послуг (комунікація повсякденної діяльності та розвитку дитини)	
Суб'єкт даних	Діти і батьки	
Засоби обробки	Веб-інтерфейс	
Одержувачі даних	Внутрішні	Секретаріат, Педагоги
	Зовнішні	Батьки
Персональні дані обробляються	Провайдер веб-хостингу	

2) Оцінка впливу

Дотримуючись підходу, описаного в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності

У рамках конкретної операції обробки вплив від втрати конфіденційності вважається СЕРЕДНІМ, оскільки в деяких випадках особи (діти та батьки) можуть зіткнутися зі значними незручностями внаслідок розкриття певних даних (наприклад, щодо поведінки дитини, її спілкування чи харчування). візерунки).

✓ Втрата цілісності

Втрату цілісності також можна вважати СЕРЕДНЬОЮ, оскільки несанкціонована зміна цих даних може перешкодити належному наданню послуг яслами (особливо щодо алергії, режиму харчування та інших пов'язаних даних).

✓ Втрата доступності

Втрату доступності можна вважати НИЗЬКОЮ, оскільки недоступність даних може призвести до деяких незначних незручностей, які можна легко подолати (наприклад, шляхом повторного введення даних на платформі або спілкування з батьками за допомогою інших засобів).

Таблиця 4.30

Визначення загальної оцінки впливу операцій обробки персональних даних

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Середній	**Середній**	**Низький**
	Загальна оцінка впливу	**СЕРЕДНІЙ**

Загальний результат оцінки впливу є найвищим визначеним, тому загальний оцінений вплив є СЕРЕДНІМ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може бути вищим, ніж розрахований вище. Прикладом такого випадку є певні плани дієти, яких дотримуються конкретні діти (наприклад, через релігійні переконання). Іншим прикладом є випадок школи, спеціально призначеної для дітей з особливими умовами чи вадами.

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в Розділі 2.1.3, можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання:

- ***Мережа та технічні ресурси:*** Імовірність виникнення загрози СЕРЕДНЯ, оскільки система підключена до Інтернету та є можливість надати доступ до внутрішньої системи обробки персональних даних через Інтернет. Однак для запобігання несанкціонованому доступу використовуються найкращі методи, і передбачається, що вони є актуальними.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки різні сторони мають доступ до однієї платформи, і незрозуміло, чи чітко визначено ролі та обов'язки. Тим не менш, існує прийнятна політика використання, і файли журналів створюються для будь-якої операції обробки.
- ***Сторони/люди, які беруть участь в обробці персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки використовується сторонній обробник даних і працівники можуть передавати, зберігати чи іншим чином обробляти персональні дані за межами приміщення школи. Однак передбачається, що прийнятне використання мережі, системи та фізичних ресурсів чітко визначено.
- ***Бізнес-сектор і масштаб обробки:*** ймовірність виникнення загрози НИЗЬКА, оскільки бізнес-сектор МСП (освіта) загалом не вважається схильним до кібератак, а операція обробки не стосується великої кількості осіб. Передбачається, що жодного порушення персональних даних навіть не було в минулому.

Таблиця 4.31

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Середній	2
Процеси/Процедури, пов'язані з обробкою персональних даних	Середній	2
Сторони/люди, залучені до обробки персональних даних	Середній	2
Сфера діяльності та масштаби переробки	Низький	1
Загальна ймовірність виникнення загрози	**СЕРЕДНІЙ (7)**	

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 3 (крок 4).

Таблиця 4.32

Оцінка ризику витоку персональних даних в системі

ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	РІВЕНЬ ВПЛИВУ		
	Низький	Середній	Високий/Дуже високий
Низький			
Середній		X	
Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається СЕРЕДНІМ. Додаток А (А.1 і А.2) можна використовувати для вжиття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути іншим (вищим) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози (див. також відповідні міркування в розділі 7.1.2).

4.5.2. Університетська платформа електронного навчання

В межах цього випадку використання розглянемо університет, який пропонує платформу електронного навчання та керування курсами, розміщену на внутрішньому веб-сервері. За допомогою платформи викладачі та адміністрація можуть надсилати оголошення студентам, а студенти можуть отримувати матеріали курсу, конспекти лекцій і слайди, надсилати завдання, проводити оцінювання та тести та отримувати результати оцінювання та оцінки. На початку кожного семестру ректорат Університету проводить набір студентів на модулі (курси) та призначає відповідні привілеї як студентам, так і викладачам. Передбачається, що для запобігання несанкціонованому доступу використовуються найкращі практики, ролі та обов'язки залучених працівників чітко визначені та повідомлені, а для всіх дій з обробки даних створюються файли журналів. Для результатів оцінювання професори передають остаточні бали адміністрації в паперовому вигляді, а адміністрація кодує їх на платформі. Платформа обробляє такі дані: a) Студенти: ім'я та прізвище, дата народження, дата вступу, вибраний курс(и), результати оцінювання, оцінки; b) Академічний персонал: ім'я та прізвище, дата народження, призначений курс(и).

1) Визначення операції обробки та її контексту

Конкретну операцію обробки даних можна деталізувати таким чином, як зображено в таблиці 4.13.

Таблиця 4.33

Опис операцій обробки персональних даних

ОПИС ОПЕРАЦІЇ ОБРОБКИ	УНІВЕРСИТЕТСЬКА ПЛАТФОРМА ДЛЯ НАВЧАННЯ	
Персональні дані обробляються	Студенти: ПІБ, дата народження, дата вступу, обраний курс(и), результати оцінювання, оцінки; Викладацький склад: ім'я та прізвище, дата народження, призначений курс(и).	
Мета обробки	Платформа електронного навчання та керування курсами, включаючи виконання завдань і тестування	
Суб'єкт даних	Студенти, професори	
Засоби обробки	платформа електронного навчання та керування курсами	
Одержувачі даних	Внутрішні	Адміністрація університету
	Внутрішні	Начальник відділів
Персональні дані обробляються	Власний (без процесора даних)	

2) Оцінка впливу

Дотримуючись підходу, описаного в розділі 3 (крок 2), можна зробити наступний аналіз:

✓ Втрата конфіденційності

У рамках конкретної операції обробки вплив від втрати конфіденційності вважається СЕРЕДНІМ, оскільки очікується, що суб’єкти даних зіткнуться зі значними незручностями через несанкціоноване розкриття персональних даних, що стосуються їх успішності, оцінок і результатів.

✓ Втрата цілісності

Вплив від втрати конфіденційності також вважається СЕРЕДНІМ, оскільки очікується, що суб’єкти даних зіткнуться зі значними незручностями через несанкціоновану зміну персональних даних, що безпосередньо впливає на їх успішність та оцінки.

✓ Втрата доступності

Вплив від втрати конфіденційності вважається НИЗЬКИМ, оскільки очікується, що суб’єкти даних зіткнуться з незначними незручностями через недоступність персональних даних, які можна легко подолати (за умови, що існують резервні копії та інформація про результати оцінювання та оцінки також зберігається в автономному режимі) .

Таблиця 4.34

Визначення загальної оцінки впливу операцій обробки персональних даних

ОЦІНКА ВПЛИВУ		
Конфіденційність	Цілісність	Доступність
Середній	**Середній**	**Низький**
	Загальна оцінка впливу	**СЕРЕДНІЙ**

Загальний результат оцінки впливу є найвищим визначеним, тому загальний оцінений вплив є СЕРЕДНІМ.

Додатково до припущень, зроблених у цьому прикладі, можуть бути випадки, коли загальний вплив може бути іншим (вищим), ніж розрахований вище. Прикладом такого випадку може бути можлива інтеграція платформи з профілями соціальних мереж, де також збираються інші дані про студентів (наприклад спосіб життя, звички тощо). Іншим прикладом може бути можливе використання платформи для статистики та аналітика. Слід зауважити, що в обох цих випадках слід ретельно оцінити загальну законність операцій з обробки даних.

3) Імовірність виникнення загрози

На основі питань і підходу, наведеного в Розділі 2.1.3, можна зробити таку оцінку для кожного виміру конкретного середовища обробки даних у цьому випадку використання:

- ***Мережа та технічні ресурси:*** Імовірність виникнення загрози СЕРЕДНЯ, оскільки система підключена до Інтернету та є можливість надати доступ до внутрішньої системи обробки персональних даних через Інтернет. Однак передбачається, що для запобігання несанкціонованому доступу використовуються найкращі методи та що вони є актуальними.
- ***Процеси/процедури, пов'язані з обробкою персональних даних:*** ймовірність виникнення загрози СЕРЕДНЯ через різні сторони, які мають доступ до системи, а також тому, що ролі та обов'язки мають бути дуже чітко визначені. Тим не менш, передбачається, що існує конкретна прийнятна політика використання, а файли журналу створюються для будь-якої виконаної обробки.
- ***Сторони/люди, залучені до обробки персональних даних:*** ймовірність виникнення загрози НИЗЬКА, оскільки використовується сторонній обробник даних. Однак передбачається, що прийнятне використання мережі, системи та фізичних ресурсів чітко визначено, і працівники можуть передавати, зберігати чи іншим чином обробляти персональні дані поза приміщенням школи.

- ***Бізнес-сектор і масштаб обробки:*** ймовірність виникнення загрози СЕРЕДНЯ, оскільки операція обробки стосується великої кількості осіб, а бізнес-сектор МСП (вища освіта – університет) потенційно може бути схильний до кібератак. Передбачається, що жодного порушення персональних даних у минулому не було

Таблиця 4.35

Визначення загальної ймовірності виникнення загрози

ОБЛАСТЬ ОЦІНКИ	ЙМОВІРНІСТЬ	
	РІВЕНЬ	БАЛИ
Мережа та технічні ресурси	Середній	2
Процеси/Процедури, пов'язані з обробкою персональних даних	Середній	2
Сторони/люди, залучені до обробки персональних даних	Низький	1
Сфера діяльності та масштаби переробки	Середній	2
Загальна ймовірність виникнення загрози	**СЕРЕДНІЙ (7)**	

4) Оцінка ризику

Використовуючи результати оцінки впливу та ймовірність виникнення загрози, ризик розраховується на основі розділу 2.1.4.

Таблиця 4.36

Оцінка ризику витоку персональних даних в системі

		РІВЕНЬ ВПЛИВУ		
		Низький	Середній	Високий/Дуже високий
ЙМОВІРНІСТЬ ВИНИКНЕННЯ ЗАГРОЗИ	Низький			
	Середній		X	
	Високий			

Зокрема, загальний ризик для цього конкретного випадку зазвичай вважається СЕРЕДНІМ. Додаток А (А.1 і А.2) можна використовувати для прийняття заходів, що відповідають наявному ризику.

Варто зазначити, що ризик може бути іншим (вищим) за умов, безпосередньо пов'язаних із конкретною операцією обробки даних і впливаючи на вплив або ймовірність виникнення загрози (див. також відповідні міркування в розділі 7.2.2).

5. Захист персональних даних у сфері IoT на прикладі розумного будинку та медичних застосунків

Розглянемо особливості захисту персональних даних із дотриманням існуючих законодавчих вимог (GDPR) для двох надзвичайно популярних сьогодні предметних областей серед наукових досліджень аспірантів напряму «Комп'ютерні науки». Це створення інтелектуалізованих інформаційних систем та застосування методів штучного інтелекту в завданнях, що стосуються медичних досліджень, персоналізованої медицини та створення смарт-систем (розумні будинки, розумні міста, промисловий Інтернет речей).

Інтелектуальні будинки – це системи на основі Інтернету речей, у яких об'єднуються дані про керування будівлею (наприклад, споживання енергії) і дані користувачів, отримані через портативні та безконтактні пристрої. Такі середовища можуть мати кілька операцій з даними (з використанням датчиків, приводів і пристроїв), які виконуються з особистими даними користувача, які вимагають відповідності до GDPR [41].

Такі системи включають вбудоване обладнання для моніторингу та контролю з потенціалом спостерігати за користувачами та їхнім медичним станом за допомогою датчиків браслетів і розумних об'єктів моніторингу, які можуть реєструвати частоту серцевих скорочень, артеріальний тиск, фізичні рухи та розташування в приміщенні [30]. Потім дані користувача аналізуються локально або в хмарній системі, і на основі результатів третім особам можна повідомити про втручання для запобігання потенційним інцидентам для користувачів, які контролюються [31].

У таких системах дані про будівлю та користувачів інтегровані в ***систему керування будівлею*** (BMCS) і низку електронних приводів для досягнення балансу споживання ресурсів будівлі (наприклад, енергії для опалення, вентиляції та кондиціонування (HVAC)) і комфорту, а також для визначення медичного/фізичного стану користувачів.

Кардіомонітор — вимірює та відображає частоту серцевих скорочень користувача та зберігає її локально. Якщо швидкість є ненормальною, виміряні дані надсилаються до BMCS для екстрених дій.

Монітор артеріального тиску — вимірює артеріальний тиск користувача та зберігає такі виміряні дані у локальному сховищі. У разі ненормальних умов дані передаються до BMCS, і користувач отримує сповіщення через попереджувальний сигнал.

Пристрій виявлення руху —відстежує певну зону, відчуває фізичні рухи та передає місцезнаходження контрольованого користувача до BMCS. Він

попереджає користувачів, якщо вони входять до забороненої зони всередині будівлі.

Система керування будівлею — інтерпретує повідомлення або дані, отримані вищезазначеними пристроями. У разі критичного стану здоров'я викликає швидку допомогу. В іншому випадку відображається нормальна ситуація. Він профілює або аналізує статус або поведінку користувачів на основі їхньої медичної інформації або фізичних рухів протягом певного періоду часу, що називається профільованими даними. Крім того, такі дані зберігаються локально, а копія надсилається в хмарне сховище, щоб отримати до неї доступ уповноваженим лікарям або іншим службам підтримки. BMCS також керує доступом до підключених пристроїв, щоб контролювати їхню роботу, і за потреби отримує дані користувача з цих пристроїв [42].

На рис. 5.1 показано бізнес-процеси кардіомонітора, інтелектуального пристрою з детектором руху, монітора артеріального тиску та BMCS, які використовуються в розумній будівлі.

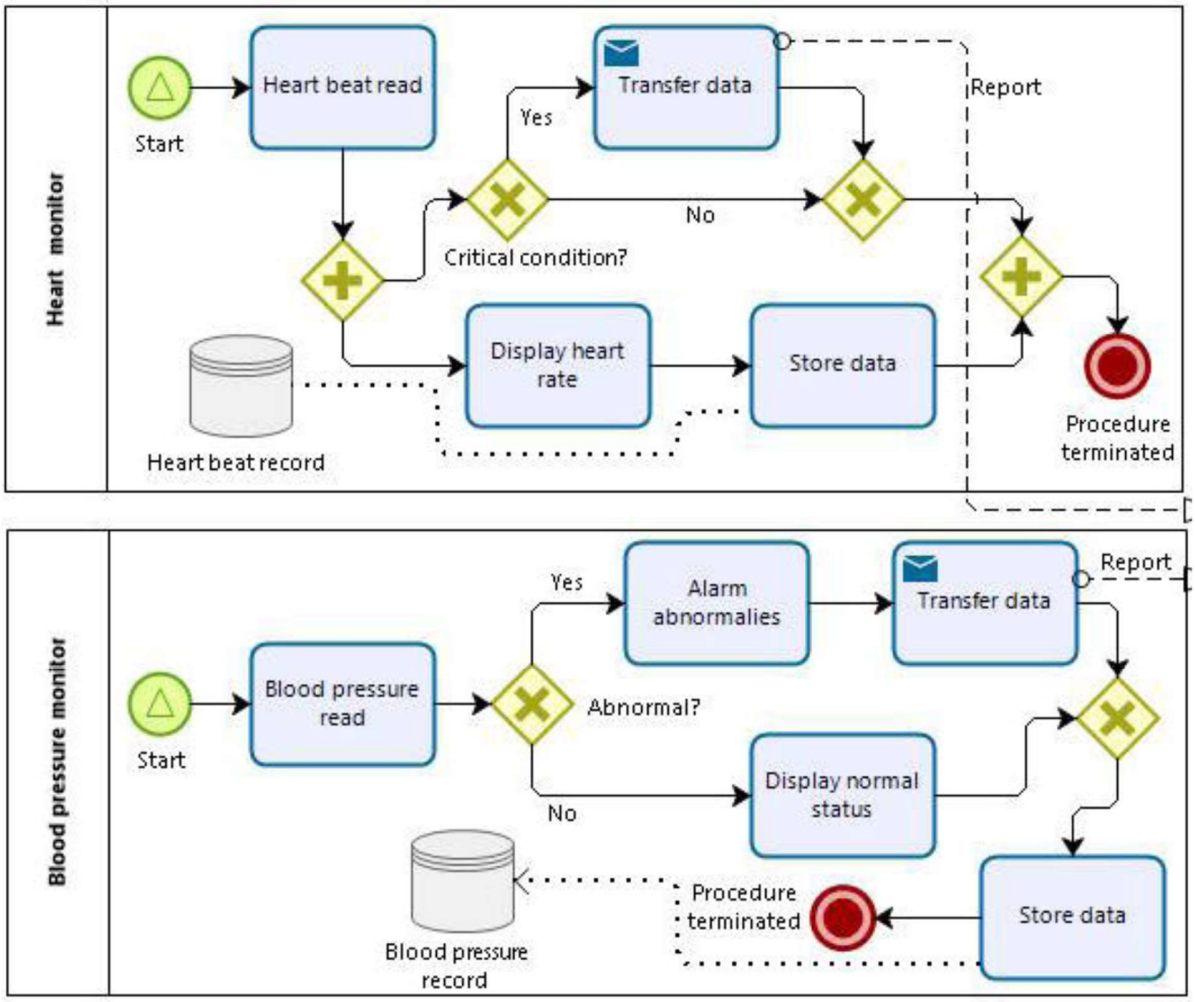


Рис.5.1. Бізнес-процеси кардіомонітора та монітора артеріального тиску

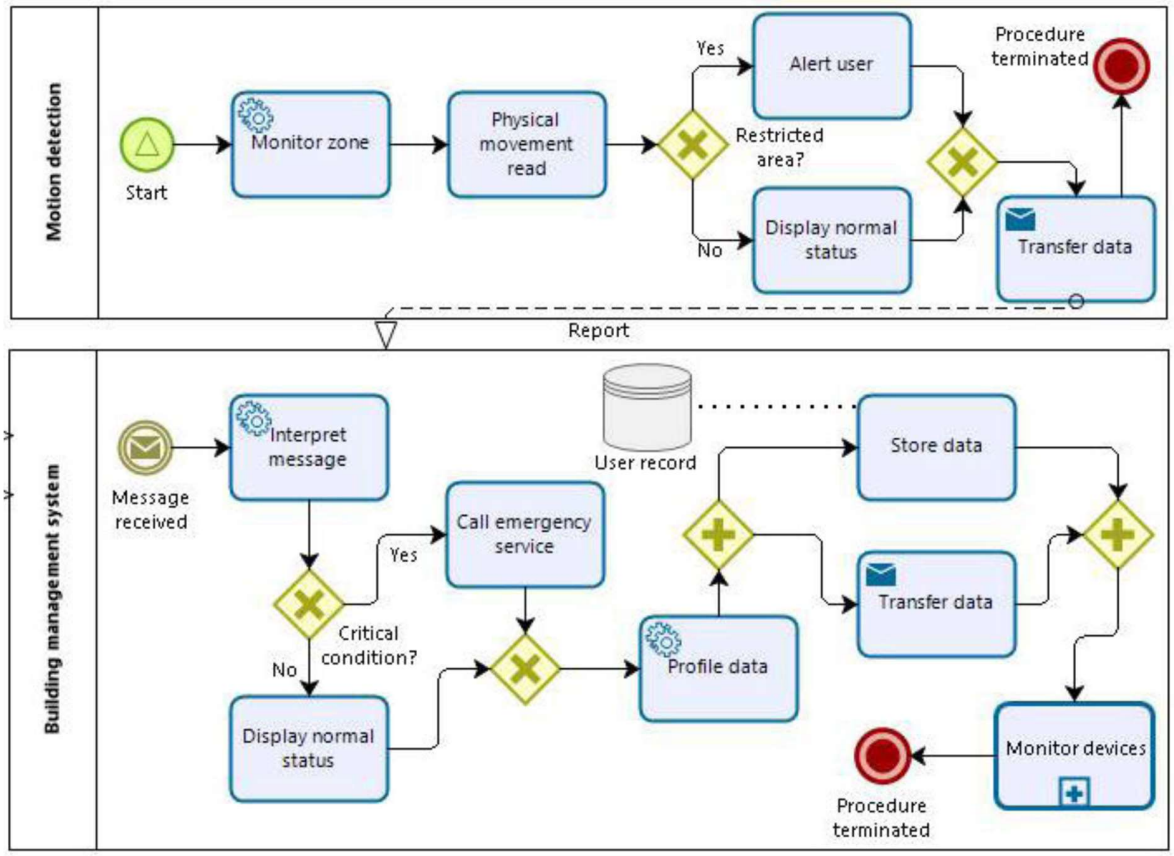


Рис.5.2. Бізнес-процеси інтелектуального пристрою з детектором руху та BMCS

Практичне завдання

Для кожної з описаних підсистем необхідно провести оцінку ризику обробки персональних даних. Для цього поділіться на команди по 5-6 людей.

1. Кожна з команд, використовуючи шаблони з Додатку 1 або Додатку 2 проводить оцінювання впливу на захист даних (DPIA, Data protection impact assessment) для системи розумного будинку, описаної в розділі 5.
2. Кожна з команд обирає одну підсистему (кардіомонітора, інтелектуального пристрою з детектором руху, монітора артеріального тиску чи BMCS).

3. Для обраної підсистеми необхідно оцінити ризики обробки персональних даних, аналогічно до прикладів, описаних в розділі 3, використовуючи методологію, описану в розділі 2.
4. Після того, як визначено загальну оцінку ризику в системі необхідно обрати організаційно-технічні заходи з Додатку 3, які відповідають визначеному рівню ризику, а також описати ваші пропозиції щодо того, як їх доцільно застосувати для вашої підсистеми чи системи загалом.

Висновки

Безпека обробки персональних даних уже є юридичним зобов'язанням для контролерів даних, однак Загальний регламент із захисту даних посилює відповідні положення (як за змістом, так і за контекстом) і поширює цю відповідальність безпосередньо на обробників даних. Беручи до уваги особливі характеристики МСП, такі як обмежені ресурси та відсутність кваліфікованого персоналу, цей звіт базується на методологічних кроках ENISA від 2016 року для МСП (щодо безпеки обробки персональних даних) і надає практичну демонстрацію вищезазначених кроків для конкретних випадків використання. Кожен варіант використання відповідає конкретній операції обробки персональних даних і робить певні припущення щодо середовища обробки даних і загального контексту обробки. Наведені приклади зосереджені лише на заходах безпеки та не спрямовані на надання будь-якого правового аналізу чи оцінки відповідності GDPR для конкретних операцій обробки даних.

Під час аналізу вибраних випадків використання було зроблено ряд висновків і відповідних рекомендацій, які обговорюються нижче.

Потрібне керівництво

Подібні операції з обробки персональних даних можуть відрізнятися у різних контролерів даних, враховуючи їх особливості, засоби, що використовуються для обробки персональних даних, категорії суб'єктів даних, обробників даних та одержувачів даних. Таким чином, універсальний підхід на основі загального підходу, що ґрунтується на ризиках, який виходить за межі положень безпеки даних, не можна вважати життєздатним і прагматичним. Кожну операцію обробки слід розглядати окремо, беручи до уваги контекст і середовище обробки. Тобто, замість того, щоб апріорі класифікувати операції обробки за рівнями ризику, слід зосередитися на наданні повноважень і керівництві контролерами даних, щоб спочатку зрозуміти свої операції обробки, а потім оцінити рівень ризику та застосувати відповідні заходи безпеки.

Компетентні органи ЄС, політики та регулятори ЄС (наприклад, органи із захисту даних) повинні розробити практичні та масштабовані рекомендації, які зможуть підтримувати та допомагати різним типам контролерів даних і звертатися до конкретних спільнот зацікавлених сторін.

Кваліфіковані DPO

Розширення повноважень контролерів даних також можна сприймати як питання підвищення їх обізнаності щодо їхніх операцій обробки та загальних положень GDPR. Однак для того, щоб мати можливість керувати своєю відповідністю до GDPR у більш структурований спосіб, а не завдяки корекційним заходам, очікується, що вони шукатимуть підтримки та керівництва. Роль відповідної

кваліфікованої особи із захисту даних (DPO) є центральною за цим підходом, навіть якщо призначення DPO не є обов'язковим відповідно до статті GDPR.

Важливо зазначити, що виконання цієї ролі вимагає як хорошого розуміння законодавчої бази захисту даних, так і сучасних IT-технологій (і відповідних передових практик безпеки), які є основою для більшості поширених сьогодні засобів обробки даних.

Компетентні органи ЄС, політики та регулятори ЄС (наприклад, органи із захисту даних) повинні оприлюднити набір базових професійних навичок і вимог, яким повинні відповідати спеціалісти із захисту даних.

Демонстрація відповідності

Як обговорювалося раніше, контролери даних не повинні розглядати безпеку обробки персональних даних як окреме зобов'язання відповідно до GDPR, а як частину загальної системи відповідності, яку вони повинні розробити, запровадити та підтримувати. Методологія ENISA може бути корисною в цьому відношенні у всіх випадках, коли оцінка ризику передбачена Регламентом (наприклад, повідомлення про порушення персональних даних). Під час розробки вищезазначеної структури відповідності контролери даних повинні намагатися розширити документацію свого підходу за межі рівня, встановленого положеннями GDPR. Це не тільки гарантує, що вони активно та позитивно розглядають ризики будь-якої обробки даних, яку вони здійснюють, але також активізують свої зусилля щодо принципу підзвітності та демонстрації відповідності. Крім того, оскільки підхід, що ґрунтується на ризиках, є невід'ємною частиною Оцінки впливу на захист даних (DPIA), очікується, що наявність документації також полегшить проведення, навіть на добровільній основі, DPIA.

Спільноти/асоціації малого та середнього бізнесу та контролери даних повинні брати участь у оцінці ризиків та відповідній структурованій документації як невід'ємній частині систем управління інформацією для персональних даних.

Регуляторні органи (наприклад, органи із захисту даних) повинні надати керівництво та підтримати навчання для контролерів даних у цьому контексті.

Масштабовані схеми сертифікації

Механізми сертифікації захисту даних GDPR (статті 42 і 43) можуть зіграти значну роль у дозволі контролерам даних досягти та продемонструвати наявність відповідних гарантій, включаючи заходи безпеки, і, отже, відповідність їх операцій з обробки положенням GDPR. Оскільки контролери даних, і особливо МСП, все більше і більше покладаються на технології, продукти та послуги третіх сторін, важливо заохочувати та мотивувати оцінювати рівень відповідності цих сторін і, якщо можливо, отримувати такі сертифікати. Враховуючи добровільний характер механізмів сертифікації відповідно до GDPR, вкрай важливо, щоб контролери даних були мотивовані та заохочені дотримуватись схем сертифікації, а також вибирали обробників даних, які дотримуються подібної практики.

Політики та регулятори ЄС (наприклад, органи із захисту даних) повинні визначати та просувати масштабовані схеми сертифікації захисту даних, які відповідають потребам малих і середніх підприємств і дають їм змогу досягти та продемонструвати відповідність.

Спільноти/асоціації малого та середнього бізнесу та контролери даних повинні обирати обробників даних, які дотримуються найкращих практик безпеки та відповідних механізмів сертифікації.

Нові методології управління ризиками

Управління ризиками інформаційної безпеки та управління ризиками безпеки персональних даних розглядають розрахунок рівнів ризику з двох різних поглядів: перший зосереджується на впливі для контролера даних, а другий — на впливі на суб'єктів даних. Однак обидва підходи призводять до запропонованих наборів організаційних і технічних заходів, які повинні бути впроваджені, підтримувані та перевірені контролером даних. Незалежно від специфіки, описаної раніше, загальна методологія, яка охоплює обидва аспекти, могла б дозволити контролерам даних, зокрема малим і середнім підприємствам, дотримуватися систематичного підходу до досягнення відповідності.

Дослідницьке співтовариство та компетентні органи ЄС у тісній співпраці з регуляторними органами (наприклад, органами захисту даних) повинні запропонувати та висунути методології, які поєднують управління ризиками безпеки та управління ризиками персональних даних.

Комунікація та підвищення обізнаності

МСП лише починають розглядати зміни, які вони повинні запровадити, і розширити перспективи своїх стратегій інформаційної безпеки та бізнес-стратегії, щоб відповідати вимогам законодавства. Проте обсяг змін, необхідних для їх інтеграції в існуючі бізнес-процеси, неможливо передбачити. Контролери даних часто неохоче сприймають такі зміни як перешкоду, а не можливість позиціонувати себе на новоствореному ринку, зміцнюючи також впевненість і довіру своїх клієнтів.

Спільноти та асоціації малого та середнього бізнесу, тісно співпрацюючи з компетентними органами та регуляторами ЄС (наприклад, органами із захисту даних), повинні спілкуватися та заохочувати контролерів даних вживати заходів щодо дотримання вимог безпеки та конфіденційності як конкурентної переваги поряд із основними юридичними зобов'язаннями.

Список використаної літератури

1. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890;4(5):193–220.
2. Universal Declaration of Human Rights. New York: United Nations; 1948. URL: https://www.un.org/ru/universal-declaration-human-rights/index.html (дата звернення: 15.08.2023).
3. OECD work on privacy. In: Organisation for Economic Co-operation and Development [веб-сайт]. Paris: OECD Publishing; 2020 URL: http://www.oecd.org/sti/ieconomy/privacy.htm (дата звернення: 15.08.2023).
4. Конвенція № 108 та протоколи до неї. Страсбург: Рада Європи; 2020 URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680078c46). (дата звернення: 15.08.2023).
5. Витяг з рішення Федерального конституційного суду Німеччини від 15 грудня 1983 р., 1 BvR 209, 269, 362, 420, 440, 484/83. Karlsruhe: Federal Constitutional Court; 1993 URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html (дата звернення: 15.08.2023).
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504 (дата звернення: 1.08.2023).
7. Personal data protection and privacy principles. Geneva: United Nations System; 2018. URL: https://www.unsystem.org/ personal-data-protection-and-privacy-principles) (дата звернення: 15.08.2023).
8. Хартія Європейського Союзу про основні права. URL: https://eulaw.ru/treaties/charter/ (дата звернення: 1.08.2023).
9. Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018 (https://fra.europa.eu/en/publication/2018/ handbook-european-data-protection-law-2018-edition).
10. Lawful basis for processing. In: ICO. Wilmslow: Information Commissioner's Office; 2020 URL: https://ico.org.uk/for-organisations/guide-todata-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (дата звернення: 17.08.2023).
11. Про інформовану згоду.: Guidelines 05/2020 on consent under Regulation 2016/679. In: EDPB. Brussels: European Data Protection Board; 2020. URL: https://edpb.europa.eu/our-work-tools/our-documents/ guidelines/guidelines-052020-consent-under-regulation-2016679_en (дата звернення: 17.08.2023).
12. Guidelines 05/2020 on consent under Regulation 2016/679. In: EDPB. Brussels: European Data Protection Board; 2020. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (дата звернення: 17.08.2023).
13. Donnelly M, McDonagh M. Health research, consent and the GDPR exemption. Eur J Health Law. 2019;26(2):97–119.
14. Voigt P, von dem Bussche A. Rights of data subjects. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: 141–87.
15. Chapter 6.1 of Handbook on European data protection law – 2018 edition. Vienna: European Union Agency for Fundamental Rights; 2018. URL: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (дата звернення: 17.08.2023).
16. Hodges C. Delivering data protection: trust and ethical culture. Eur Data Prot L Rev. 2018;4(1): pp. 65-79.
17. Sample DPIA template. URL: https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf (дата звернення: 17.08.2023).

18. Template for Data Protection Impact Assessment (DPIA) URL: https://iapp.org/resources/article/template-for-data-protection-impact-assessment-dpia/ (дата звернення: 17.08.2023).
19. European Union Agency for Cybersecurity, Handbook on security of personal data processing, European Network and Information Security Agency, 2017. URL: https://data.europa.eu/doi/10.2824/569768 (дата звернення: 22.08.2023).
20. Directive 2002/58/EC on privacy and electronic communications: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32002L0058
21. Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1481193515962&uri=CELEX:32016L1148
22. ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=54534
23. G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," Journal of Information Security, Vol. 4 No. 2, 2013, pp. 92-100. doi: 10.4236/jis.2013.42011.
24. S. Wachter, ‘‘Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR,’’ Comput. Law Secur. Rev., vol. 34, no. 3, pp. 436–449, Jun. 2018.
25. M. Barati and O. Rana, ‘‘Enhancing user privacy in IoT: Integration of GDPR and blockchain,’’ in Blockchain Trustworthy Systems (Communications in Computer and Information Science), vol. 1156, Z. Zheng, H. N. Dai, M. Tang, and X. Chen, eds. Singapore: Springer, 2020, pp. 322–335.
26. J. Seo, K. Kim, M. Park, M. Park and K. Lee, "An analysis of economic impact on IoT under GDPR," *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), 2017, pp. 879-881, doi: 10.1109/ICTC.2017.8190804.
27. O. Amaral, S. Abualhaija, M. Sabetzadeh and L. Briand, "A Model-based Conceptualization of Requirements for Compliance Checking of Data Processing against GDPR," *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*, Notre Dame, IN, USA, 2021, pp. 16-20, doi: 10.1109/REW53955.2021.00009.
28. J. Meszaros, "The Conflict Between Privacy and Scientific Research in the GDPR," *2018 Pacific Neighborhood Consortium Annual Conference and Joint Meetings (PNC)*, San Francisco, CA, USA, 2018, pp. 1-6, doi: 10.23919/PNC.2018.8579471.
29. E. C. Groen and M. Ochs, "CrowdRE, User Feedback and GDPR: Towards Tackling GDPR Implications with Adequate Technical and Organizational Measures in an Effort-Minimal Way," *2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)*, Jeju, Korea (South), 2019, pp. 180-185, doi: 10.1109/REW.2019.00038.
30. Antoni Gobeo; Connor Fowler; William J. Buchanan, "GDPR and Cyber Security for Business Information Systems," in *GDPR and Cyber Security for Business Information Systems* , River Publishers, 2020, pp.i-xix.
31. M. Rhahla, T. Abdellatif, R. Attia and W. Berrayana, "A GDPR Controller for IoT Systems: Application to e-Health," *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, Napoli, Italy, 2019, pp. 170-173, doi: 10.1109/WETICE.2019.00044.
32. G. Vojkovic, "Will the GDPR slow down development of smart cities?," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2018, pp. 1295-1297, doi: 10.23919/MIPRO.2018.8400234.
33. E. Barnoviciu, V. Ghenescu, S. -V. Carata, M. Ghenescu, R. Mihaescu and M. Chindea, "GDPR compliance in Video Surveillance and Video Processing Application," *2019 International Conference on Speech Technology and Human-Computer Dialogue (SpeD)*, Timisoara, Romania, 2019, pp. 1-6, doi: 10.1109/SPED.2019.8906553.
34. K. Ider, "Assessment of the quality of user awareness of GDPR in healthcare IOT," *2021 International Conference on Biomedical Innovations and Applications (BIA)*, Varna, Bulgaria, 2022, pp. 25-28, doi: 10.1109/BIA52594.2022.9831287.

35. M. Dutta and S. Dhal, "GDPR-Compliant Data Management Protocol: A Scalable Solution," *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Bangalore, India, 2022, pp. 256-259, doi: 10.1109/COMSNETS53615.2022.9667791.
36. G. Y. Lee, K. J. Cha and H. J. Kim, "Designing the GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment," *2019 IEEE International Congress on Internet of Things (ICIOT)*, Milan, Italy, 2019, pp. 79-81, doi: 10.1109/ICIOT.2019.00025.
37. T. Tzolov, "One Model For Implementation GDPR Based On ISO Standards," *2018 International Conference on Information Technologies (InfoTech)*, Varna, Bulgaria, 2018, pp. 1-3, doi: 10.1109/InfoTech.2018.8510716.
38. Nurse, J.R.C., Creese, S., De Roure, D.: Security risk assessment in Internet of Things systems. IEEE IT Prof. 19(5), 20–26 (2017)
39. Lopes, I.M., Guarda, T., Oliveira, P. (2020). The Four Dimensions of the GDPR Framework: An Institutional Theory Perspective. In: Rocha, Á., Pereira, R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 152. Springer, Singapore. https://doi.org/10.1007/978-981-13-9155-2_39
40. C. Metallidou, K. E. Psannis and E. Alexandropoulou-Egyptiadou, "An Efficient IoT System Respecting the GDPR," *2020 3rd World Symposium on Communication Engineering (WSCE)*, Thessaloniki, Greece, 2020, pp. 79-83, doi: 10.1109/WSCE51339.2020.9275573.
41. J. Willemson, "Analysis of Information Security Measures Embedded in the GDPR," *2023 IEEE 31st International Requirements Engineering Conference Workshops (REW)*, Hannover, Germany, 2023, pp. 214-217, doi: 10.1109/REW57809.2023.00043.
42. N. Azam, A. L. Michala, S. Ansari and N. B. Truong, "Modelling Technique for GDPR-Compliance: Toward a Comprehensive Solution," *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, Kuala Lumpur, Malaysia, 2023, pp. 3300-3305, doi: 10.1109/GLOBECOM54140.2023.10437389.

Додаток 1. Шаблон DPIA, розроблений Information Comissioner`s Office

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Додаток 2 Шаблон для оцінки впливу на захист даних (DPIA) від міжнародної асоціації фахівців з питань конфіденційності (Iapp)

Family Links Network
Code of Conduct for Data Protection
Template for Data Protection Impact Assessment (DPIA)

International Association of Privacy Professionals

Data protection issue	Code of conduct	Assessment of risks	Mitigation measures	Conclusion
Purpose specification Is the data to be collected to be used only for a specified purpose? Will the data collected be used for anything other than the specified purpose?	2.1 Specified Purpose	**Example**: "Function creep" – National Societies may want to gain more value from the data they collect. **In practice:** • National Societies may ignore or are not aware that they cannot repurpose personal data (i.e., to use the data they originally collected for some additional purposes) without seeking consent again. • The National Society may not comply with the RFL Code of Conduct	**Examples:** ▪ Specify/document the purposes for which personal data will be collected/used ▪ Raise awareness on RFL Code of Conduct that provides for the purpose specification principle and for further processing only if for purposes compatible with the original purpose of data collection. ▪ Improve training of staff regarding purpose specification/compatible further processing. ▪ Use of database: As part of a privacy-by-design approach, insert reference in the file to ensure the purpose of the data processing operations is always specified. Where applicable, also link the purpose of the data processing	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

			operations to the consent that may have been provided.	
Data limitation Is all the personal data collected necessary for the RFL activity? When people engage with you seeking help, are they told how the personal information they supply will be used?	2.3.2 Processing adequate relevant and updated data 2.3.1 Responsibility and accountability 2.2.1 Consent 3.1 Information and access	**Example:** • National Societies may collect more personal data than necessary for the specified purpose. • **In practice:** National Societies may suffer reputational damage when it becomes publicly known that staff are collecting more personal data than they actually need. ➢ The additional personal data collected creates a bigger risk for the beneficiaries/ their families/witnesses/ or others if the system is hacked or otherwise compromised (unauthorized use/disclosure or security breach.) ➢ Collecting more detail than needed also increases the risk of identity fraud or theft.	**Examples:** ▪ Ensure the staff collects only the pieces of data which are necessary to achieve the purpose specified originally ▪ If possible, give people prior notice regarding the modalities/purposes of the data collection and processing. Give individuals an opportunity to question the manner and purpose for which their data is collected and processed.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable
Right to information Are individuals explicitly informed about why their personal data is being collected and how it may be used?	3.1 Information and access	**Example:** National Societies do not provide individuals with clear and easily accessible information regarding their policies, procedures and practices on the collection of information. **In practice:** An individual would like to trace his/her relative but does not feel at ease in doing so as he/she is not fully aware of data processing/sharing procedures	**Examples:** ▪ Should National Societies have a dedicated web page, they could have a tab that links the individual with the RFL Code of Conduct. ▪ Alternatively, National Societies could develop Q&A summarizing the RFL Code of Conduct and make hard copies available to data subjects.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

		implemented by the National Society. ➢ If data collection/processing standards and procedure are not transparent, individuals may not trust the Organization and refrain from sharing their personal data. ➢ The National Society may not be compliant with the RFL Code of Conduct	▪ In addition, a link should be created on the Family Links website or national websites to present general activities as well as general data collection/processing modalities.	
<u>Legal basis for data processing /transfer</u> <u>Consent</u> Are individuals able to appreciate the most likely consequences (including negative)? Does the processing involve complex technologies? Does the person have a genuine free choice as to whether to consent? Are they able to refuse to provide some or all information without being penalised in any way or deprived of any assistance that your organisation might otherwise provide? How do individuals provide consent for	2.1 Purpose specification 2.2 Lawful and fair processing 2.2.1 Consent 3.1 Information and access	**Example:** ➢ One or more individuals threaten to announce publicly that they did not give their consent to the National Society's collection of their personal data. ➢ An advocacy organization might discover instances where the National Society did not get the consent of the individual. ➢ A rogue employee leaks memos showing that the National Society does not get informed consent. **In practice:** ➢ The National Society does not routinely obtain a signed form from the	**Example:** • Review the process by which consent is sought. Explain to beneficiaries or their families, witnesses or other relevant third parties the implications of registering with the National Society, how their data could be used in the database and to whom it could be further transferred. • Attempt, where possible, to get a signed informed consent form. • It would be worthwhile having a tab dedicated to what is informed consent on the National Society web page • Ensure that the consent form is	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

their information to be collected? If consent is not written, do you see any risks involved? Is consent limited to a specified purpose? If the personal data were to be used for a purpose other than that originally specified (a secondary purpose), will a new consent be sought from the individual? Has the individual explicitly agreed to how their information can be used, or that it can be shared with other agencies? Are there instances or circumstances where an individual has consented to the sharing or disclosure of personal information, but where the staff in charge does not think it is wise to do so? **<u>Alternative legal basis</u>** Is data also collected of individuals who are not present?		individual consenting to the collection and use of his or her personal data. ➢ Damage to the National Society's reputation. ➢ Other potential informants decide it is not prudent or safe to talk to the National Society.	consistent and accessible across all methods of collection, including hardcopy/online forms and via telephone. • Ensure that the consent form is available in an appropriate range of languages for the target group.	

			If it is not possible to obtain an informed consent: process/transfer personal data on an alternative legal basis (vital interest , public interest , legitimate interest, compliance with a legal obligation)	
Right to access / Rectification / Deletion Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information? Is it necessary to restrict access to data? If so, are these restrictions adequately circumscribed and explained?	3.1 Information and access 3.3 Rectification and deletion	**Example:** Some individuals may complain about how difficult it is to see and, if necessary, amend (or even delete) their personal data. **In practice:** National Societies may not have specific/transparent procedures to provide data subjects access to their personal data. ➢ Reputation damage ➢ individuals' complaints could reach the media or advocacy organizations.	**Examples:** ▪ Should National Societies have a dedicated web page, they could have a tab that links the individual with the assurance that they will help individuals in their requests for sight of their data. ▪ The web page could also specify the modalities of access (without prejudice to the confidentiality which may apply to certain pieces of information.)	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated
<u>Information quality and accuracy</u> What processes are in place for ensuring information quality, i.e., that the information is relevant, reliable, accurate, actionable?	2.3.2 Processing adequate, relevant and updated data 3.3 Rectification and deletion 3.4 Objection	**Example:** ▪ National Societies' staff do not have enough time to check the reliability of the information they receive from the beneficiaries, their families or witnesses.	**Examples:** ▪ Ensure a process of quality control to minimize errors or unauthorized modifications prior to recording the data. ▪ Where possible, cross-check information	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated

Is there a policy or procedure in place to correct data that has already been shared with partners, or to notify partners about updates?		▪ Few or no people actually witness an event or only see individuals taken away, but with no knowledge of what happens to them. National Society staff have to rely on incomplete information or are unable to verify information. Staff have insufficient resources to verify claims. ▪ Some staff are of the view that people should be given assistance anyway even if it is not possible to verify claims. **In practice:** Migrating paper records to a digital or online format by transcribing data increases the risk of introducing inaccuracies. ➢ National Societies may take decisions based on incomplete, unreliable or false information. ➢ Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	received from an individual with other organizations who may also have interviewed the individual or other witnesses. ▪ Establish procedures to determine when and how often personal information should be reviewed and/or updated and when data should be deleted or archived ▪ Establish a procedure to notify recipients of your data of subsequent corrections to the data. ▪ <u>Distinguish between primary and secondary sources of data and reflect this distinction in a caveat in the file.</u>	nor acceptable
<u>Appropriate security measures</u> What personal information is to be collected? Could disclosure of this information put the person in danger (for example information relating to ethnicity,	2.3.7 Security 2.3.8 Data breaches 2.3.1 Responsibility and accountability	**Example:** ➢ External hackers and rogue employees may seek to exploit personal data. ➢ Host governments may want details of all people to whom the ICRC provides assistance.	**Examples:** ▪ Encourage (warn) employees to avoid use of unsecured portable storage devices, such as memory sticks. ▪ Develop robust access control protocols which limit access on a	Risk sufficiently mitigated Risk not necessarily mitigated but accepted

religion, sexual orientation,political views, trade union membership, etc.) Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organisation subject to surveillance? What preventative measures are in place? Does the processing involve external organisations or third parties? Does this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? Is information limited to others on a "need to know" basis? How is this implemented in practice? Are staff reminded to keep paper files, CDs and/or memory sticks locked up or with them at all times when they are not in use? Are staff encouraged to encrypt memory sticks? Is training given to all staff on good data protection and information security practices? Are e-mails encrypted? What kind of encryption is used? What action will be taken if there is a data breach? Are individuals informed if their	6. Application of the Code of Conduct	➢ In a situation of violence offices of National Societies may be ransacked. **In practice:** ▪ The National Society may not impart to employees good information security practices. ▪ It may not put in place strong controls for access to its database ▪ Employees may use weak passwords or may not encrypt data. ▪ Some data (e.g., notebooks) in paper form is not backed up and may be found only in offices. ➢ The security controls of the National Society's system are breached and personal data is compromised. ➢ The National Society does not know when the personal data it holds is compromised. ➢ It suffers damage to its reputation. ➢ Compromised data puts lives at risk.	'need to know' basis. Users should only have access to that portion of data they need to carry out their legitimate functions. ▪ Ensure clarity re who has the authority to assign, change or revoke access privileges. ▪ Ensure all accesses to the databases are logged into a register of processing operations. ▪ Set-up data breach notification procedures to inform the data subjects.	Risk neither mitigated

personal data is lost, stolen or other compromised? Will any other organisations be informed? Have you considered some worst-case scenarios regarding what might happen if the personal data collected by your organisation was compromised or deleted either by accident or purposely? How would you decide which risks are the most likely and those that are likely to have the greatest impact if the personal information were stolen, hacked, altered or stolen?				
<u>Data sharing, disclosure/publication and/or transfer</u> Will the personal information be shared with or disclosed to other organisations, including other National Societies? Why? Have they provided written assurances that they will safeguard the information and not share it further? Does the organisation have an adequate data protection policy? Has the individual data subject explicitly agreed to the sharing of their data? Where your organisation develops promotional videos, brochures or press stories, has your	4. Transfers 2.3.1 Accountability and Responsibility 1.4.3 Confidentiality 2.3.2 Processing Adequate Relevant and Updated Data 2.3.7 Data Security 5. Publication	**Example:** Staff may share personal data with other organizations or authorities over which they have no control regarding how the other organizations or authorities may use that data or further share it. **In practice:** Publications of photos of unaccompanied minors could attract attention of child traffickers ➢ The data subject/family can be put at risk if the organisation does not process the data according to adequate data protection standards ➢ Individuals may complain about the disclosure of their data	**Examples:** • Share personal information with other organizations or authorities only if a specific legal basis exists (consent, public interest etc.) Additionally, share personal information with other organizations or authorities only if they observe adequate data protection to at least the same standard as the RFL Code of Conduct. • Only publish the photo and a central phone number, no other details. Cross check reliability of alleged relatives against other data available and the beneficiaries themselves before accepting to restore contact	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable

organisation anonymised personal information so that even if it were linked to other data, it would not be possible to identify the person?				
Data retention Is personal information being entered into databases? Is it necessary to keep all of the data that is being processed? Are there procedures for reviewing how long data should be retained? Is there a policy, procedure, rationale for archiving personal information? Is too much data being kept for auditing purposes? Could this be minimised?	2.3.6 Data Retention	**Examples:** The personal data originally collected is collected without specifying the retention period and is kept for an unlimited period. **In practice**: Large amounts of data are recorded in the National Societies' databases but are not necessary anymore to fulfil the purpose for which they were originally collected ➢ Information-overload: data management in this context is timeconsuming for the case worker and might not be worth it if the data is not necessary to carry out RFLactivities ➢ The National Society does not comply with the RFL Code of Conduct	**Examples:** ▪ Limiting the retention of personal data to what is necessary to fulfil specific, explicit and legitimate purposes. ▪ Use of database: As part of a privacy-by-design approach, insert reference in the file to ensure the data retention period is always specified. Also link the data retention period to the purpose of the data processing operations. An initial retention period could be extended if it is considered necessary to keep the data to fulfil the purpose for which it was originally collected.	Risk sufficiently mitigated Risk not necessarily mitigated but accepted Risk neither mitigated nor acceptable
Risks to individuals other than the risks identified above: Is the activity in question, in and of itself, likely to give rise to risks to the				

physical or moral integrity of the individuals concerned?				
Accountability/Oversight mechanism: Are data protection standards and procedures effectively implemented?	6. Application of the RFL Code of Conduct	**Example:** Insider threat -- Since no one may have the specific responsibility for safeguarding personal data, the National Society staff	**Example:** A data protection focal point is entrusted with the specific responsibility for ensuring the adequacy of national societies'	Risk sufficiently mitigated Risk not necessarily mitigated but accepted

Додаток 3 Організаційно-технічні заходи, запропоновані ENISA

Під кожним розділом представлено заходи для рівня ризику (низький: зелений, середній: жовтий, високий: червоний). Щоб досягти масштабованості, передбачається, що всі заходи, описані під низьким рівнем (зелений), застосовні до всіх рівнів. Подібним чином заходи, представлені під середнім рівнем (жовтий), також застосовуються до високого рівня ризику. Заходи, представлені під високим рівнем (червоний), не застосовуються до будь-якого іншого рівня ризику.

A.1. Запропоновані заходи для низького рівня ризику

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Політика безпеки та процедури захисту персональних даних	A.1	Організація повинна задокументувати свою політику щодо обробки персональних даних як частину політики інформаційної безпеки.	A.5 Політика безпеки
Політика безпеки та процедури захисту персональних даних	A.2	Політика безпеки повинна переглядатися та переглядатися, якщо необхідно, щороку.	A.5 Політика безпеки
Ролі та обов'язки	B.1	Ролі та обов’язки, пов’язані з обробкою персональних даних, мають бути чітко визначені та розподілені відповідно до політики безпеки.	A.6.1.1 Ролі та обов’язки щодо інформаційної безпеки
Ролі та обов'язки	B.2	Під час внутрішньої реорганізації або звільнення та зміни місця роботи, скасування прав та обов'язків з відповідними процедурами передачі повинні бути чітко визначені.	A.6.1.1 Ролі та обов’язки щодо інформаційної безпеки
Політика контролю доступу	C.1	Для кожної ролі (залученої до обробки персональних даних) слід надати певні права контролю доступу відповідно до принципу «необхідності знати».	A.9.1.1 Політика контролю доступу

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Управління ресурсами/активами	D.1	Організація повинна мати реєстр IT-ресурсів, які використовуються для обробки персональних даних (апаратне, програмне та мережеве). Реєстр може містити принаймні таку інформацію: IT-ресурс, тип (наприклад, сервер, робоча станція), місцезнаходження (фізичне чи електронне). Завдання щодо ведення та оновлення реєстру має бути доручено конкретній особі (наприклад, IT-офіцеру).	A.8 Управління активами
Управління ресурсами/активами	D.2	IT-ресурси слід переглядати та оновлювати на регулярній основі.	A.8 Управління активами
Управління змінами	E.1	Організація повинна переконатися, що всі зміни в IT-системі реєструються та контролюються конкретною особою (наприклад, спеціалістом із IT або служби безпеки). Необхідно регулярно контролювати цей процес.	A. 12.1 Операційні процедури та обов'язки
Управління змінами	E.2	Розробка програмного забезпечення повинна виконуватися в спеціальному середовищі, яке не пов’язане з IT-системою, яка використовується для обробки персональних даних. Коли потрібне тестування, слід використовувати фіктивні дані. У випадках, коли це неможливо, повинні бути встановлені спеціальні процедури для захисту персональних даних, які використовуються під час тестування.	A. 12.1 Операційні процедури та обов'язки

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Процесори даних	F.1	Офіційні вказівки та процедури, що стосуються обробки персональних даних обробниками даних	A.15 Відносини з постачальниками
Процесори даних	F.2	(підрядники/аутсорсинг) мають бути визначені, задокументовані та узгоджені між контролером даних і обробником даних до початку діяльності з обробки. Ці вказівки та процедури повинні в обов'язковому порядку встановлювати той самий рівень безпеки персональних даних, який передбачено політикою безпеки організації.	A.15 Відносини з постачальниками
Процесори даних	F.3	Виявивши порушення персональних даних, обробник даних повідомляє про це контролера без зайвої затримки.	A.15 Відносини з постачальниками
Обробка інцидентів / порушення персональних даних	G.1	Формальні вимоги та зобов'язання мають бути офіційно узгоджені між контролером даних і обробником даних. Обробник даних повинен надати достатні документальні докази відповідності.	A.16 Управління інцидентами інформаційної безпеки
Обробка інцидентів / порушення персональних даних	G.2	Необхідно визначити план реагування на інциденти з детальними процедурами, щоб забезпечити ефективне та впорядковане реагування на інциденти, пов'язані з персональними даними.	A.16 Управління інцидентами інформаційної безпеки

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Безперервність бізнесу	H.1	Організація повинна встановити основні процедури та засоби контролю, яких слід дотримуватися, щоб забезпечити необхідний рівень безперервності та доступності IT-системи, що обробляє персональні дані (у разі інциденту/порушення персональних даних).	A. 17 Аспекти інформаційної безпеки безперервності бізнесу управління
Конфіденційність персоналу	I.1	Організація повинна переконатися, що всі працівники розуміють свою відповідальність і зобов'язання, пов'язані з обробкою персональних даних. Ролі та обов'язки мають бути чітко повідомлені під час процесу перед працевлаштуванням та/або вступним процесом.	A. 17 Аспекти інформаційної безпеки безперервності бізнесу управління
Навчання	J.1	Організація повинна забезпечити належне інформування всіх співробітників про засоби контролю безпеки IT-системи, які стосуються їх повсякденної роботи. Співробітники, які беруть участь в обробці персональних даних, також повинні бути належним чином поінформовані про відповідні вимоги щодо захисту даних та юридичні зобов'язання за допомогою регулярних інформаційних кампаній.	A.7 Безпека людських ресурсів

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Контроль доступу та аутентифікація	К.1	Необхідно впровадити систему контролю доступу, застосовну до всіх користувачів, які отримують доступ до IT-системи. Система повинна дозволяти створювати, затверджувати, переглядати та видаляти облікові записи користувачів.	A.7.2.2 Інформаційна безпека, освіта та навчання
Контроль доступу та аутентифікація	К.2	Слід уникати використання звичайних облікових записів користувачів. У випадках, коли це необхідно, слід переконатися, що всі користувачі спільного облікового запису мають однакові ролі та обов'язки.	A.7.2.2 Інформаційна безпека, освіта та навчання
Контроль доступу та аутентифікація	К.3	Механізм автентифікації має бути на місці, що дозволяє отримати доступ до IT-системи (на основі політики та системи контролю доступу). Як мінімум слід використовувати комбінацію імені користувача та пароля. Паролі мають відповідати певному (настроюваному) рівню складності.	A.9 Контроль доступу
Контроль доступу та аутентифікація	К.4	Система контролю доступу повинна мати можливість виявляти та не дозволяти використання паролів, які не відповідають певному (настроюваному) рівню складності.	A.9 Контроль доступу

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Ведення журналів і моніторинг	L.1	Файли журналу повинні бути активовані для кожної системи/програми, яка використовується для обробки персональних даних. Вони повинні включати всі види доступу до даних (перегляд, зміна, видалення).	A.12.4 Реєстрація та моніторинг
Ведення журналів і моніторинг	L.2	Журнальні файли повинні мати мітку часу та належним чином захищені від підробки та несанкціонованого доступу. Годинники повинні бути синхронізовані з єдиним джерелом еталонного часу	A.12.4 Реєстрація та моніторинг
Безпека сервера/бази даних	M.1	Сервери баз даних і додатків мають бути налаштовані для роботи з використанням окремого облікового запису з мінімальними привілеями ОС для правильної роботи.	A. 12 Безпека операцій
Безпека сервера/бази даних	M.2	Сервери баз даних і додатків повинні обробляти лише ті особисті дані, які дійсно необхідні для обробки для досягнення цілей обробки.	A. 12 Безпека операцій
Безпека робочої станції	N.1	Користувачі не повинні мати можливість дезактивувати або обійти налаштування безпеки.	A. 14.1 Вимоги безпеки інформаційних систем
Безпека робочої станції	N.2	Антивірусні програми та сигнатури виявлення слід налаштовувати щотижня.	A. 14.1 Вимоги безпеки інформаційних систем
Безпека робочої станції	N.3	Користувачі не повинні мати привілеїв для встановлення або дезактивації несанкціонованих програм.	A. 14.1 Вимоги безпеки інформаційних систем

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Безпека робочої станції	N.4	Система повинна мати тайм-аути сеансу, коли користувач не був активним протягом певного періоду часу.	A. 14.1 Вимоги безпеки інформаційних систем
Безпека робочої станції	N.5	Необхідно регулярно встановлювати критичні оновлення безпеки, випущені розробником операційної системи.	A. 14.1 Вимоги безпеки інформаційних систем
Безпека мережі/зв’язку	O.1	Щоразу, коли доступ здійснюється через Інтернет, зв’язок має бути зашифрований за допомогою криптографічних протоколів (TLS/SSL).	A.13 Безпека зв'язку
Резервні копії	P.1	Процедури резервного копіювання та відновлення даних мають бути визначені, задокументовані та	A.12.3 Резервне копіювання
Резервні копії	P.2	чітко пов’язані з ролями та обов’язками.	A.12.3 Резервне копіювання
Резервні копії	P.3	Резервні копії повинні мати відповідний рівень фізичного захисту та захисту навколишнього середовища відповідно до стандартів, що застосовуються до вихідних даних.	A.12.3 Резервне копіювання
Резервні копії	P.4	Повне резервне копіювання слід виконувати регулярно.	A.12.3 Резервне копіювання
Мобільні/портативні пристрої	Q.1	Необхідно визначити та задокументувати процедури керування мобільними та портативними пристроями, встановлюючи чіткі правила їх належного використання.	A. 6.2 Мобільні пристрої та дистанційна робота

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Мобільні/портативні пристрої	Q.2	Мобільні пристрої, які мають доступ до інформаційної системи, повинні бути попередньо зареєстровані та авторизовані.	A. 6.2 Мобільні пристрої та дистанційна робота
Мобільні/портативні пристрої	Q.3	Мобільні пристрої повинні підлягати тим самим рівням процедур контролю доступу (до системи обробки даних), що й інше термінальне обладнання.	A. 6.2 Мобільні пристрої та дистанційна робота
Безпека життєвого циклу програми	R.1	Під час життєвого циклу розробки слід дотримуватися найкращих практик, сучасного стану та добре визнаних безпечних практик розробки, фреймворків або стандартів.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у процесах розробки та підтримки
Безпека життєвого циклу програми	R.2	Конкретні вимоги безпеки слід визначити на ранніх стадіях життєвого циклу розробки.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у процесах розробки та підтримки
Безпека життєвого циклу програми	R.3	Конкретні технології та методи, розроблені для підтримки конфіденційності та захисту даних (також відомі як технології підвищення конфіденційності (PET)), повинні бути прийняті за аналогією з вимогами безпеки.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у процесах розробки та підтримки

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Безпека життєвого циклу програми	R.4	Необхідно дотримуватися стандартів і практик безпечного кодування.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у процесах розробки та підтримки
Безпека життєвого циклу програми	R.5	Під час розробки слід проводити тестування та перевірку щодо реалізації початкових вимог безпеки.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у процесах розробки та підтримки
Видалення/утилізація даних	S.1	Перед утилізацією на всіх носіях має бути виконано програмне перезаписування. У випадках, коли це неможливо (CD, DVD тощо), слід виконати фізичне знищення.	A. 8.3.2 Утилізація носія та A.11.2.7 Безпечна утилізація або повторне використання обладнання
Видалення/утилізація даних	S.2	Проводиться подрібнення паперових та портативних носіїв, на яких зберігаються персональні дані.	A. 8.3.2 Утилізація носія та A.11.2.7 Безпечна утилізація або повторне використання обладнання
Фізична охорона	T.1	Фізичний периметр інфраструктури IT-системи не повинен бути доступним для неавторизованого персоналу.	A.11 – Фізична та екологічна безпека

A.2. Запропоновані заходи для середнього рівня ризику

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Політика безпеки та процедури захисту персональних даних	A.3	Організація повинна задокументувати окрему спеціальну політику безпеки щодо обробки персональних даних. Політика має бути затверджена керівництвом і доведена до відома всіх співробітників і відповідних зовнішніх сторін	A.5 Політика безпеки
Політика безпеки та процедури захисту персональних даних	A.4	Політика безпеки повинна принаймні вказувати на: ролі та обов’язки персоналу, базові технічні та організаційні заходи, прийняті для безпеки персональних даних, обробників даних або інших третіх сторін, залучених до обробки персональних даних.	A.5 Політика безпеки
Політика безпеки та процедури захисту персональних даних	A.5	Слід створити та підтримувати перелік конкретних політик/процедур, пов’язаних із безпекою персональних даних, на основі загальної політики безпеки.	A.5 Політика безпеки
Ролі та обов'язки	B.3	Має бути здійснене чітке призначення осіб, відповідальних за конкретні завдання безпеки, включно з призначенням DPO.	A.6.1.1 Ролі та обов’язки щодо інформаційної безпеки
Політика контролю доступу	C.2	Політика контролю доступу має бути деталізована та задокументована. Організація повинна визначити в цьому документі відповідні правила контролю доступу, права доступу та обмеження для конкретних ролей користувачів щодо процесів і процедур, пов’язаних з персональними даними.	A.9.1.1 Політика контролю доступу

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Політика контролю доступу	C.3	Розподіл ролей контролю доступу	A.9.1.1 Політика контролю доступу
Управління ресурсами/активами	D.3	(наприклад, запит на доступ, авторизація доступу, адміністрування доступу) мають бути чітко визначені та задокументовані.	A.8 Управління активами
Управління змінами	E.3	Ролі, які мають доступ до певних ресурсів, повинні бути визначені та задокументовані.	A. 12.1 Операційні процедури та обов'язки
Процесори даних	F.4	Організація контролера даних повинна регулярно перевіряти відповідність обробника даних узгодженому рівню вимог і зобов’язань.	A.15 Відносини з постачальниками
Обробка інцидентів / порушення персональних даних	G.3	План реагування на інциденти має бути задокументований, включаючи перелік можливих заходів щодо пом’якшення наслідків та чіткий розподіл ролей.	A.16 Управління інцидентами інформаційної безпеки
Безперервність бізнесу	H.2	BCP має бути деталізовано та задокументовано (дотримуючись загальної політики безпеки). Він повинен містити чіткі дії та розподіл ролей.	A. 17 Аспекти інформаційної безпеки безперервності бізнесу управління
Безперервність бізнесу	H.3	Рівень гарантованої якості обслуговування повинен бути визначений у BCP для основних бізнес-процесів, які забезпечують безпеку персональних даних.	A. 17 Аспекти інформаційної безпеки безперервності бізнесу

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Конфіденційність персоналу	I.2	Перед тим, як приступити до виконання своїх обов'язків, співробітників слід попросити переглянути та погодити політику безпеки організації та підписати відповідні угоди про конфіденційність і нерозголошення.	A.7 Безпека людських ресурсів
Навчання	J.2	Організація повинна мати структуровані та регулярні навчальні програми для персоналу, включно зі спеціальними програмістами для введення (в питання захисту даних) новачків.	A.7.2.2 Поінформованість про інформаційну безпеку, освіта та навчання
Контроль доступу та аутентифікація	K.5	Слід визначити та задокументувати конкретну політику паролів. Політика повинна містити принаймні довжину пароля, складність, термін дії, а також кількість допустимих невдалих спроб входу.	A.9 Контроль доступу
Контроль доступу та аутентифікація	K.6	Паролі користувачів повинні зберігатися в «хешованій» формі.	A.9 Контроль доступу
Ведення журналів і моніторинг	L.3	Дії системних адміністраторів і системних операторів, включаючи додавання/видалення/зміну прав користувача, повинні реєструватися.	A.12.4 Реєстрація та моніторинг
Ведення журналів і моніторинг	L.4	Не повинно бути можливості видалення або зміни вмісту файлів журналу. Доступ до файлів журналу також слід реєструвати на додаток до моніторингу для виявлення незвичної діяльності.	A.12.4 Реєстрація та моніторинг

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Ведення журналів і моніторинг	L.5	Система моніторингу повинна обробляти файли журналів і створювати звіти про стан системи та сповіщати про можливі попередження.	A.12.4 Реєстрація та моніторинг
Безпека сервера/бази даних	M.3	Слід розглянути рішення щодо шифрування конкретних файлів або записів за допомогою програмного чи апаратного забезпечення.	A. 12 Безпека операцій
Безпека сервера/бази даних	M.4	Слід розглянути можливість шифрування накопичувачів	A. 12 Безпека операцій
Безпека сервера/бази даних	M.5	Слід застосовувати методи псевдонімізації шляхом відокремлення даних від прямих ідентифікаторів, щоб уникнути зв’язування із суб’єктом даних без додаткової інформації	A. 12 Безпека операцій
Безпека робочої станції	N.6	Антивірусні програми та сигнатури виявлення слід налаштовувати щодня.	A. 14.1 Вимоги безпеки інформаційних систем
Безпека мережі/зв’язку	O.2	Бездротовий доступ до IT-системи повинен бути дозволений лише для окремих користувачів і процесів. Він повинен бути захищений механізмами шифрування.	A.13 Безпека зв'язку
Безпека мережі/зв’язку	O.3	Загалом слід уникати віддаленого доступу до IT-системи. У випадках, коли це абсолютно необхідно, це слід виконувати лише під контролем і моніторингом конкретної особи з організації за допомогою попередньо визначених пристроїв.	A.13 Безпека зв'язку

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Безпека мережі/зв’язку	O.4	Трафік до IT-системи та від неї слід відстежувати та контролювати за допомогою брандмауерів і систем виявлення вторгнень.	A.13 Безпека зв'язку
Резервні копії	P.5	Резервні носії слід регулярно перевіряти, щоб переконатися, що на них можна покластися в екстрених випадках.	A.12.3 Резервне копіювання
Резервні копії	P.6	Заплановане додаткове резервне копіювання слід виконувати принаймні щодня.	A.12.3 Резервне копіювання
Резервні копії	P.7	Копії резервної копії слід надійно зберігати в різних місцях.	A.12.3 Резервне копіювання
Резервні копії	P.8	У разі використання третьої сторони для зберігання резервних копій копію потрібно зашифрувати перед передачею від контролера даних.	A.12.3 Резервне копіювання
Мобільні/портативні пристрої	Q.4	Слід чітко визначити конкретні ролі та обов’язки щодо керування мобільними та портативними пристроями.	A. 6.2 Мобільні пристрої та дистанційна робота
Мобільні/портативні пристрої	Q.5	Організація повинна мати можливість дистанційно стерти особисті дані (пов’язані з операцією їх обробки) на мобільному пристрої, який було скомпрометовано.	A. 6.2 Мобільні пристрої та дистанційна робота
Мобільні/портативні пристрої	Q.6	Мобільні пристрої повинні підтримувати розділення приватного та комерційного використання пристрою через захищені програмні контейнери.	A. 6.2 Мобільні пристрої та дистанційна робота

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Мобільні/портативні пристрої	Q.7	Мобільні пристрої повинні бути фізично захищені від крадіжки, коли вони не використовуються.	A. 6.2 Мобільні пристрої та дистанційна робота
Безпека життєвого циклу програми	R.6	Оцінка вразливості, додатки та тестування на проникнення в інфраструктуру повинні бути виконані довіреною третьою стороною до прийняття в експлуатацію. Заява не буде прийнята, якщо не буде досягнуто необхідного рівня безпеки.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у розвитку та підтримці
Безпека життєвого циклу програми	R.7	Слід проводити періодичне тестування на проникнення.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у розвитку та підтримці
Безпека життєвого циклу програми	R.8	Слід отримати інформацію про технічні вразливості використовуваних інформаційних систем.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у розвитку та підтримці
Безпека життєвого циклу програми	R.9	Патчі програмного забезпечення слід протестувати та оцінити перед їх встановленням у робочому середовищі.	A.12.6 Керування технічною вразливістю та A.14.2 Безпека у розвитку та підтримці
Видалення/утилізація даних	S.3	Перед утилізацією на всіх носіях слід виконати кілька проходів програмного перезапису.	A. 8.3.2 Утилізація носія та A.11.2.7 Безпечна утилізація або повторне використання обладнання

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Видалення/утилізація даних	S.4	Якщо послуги третьої сторони використовуються для безпечної утилізації носіїв інформації або паперових записів, має бути укладена угода про надання послуг і створений відповідний запис про знищення записів.	A. 8.3.2 Утилізація носія та A.11.2.7 Безпечна утилізація або повторне використання обладнання
Фізична охорона	T.2	Чітка ідентифікація за допомогою відповідних засобів, напр. Для всього персоналу та відвідувачів, які мають доступ до приміщень організації, мають бути встановлені ідентифікаційні бейджи.	A.11 – Фізична та екологічна безпека
Фізична безпека	T.3	Повинні бути визначені зони безпеки та захищені відповідними засобами контролю входу. Необхідно надійно зберігати та контролювати фізичний журнал або електронний контрольний журнал усіх видів доступу	A.11 – Фізична та екологічна безпека
Фізична безпека	T.4	У всіх охоронних зонах повинні бути встановлені системи виявлення порушників.	A.11 – Фізична та екологічна безпека
Фізична безпека	T.5	Фізичні бар’єри, де це можливо, повинні бути побудовані для запобігання несанкціонованому фізичному доступу.	A.11 – Фізична та екологічна безпека
Фізична безпека	T.6	Вільні безпечні зони повинні бути фізично замкнені та періодично переглядатися	A.11 – Фізична та екологічна безпека
Фізична безпека	T.7	Автоматична система пожежогасіння, спеціальна система кондиціонування повітря з закритим керуванням і джерело	A.11 – Фізична та екологічна безпека

			безперебійного живлення (UPS) повинні бути реалізовані в серверній кімнаті	
	Фізична безпека	T.8	Персонал сторонньої служби підтримки повинен мати обмежений доступ до безпечних зон.	A.11 – Фізична та екологічна безпека

A.3 Запропоновані заходи для високого рівня ризику

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Політика безпеки та процедури захисту персональних даних	A.6	Політику безпеки слід переглядати та переглядати, якщо необхідно, на семестровій основі.	A.5 Політика безпеки
Ролі та обов'язки	B.4	Офіцер безпеки має бути офіційно призначений (задокументовано). Завдання та обов'язки охоронця також мають бути чітко визначені та задокументовані.	A.6.1.1 Ролі та обов’язки щодо інформаційної безпеки
Ролі та обов'язки	B.5	Конфліктні обов’язки та сфери відповідальності, наприклад, ролі офіцера безпеки, аудитора безпеки та DPO, слід розглядати як розділені, щоб зменшити можливості для несанкціонованої або ненавмисної зміни або неправомірного використання персональних даних.	A.6.1.1 Ролі та обов’язки щодо інформаційної безпеки
Політика контролю доступу	C.4	Ролі з надмірними правами доступу мають бути чітко визначені та призначені обмеженим конкретним членам персоналу.	A.9.1.1 Політика контролю доступу
Управління ресурсами/активами	D.4	IT-ресурси слід переглядати та оновлювати щорічно.	A.8 Управління активами
Процесори даних	F.5	Співробітники обробника даних, які обробляють персональні дані, повинні підпорядковуватися конкретним задокументованим угодам про конфіденційність/нерозголошення.	A.15 Відносини з постачальниками
Обробка інцидентів / порушення персональних даних	G.4	Інциденти та порушення персональних даних слід фіксувати разом із детальною інформацією про подію та подальші вжиті заходи пом’якшення.	A.16 Управління інцидентами інформаційної безпеки
Безперервність бізнесу	H.4	Має бути призначений конкретний персонал з необхідною відповідальністю, повноваженнями та компетенцією для управління безперервністю бізнесу в разі інциденту.	A. 17 Аспекти інформаційної безпеки безперервності бізнесу управління

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Безперервність бізнесу	H.5	Залежно від організації та прийнятного часу простою IT-системи слід розглянути альтернативне приміщення.	A. 17 Аспекти інформаційної безпеки безперервності бізнесу управління
Конфіденційність персоналу	I.3	Співробітники, які беруть участь у обробці персональних даних із високим рівнем ризику, повинні бути зобов'язані дотримуватись певних положень про конфіденційність (згідно з їхнім трудовим договором або іншим правовим актом).	A.7 Безпека людських ресурсів управління
Навчання	J.3	Тренінговий план із визначеними цілями та завданнями повинен бути підготовлений і виконаний на щорічній основі.	A.7.2.2 Інформаційна безпека, освіта та навчання
Контроль доступу та аутентифікація	K.7	Для доступу до систем, які обробляють персональні дані, бажано використовувати двофакторну автентифікацію. Факторами автентифікації можуть бути паролі, маркери безпеки, USB-накопичувачі з секретним маркером, біометрія тощо.	A.9 Контроль доступу
Контроль доступу та аутентифікація	K.8	Аутентифікація пристрою повинна використовуватися, щоб гарантувати, що обробка персональних даних виконується лише через певні ресурси в мережі.	A.9 Контроль доступу
Безпека сервера/бази даних	M.6	Слід розглянути методи підтримки конфіденційності на рівні бази даних, такі як авторизовані запити, запити до бази даних із збереженням конфіденційності, шифрування з можливістю пошуку тощо.	A. 12 Безпека операцій
Безпека робочої станції	N.7	Не можна дозволяти передавати особисті дані з робочих станцій на зовнішні пристрої зберігання	A. 14.1 Вимоги безпеки інформаційних систем

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Безпека робочої станції	N.8	Робочі станції, які використовуються для обробки персональних даних, бажано не підключати до Інтернету, якщо не вжито заходів безпеки для запобігання несанкціонованій обробці, копіюванню та передачі персональних даних у сховище.	A. 14.1 Вимоги безпеки інформаційних систем
Безпека робочої станції	N.9	На дисках операційної системи робочої станції має бути ввімкнено повне шифрування диска	A. 14.1 Вимоги безпеки інформаційних систем
Безпека мережі/зв’язку	O.5	Підключення до Інтернету не повинно бути дозволено для серверів і робочих станцій, які використовуються для обробки персональних даних.	A.13 Безпека зв'язку
Безпека мережі/зв’язку	O.6	Мережа інформаційної системи має бути відокремлена від інших мереж контролера даних.	A.13 Безпека зв'язку
Безпека мережі/зв’язку	O.7	Доступ до IT-системи має здійснюватися лише за допомогою попередньо авторизованих пристроїв і терміналів	A.13 Безпека зв'язку
Резервні копії	P.9	такі методи, як фільтрація MAC або	A.12.3 Резервне копіювання
Мобільні/портативні пристрої	Q.8	Контроль доступу до мережі (NAC)	A. 6.2 Мобільні пристрої та дистанційна робота
Мобільні/портативні пристрої	Q.9	Копії резервних копій також мають бути зашифровані та безпечно зберігатися в автономному режимі.	A. 6.2 Мобільні пристрої та дистанційна робота
Видалення/утилізація даних	S.5	Для доступу до мобільних пристроїв слід враховувати двофакторну автентифікацію	A. 8.3.2 Утилізація носія та A.11.2.7 Безпечна утилізація або повторне використання обладнання

КАТЕГОРІЯ	ІДЕНТИФІКАТОР КАТЕГОРІЇ	ОПИС ЗАХОДУ	ВІДПОВІДНІСТЬ СТАНДАРТУ ISO/IEC 27001: 2022 КОНТРОЛЬ
Видалення/утилізація даних	S.6	Якщо третя сторона, тобто обробник даних, використовується для знищення медіафайлів або файлів на паперових носіях, слід враховувати, що процес відбувається в приміщеннях контролера даних (і уникати передачі персональних даних за межі сайту.	A. 8.3.2 Утилізація носія та A.11.2.7 Безпечна утилізація або повторне використання обладнання