



ПРОЦЕДУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РОБОТИ З ПЕРСОНАЛЬНИМИ ДАНИМИ

ЗМІСТ

1. Сфера застосування.....	2
2. Довідкова документація	2
3. Терміни та визначення	2
4. Політика Інформаційної безпеки	2
5. Отримання згоди на обробку персональних даних	3
6. Управління базами даних, які містять інформацію про персональні дані	5
7. Дій у випадках виявлення витоку персональних даних	6
8. Відповідальність	8

Інформація та робота з інформацією та даними у []
здійснюється відповідно до вимог законодавства України.

Інформаційна безпека підприємства постійно покращується, шляхом виконання умов стандарту керівництвом та працівниками, виділенням ресурсів на інформаційну безпеку та здійснення заходів по підвищенню рівня інформаційної безпеки організації.

Політика інформаційної безпеки спрямована на досягнення таких основних цілей як забезпечення безперервності виконання основних бізнес-процесів і проектів та мінімізація можливої шкоди від порушень в сфері інформаційної безпеки.

Завданнями системи інформаційної безпеки є:

1. Дотримання вимог законодавства
2. Класифікація інформації на рівні секретності та забезпечення відповідних прав доступу для працівників організації та клієнтів
3. Керування ризиками, пов'язаними з інформаційною безпекою
4. Розроблення та підтримка процедур реагування на інциденти
5. Організація тренінгів для персоналу щодо питань забезпечення інформаційної безпеки
6. Забезпечення функціонування системи фізичного захисту інформації та активів організації

5

Згоду на обробку персональних даних отримують у працівників, поставальників, клієнтів.

Згідно із **Законом України «Про захист персональних даних»** (№ 2297-VI від 1 червня 2010 року), персональні дані визначаються як **відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.**

Персональні дані включають, але не обмежуються, такими категоріями інформації:

1. Основні ідентифікаційні дані:

- Прізвище, ім'я, по батькові.
- Дата та місце народження.
- Ідентифікаційний номер (РНОКПП).
- Паспортні дані (серія, номер, дата видачі, орган, що видав паспорт).
- Відомості про громадянство.

2. Контактні дані:

- Адреса проживання або реєстрації.
- Номер телефону, email.

3. Дані про сімейний стан:

- Одруження, розлучення.
- Відомості про дітей та членів сім'ї.

4. Освітні та професійні дані:

- Освіта, кваліфікація.
- Інформація про місце роботи та посаду.
- Професійна діяльність, досвід роботи.

5. Фінансова інформація:

- Дані про доходи, банківські рахунки.
- Кредитна історія.
- Податкові зобов'язання.

6. Дані, що стосуються здоров'я (чутливі персональні дані):

- Медичні діагнози, історія хвороб.
- Інвалідність.
- Інформація про групу крові, результати аналізів.

7. Біометричні та генетичні дані:

- Відбитки пальців.
- Фотографії, що можуть використовуватися для ідентифікації особи.
- ДНК-аналізи.

8. Інші дані:

- Інформація про судимість або адміністративні правопорушення.
- Геолокаційні дані (місце перебування особи).
- Відомості про участь у громадських організаціях, політичних партіях.

Особливі категорії персональних даних

Закон передбачає підвищений рівень захисту для **чутливих** даних, зокрема:

- Дані про расове чи етнічне походження.
- Політичні, релігійні або світоглядні переконання.
- Членство в профспілках.
- Стан здоров'я, статеве життя.

Обробка персональних даних

Обробка персональних даних допускається лише за згодою особи, за винятком випадків, передбачених законом (наприклад, для виконання службових обов'язків, судових рішень тощо).

Перед отриманням згоди необхідно чітко визначити, для яких цілей будуть використовуватися персональні дані.

Згода містить:

- Найменування особи (компанії), що здійснює обробку даних.
- Перелік персональних даних, що підлягають обробці.
- Конкретну мету обробки.
- Спосіб обробки та передачі даних третім особам (за наявності).
- Права суб'єкта даних (наприклад, відкликання згоди).
- Строк дії згоди (або умови її припинення).

Додаток 1 до цієї процедури.

Перед підписанням згоди особа повинна отримати всю необхідну інформацію про те, як будуть використовуватися її дані.

Згода може надаватися у письмовій, електронній або іншій формі, що підтверджує факт її отримання. У деяких випадках згодою може вважатися проставлення позначки у відповідному полі на сайті.

Згода має бути:

- **Добровільною:** без тиску або умов отримання послуг (якщо обробка не є обов'язковою для виконання договору).
- **Конкретною:** окремо для кожної мети обробки.
- **Неоднозначною:** виражена чіткою дією (наприклад, галочка у незаповненому полі, підпис, кнопка «Погоджуюсь»).

Важливо:

Не допускається «мовчазна» згода або автоматичне погодження через умови користування.

Організація, що отримує згоду, забезпечує її належне зберігання протягом визначеного періоду для можливого підтвердження законності обробки.

Суб'єкт персональних даних має можливість відкликати згоду на обробку своїх даних. Організація зобов'язана припинити обробку таких даних, якщо немає іншої законної підстави для цього.

6

Управління базами даних, які містять інформацію про персональні дані

Усі персональні дані, які обробляються в організації зберігаються у захищених базах даних.

Перелік баз даних наведено у таблиці 1 – картотека баз даних, які містять персональні дані.

Відповідальний працівник реєструє базу даних у картотеці.

Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них згідно з вимогами ЗУ Про захист персональних даних.

Таблиця 1. Реєстр баз даних, які містять персональні дані

№	Назва бази даних	Вид персональних даних	Розміщення	Тип інформації	Відповідальна особа	Дата початку ведення бази
	Телефонний довідник					
	Особові					
	Договори ФОП					
	Резюме					

У випадку, коли сформована нова база даних, її вносять у реєстр.

Політика інформаційної безпеки надається на ознайомлення для всіх працівників.

Вимоги політики охоплюють всі види діяльності, що виконуються в організації та є обов'язковими до виконання для всіх працівників компанії, а також для осіб, які залучаються до окремих робіт на договірній основі.

7 Дії у випадку виявлення витоку персональних даних

У разі виявлення витоку персональних даних слід негайно вжити заходів для мінімізації ризиків та захисту постраждалих осіб. Ось ключові кроки, які необхідно виконати:

Оцінка ситуації

- Визначити джерело витоку та обсяг скомпрометованих даних.
- Перевірити, які категорії персональних даних були розголошені (ПІБ, контакти, фінансові дані тощо).
- Оцінити можливі наслідки для суб'єктів даних.

Негайні заходи

- Обмежити доступ до системи або бази даних, де стався витік.
- Усунути причину витоку (наприклад, закрити вразливість, змінити паролі, зупинити роботу скомпрометованих сервісів).
- Якщо витік стався через злочинні дії (хакерська атака, злом), залучити фахівців із кібербезпеки.

Повідомлення відповідних органів

- В Україні слід повідомити Кіберполіцію (якщо витік має ознаки кібератаки).

Інформування постраждалих осіб

- Повідомити осіб, чиї дані постраждали, про ризики (наприклад, можливість шахрайства).
- Надати рекомендації щодо дій (зміна паролів, моніторинг фінансових операцій тощо).

Розслідування та запобігання подібним інцидентам

- Провести внутрішнє розслідування для виявлення причин інциденту.
- Оновити політики безпеки, посилити контроль доступу до персональних даних.
- Провести навчання співробітників щодо захисту інформації.

Юридичні та репутаційні заходи

- Якщо витік значний, підготувати офіційну заяву для громадськості.
- За потреби звернутися до юристів для мінімізації юридичних ризиків.

Правильні та своєчасні дії допоможуть зменшити наслідки витоку персональних даних і запобігти подібним ситуаціям у майбутньому.

8

Механізм надання інформації та персональних даних третім особам

Надання інформації та персональних даних третім особам регулюється законодавством про **захист персональних даних** (Закон про захист персональних даних в Україні) та міжнародними нормами, що гарантують **конфіденційність** і безпеку даних.

Загальні принципи обробки та передачі персональних даних

Передача даних можлива лише за умови дотримання таких принципів:

- ✓ **Законність** – передача має відбуватися на підставі законодавства або угоди.
- ✓ **Прозорість** – особа має бути поінформована про передачу її даних.
- ✓ **Обмеження мети** – передача можлива лише для конкретних цілей, визначених під час збору даних.
- ✓ **Мінімізація даних** – передаються лише необхідні дані.
- ✓ **Безпека** – дані мають бути захищені від несанкціонованого доступу.

Випадки, коли передача персональних даних заборонена

- ✗ **Без згоди суб'єкта даних** – якщо особа не дала явної згоди на передачу (винятки – передбачені законом).
- ✗ **Якщо це суперечить законодавству** – наприклад, передача конфіденційних даних без законних підстав.
- ✗ **Якщо є ризик шкоди особі** – наприклад, розголошення медичних, фінансових чи особистих даних без потреби.
- ✗ **Комерційний продаж або незаконне використання** – передача даних з метою вигоди без дозволу суб'єкта.
- ✗ **Передача даних неповнолітніх без дозволу батьків/опікунів** – особливо вразливі категорії, такі як діти, потребують посиленої конфіденційності.

Випадки, коли передача персональних даних дозволена

- ✓ **За згодою особи** – якщо суб'єкт даних дав явний дозвіл на передачу.
- ✓ **Для виконання договору** – якщо передача необхідна для виконання зобов'язань (наприклад, банківські операції).
- ✓ **На вимогу державних органів** – поліції, суду, прокуратури за наявності відповідного запиту.
- ✓ **Для захисту життєво важливих інтересів** – у разі загрози життю чи здоров'ю особи (наприклад, передача медичних даних лікарям).
- ✓ **Законодавчо визначені випадки** – наприклад, передача податкових або соціальних даних до відповідних установ.

Механізм передачі персональних даних

Якщо передача дозволена

- Оформлення згоди суб'єкта даних (якщо потрібно).
- Перевірка правових підстав передачі.
- Забезпечення захисту (шифрування, анонімізація).
- Фіксація факту передачі (ведення журналу дій).

Якщо передача заборонена

- Відмова в передачі з поясненням причини.
- Інформування суб'єкта даних про його права.
- Звернення до органів захисту даних, якщо є порушення.

Відповідальність

Відповідальним за розробку цієї процедури є _____

Відповідальним за моніторинг відповідності цієї політики є _____

ЗГОДА
на обробку персональних даних

Я, _____
(прізвище, ім'я та по батькові)

(_____ 19__ року народження, паспорт серія ____ № _____ ,
виданий _____),

відповідно до Закону України «Про захист персональних даних» з метою ведення бази персональних даних, забезпечення кадрового діловодства, підготовки відповідно до вимог законодавства статистичної, адміністративної та іншої інформації з питань персоналу, а також з питань реалізації визначених законодавством прав та обов'язків у сфері трудових правовідносин даю згоду на:

обробку моїх персональних даних з первинних джерел, зокрема відомостей про освіту, професію, спеціальність та кваліфікацію, науковий ступінь, вчене звання, підвищення кваліфікації, паспортних даних, даних про нагороди, відомостей про декларування доходів, зобов'язання фінансового характеру, про майновий стан щодо себе та членів своєї сім'ї (для державного службовця і особи, яка претендує на зайняття посади державного службовця), автобіографічних даних, відомостей про трудову діяльність, особистих відомостей (вік, стать, родинний стан, склад сім'ї тощо), відомостей про зареєстроване або фактичне місце проживання, про перебування на військовому обліку, даних щодо стану здоров'я в межах, визначених законодавством, щодо періоду надання відпусток, щодо підтвердження права на пільги, встановлені законодавством, щодо реєстрації фізичної особи у Державному реєстрі фізичних осіб – платників податків, ідентифікаційних даних в електронному вигляді (біографічні довідки, номери телефонів), запису зображення (фото);

використання персональних даних, що передбачає будь-які дії володільця персональних даних з обробки таких даних, їх захисту, а також дії з надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних з персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону (стаття 10 зазначеного Закону);

поширення персональних даних, що передбачає дії з передачі відомостей про фізичну особу за згодою суб'єкта персональних даних (стаття 14 зазначеного Закону);

доступ до персональних даних третіх осіб, що здійснюється відповідно до цієї згоди або вимог закону (стаття 16 зазначеного Закону).

Зобов'язуюся у разі зміни моїх персональних даних надавати у найкоротший строк уточнену, достовірну інформацію та оригінали відповідних документів для оновлення моїх персональних даних.

_____ 20__ р.

_____ (підпис)