ОКРЕМІ ВИДИ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПРАВИЛА ЇХ ЗАХИСТУ

1. Персональні дані у інформаційно-телекомунікаційних системах.
2. Персональні дані про працевлаштування.
3. Персональні дані в сфері охорони здоров’я.
4. Персональні дані у фінансовій та банківській сферах.

1. Персональні дані у інформаційно-телекомунікаційних системах.

У сучасну цифрову епоху телекомунікаційна галузь відіграє ключову роль у з’єднанні людей по всьому світу. Незважаючи на те, що розвиток технологій зробив зв’язок доступнішим, швидшим і зручнішим, він також викликав занепокоєння щодо прав особи на конфіденційність. В останні роки складна взаємодія між телекомунікаціями та правами на конфіденційність стала гарячою темою дискусій. У цій статті ми досліджуємо різні аспекти цієї проблеми, обговорюючи її наслідки, проблеми та потенційні рішення. Важливість телекомунікацій Телекомунікації революціонізували наш спосіб спілкування, уможлививши взаємодію в реальному часі незалежно від географічних кордонів. Від надання голосових дзвінків до відеоконференцій, обміну миттєвими повідомленнями та обміну файлами, телекомунікаційна галузь змінила спосіб зв’язку та роботи окремих осіб і компаній.

Телекомунікації революціонізували спосіб спілкування, уможлививши взаємодію в реальному часі незалежно від географічних кордонів. Від надання голосових дзвінків до відеоконференцій, обміну миттєвими повідомленнями та обміну файлами, телекомунікаційна галузь змінила спосіб зв’язку та роботи окремих осіб і компаній. Згідно з останніми статистичними даними:

У 2021 році кількість глобальних абонентів мобільного зв’язку досягла 5,27 мільярда, що вказує на рівень проникнення 67 відсотків.

За прогнозами, до 2026 року світовий ринок телекомунікаційних послуг досягне понад 2 трильйонів доларів.

Зростання кількості смартфонів значно сприяло зростанню телекомунікаційної галузі: станом на 2021 рік у світі користувалися 3,8 мільярда смартфонів.

Виклик прав на конфіденційність

Користуючись перевагами телекомунікацій, люди часто стикаються з проблемами конфіденційності. Обмін особистими даними, розмовами та інформацією про місцезнаходження через телекомунікаційні мережі викликає питання щодо захисту прав особи на конфіденційність. З розвитком технологій збору й аналізу даних компанії можуть збирати величезні обсяги особистої інформації, що викликає занепокоєння щодо витоку даних, крадіжки особистих даних і стеження.

Основні виклики:

Безпека даних: забезпечення конфіденційності, цілісності та доступності особистої інформації, що передається та зберігається телекомунікаційними мережами.

Збір і використання даних: баланс між необхідністю збору даних для покращення сервісу та правами конфіденційності та згодою користувачів.

Спостереження: вирішення питань щодо державного стеження та несанкціонованого доступу до особистих даних третіми сторонами.

Закони та нормативні акти щодо конфіденційності, такі як Загальний регламент захисту даних (GDPR) і Каліфорнійський закон про конфіденційність споживачів (CCPA), були прийняті для захисту прав особи на конфіденційність. Телекомунікаційні компанії повинні дотримуватися цих правил, впроваджувати надійні заходи безпеки та запроваджувати прозорі методи обробки даних, щоб зменшити ризики конфіденційності.

Рішення та шлях вперед

Вирішення складної взаємодії між телекомунікаціями та індивідуальними правами на конфіденційність вимагає багатогранного підходу із залученням різних зацікавлених сторін:

1. Телекомунікаційні компанії:

Інвестуйте в надійні засоби кібербезпеки для захисту даних користувачів від несанкціонованого доступу.

Впроваджуйте прозорі методи обробки даних, надаючи користувачам чітку інформацію про збір і використання даних.

Увімкніть функції, орієнтовані на конфіденційність, як-от наскрізне шифрування та параметри анонімного перегляду.

2. Уряди та регулюючі органи:

Встановіть суворіші правила, щоб гарантувати захист прав на конфіденційність, накладаючи штрафи за їх невиконання.

Сприяти прозорості та підзвітності, вимагаючи від телекомунікаційних компаній звітів про прозорість.

Сприяти дослідженню та розробці технологій підвищення конфіденційності для протидії загрозам конфіденційності.

3. Фізичні особи:

Ознайомтеся з правами на конфіденційність, передовими методами та інструментами, доступними для захисту їх особистої інформації.

Регулярно переглядайте налаштування конфіденційності на своїх пристроях і програмах, щоб забезпечити контроль над обміном даними.

Підтримуйте організації та ініціативи, які відстоюють права на конфіденційність і прозорість у телекомунікаційній галузі.

Інтегруючи заходи захисту конфіденційності в основу телекомунікаційних послуг, зацікавлені сторони можуть знайти баланс між технологічним прогресом і індивідуальними правами конфіденційності.

2. Персональні дані про працевлаштування

Роботодавці повинні зберігати персональні дані своїх працівників у безпеці, надійності й актуальності. Роботодавці можуть зберігати такі дані про своїх працівників без їхнього дозволу:

- назва
- адресу
- дата народження
- секс
- освіта та кваліфікація
- досвід роботи
- номер соціального страхування
- Податковий код
- контактні дані для екстрених випадків
- стаж роботи в організації
- умови працевлаштування (наприклад, оплата, години роботи, відпустки, пільги, відсутність)
- будь-які нещасні випадки, пов'язані з роботою
- будь-яке навчання
- будь-які дисциплінарні стягнення

Роботодавцям потрібен дозвіл своїх працівників на зберігання певних типів «конфіденційних» даних, зокрема:

- расова та етнічна приналежність
- релігія
- політичне членство чи погляди
- членство в профспілці
- генетика
- біометричні дані, наприклад, якщо ваші відбитки пальців використовуються для ідентифікації
- здоров'я та медичні умови

- сексуальна історія або орієнтація

Роботодавці повинні зберігати конфіденційні дані більш безпечно, ніж інші типи даних.

Працівник має право отримати повідомлення:

- які записи зберігаються та як вони використовуються
- конфіденційність записів
- як ці записи можуть допомогти в їх навчанні та розвитку на роботі
- Якщо працівник попросить дізнатися, які дані про нього зберігаються, роботодавець матиме 30 днів, щоб надати копію інформації.

3. Персональні дані в сфері охорони здоров'я.

Європейський простір даних про охорону здоров'я – це екосистема, яка складається з правил, загальних стандартів і практик, інфраструктури та структури управління, яка спрямована на:

1. Розширення прав і можливостей людей за рахунок посилення цифрового доступу до їхніх електронних персональних даних про здоров'я та контролю над ними на національному рівні та в усьому ЄС.

2. Стимулювання єдиного ринку для електронних систем медичних записів, відповідних медичних пристроїв і систем ШІ високого ризику.

3. Забезпечення надійної та ефективної установки для використання даних про здоров'я для досліджень, інновацій, розробки політики та регуляторної діяльності (вторинне використання даних).

Європейський простір даних охорони здоров'я є ключовим стовпом Європейського союзу охорони здоров'я. Він також ґрунтується на Загальному регламенті захисту даних (GDPR) і Директиві NIS 2.

Європейський Союз будує потужний Європейський союз охорони здоров'я, у якому всі країни ЄС готуються та реагують на кризи в галузі

охорони здоров’я, мають доступні, доступні, інноваційні та адекватні медичні засоби, а країни-члени працюють разом, щоб покращити профілактику, лікування та догляд за хворобами.

Пандемія COVID-19 демонструє важливість координації між європейськими країнами для захисту здоров’я як під час кризи, так і в звичайний час. Європейський союз охорони здоров’я покращує захист, профілактику, готовність і реагування на небезпеки для здоров’я людини на рівні ЄС.

3 травня 2022 р. – Європейська комісія запустила Європейський простір даних охорони здоров’я (EHDS)

1. Завдяки EHDS люди матимуть миттєвий і простий доступ до даних в електронному вигляді безкоштовно. Вони можуть легко ділитися цими даними з іншими медичними працівниками в державах-членах і між ними, щоб покращити надання медичної допомоги. Громадяни матимуть повний контроль над своїми даними та зможуть додавати інформацію, виправляти неправильні дані, обмежувати доступ для інших і отримувати інформацію про те, як і з якою метою використовуються їхні дані.

2. Держави-члени забезпечуватимуть, щоб резюме пацієнтів, електронні рецепти, зображення та звіти про зображення, лабораторні результати, звіти про виписку видавалися та приймалися в загальному європейському форматі.

3. Сумісність і безпека стануть обов'язковими вимогами. Виробники електронних систем медичних записів повинні будуть сертифікувати відповідність цим стандартам.

4. Щоб забезпечити захист прав громадян, усі держави-члени мають призначити цифрові органи охорони здоров’я. Ці органи влади братимуть участь у транскордонній цифровій інфраструктурі (MyHealth@EU), яка підтримуватиме пацієнтів у обміні даними за кордоном.

5. EHDS створює надійну правову основу для використання даних про здоров’я для досліджень, інновацій, охорони здоров’я, розробки політики та регулювання. За суворих умов дослідники, інноватори, державні установи чи

промисловість матимуть доступ до великої кількості високоякісних даних про здоров'я, що має вирішальне значення для розробки життєво важливих методів лікування, вакцин або медичних пристроїв і забезпечення кращого доступу до медичної допомоги та більш стійких систем охорони здоров'я.

6. Для доступу дослідників, компаній або установ до таких даних потрібен дозвіл від органу доступу до даних про здоров'я, який буде створено в усіх державах-членах. Доступ буде надано, лише якщо запитувані дані використовуються для певних цілей, у закритому безпечному середовищі та без розкриття особи особи. Також суворо заборонено використовувати дані для прийняття рішень, які завдають шкоди громадянам, таких як розробка шкідливих продуктів чи послуг або підвищення страхової премії.

7. Органи доступу до медичних даних будуть підключені до нової децентралізованої інфраструктури ЄС для вторинного використання (HealthData@EU), яка буде створена для підтримки транскордонних проектів.

Цифровізація є важливою для майбутнього охорони здоров'я. Цифрова трансформація має вирішальне значення для надання кращої медичної допомоги громадянам, створення міцніших і стійкіших систем охорони здоров'я, підтримки довгострокової конкурентоспроможності та інновацій у медичній галузі ЄС, а також для того, щоб допомогти ЄС оговтатися від пандемії.

Дані є невід'ємною частиною сучасного світу. При відповідальному використанні та повній повазі до фундаментальних прав він може принести неймовірну користь кожному аспекту нашого повсякденного життя, включаючи наше здоров'я. Системи охорони здоров'я держав-членів уже створюють, обробляють і зберігають величезну кількість даних. Проте громадянам часто залишається важко отримати доступ до своїх даних про здоров'я в електронному вигляді, а дослідникам – використовувати їх для покращення діагностики та лікування.

Величезна кількість даних про здоров'я генерується щосекунди, надаючи медичним службам і дослідникам потенційну цінну інформацію. За

оцінками, повторне використання даних про здоров’я коштує близько 25-30 мільярдів євро на рік. Очікується, що протягом 10 років ця цифра досягне близько 50 мільярдів євро.

Однак складність і розбіжність правил, структур і процесів усередині та між державами-членами ускладнює легкий доступ до даних про здоров’я та обмін ними. Це створює перешкоди для надання медичної допомоги та інновацій, не даючи пацієнтам можливості скористатися її потенціалом.

Крім того, системи охорони здоров'я стають об'єктами кібератак. Таким чином, сектор охорони здоров’я та відповідні органи кібербезпеки повинні розглядати кібербезпеку як ключовий фактор для забезпечення стійкості та доступності ключових медичних послуг.

По суті, сектор охорони здоров’я ЄС багатий на дані, але бідний у тому, щоб зробити його корисним для людей і науки. ЄС має використати цей величезний потенціал, щоб перетворити багатство даних про здоров’я по всій Європі в знання на службі громадян, а також для кращої профілактики, діагностики та лікування захворювань.

Дані про стан здоров’я можуть допомогти досягти ефективнішого, якіснішого, безпечнішого та більш персоналізованого догляду, а також покращити надання медичних послуг. Дані про охорону здоров’я3 та наука про дані можуть кардинально змінити громадську охорону здоров’я та революціонізувати системи охорони здоров’я, уможлививши покращення охорони здоров’я, що рятує життя. Дані про здоров’я також можуть відігравати вирішальну роль у прискоренні розробки нових медичних продуктів і методів лікування для пацієнтів, які їх найбільше потребують.

Пандемія COVID-19 чітко продемонструвала важливість цифрових послуг у сфері охорони здоров’я. Було показано, що актуальні, надійні та ЧЕСНІ дані про здоров’я є ключовими для забезпечення ефективної відповіді громадської охорони здоров’я на кризу та для розробки ефективних методів лікування та вакцин. Це також значно прискорило впровадження цифрових інструментів, таких як електронні медичні записи (особисті медичні записи

або аналогічні документи в цифровій формі), електронні рецепти та цифрові програми охорони здоров'я, а також обмін даними досліджень. Цифрові медичні продукти та послуги, включно з телемедициною, більше не є новинкою. Вони стають частиною повсякденного догляду.

Використання потужності даних про здоров'я за допомогою цифрової трансформації є особливо актуальним, коли пацієнти переїжджають у межах або в інші країни ЄС; і коли дослідникам, новаторам, політикам або регуляторам потрібні важливі дані, які можуть допомогти пацієнтам за допомогою науки. Подібним чином обмін даними про здоров'я в прикордонних регіонах, де люди набагато частіше отримують доступ до медичних послуг через кордон, буде набагато легшим.

Люди не завжди можуть легко отримати доступ до даних про своє здоров'я в електронному вигляді, і якщо вони хочуть проконсультуватися з лікарями в кількох лікарнях чи медичних центрах, вони часто не можуть поділитися даними з іншими медичними працівниками. Сьогодні дані про здоров'я пацієнта часто все ще записуються на папері, їх неможливо відстежити та розкидані по різних місцях (лікарнях, закладах загальної практики, медичних центрах тощо).

Ситуація стає ще складнішою при перетині державних кордонів. Якщо пацієнт звертається до лікаря в іншій країні, його медична інформація (зокрема діагностичні зображення) часто недоступна, що може призвести до затримок і помилок у діагностиці чи лікуванні. У більшості випадків лікарі не можуть бачити дані про стан здоров'я пацієнта, якщо він пройшов медичне втручання в іншій країні. Безперервність надання медичної допомоги та швидкий доступ до персональних електронних даних про здоров'я є ще більш важливими для жителів прикордонних регіонів, які часто перетинають кордон, щоб отримати медичну допомогу.

Відкриті публічні консультації23 щодо пропозиції Європейського простору даних про здоров'я показали, що 88% респондентів вважають, що це має сприяти контролю громадян над даними про їхнє здоров'я, включаючи

доступ до даних про здоров’я та передачу даних про здоров’я в електронному форматі. 84% респондентів стверджують, що громадяни повинні мати право передавати дані про своє здоров’я в електронному форматі іншому фахівцю чи організації на свій вибір, а 82% вважають, що вони повинні мати право вимагати від державних постачальників медичних послуг обмінюватися даними про їхнє здоров’я в електронному вигляді з іншими постачальників медичних послуг/організацій за їх вибором. 83% респондентів кажуть, що Європейський простір даних про здоров’я має сприяти наданню медичної допомоги громадянам за кордоном.

Дослідники та промисловість, а також політики та інноватори стикаються з серйозними перешкодами в доступі до даних, необхідних для розробки нових продуктів, прийняття обґрунтованих рішень або моніторингу побічних ефектів лікарських засобів у довгостроковій перспективі на основі фактичних даних. , що впливає на безпеку пацієнтів. У багатьох випадках згода є єдиним способом отримати доступ до даних для досліджень, розробки політики та регуляторних цілей. Для дослідників дуже дорого та обтяжливо отримати згоду від кожного пацієнта на використання даних пацієнта у своїх дослідженнях.

Навіть якщо пацієнт дає згоду, власники даних іноді не бажають надавати дані з причин, відмінних від захисту даних, і вважають за краще зберігати дані про здоров’я для своєї діяльності. Нинішня нормативна фрагментація між державами-членами перешкоджає дослідженням та інноваціям малих гравців, а також транскордонним дослідженням.

4. Персональні дані у фінансовій та банківській сферах.

Захист особистих даних протягом деякого часу був фундаментальною частиною бізнес-процесів і державних постанов через важливість захисту інформації окремих осіб, організацій і компаній у мережах, а також оскільки в наш час дані все ще вразливі до витоку, крадіжки, і неправильне використання.

Фінансовий сектор не є винятком. Завдяки зусиллям багатьох банківських компаній і фінансових установ, а також, звісно, появі фінтехів, засоби контролю та регулювання, які гарантують захист персональних даних, кардинально змінилися. Чималий внесок також зробили цифровізація, конвергенція галузей і популяризація «цифрових екосистем», які швидко обмінюються інформацією.

У цій публікації ми детально пояснимо, що насправді означає захист персональних даних у фінансовому секторі та як це робити правильно, щоб уникнути переважної більшості проблем, пов'язаних із неналежним використанням інформації.

Контекст захисту даних у фінансових компаніях

Обмін особистою інформацією під час ділової операції став звичним явищем для більшості фінансових установ. Це може призвести до обміну не лише банківськими даними, але й номерами рахунків і кредитних карток, а також особистою інформацією, включаючи імена, посвідчення особи та електронну адресу.

Тому організаціям довелося вжити нових заходів для захисту даних клієнтів установ. Це включає таку інформацію, як імена, адреси, номери соціального страхування, кредитна історія та інші конфіденційні дані, які можна використовувати для ідентифікації особи чи її фінансового стану.

Чому це важливо?

Операційна структура фінансових послуг вимагає більш надійних механізмів безпеки даних порівняно з іншими галузями. Повсякденно фірми, які надають фінансові послуги, мають справу з великою кількістю особистої інформації своїх клієнтів, і цілісність ресурсів користувача та репутація організації залежать від належного управління персональними даними.

Успіх чи поразка фінансової установи сьогодні значною мірою залежить від балансу, який існує у використанні конфіденційної інформації та стандартів її захисту.

Це створило нові виклики для галузі, про які ви повинні знати.

Основні виклики щодо безпеки даних у галузі

Оскільки захист персональних даних у фінансовому секторі дуже важливий для регуляторів і засобів масової інформації, організації в цій галузі продовжують стикатися з тиском щодо підтримки високих стандартів безпеки. Це спричиняє неминучі проблеми, такі як:

Інформаційна гнучкість

Фінансові установи повинні забезпечувати механізми динамічного доступу для надання конфіденційних персональних даних своїм клієнтам, співробітникам і зовнішнім партнерам через великий потік інформації, якою вони обмінюються, яку важко контролювати.

Поширення соціальних мереж

Соціальні мережі дуже активно використовуються фінансовими компаніями для створення брендів і налагодження стосунків зі споживачами.

Хоча ці платформи пропонують відносно недорогі методи створення маркетингових кампаній для продуктів і послуг, вони також створюють нові ризики та виклики для підтримки безпеки даних, оскільки взаємодії можуть містити особисту інформацію клієнтів.

Витонченість зовнішніх хакерів

Ні для кого не секрет, що поширення кіберзагроз за останні роки надзвичайно зросло. Наприклад, кількість атак програм-вимагачів у 2021 та 2022 роках зросла втричі порівняно з 2020 роком. Це свідчить про важливість кібербезпеки для компаній у фінансовому секторі.

Кіберзлочинці вдосконалили свої методи викрадення та фільтрації особистої інформації клієнтів за допомогою вірусів, шкідливих програм та інших альтернатив, призначених для обходу традиційних технологій кібербезпеки та доступу до конфіденційних даних.

Навчання співробітників захисту даних

У той час як фірми використовують рішення для запобігання втраті даних або DLP, співробітники цих фірм продовжують відігравати важливу роль у запобіганні витоку даних і обробці конфіденційної інформації.

Як наслідок, для фінансових компаній може бути досить складно постійно навчати свій існуючий персонал і навчати нових членів щодо безлічі існуючих кіберзагроз і загроз безпеці.

Це спонукає нас говорити про рішення, які можуть зменшити ці ризики та дозволити фінансовим установам ефективно виконувати свою політику захисту персональних даних.

Поради щодо забезпечення захисту даних у фінансовому секторі

Щоб допомогти вам адаптувати методи, техніки та політику захисту даних у вашій організації, ми надамо вам найкращі поради для початку:

Визначте та класифікуйте конфіденційну інформацію: визначте, яку інформацію можна вважати конфіденційною інформацією, і класифікуйте її відповідно до рівня важливості.

Зменшіть доступ до інформації: запровадьте моніторинг даних, аутентифікацію та рішення для керування доступом.

Використовуйте інструменти безпеки: захищайте інформацію клієнтів за допомогою різноманітних елементів керування безпекою та передових технологій, таких як шифрування, токенізація та маскування даних.

Створіть чітку внутрішню політику: детально визначте процеси, рішення, кроки та механізми безпеки та захисту даних для співавторів, зовнішніх партнерів і користувачів.

Сплануйте заходи на випадок витоку даних: визначте механізми управління кризою та протоколи, яких слід дотримуватися під час витоків або загроз.

Список використаних джерел:

1. Personal data an employer can keep about an employee. *GOV.UK* : website. URL : https://www.gov.uk/personal-data-my-employer-can-keep-about-me

2. Protecting Personal Data in the Financial Sector. *SYDLE* : website. URL : https://www.sydle.com/blog/protecting-personal-data-financial-sector-64b574331b980e466f1eb4df

3. Telecommunications and Personal Privacy Navigating the Challenges. *Utilities One* : website. URL : https://utilitiesone.com/telecommunications-and-personal-privacy-navigating-the-challenges

4. The European Health Data Space. *EHDS* : website. URL : https://www.european-health-data-space.com/