



**Розділ десятий**  
**зі звіту 2018 Deloitte**  
**Global Human Capital**  
**Trends**

# Дані про працівників: як далеко може зайти аналітика?

---

Упродовж останніх декількох років неймовірної популярності набуло використання даних про працівників для аналізу, прогнозування та підвищення показників їхньої продуктивності. Проте, використання персональних даних про працівників – це можливості та ризики водночас.

---

## Аналіз даних про працівників стає поширеною практикою

Напрямок застосування аналізу даних про працівників швидко розвивається, з'являються нові можливості для створення ефективних процесів підбору, управління, утримання та оптимізації робочої сили. Організації, які накопичують все більшу кількість інформації про працівників зіштовхуються з ризиками та етичними питаннями, пов'язаними із безпекою і прозорістю даних, а також необхідністю отримувати дозвіл на їх використання та зберігання. Наразі організаціям потрібні надійні політики безпеки та прозорості інформації, задля запобігання занепокоєння у працівників через порушення конфіденційності та можливість зловживання.

За останні роки важливість цього інструмента надзвичайно зросла. 84% респондентів цього річного дослідження оцінили питання аналізу даних про працівників як «важливе» або «дуже важливе» (данний тренд є другим

за рівнем важливості серед усіх десяти трендів цього року).

Чим пояснюється стрімке підвищення інтересу до аналізу даних про працівників? По результатам дослідження нами було виявлено три переваги, які у сукупності створюють вагомий цінність.

Посилена увага до рівня продуктивності праці, залученості працівників та питань різноманітності й гендерної рівності, піднімає питання про удосконалення методів управління персоналом на рівень керівництва.

Великі інвестиції у сферу HR, зокрема в аналіз даних про працівників, відкривають багато нових джерел даних. За результатами дослідження понад 70% респондентів сьогодні займаються реалізацією великих проектів, пов'язаних з аналізом та інтеграцією даних у процес прийняття рішень.

В організаціях наростає занепокоєння щодо захисту даних про працівників, і на це є вагомий причини. Цього року лише 10% респондентів вважають, що їхні компанії «цілком готові» до протистояння такому виклику.

## Дані про працівників як потужний інструмент

Революція у сфері обробки даних про працівників, яку пророкували роками, нарешті настала. 69% організацій будують інтегровані системи аналізу даних про працівників, а 17% уже мають інформаційні панелі, що відображають дані в режимі реального часу, упорядковуючи їх новими високоефективними способами.<sup>1</sup> Серед компаній 3-4-го рівнів у моделі зрілості функції з аналізу даних про працівників, розробленій Джошем Берсіном,<sup>2</sup> Провідні компанії здійснюють моніторинг даних про працівників, що надходять з різних джерел: ЗМІ (17%), опитування (76%), інтегровані бази даних систем HR-функції та фінансів (87%).<sup>3</sup> На базі такого різноманіття джерел сучасні організації здійснюють інтелектуальний аналіз даних та створюють їх комплексну архітектуру, що генерує аналітичні дані про увесь досвід співробітників, їх просування, кар'єрну мобільність та ефективність.

Провідні методи аналізу даних тепер можуть відстежувати та аналізувати велику кількість інформації, зокрема дані, отримані за допомогою голосових повідомлень, відео дзвінків та особистої комунікацій. Навіть більше, відтепер є можливість відслідковувати та вимірювати емоційний настрій працівників через електронні листи.<sup>4</sup> Деякі компанії пропонують програмне забезпечення для організаційного аналізу мереж (organizational network analysis – ONA), яке інтерпретує дані трафіку електронної пошти для контролю рівня стресу працівників

та допомагає виявляти випадки шахрайства, зловживань та недоліків в управлінні. Інші ONA-інструменти можуть аналізувати відгуки працівників, надсилати поради керівникам різних напрямів і визначати ключові ресурси управління знаннями.<sup>5</sup>

## Більша винагорода – вищі ризики

Інструменти аналітики пропонують величезні можливості. Проте, всупереч очевидним перевагам, багато керівників повільно або неохоче визнають можливі ризики.

Насправді, деякі організації вважають, що сам факт зберігання даних вже створює ризики, через що в Європейському Союзі (ЄС) та інших країнах існує вимога видаляти будь-які дані одразу після того, як зникає потреба в їхній обробці. Новий Загальний регламент ЄС щодо захисту даних (General Data Protection Regulation – GDPR), який набрав чинності 25 травня 2018 року, розширює цю концепцію, визначаючи дані з високим ступенем ризику як такі, що «можуть створити великі ризики для прав і свобод громадян».<sup>6</sup> Організації приватного сектора повинні йти в ногу з передовими практиками, спрямованими на посилення регулювання конфіденційності даних. За порушення нових правил GDPR компаніям загрожує штраф у розмірі 20 мільйонів євро,



Організації наближаються до критичного обсягу даних про працівників, що використовуються, і це може призвести до негативної реакції з боку працівників, клієнтів та громадськості.

що є вагомим стимулом для організацій серйозніше ставитися до захисту даних.<sup>7</sup>

Які ризики створюють найбільшу загрозу? Цьогорічне дослідження формує чітку аналітичну картину. 64% респондентів повідомили, що вони активно управляють юридичною відповідальністю, пов'язаною з даними про працівників їхніх організацій. 6 із 10 компаній зазначили, що вони стурбовані тим, як працівники сприймають той факт, що їхні дані використовуються. Проте, лише чверть респондентів повідомили, що їхні організації регулюють вплив цих ризиків на бренд компанії.

Побоювання щодо конфіденційності даних працівників виправдовуються. Існують приклади, коли роботодавці встановлюють на робочих місцях датчики температури тіла, щоб відстежувати, скільки годин працівники проводять у офісі. Обурені працівники закидали менеджерів скаргами та розповідали невітні історії у ЗМІ.

Хоча 75% компаній усвідомлюють необхідність забезпечення безпеки даних, лише 22% мають надійні механізми захисту даних про працівників.<sup>8</sup> Натомість, дослідження показує, що існує 30% компаній, які не мають структур з управління даними та вважають, що інформація про працівників не може бути розкритою.<sup>9</sup>

### **Занепокоєння щодо управління даними про працівників із застосуванням штучного інтелекту**

Ризики, пов'язані з безпекою даних, існують вже давно, проте зараз вони набувають особливої актуальності. Поєднання даних про працівників та штучного інтелекту потребує втручання людини, адже рішення машин в даному випадку може бути не зовсім точним та зрозумілим.

Навіть такі високотехнологічні компанії, як Facebook та Twitter, виявили, що штучний інтелект без людини може зашкодити.<sup>10</sup> Враховуючи це, вони наймають тисячі людей для спостереження за алгоритмами функціонування соціальних мереж і реклами на основі штучного інтелекту.<sup>11</sup> HR-організації повинні бути максимально пильними в процесі моніторингу рішень пов'язаних з машинами, задля забезпечення їх неупередженості.

Провідні технологічні компанії починають більше інвестувати у вирішення цих проблем. Консорціум експертів у сфері обробки даних нещодавно організував «Партнерство зі штучного інтелекту» - платформу, що фінансується Amazon, Apple,<sup>12</sup> Facebook, Google, IBM і Microsoft. Метою її створення є формулювання методів роботи зі штучним інтелектом з урахуванням його впливу на людей та суспільство в цілому.<sup>13</sup> Джинні Рометті (Ginny Rometti), генеральний директор IBM, також виклав цілу низку етичних принципів стосовно використання даних та штучного інтелекту.<sup>14</sup>

### **Як протистояти ризикам**

Незважаючи на потенційні ризики, інформація, отримувана в ході аналізу даних про працівників, залишається надто цінною, щоб організації могли від неї так просто відмовитися. Наприклад, GE, Visa, IBM та інші компанії розробляють набір аналітичних інструментів, які здійснюють пошук потенційних кандидатів на посади та рекомендують їм навчання.<sup>15</sup> Група HR-аналітиків компанії GE використовує дані, які відстежують «історію пересування працівників та сукупність виконуваних ними робіт», таким чином розкривають нові можливості для працівників у межах всієї компанії, незалежно від підрозділу чи регіону.<sup>16</sup> Для підвищення продуктивності компанія Hitachi Data Systems використовує «розумні значки» (smart badges), які відстежують ті поведінкові реакції, що створюють у працівника відчуття задоволеності та підвищують його продуктивність. Потім ці дані використовуються для реорганізації робочих місць і команд.<sup>17</sup>

Передбачається, що наступного року відбудеться вибухове зростання попиту на інтелектуальні продукти, які використовують дані про працівників. Саме тому необхідно забезпечити ефективно управління усім спектром ризиків, пов'язаних зі збором, зберіганням та використанням даних. Серед основних стратегій, що дають змогу ефективно використовувати дані про працівників та управляти ризиками є шифрування персональної інформації.

### Створення безпечного організаційного клімату

Цілком зрозуміло, що управління даними про працівників вимагає суворих політик з безпеки та прозорості. Одним із важливих аспектів управління ризиками, є вимога знати всі місця, де зберігаються персональні дані. Для забезпечення належного рівня прозорості та застосування відповідних засобів захисту необхідно скласти карту вхідних та вихідних потоків персональних даних.

У провідних організаціях IT-, HR- та юридичний департаменти колективними зусиллями розробляють рекомендації для організацій, які допомагають управляти існуючими ризиками. Такі компанії мають чітку політику та інформаційні ресурси, які пояснюють працівникам, які саме дані збираються та як вони використовуються. Даний підхід допомагає донести до працівників переваги використання даних та їх позитивний вплив на процес роботи та розвитку кар'єри.

### Висновки

Організаціям слід чітко усвідомлювати всі можливості та ризики використання даних про працівників. Особливої уваги потребують питання якості та безпеки даних, управління якими здійснюється за допомогою машин та технологій штучного інтелекту. Даний виклик у сфері HR швидко та не без підстав набуває пріоритетності.



## Джерела

1. Bersin, Deloitte Consulting LLP, High-impact people analytics research, 2017.
2. Madhura Chakrabarti, The people analytics maturity model, Bersin, Deloitte Consulting LLP, 2017.
3. Madhura Chakrabarti, Seven top findings for driving high-impact people analytics, Bersin, Deloitte Consulting LLP, 2017.
4. Bersin, Deloitte Consulting LLP, Predictions for 2018: Embracing radical transparency, 2018.
5. Josh Bersin, conversations with vendor executives.
6. [The General Data Protection Regulation \(GDPR\) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union \(EU\). It also addresses the export of personal data outside the EU. EU Publications, "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 \(General Data Protection Regulation\)," accessed March 8, 2018.](#)
7. [Cheryl O'Neill, "GDPR Series, part 4: The penalties for non-compliance," Imperva, March 14, 2017.](#)
8. Bersin, Deloitte Consulting LLP, High-impact people analytics research, 2017.
9. [Mary Young and Patti Phillips, Big data doesn't mean 'Big Brother': Employee trust and the next generation of human capital analytics, The Conference Board, 2016.](#)
10. [Christopher Mims, "Without humans, artificial intelligence is still pretty stupid," Wall Street Journal, November 12, 2017.](#)
11. **Попереднє джерело;** [Todd Spangler, "Mark Zuckerberg: Facebook will hire 3,000 staffers to review violent content, hate speech," Variety, May 3, 2017;](#) [Benjamin Mullen, "Twitter is hiring people with 'newsroom backgrounds' as real-time curators," Poynter, June 18, 2015.](#)
12. Global Human Capital Trends 2018 is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc.
13. [Partnership on AI to Benefit People and Society, "Goals," accessed March 8, 2018.](#)
14. [Larry Dignan, "IBM's Rometty lays out AI considerations, ethical principles," ZDNet, January 17, 2017.](#)
15. [Andrew McIlvaine, "GE is reinventing talent management," Human Resource Executive, September 14, 2017.](#)
16. Josh Bersin, conversations with GE executives, November 2017.
17. [Josh Bersin, conversations with Hitachi executives; AI Business, "Hitachi developing AI to improve workforce efficiencies," September 28, 2015.](#)

# Deloitte. Insights

Підпишіться на оновлення Deloitte Insights на веб-сайті [www.deloitte.com/insights](http://www.deloitte.com/insights)



Deloitte в Твіттері @DeloitteInsight

## Автори Deloitte Insights

**Редакційна колегія:** Junko Kaji, Karen Edelman, Abrar Khan, Nikita Garia, Matthew Budman, Rithu Thomas, Preetha Devan

**Творча команда:** Sonya Vasilieff, Molly Woodworth

**Реклама:** Amy Bergstrom, Alex Kawecky

**Графічне оформлення:** Traci Daberko

### Про Deloitte Insights

Deloitte Insights публікує оригінальні статті, звіти та періодичні видання, що надають цінну інформацію для бізнесу, підприємств державного сектору та неурядових організацій. Наша мета полягає в тому, щоб на основі даних досліджень та досвіду, отриманих від усієї нашої організації, що надає професійні послуги, а також від співавторів з наукових та бізнесових кіл, сприяти конструктивній розмові з широкого спектра питань, що цікавлять керівників та державних діячів.

Deloitte Insights є виданням компанії Deloitte Development LLC.

### Про цю публікацію

Ця публікація містить лише загальну інформацію, і ані «Делойт Туш Томацу Лімітед», ані фірми у її складі або її чи їхні афілійовані особи не надають бухгалтерські, ділові, фінансові, інвестиційні, юридичні, податкові чи інші професійні консультації або послуги за допомогою цієї публікації. Ця публікація не замінює собою такі професійні консультації чи послуги, а також не повинна використовуватися як підстава для будь-яких рішень або дій, які можуть вплинути на ваше фінансове становище чи ваш бізнес. Перш ніж прийняти будь-яке рішення або вжити заходів, які можуть позначитися на ваших фінансах чи вашому бізнесі, вам слід звернутися до кваліфікованого професійного консультанта.

Ані «Делойт Туш Томацу Лімітед», ані фірми у її складі або її чи їхні афілійовані особи не несуть жодної відповідальності за будь-які збитки, зазанані будь-якою особою, яка покладається на цю публікацію.

### Про «Делойт»

Назва «Делойт» стосується однієї чи кількох юридичних осіб: «Делойт Туш Томацу Лімітед», приватної компанії з відповідальністю учасників в гарантованих ними межах, зареєстрованої за законодавством Великої Британії («ДТТЛ»), мережі фірм-учасників ДТТЛ та пов'язаних

з ними осіб. ДТТЛ і кожна з її фірм-учасників є самостійними та незалежними юридичними особами. ДТТЛ (також іменується як «Делойт Глобал») не надає послуги клієнтам. У Сполучених Штатах назва «Делойт» стосується однієї чи кількох американських фірм-учасників ДТТЛ, пов'язаних з ними осіб, які здійснюють свою діяльність у Сполучених Штатах, використовуючи назву «Делойт», та їхніх афілійованих осіб. Деякі послуги можуть бути недоступними для замовників аудиторської перевірки відповідно до правил і положень державного бухгалтерського обліку та незалежної аудиторської діяльності. Докладну інформацію про нашу глобальну мережу фірм-учасників розміщено за посиланням [www.deloitte.com/about](http://www.deloitte.com/about).

© 2018 Deloitte Development LLC. Усі права захищені.

Учасник «Делойт Туш Томацу Лімітед»