Baker Tilly tells clients of a data breach at a third-party provider



Baker Tilly Advisory Group is notifying clients that a breach compromised certain personal information about them and their dependents. The source excerpt is brief and gives no further detail.

- Baker Tilly Advisory Group is sending notifications to clients.
- The breach is linked to a third-party provider.
- Certain personal information about clients and their dependents was compromised.
- The available source text does not state the number affected, the data types, or the dates.

What was reported

Baker Tilly Advisory Group has begun notifying clients that a data breach has compromised certain personal information about them and their dependents. According to the report, the incident occurred at a third-party provider rather than being described as a breach of the firm's own systems.

The portion of the report available to us is short. It does not say how many people are affected, which categories of personal data were involved, when the incident took place, or which provider was responsible. We have therefore not included any of these details.

Why it matters for regulated institutions

The case is a reminder that personal data held by suppliers, including advisory and professional-services firms, can be exposed even when the institution's own environment is not affected. Information about dependents adds to the sensitivity, since those individuals may never have dealt with the supplier directly.

Institutions in the Kingdom that share employee, client or family-related data with external advisers should treat third-party exposure as part of their normal risk and data-protection oversight.

Suggested approach

No action is required from the news alone unless your organisation uses Baker Tilly or shares personal data with a similar provider. In that case, review what data is shared, confirm how incidents are notified to you, and wait for the details the provider sends before drawing conclusions.

What to do now

1. Check whether your organisation or its staff are clients of Baker Tilly or share personal data with it.
2. Inventory the personal data, including dependents' data, shared with external advisers and professional-services providers.
3. Confirm that supplier contracts require timely breach notification and define what information must be provided.
4. If you receive a notice, assess the PDPL implications and your notification duties before responding.
5. Add third-party data exposure scenarios to incident response and supplier review plans.