The disconnect between policy and reality

As business consultants, we frequently audit corporate privacy frameworks. The most common vulnerability we find is the disconnect between Legal and IT.

Legal departments draft comprehensive privacy statements and retention schedules. These documents look great on paper and satisfy the regulators during an initial check. However, these policies are rarely operationalized. IT departments are tasked with keeping systems running and ensuring data is available, not necessarily deleting it. Without a clear mandate and translated requirements, the default IT setting is often to keep everything forever.

When a breach occurs, this disconnect transforms a theoretical compliance issue into a severe reputational and financial crisis. You cannot defend a leak of data that you publicly claimed you no longer possessed.

What we do

A privacy statement that does not reflect your actual IT practices is maybe worse than no statement at all. We have guided numerous organizations through the complex journey of aligning their business processes, implementing the right tooling, and turning their data retention policies into a verifiable reality.

Do not wait for a breach to find out your retention policy is broken.

The cost of data hoarding: Why your privacy statement means nothing without a data retention strategy

A privacy statement is just a piece of paper until it is hardcoded into your IT infrastructure

Across Europe, regulators are increasingly confronting a recurring pattern in data breach investigations: organizations suffer a cyberattack, only to discover that the data exposed should never have been there in the first place. Retention periods promised in privacy statements had simply not been enforced in practice. The GDPR is unambiguous on this point. Article 5 requires that personal data be kept no longer than necessary. Yet time and again, the gap between policy and IT reality turns a security incident into a full-scale compliance crisis. Supervisory authorities across the EU have issued substantial fines specifically for excessive data retention following breaches. This pattern highlights a harsh reality. Storing customer data indefinitely is no longer a business asset, but it is a liability. If you suffer a breach, the regulator and the public will not just ask how the hackers got in. They will ask why you still had that data in the first place.

The solution

Fixing the data retention problem requires moving beyond manual clean-ups and Excel sheets. Based on our extensive work helping clients successfully operationalize data retention and prevent leaks, success relies on two critical pillars:

- **Bridging the IT-business gap** Retention cannot be an isolated exercise. Protiviti play a crucial role in translating legal requirements into technical rules that data architects and system administrators can actually build into the databases. There must be shared ownership: Legal defines the what and when, Business defines the impact, and IT executes the how.
- **Automated tooling** Humans having a hard time deleting information. Relying on account managers to manually purge old customer records is a guaranteed path to failure. Organizations must invest in automated Data Lifecycle Management (DLM) tooling such as OneTrust. OneTrust is able to map where sensitive data lives across the organization and enforce automated retention and deletion schedules based on the rules agreed upon by the business.

Contacts

Yvonne van der Schoot
Senior Manager,
Protiviti The Netherlands
T. +3120.346.0400
yvonne.vanderschoot@protiviti.com

Tim van Grinsven
Senior Manager,
Protiviti The Netherlands
T. +3120.346.0400
tim.vangrinsven@protiviti.com

Tjakko de Boer
Managing Director,
Technology Consulting
Protiviti The Netherlands
T. +3120.346.0400
tjakko.deboer@protiviti.com

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organizations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the *Fortune 100 Best Companies to Work For®* list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

protiviti®