

CASE STUDY

SaaS Company Manages Data Breach with No Enforcement Action

Company profile

- B2B SaaS, Series B, ~120 employees, existing DPO client
- EU and US customers, processing business and employee data

The incident

A misconfigured cloud storage bucket exposed a subset of customer records for ~48 hours: business contact information and some employee records from HR integrations. Discovered Friday evening.

What we did

Friday evening:

- Incident call within 30 minutes (24/7 breach support)
- Containment guidance, initial risk assessment, notification threshold determination

Weekend:

- Detailed impact assessment, supervisory authority notification filed within 72 hours
- Customer notification drafted, internal incident report for management and board

Following week:

- Customer and data subject notifications sent
- Remediation plan implemented, post-incident review, updated access controls

Results

- Authority notification filed within 72 hours
- No enforcement action
- No customer churn in the quarter following the incident
- Customers acknowledged transparency and speed

Key takeaway

Having a DPO on retainer with 24/7 breach support meant expert guidance within 30 minutes. That speed made the difference between a managed incident and a potential crisis.

Ready to talk? Book a free scoping call: engagecompliance.co/contact

Engage Compliance: senior-led outsourced DPO for tech companies. DPO and privacy lead across 100+ organizations including Amazon, Coinbase, Robinhood, and Medtronic (prior experience, not endorsements).

Transparent pricing from EUR 500/month. PI insurance on all engagements. 24/7 breach support.

engagecompliance.co/contact | info@engagecompliance.co