How to stay on top of a catastrophe

A guide for multi-national data breaches

Agenda outline

Session outline

I. Welcome, introductions (2 mins) KW & MB
II. Who's in the room – live polls (3 mins) KW
III. Set the scene – who are City Airports Group? (5 mins) MB
IV. One scenario (10 mins) KW
V. Best practices (8 mins) MB:
    - Ownership and RACI, coordinating authorities, consistent decision-making, difficult calls and the after action review
VI. Feedback, closing remarks and resource list (2 mins) KW & MB

Welcome and introductions



Katharina Weimer
Partner
Fieldfisher



Maddie Bonvin
CIPP/E, CIPM, CIPT
Head of Data Protection
The Bicester Collection

Who's in the room

transition

Poll 1 – Your privacy oversight territory

- Germany only
- EU / EEA
- Germany and EU / EEA
- Global – multiple regions

Poll 2 – What is your role?

- DPO or privacy lead
- Legal counsel or external adviser
- IT, security or incident response
- Compliance, risk, commercial or other business role

Poll 3 – How long have you worked in privacy law?

- Under 3 years
- 3 to 7 years
- 8 to 15 years
- More than 15 years

Set the scene

Who are City Airports Group?

Owner and operator of airports with terminal retail — fashion, beauty and food — across several jurisdictions.

The business is centred around these key activities:

1

Leasing

Rent terminal retail units to **Brand partners**. Brands run their own sales independently — tills, stock and staff.

2

Loyalty & Guest Experience

"**Fly and Buy**" loyalty scheme and app — linking boarding passes, recording spend, redeeming rewards — plus gift cards, reserve & collect and personal shopping.

3

Data Ownership

Loyalty database solely owned by City Airports. No personal data is shared with Brands, who hold their own sales data.

4

Real Estate

Management of airport terminal facilities, including security, passenger flow and health and safety.

Scenario

KATHARINA

Facts

A supplier of City Airports Group (UK) located in a 3rd country suffered from a phishing attack. This has resulted in unauthorised access to the data of employees at City Airports SARL (France). The supplier has notified City Airports Group of the incident within 24 hours. It is not clear whether the data was downloaded by the malicious actor.

Consider

1. Ownership:
   - which City Airports entity is the controller, who is responsible and accountable for the data in question, and what do you require from the supplier?
2. Coordinating authorities:
   - will you notify? If yes, which regulator(s) are notified, which entity reports, and who is named as the point of contact?
3. Consistent decisions:
   - how do you assess the risk and evidence the decision – including a decision not to report?
4. Data subjects:
   - will you tell the affected employees? On what test, in which language, and by when?
5. Difficult calls:
   - what do you say to the supplier, employees and executives while it is unclear whether data was downloaded, and which steps mitigate and prevent re-occurrence?

Incident and Breach Assessment Template Content

Best practice 1

1. Incident Summary and Data Impacted
2. Investigation and Actions
3. Control Measures in Place
4. Risk Rating
5. Breach Harm Risk Assessment
6. Notification Approach
7. Points for Clarification & Recommendations
8. Evidence and Sign-Off

Using this template

- Complete sections 1–4 for every incident, reportable or not
- Sections 5-8 onwards only where the breach threshold is met
- Show your working – this is the accountability record
- Depending the scale of breach, allocate a 'loggist' to complete the template
- Feeds the breach register, battleship grid and AAR

RACI
Responsible, Accountable, Informed, Consulted
Best practice 2

Breach Response Activity	Privacy / DPO	Legal	IT & Security	Comms	Executive Sponsor
1. Detect, log and triage the incident	**A**	**C**	**R**	**I**	**I**
2. Contain, investigate and remediate	**C**	**I**	**R**	**I**	**A**
3. Assess risk, severity and scope	**R**	**C**	**C**	**I**	**A**
4. Decide whether the breach is notifiable	**R**	**A**	**C**	**I**	**C**
5. Notify the regulator(s) within 72 hours	**R**	**A**	**I**	**C**	**I**
6. Communicate to affected data subjects	**C**	**A**	**I**	**R**	**C**
7. Maintain the breach register and evidence	**A**	**C**	**R**	**I**	**I**
8. After action review and lessons learned	**A**	**C**	**R**	**C**	**I**

How to use a RACI for breach response

- **Agree it before an incident** – a live breach is not the time to debate who decides.
- **One Accountable per activity** – a single named owner who signs off. Two A's means delay.
- **Responsible does the work** – name deputies for out-of-hours, holiday and sickness cover.
- **Consulted is two-way** (local counsel, processors, Brand partners); Informed is a one-way update.
- **Map it to the 72-hour clock** – mark which activities must complete before the notification deadline.
- **Run it per jurisdiction** – the Accountable entity changes where a local regulator leads.
- **Record names and contact details**, not just job titles, and keep an escalation route.
- **Test and refresh it** in the After Action Review and whenever teams or suppliers change.

Key:
R = Responsible (does the work) A = Accountable (owns the decision, one only) C = Consulted (two-way input) I = Informed (kept updated)

Battleship Visual Data Mapping!

Best practice 3

Sum up the scope of impact to internal and external stakeholders, regulators and customers.

One colour-coded grid shows every system in scope, how far each search has got and where the gaps are, without anyone reading a single report.

Not Applicable	Applicable	Affected	Contained	Remediated

Data source category	System 1	System 2	System 3	System 4	System 5	System 6
Personnel & HR systems						
Office 365 & collaboration tools						
Instant messaging						
Printed & physical records						
Enterprise platforms & applications						
Loyalty database						
Mobile devices						
Recordings & transcripts						
Backups, archives & security tooling						
Third parties, processors & business partners						

Maintaining a battleship for breach purposes

- **Build it before an incident** use details from your ROPA – every system, site, device and supplier that could hold personal data.
- **One row owner, named in the RACI**, so no category is left unchecked.
- **Colour each tile as it moves** through the legend; a tile that has not moved since the last stand-up is an escalation.
- **Log date, searcher and evidence link** for every tile – the grid is your audit trail of accountability.
- **Do not skip the hard tiles** – backups, archives, mobile devices, CCTV and paper are the ones most often missed.
- **Include processors and Brand partners**; you remain accountable for searches carried out on your behalf.
- **Timestamp every status change** so you can reconstruct the 72-hour timeline for the regulator.
- **File the completed grid** with the breach register and the After Action Review as evidence of a complete investigation.

AAR (After Action Review)
Business continuous improvement

Best practice 4

Learnings are key to getting back to business as usual!

1. What was the objective?

The incident, the entities and data involved, and what the playbook required us to achieve – contain, assess, decide and notify on time.

2. What went well?

The practices, decisions and people that worked. What we keep, repeat and write into the playbook.

3. What did not go well?

Gaps in detection, ownership, the data map, supplier response or communications. Process and facts, never individuals.

4. What did we learn?

Root cause, the decision and its rationale (including a decision not to report), and corrective actions with named owners and due dates.

Using the AAR after an incident or breach

- **Run it within 10 working days** of closing the incident, while recollection and evidence are fresh.
- **Keep it no-blame** – review the process and the facts, never the individual.
- **Invite the whole RACI**, plus the processor or Brand partner where they were part of the response.
- **Evidence a decision NOT to report**: record the risk assessment, the test applied, who decided, when, and the evidence relied on.
- **Log every incident in the breach register**, reported or not – the register plus the AAR is what a regulator asks to see.
- **Attach the artefacts** – battleship grid, decision log, RACI, notification drafts and communications.
- **Convert findings into owned, dated actions**; an AAR without actions is not accountability.
- **Feed it back** into the playbook, RACI, data map and training, and re-test at the next dry run.