www.complykey.com

COMPLYKEY

DATA BREACH MANAGEMENT

BREACH RESPONSE AND MONITORING

MAKING THE CASE FOR COMPLIANCE

Data breaches, whether minor like misdirected emails or significant like cyber-attacks, can affect all organisations. According to GDPR, controllers must report personal data breaches unless they can prove there's a low risk to individuals' rights and freedoms.

Risks of not Following DPC Guidelines

‘The DPC requires all organizations with personal data to have procedures for detecting, managing, and recording data incidents and breaches. Non-compliance carries penalties, including fines of up to €10M or 2% of turnover.’

DPC Expectations

1 You need to be able to detect, investigate, risk-assess, and record any breaches.

2 Under Article 33(1) of the GDPR, the controller must report data breaches as appropriate.

3 You must centrally log/record/document both actual breaches and near misses (even if they do not need to be reported to the DPC or individuals).

4 You must have procedures in place to assess all security incidents and report relevant breaches to the DPC not later than 72 hours. (Even when all the information is not yet available). (Article 33(1) GDPR).

5 If you consider it unnecessary to report a breach, controllers must record at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response, as required by Article 33(5) GDPR.

6 You must record how you notified affected individuals where the breach is likely to result in a high risk to their rights and freedoms. (Article 34(1) GDPR).

7 You must show how you analyse all personal data breach reports to prevent a recurrence.

CONTACT US

HOW EFFECTIVE ARE YOUR BREACH ACCOUNTABILITY MEASURES?

1. Could staff explain what constitutes a personal data breach and could they identify one? □
2. Do they know how to report an incident? □
3. Are staff aware of the policies and procedures and are they easy to find? □
4. Do staff understand how to conduct the risk assessment? □
5. Do they know when a breach needs to be reported to the DPC? □
6. Do you analyse all personal data breach reports to prevent a recurrence? □
7. Do you record recommendations that are made and if and when they are actioned? □
8. Do you have procedures in place to detect, manage, and appropriately record data incidents and breaches? □
9. Can your staff escalate a breach notification? □
10. Does your logging, recording, documenting, and actioning of breach data have a full audit trail that is easily searchable? □
11. Can you clearly see who is responsible for what actions? □

HOW COMPLYKEY MEETS DPC GUIDANCE

Data breach management provides a framework and means to record, investigate, manage, and most importantly, demonstrate intent to prevent repeat occurrences and improve processes keeping the regulatory bodies at bay.

1 -Detecting, managing, and recording incidents and breaches. Article 33(5) GDPR.

Simplified dashboard for quick insights into all breaches and incidents, even those not requiring DPC or individual reports. Streamlined access for dedicated teams to handle security incidents and personal data breaches, with easy escalation to the right personnel for assessment.

2 -Assessing and reporting breaches. Article 33 GDPR.

Notify the DPC within 72 hours of learning about a breach in workflow steps. Guidance in the workflow to determine if a breach requires reporting. Clear instructions in the workflow on what info to provide the DPC about the breach. Detailed documentation for each reported or unreported breach.

3 -Notifying individuals. Article 34 GDPR.

A safe secure hub to document the reasons why your organisation considers a breach likely or unlikely to result in a risk to the rights, and freedoms of individuals.

4 -Reviewing and monitoring.

Analyse all personal data breach reports to prevent a recurrence. Monitor the type, volume, and cost of incidents. A central dashboard to understand data breach themes or issues over time. This analysis can be reviewed by groups with oversight for data protection and information governance.

5 -Internal audit programme.

Monitor your own data protection compliance, and regularly test the effectiveness of the measures you have in place.