WATERFORD TECHNOLOGIES

Data Breach Case Management

Breach Reponse and Monitoring

At a glance

The Data Breach Case Management module provides a framework and means to report, record, investigate, manage and most importantly, demonstrate intent to prevent repeat occurrences and improve processes.

Risks of not following DPC guidelines

There are serious impacts for organisations, their employees, and customers, such as financial penalties reputational damage, loss of business and disciplinary action.
As set out in the GDPR, violations of the organisation's obligations to report on data breaches, will be subject to;

€10M Up to

2% Global Turnover

CHALLENGES

All organisations are subject to data breaches to some level. From misdirected emails to cyber-attacks stealing and exposing confidential data. Under the GDPR a controller is obliged to notify the DPC of any personal data breach that has occurred unless they are able to demonstrate that the personal data breach is 'unlikely' to result in a risk to the rights and freedoms of natural persons.

BREACH RESPONSE AND MONITORING

The DPC expects every organisation that holds personal data to have procedures in place to make sure that you detect, manage, and appropriately record personal data incidents and breaches.

Log & Investigate

Risk Assess & Report

Record & Prevent

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.

Book a Demo

WATERFORD TECHNOLOGIES

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 WATERFORD TECHNOLOGIES MEETS DPC GUIDANCE

The data breach case 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.

- You have a central dashboard giving a high-level summary of all actual breaches and near misses (even if they do not need to be reported to the DPC or individuals).
- Dedicated roles or team access to manage security incidents and personal data breaches.
- Easy escalation of a security incident to the appropriate person or team to determine whether a breach has occurred.

2 -Assessing and reporting breaches. Article 33 GDPR.

- In workflow steps to notify the DPC of a breach within 72 hours of becoming aware of it.
- In workflow guidance on whether a breach needs to be reported or not.
- Clear in workflow guidance on what information must be given to the DPC about the breach.
- Clear documentation on each breach reported or not.

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.

Book a Demo