Why Crises Control is required for GDPR

GDPR SECURITY - Confidentiality, Integrity, Availability' and 'Resilience'

Collectively known as the 'CIA triad', confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for you as a data controller, and for the individuals whose data you process.

EU GDPR COMPLIANT

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

You are also required to have the ability to ensure the 'resilience' of your processing systems and services. To put this into contest, resilience refers to your capacity to recover quickly from difficulties, which include things like business continuity plans, disaster recovery, and cybercrime actions and tasks that need to be performed in a timely manner to recover as quickly as possible.

Crises Control offers a platform to: Create, Test, Execute, Audit and review Business continuity, Incident management and Cybercrime plans.

GDPR SECURITY - What organisational measures do you need to consider?

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on your size and the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security principle.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- Co-ordination between key people in your organisation when there is an incident (e.g. the security manager will need to know about commissioning and disposing of any IT equipment);
- Secure and private communications that are required when managing an incident which include supply chain partners, Legal, PR professionals, and other third parties.
- Access to premises or equipment given to anyone outside your organisation (e.g. for computer maintenance) and the additional security considerations this will generate;
- Business continuity arrangements that identify how you will protect and recover any personal data you hold; and
- Periodic checks to ensure that your security measures remain appropriate and up to date.

Crises Control provides a private, secure, mass communication platform that can be used to communicate like “WhatsApp” when you need it. It lets the right people know what is going on. It also provides a platform for more formally managing Incidents that require a process to be followed or Task to be completed in a timely manner.

Crises Control’s real-time reporting and Audit data help you learn and make improvement to our plans for faster recovery.

GDPR REPORTING - A breach-personal data breach

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Crises Control offers a solution to; Automate Incident Alerts, create TASK workflow with time KPIs and capture process audit data.