Personal data breach and incident management services

The GDPR defines a 'personal data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. The regulation enforces specific obligations on organizations to report a breach to the relevant supervisory authority within 72 hours of becoming aware of the breach.

If the personal data breach represents a high risk to the data subject, the data subject must also be notified without undue delay.

Therefore, an organization's incident response programme should deliver the ability to quickly react to a data protection or security incident and limit the reputational, operational or regulatory damage it could cause. Not every incident is going to be the same and as such, incident responders must have the ability to react to different situations.

Breach and incident support - What we offer

Response planning - when implementing an incident response plan in an organization, our tailored approach ensures that:

- Roles and responsibilities are defined and allocated
- Staff are trained on how to respond to a security incident in a methodical manner, using a defined framework
- Incident scenarios are drilled to ensure that the organization's response is effective
- Legal, regulatory and contractual obligations are defined and documented
- Regulatory and data subject notification protocols and processes are documented and effective

Real time support - in addition to assisting your organization to develop incident response capabilities, we also provide real-time first responder services to provide immediate support to organizations when a personal data breach is identified. Our experienced staff will assist your organization from initial response, through containment, recovery, reporting and regulatory and data subject notification.

Real time support is available to respond to personal data breaches such as:

- Unauthorized disclosure of personal data
- Loss of a device which includes personal data
- Security breach incident where personal data may have been compromised
- Verbal disclosure to an unauthorized party
- Emails containing personal information sent to the wrong destination
- Unauthorized changes to data, including forensic capabilities to investigate

Find out more
Call: +1 800 862 4977
Email: cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-us

Relevant GDPR Articles: 33, 34

Personal data breach and incident management services

We provide support services across all the critical by key stages of personal data breach and incident response

Prepare

- Incident response training (planning and responder)
- Policy and procedure development
- Readiness (maturity) assessment
- Simulation tests (desk based and full simulation)
- Proactive threat hunting/ analysis

Identify

- Initial incident assessment support
- Classification - ensuring personal data breaches are identified, classified and managed in line with the GDPR
- Define incident management team and procedures
- Forensic acquisition – investigation whether a specific breach of personal data occurred
- Review asset inventories
- Log review
- Monitor activity

Contain

- Devise breach containment strategy
- Communication strategy
- Engage third party data processors
- Log review
- Notify supervisory authority
- Notify affected data subjects
- Monitor

Eradicate

- Verify eradication
- Log review
- Monitor

Recover/lessons learned

- Complete post breach incident report
- Identify lessons learned
- Incident post mortem
- Update policies and procedures
- Further notifications to supervisory authority/data subjects

Find out more
Call: +1 800 862 4977
Email: cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-us

bsi.