Simmons & Simmons

Data Protection Regulation

Data Security and data breaches checklist

The following is a list of issues relevant to your data security and breach notification obligations under the Data Protection Regulation.

- Have you carried out a risk assessment with regard to the personal data that you process and the processing activities that you carry out? Based on the risks you have identified, have you implemented security measures which are tailored to the personal data you process and the processing activities you carry out?
- Have you made an assessment of how you will ensure the resilience and availability of data processing systems?
- Whether you process personal data for your own purposes or on behalf of others, have you implemented a security policy which guides your organisation on how to:
  - verify the accuracy of personal data;
  - maintain the confidentiality, integrity, availability and resilience of systems and services processing personal data;
  - restore access to personal data in a timely manner following a disaster event;
  - be aware of particular risks in the processing of sensitive personal data (such as data relating to a person's race, gender or criminal history); and
  - test and evaluate the effectiveness of security policies and procedures?
- Do you continually monitor your security measures to ensure that they continue to reflect the risks posed by the data you process and your processing activities?
- Do you regularly test the implementation of your security policy and security measures? Do you conduct stress testing or penetration testing of your security systems? Do you keep records of the test results and the remediation required if deficiencies are found?
- Where you allow third parties to process personal data on your behalf, have you entered into written agreements with the relevant parties requiring them to implement security measures in accordance with the Regulation?
- Have procedures for the monitoring and reporting of security incidents been implemented within your organisation? Have you implemented procedures enabling you to notify your national data protection authority and affected individuals about data security breaches promptly after they occur?
- Do you keep easily-accessible records of security breaches involving personal data which occur within your organisation?