

Data Protection Services Overview



Securing information assets is fast becoming a top priority for all companies. The risks surrounding the collection, management and use of personal data have significantly increased as evidenced by the increasing number of data breaches e.g. HSBC, Nationwide, Zurich Insurance etc. The Information Commissioners Office (ICO), the entity charged with overseeing and enforcing the Data Protection Act 1998, now has the power to fine organisations up to £500,000 for serious contraventions of the Act. The Financial Standards Authority (FSA) has even greater powers when it comes to issuing fines, the highest to date being circa £2.2M. Whilst this in itself should act as a suitable deterrent, in many cases the

reputational damage resulting from a breach far outweighs any fines that may be levied. As such, having a robust Data Protection framework is essential and will continue to be so as companies share more and more information. Increasingly, data protection frameworks are being devised and subsequently revised, with the aim of managing data protection risks and complying with relevant laws and regulations.

Although there is no “one size fits all solution” they typically all have similar components which have been summarised in this paper along with how Kingston Smith Consulting LLP (KSC) can assist you.

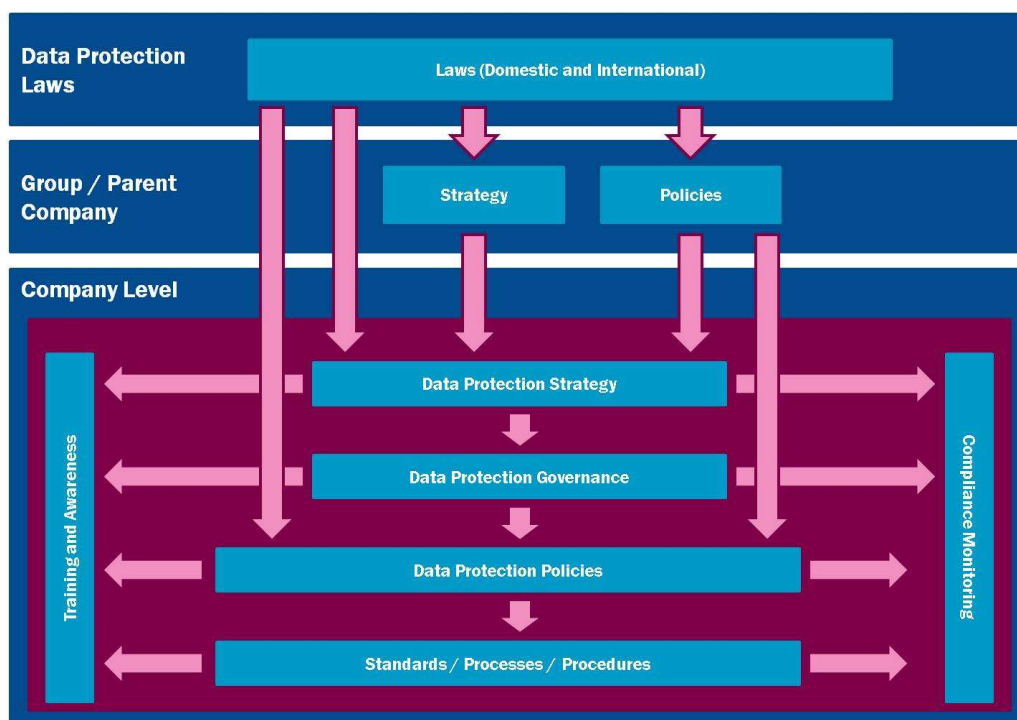


Figure 1. Overall Data Protection Framework

Overall Data Protection Framework

A data protection framework typically starts with the interpretation of laws and regulations (domestic and international) which guide the company strategy and policies in relation to data protection. These may be high level strategies and policies adopted by Group/Parent companies that filter down to a local level before being tailored to ensure they comply with the specific jurisdictional requirements.

At a local level a number of components interface and operate to build a robust framework. Figure 1 above depicts the pieces that form a typical data protection framework.

Data Protection Laws:

There are numerous laws and regulations in relation to the protection of data and these vary (sometimes significantly) from country to country. With increased reliance on third parties, the likelihood of data being transferred and processed across borders increases; it is therefore paramount that you first establish your “compliance footprint” and understand the different legal and regulatory requirements that fall in scope of the data protection programme. These will, in turn, guide the business strategies and policies in relation to data protection.

KSC can help identify the relevant legal and regulatory requirements that are applicable to companies from a data protection perspective, not only taking into account the country specific data protection acts; but also industry specific regulations and requirements in relation to regulated data.

Group / Parent Company Strategy and Policies:

This may be relevant where a company operates in a group structure where the parent company provides the high level guidance on strategy and policies. These set the tone and provide the overall governance structure to demonstrate the group’s compliance with applicable data protection laws and regulations.

Group guidance should be specific enough to enable reporting companies to provide a homogenous view across the group of their data protection status

whilst being flexible enough to enable reporting companies to adapt the strategies and policies to the nature and location of their operations.

KSC can help with formulating a group level data protection strategy, as well as policies that provide a consistent approach across the group for reporting and managing the data protection risk, which would typically be integrated into existing group risk policies and frameworks.

Company Level Data Protection Framework:

With inputs from Data Protection Laws and the Group / Parent company’s strategies and policies (where applicable), the company level data protection framework should be all encompassing and provide the tools and mechanisms for operating a data protection programme. The key components at this level typically include:

Company Data Protection Strategy:

This takes into account laws, rules and regulations as well as parent company requirements and defines the risk appetite and the company’s commitment to data protection. The company’s existing processes for risk management, governance, compliance and information security should be reviewed while defining the data protection strategy. Leveraging existing processes will significantly reduce overheads and facilitate effective integration.

The data protection strategy will enable the appropriate governance structure to be put in place as well as defining expectations in terms of monitoring and compliance and training and awareness.

KSC can help formulate your data protection strategy, identifying how to embed it within the existing structure of the company to achieve a leaner approach to data protection compliance.

Data Protection Governance:

Governance of the data protection function starts from the registration process with the relevant registration body, through to defining the roles and responsibilities within the organisation for those overseeing the data protection programme. One

proven approach is the creation of a Data Privacy Steering Committee which should include senior representatives from e.g. legal, information security, IT, audit, compliance and relevant business functions such as marketing and operations.

The tasks typically operated as part of the framework should be defined as part of the governance component by creating RASCI charts (Responsible, Accountable, Support, Consulted, and Informed) establishing the expectations from each function within the company.

KSC can help define the required data protection governance structure that will form the core component in managing your data protection risks. We achieve this by gaining a deep understanding of your company structure, culture and existing governance to ensure you become fully operational in the minimum amount of time.

Data Protection Policies:

Policies should include the minimum control requirements for managing data protection within the company. Alignment and embedding with existing information security policies is essential as they both share similar objectives. This also provides the company a chance to review their existing policy sets and identify any potential gaps with data protection and other legal and regulatory requirements.

KSC can help by reviewing existing policies, identifying any gaps in addressing data protection and bridging the gaps by enhancing the existing policy sets.

Standards, Processes and Procedures:

Processes and procedures should be embedded within existing documentation where at all possible. For example, existing data classification procedures should include personal data and incorporate requirements for handling personal data; existing incident management processes could include a data protection component defining how to deal with a data protection breach.

Inevitably there will be instances where new procedures will need to be developed; these may

include a process for subject matter access requests (SMARs), registration procedures, and periodic reviews of consent forms and notices.

Processes for mapping the flow of data within the company also need to be established; these typically provide an overview of the lifecycle of personal data from the point of entry, use, processing, transfer, retention, storage, and destruction. This mapping is critical as more often than not it shows areas where data may exist or have been transferred to/from, which were not on a company's radar. The mapping is then used to assess the level of compliance with the data protection controls defined in the data protection policies - any gaps identified can then be addressed.

KSC can help with the creation and embedding of data protection processes and procedures. We can help to define the data estate and map the data flows throughout your company, identifying any areas where significant risk may exist and provide recommendations which enable you to comply with the laws and regulations with as little impact as possible to your company's operations.

Compliance Monitoring:

Metrics, measures and balanced scorecards for continuous compliance monitoring need to be put in place; these should factor in compliance requirements in relation to any third parties who form part of the data lifecycle. Compliance monitoring should also include a mechanism for tracking the status of actions in place to bridge any compliance gaps or as a result of a data breach.

KSC can help define the metrics and dashboards needed to continuously monitor compliance and effectively report on compliance status to different stakeholder communities.

Training and Awareness:

A key part of any successful data protection framework is ensuring that individuals across the organisation are adequately prepared to drive the process of data governance forwards.

General awareness training should be provided to all staff regardless of their level of exposure to personal

data. Further training programmes should be tailored to specific groups within the company depending on their roles and responsibilities in relation to processing personal data.

KSC can help develop and deliver general and tailored training programmes by working with learning and development teams within your company. We also partner with online training platform providers who offer the facility to deploy specific training programmes which are accessible online and can provide you with the metrics needed to assess the awareness levels of your staff.

Can KSC Help?

Our Data Protection services range from delivery of large scale cross border solutions; embedding data protection frameworks within companies; ensuring

compliance with various data protection laws; to the delivery of specific components within an overall data protection framework.

We deliver solutions, defining and agreeing the outcome you require and charging a fee which achieves that end, so you will always understand the cost and benefit of our services.

We focus on achieving return on investment; we measure our success on the value you realise – this means solutions delivered to your specific needs and not someone else's template.

We bring expertise and experience to every engagement; all of our consultants have a strong record of successful delivery in their field of expertise.

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice of the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD