Is your programme effective?
A guide to privacy governance.

Objectives
There are a number of reasons that an organisation should implement and maintain an effective privacy governance programme. These include:

• creating a data protection policy to ensure that the business has clear guidance on how to deal with personal data and to ensure compliance with the Data Protection Act;
• developing a data protection culture throughout the organisation to ensure that all employees are aware of data protection obligations, why they exist and what the company’s policy/way of working is;
• establishing a chain of command to clearly identify appropriate channels for escalation of any data protection issues;
• adopting standards and procedures across the organisation to ensure all areas of the business are operating in the same manner;
• ensuring adequate resources are in place to handle personal data in a compliant way and to enable appropriate exploitation of data;
• keeping staff up to date with the law and the business’ internal procedures by providing training on and enforcing the strategy; and
• to formalise a procedure for regular reviews to ensure compliance across all areas of the organisation and to formulate any potential changes or tweaks as necessary.

Structure
There is no set structure that an organisation should use to implement and maintain an effective privacy governance programme.

Organisations need to clearly examine their needs and the structure of their business or operations and decide who will be involved in the programme and who will ensure compliance with the ultimate policies put in place.

Below are three popular models used by businesses:

Local responsibility
Local employees take responsibility for data protection matters such as training, policy updates and reporting.

The local responsibility model is particularly effective because:

1. local employees may be in a better position to build relationships with staff and as such, cooperation with the privacy governance programme and ultimately the data protection policy may increase;
2. local employees are likely to have good visibility within the business and can feed information back up to senior management. This will hopefully ensure that the data protection policy is complied with and that feedback on how the policy works in practice is readily available; and
3. there is a direct source of accountability. The local employee can be held accountable for localised failures in the business. This should ensure that such an employee takes data protection seriously and this should disseminate through the rest of the workforce.

Central control
A single data protection officer will be the main point of contact for all data protection related matters across the organisation. The officer will also be solely responsible for dealing with communications from the ICO and other regulators and subject access requests.

This data protection officer may be supported by a team in larger organisations. The officer and the team should be selected carefully to ensure the right skill sets and capacity to perform the obligations.

A comprehensive privacy governance programme is vital for organisations that collect and control large volumes of personal data and those businesses that rely on personal data to operate.

In this document we set out the key steps that will help you to ensure that your company has a robust programme in place.
Hybrid model

A data protection officer is appointed, as in the local control model. This officer will be the main point of contract for the whole organisation but day to day compliance is delegated to local employees, similar to the local responsibility model.

This structure is particularly effective because it ensures the data protection strategy is complied with across the entire business and at all levels.

This method may also be beneficial in terms of allocating resources and spreading workload across the business.

This structure is useful for businesses with subsidiaries or distinct departments as responsibility for compliance lies initially with those individual entities and this then feeds up to general compliance across the business via the data protection officer.

Knowledge and innovation can be gained from numerous sources, possibly creating a more comprehensive and better implemented strategy and policy.

Generally the hybrid structure is an effective method to disseminate the privacy governance programme from the top of the business right down to the individual employees conducting the day to day business.

Whilst this model does produce a clear line of accountability, it may become quite complex in large organisations and there is the potential for miscommunication and individual interpretations, which could lead to the programme and policies being implemented slightly differently across the business.

Analyising key data protection considerations for your organisation

All organisations are different and data protection laws may affect them in slightly different ways. It is important when setting up a new privacy governance programme to identify the key areas of risk across the organisation. Often this will involve carrying out an initial data mapping exercise to obtain a good understanding of how personal data is obtained, used and shared within and outside the organisation.

Clear and transparent policies should be created to deal with these key areas and these policies should then fit in to the wider privacy governance programme to ensure they are being implemented, regularly reviewed and are understood by all colleagues.

In the sections below we highlight the key issues that we recommend are addressed in all privacy governance programmes.

Governance structure and accountability

A clear data protection governance structure should be created. A senior figure in the firm (preferably a board member) should be given ultimate responsibility to ensure data protection compliance and to be ultimately accountable.

A clear chain of accountability should then be created across the organisation to ensure that there is good communication and that data protection issues are dealt with effectively.

Policies and guidance

It is advisable to create an overarching data protection policy, which sets out the framework within which all employees should deal with and handle personal data. The policy should include:

- an overview of data protection law;
- the key requirements of the Data Protection Act;
- the organisation’s specific way of working to comply with data protection law; and
- the key contacts for data protection within the organisation.

Organisations should also consider having specific policies or guidance in place to deal with key risk areas. These policies may relate to discrete areas of the organisation or certain scenarios or actions. Examples may be policies specifically relating to:

- the business’ different brands or departments and any specific data protection challenges they may face;
- employees using their own devices for work;
- employees working from home;
- marketing guidelines.

Employee training

It is vital that employees within the organisation receive comprehensive training on data protection. This will ensure that all employees are implementing the same good practice and are aware of the organisation’s specific policies.

Further to this, comprehensive employee training may create efficiencies in the privacy governance programme. Employees who are conscious of data protection may review the data protection risks of new projects from the outset and engage the data protection officer/legal department at an early stage, hopefully leading to quicker compliance and more efficient implementation of the project.

It is important to keep an audit trail of training that has been completed so that in the event of a breach or an Information Commissioner investigation accurate records can be produced to demonstrate that adequate training has been provided to all employees.

Information Security

Keeping personal data secure is one of the key requirements of the Data Protection Act and the requirement that is most likely to result in serious consequences if breached. It is therefore essential to ensure that training, policies and procedures enable employees to understand the risks and the steps they must take to minimise those risks.

It is advisable for an organisation that is implementing a robust privacy governance programme to also review its information security policy. Such a policy will sit closely with the privacy governance programme but will cover wider areas such as disaster recovery, access management and business continuity.
Data management procedures

A clear procedure should be set for the retention and ultimate destruction of any personal data collected by the organisation. An organisation that collects personal data is under an obligation to keep personal data up to date and procedures and processes should be implemented to periodically review personal data and update (where possible) or destroy old personal data.

The business should only keep personal data for as long as necessary. A process of review and secure destruction (where necessary) should be implemented and maintained.

Privacy notices and marketing consents

At the point of data collection, organisations must ensure that they are informing individuals of the purposes for which they will be using their data and to whom it may be disclosed.

Organisations must also ensure that they obtain valid consent from people to use their data for marketing.

Administrative procedures should also be put in place so that the organisation has a clear audit trail showing which privacy notices have been provided to which individuals and to accurately record marketing preferences.

Third party data processors

The Data Protection Act imposes certain obligations on organisations when they instruct third parties to process data on their behalf. Organisations need to have procedures in place to ensure that when engaging third party data processors the following requirements are met:

• due diligence should be undertaken on all third party data processors to ensure they have adequate measures in place to protect personal data;
• minimum data protection obligations must be included in a written contract with the data processor;
• after engagement, ongoing monitoring should take place to ensure that the data processor is protecting personal data in accordance with contractual requirements.

Transfer of data outside EEA

As part of a data mapping exercise the organisation should identify where all of its data is held and where it is transferred to.

If the business transfers any personal data outside the European Economic Area steps need to be taken to ensure adequate protection for that personal data.

For any new projects that may arise, the business should ensure that the relevant personnel consider data transfers at the outset of such projects.

Privacy impact assessments

It is best practice for organisations to have a set procedure for reviewing new projects from a data protection perspective right from the outset.

Such a procedure should outline any potential data protection risks that the project may create and will enable the business to create a plan or seek advice on how to mitigate such risks. The privacy impact assessment should also enable to organisation to implement the ‘privacy by design’ principle where appropriate.

The ICO has published a code of practice on privacy impact assessments and may request evidence of compliance with the code if they conduct a data protection investigation.

Breach management

The organisation should ensure that it has appropriate procedures in place to quickly and effectively deal with any data protection breaches.

Employees should be informed who they need to approach if there is, or they believe there could be, a data protection breach.

Further to this there should be a team set up that will meet in the event of a breach and will have responsibility for creating an action plan to deal with the breach. Such a team may consist of high level directors, lawyers, IT managers, HR managers and PR employees.

Regular Monitoring

Regular monitoring of compliance with policies and procedures and the adequacy of those procedures should be carried out.

Audit reports should be analysed thoroughly and any actions required to rectify highlighted issues should be implemented as soon as possible.

Keeping up to date

As with all laws, data protection law will develop in the future. A new Data Protection Regulation is on the horizon which will require all businesses to review and update their privacy governance programmes to comply with stricter obligations and new rights for individuals.

Part of an effective privacy governance programme will be to designate an employee (usually the date protection officer) to keep up to date with data protection law and to regularly update the board to ensure the strategy and policies are staying in line with laws and relevant guidance.