

Information Governance

Responsibilities for personal data holdings

Louise Bennett

Chairman BCS Security Forum Strategic Panel

INTRODUCTION

Information governance encompasses the strategic management and supervision of information. Good governance ensures that the organisation gains the benefits of collecting, using and disposing of information without suffering the financial and reputation risks of its loss or miss-use. Nowhere is this more important than when organisations hold personal data (defined by the European Data Protection Directive and the Data Protection Act as: “information that relates to an identified or identifiable individual”. This “information” may be factual or subjective, both constitute personal data if they relate to identifiable individuals.

The main information governance requirements are:

- Clear responsibility accountability and authority for information management
- Training of all staff in the information’s purpose, handling and protection.
- A clear understanding and management of processes associated with the introduction and use of new databases
- Appropriate security systems for the protection of the organisation’s data and information, including business continuity planning
- Simple clear documentation of the organisation’s use of and dependence on information that is followed throughout the organisation.

RESPONSIBILITY, ACCOUNTABILITY, AUTHORITY AND DELEGATION

Clarity about roles and responsibilities for information management and benefits realisation are essential.

Responsibility and accountability cannot be separated or delegated. Responsibility is a charge, trust or duty for which an individual or a group (e.g. a Board) is/are responsible and are liable to be called to account. Authority is derived or delegated power, and, by definition, it can be delegated, but only up to certain limits that are lower than the limits for the entity *doing the delegating*. All functions (such as data input or cleansing) can be delegated.

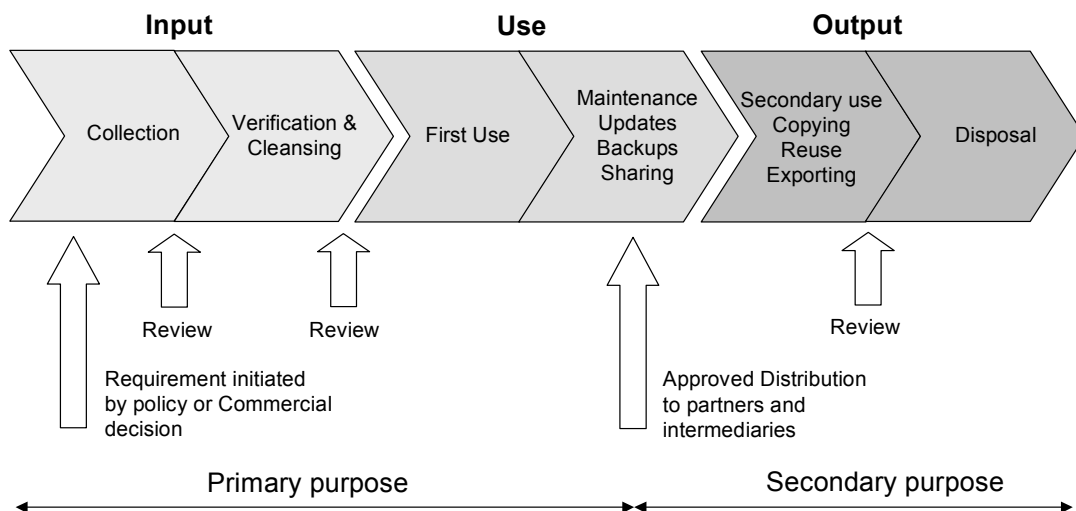
Large complex information holdings, particularly those containing personal data, need strong management from the Board. The Board needs to accept their responsibility and accountability for holding information securely and

need to be absolutely clear what authority they are delegating to each functional grouping or individual within the organisation in order to achieve that success. The greater the simplicity and clarity of responsibility, accountability, delegated authority and functions associated with information management, the more likely it is to be successful.

All organisations must have an “information assurance strategy” if they hold personal data. Part of this strategy should set out the governance arrangements for information assurance. Good governance makes clear who is responsible and accountable for the protection of all personal data collected. The person who is accountable can delegate to other people the responsibility and authority for all or part of the processes in the information life cycle, e.g. data input, data back up, data disposal. It must be clear, at all points in the life cycle, who has been authorised to handle personal data and the extent of their authorisation.

Organisations that hold personal data have a responsibility to ensure the accuracy and relevance of that data and to have effective processes in place for the review, maintenance and disposal of personal data. They also have a responsibility only to collect and hold the minimum of personal data needed for the service offered.

The Information Life Cycle



INPUT - Collection, verification and cleansing of personal data

Accountability: An organisation that collects, stores and handles personal data:

- must clearly state the purpose for which the personal data is being captured and used, and with whom and why the data will be shared,

- must ensure that appropriate governance procedures are in place to safeguard the data and its use,
- must ensure the relevance of the personal data it collects and safeguard it throughout the information life cycle.

Visibility: The organisation must openly and clearly state the purpose for which the personal data is required and should tell potential data subjects what management processes they have in place to protect personal data..

Consent: The organisation must explicitly secure the consent of the data subject before storing and/or accessing their personal data and state, at the time of collection, if the data is going to be shared with any third party.

Access: The organisation must ensure that physical and technical controls and management processes are in place to protect and secure access to all personal data in its custody from both external attack and interference and internal abuse.

Stewardship: The organisation must ensure that any personal data it collects is the minimum needed for the stated purpose. Personal data an organisation holds must have associated properties, such as: checks on accuracy; retention time or relevant expiry date, associated with it. The integrity of all information, but particularly personal data, must be maintained from collection throughout the life cycle. A risk assessment of data holdings should be carried out from the time of collection. This assessment should be associated with the data, particularly personal data, throughout the life cycle. When the collecting organisation has consent to share personal data with any third party, it should ensure that the third party understands both the risks associated with that data holding and any caveats associated with its integrity and appropriateness for use for purposes other than that for which it was originally collected. The collecting organisation must ensure that it has passed on the obligation to protect data throughout any chain of sharing.

USE - First use, maintenance, update, backup and sharing of personal data

Accountability: An organisation that uses personal data must ensure that:

- effective operating procedures and security control mechanisms, including access logging, are in place to prevent improper access to personal data.
- the integrity and sustainability of the personal data that they hold are maintained by regular maintenance, updates, backups and data matching procedures.

Visibility: Organisations must ensure that effective and timely processes are in place for dealing with Data Subject enquiries relating to personal data holdings.

Consent: Consent must be obtained to share personal data, for which consent was not obtained at the time of data collection.

Access: Organisations must maintain an audit trail of personal data that has been accessed.

Stewardship: Organisations must regularly review their business processes and personal data holdings to ensure that the accuracy and currency of that personal data are maintained.

OUTPUT - Secondary use, copying, reuse, exporting and disposal of personal data

Accountability: An organisation that uses or reuses personal data must:

- state clearly how long personal data will be held and ensure that personal data is disposed of securely.
- ensure that, if personal data is to be shared, either at the time of collection or at some later date, the relevant authorisation has been obtained.

Visibility: Organisations must maintain an accurate record of personal data shared with a third party and ensure that they have approval to do so.

Consent: Organisations should seek approval from data subjects if all or part of their personal data is to be passed to a third party not previously identified.

Access: Organisations must ensure that no third party may have access to personal data without the appropriate authority to do so.

Stewardship: An organisation that uses personal data should ensure that:

- any caveats relating to the personal data are linked to the data throughout the sharing process and the boundaries of stewardship and ownership of risks are made explicit for all parties.
- personal data no longer required to support the business process is securely deleted.