Directorate General of Administration
Directorate of Information Technology

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 14 October 2013

DGA/DIT(2013)02

Data and Information Management Policy of the Council of Europe

Content

1. Introduction

This policy document is part of the effort to establish a comprehensive data and information management process and method for the Council of Europe. It re-enforces the principle that information is a key asset of the Council of Europe and that information assets can (and should) be continuously leveraged to further the mandate and success of the Council of Europe. The principles and operational framework of this policy apply across the Organisation.

The European Court of Human Rights (ECHR) and European Directorate for the Quality of Medicines and Healthcare (EDQM) have their own information policies which conform to the principles adopted organisation-wide in so far as these are compatible with their specific missions. The ECHR and EDQM will comply directly with the overall Data and Information Management Policy where issues arise in connection with services provided centrally under the responsibility of the Directorate of Information and Technology (DGA-DIT).

All Council of Europe staff and affiliated personnel (for example contractors, experts, consultants, trainees, etc.) are bound by this policy.

2. Value of information

Information is a key enabler for achieving the objectives of the Council of Europe – from delivering field activity to effective administrative operations. All Major Administrative Entities (MAEs) create and use data and information.

- Data is collected or created. It holds facts and is organised.
- Information is the interpretation of data. It is what we use for decisions, evidence, context, etc.

Therefore, data has a cost and information has a value (Figure 1). For this value to be realised, maintained and protected, information must be timely, available and of sufficient quality.

- The ownership of data and information belongs to the Council of Europe as does the value and benefits derived from it across all our operations. The only exception is personal data (date of birth, home address, etc.)[1].
- All staff members are the guardians of data and information they import or create in the course of their duties so as to achieve timeliness, availability, quality and protection. Archived information and historical records are the responsibility of the Central Archives of DIT.

The Directorate of Information and Technology provides and enforces:

- this policy: Data and Information Management Policy of the Council of Europe;
- the operational framework required by this policy;
- advice, consultancy and training for the best use of data and information;
- the required systems and processes in order to manage information along its life cycle.

[1] ETS108 - Convention for the protection of Individuals with regard to Automatic Processing of Personal Data: link

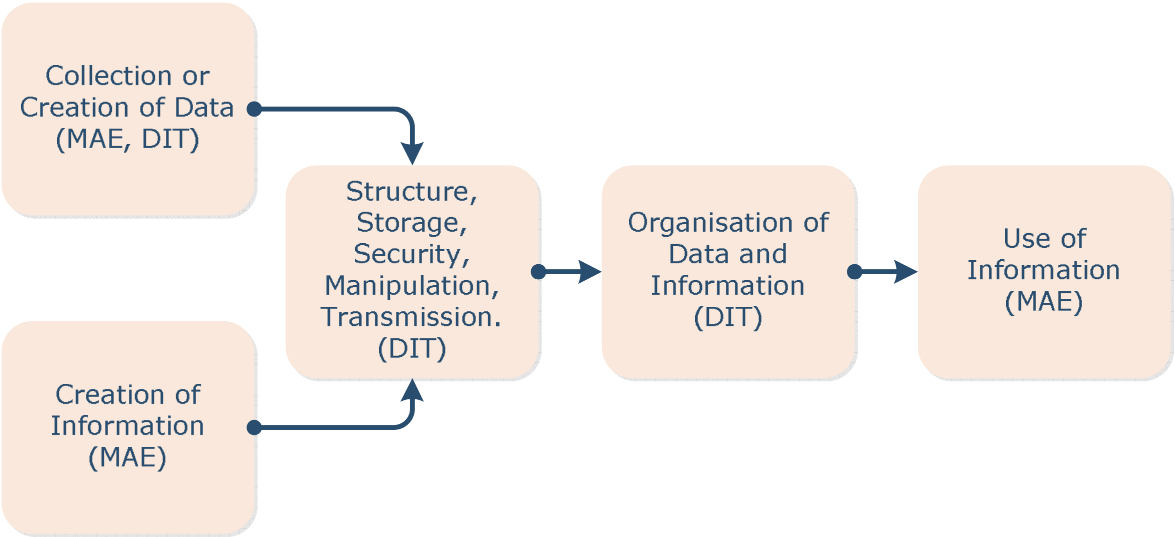
Collection or Creation of Data (MAE, DIT)
Creation of Information (MAE)
Structure, Storage, Security, Manipulation, Transmission. (DIT)
Organisation of Data and Information (DIT)
Use of Information (MAE)

Figure 1. Data and information value chain.

3. Management of information[2]

The Council of Europe Information Management and Governance is a delivery and accountability framework that includes people, processes, policy and information and technology (I&T) solutions. It ensures the effective and efficient management of information to enable the Organisation to achieve its strategic goals, business programmes and administrative activity.

It is implemented via:

- The Knowledge Management Steering Board:
  This Board makes recommendations to the Secretary General on the adoption of organisation-wide standards of information management.

- Major Administrative Entities who are responsible for:

  - Awareness of the necessity to set the required data quality levels.
  - Realise the value of the information the Organisation is holding by using information appropriately.
  - Applying this policy, best practices and meeting the regulatory compliance requirements as published in the administrative manual and dedicated Intranet pages (such as DIT, Information management pages).
  - Create and manage data and information as a Council of Europe asset.
  - Define appropriate access to the data and information they produce and manage.
  - Comply with the retention and disposal rules[3] as agreed by MAEs.
  - Manage and keep current the associated metadata.
  - Coordinate with DIT for approval on all matters regarding acquisition, development and installation of new systems and/or processes of Information and Technology[4].
  - Comply with national and international legislation in terms of use and distribution of data and information (for example, copyright laws).

[2] The discipline that analyses information as an organisational resource. It covers the definitions, uses, value and distribution of all data and information within an organisation whether processed by computer or not. It evaluates the types of data/information an organisation requires in order to function and progress effectively.

[3] Retention and disposal rules: link

[4] List of non-comforming software: link

- Computer and Archive Correspondents:[5]
  These groups function as liaison between entities and DIT. Their role is defined in the document: "The role and recognition of Computer Correspondents[6]", the RAP-INF(2001)6 and the DGAL 136 Archival Policy[7].

- Directorate of Information and Technology:
-
  - Provides the tools, the services[8], the capacity (I&T systems) and the capabilities (I&T processes and methods) for efficient execution of data and information related tasks.
  - Hosts the human resources for the I&T activities of the Organisation.
  - Provides guidance and sets the information management standards.
  - Manages the common master data (used across the whole organisation).
  - Provides long term archiving and the preservation of records and archives. Entities must use the recommended DIT tools and procedures to generate these records.
  - Ensures access to historical archives.
  - Holds the budget (investment and ordinary budgets) for all I&T activity in the Council of Europe. Any exceptions need to be justified by the requesting MAE and approved by DIT. The allocation of I&T resources is on the basis of accepted Business Cases[9] and Business Requirements[10].
  - Monitors the compliance of users and MAEs to this policy.

4. Collection and creation of data and information

1. Collection and creation:

- Creation: this is done by using the Council of Europe systems implemented by DIT to the business requirements issued by the MAEs.
- Collection: by importing from external sources using either direct links or the transfer of files. If a specific system is needed, this must be implemented and released by DIT.

2. Quality:

- The MAEs need to define the level of data quality they require. This needs to include at minimum:
  - the accuracy required;
  - the name of the source;
  - the date of the data creation (not the date of acquiring the data);
  - the validity span – until when the data is valid;
  - the Organisation's data guardian – who imported the data.

  The above (level of data quality) needs to be stated in the properties of the file holding the data. The data guardian needs to either maintain the asset (data set or information), freeze it (create a record) or dispose of it if no longer needed.

[5] Role and legitimacy of Archive Correspondents: link
[6] The role and recognition of Computer Correspondents: link
[7] Archival policy: link
[8] DGA-DIT tools and services: link
[9] Business Case template: link
[10] Business Requirements: link

5. Storage of data and information

DIT ensures appropriate storage of data and information in digital formats so as to:

- enable access, sharing, search and reuse (both in the short and long term);
- apply the appropriate access authorisation and security criteria;
- ensure preservation of digital content;
- ensure data and information are protected against loss by accident or disaster.

In brief:

- temporary personal data and information is stored in the P:\ drive and the user's mailbox. Both facilities are limited in size;
- working data and information is stored in the Public Folders, the shared drives and the collaborative spaces. These are the locations where finalised data and information must be stored;
- validated data and information is stored in the WCD (Web Cube Documentaire) space, the websites and the Public Folders;
- records are stored in the Records Management system only;
- transferring of data or information is done by using the messaging system or the website facilities. Users that must transfer data or information in different ways (CDs, DVDs, memory sticks, etc.) are reminded that they need to adhere to the confidentiality and security restrictions.

Tables 1 & 2 expand on how DIT treats information stored at various locales.

The backup[11] rota is the following:

- Daily, the data is stored on tapes and preserved for a month whilst the weekend backup is stored for 2 months. Archiving is performed by DIT in accordance with the Council of Europe Archival Policy.

The backup of the Organisation's data and information should not be treated as a storage media that users can use to access material. It is strictly a security and business continuation facility.

The storage of data and information is an area with rapid technological advances, for example Document and Record Management systems. The policy will be amended accordingly to reflect operational policy and the Council of Europe users will be informed via the Organisation's Intranet.

6. Retention management of data and information

Retention is keeping relevant data and information available for access and re-use throughout an agreed time framework. In other words, not all information is relevant for future legal or operational reference. Any data and information unnecessary for future reference must be disposed of.

Retention and disposal schedules of MAEs specify what has to be retained and the duration of the retention. They are approved by the MAEs concerned and DIT. Items not covered in these schedules are retained for five years after the last modification of the data and information asset concerned.

DIT provides the retention management tools and purges the assets in compliance with the agreed disposal procedures.

Digital preservation for long term archiving is only done centrally in the Records Management System.

[11] Backup is an image of active data that serves for recovery after a disaster (short term risk management) and should be distinguished from archiving that serves for on-going access (discovery) to important business information in the long term (more than five years).

7. Security of data and information

DIT provides all security measures and means across the Organisation and its operations in terms of:

- the Council of Europe network, its routers and TCP/IP switches;
- the data centre;
- the messaging system;
- the desktop computers, laptops, mobile phones, tablets and mobile storage devices.

The security remit covers the following:

- availability of I&T resources – physical or not;
- data and information integrity, confidentiality[12] and traceability.

Therefore, no device nor software are allowed to be connected and/or installed on the Council of Europe network without the explicit approval of DIT. For visitors, guests or Council of Europe staff members that wish to have Internet connectivity, DIT is providing open WiFi hot-spots at all the public meeting spaces of the Organisation's buildings.

If the classification (level of confidentiality) of a data or information asset is not explicitly set or defined by the owner/guardian of this asset, it will be granted the standard level of security of the Council of Europe Information System (internal access only). The level of confidentiality is set via the metadata fields of the assets.

Owners/guardians of data and information assets must be clear that they need to retain them within the perimeter of this policy. Therefore (as a non-exhaustive example) if they extract assets into portable memory devices (memory sticks, CDs, DVDs, etc.) or 'cloud' based repositories (Gmail, Drop Box, etc.) they are in breach of this policy except if the data is encrypted to a level approved by DIT. Particular attention needs to be exercised in the case of attachments on e-mails.

8. Access of data and information

Access to information is controlled by the Council of Europe policy[13] and specific agreements with author departments. It is formalised in the disposal schedule of each individual entity (current standards[14]). The register of access policies is held by DIT (http://www.transparency.coe.int).

DIT provides full access to Intranet data from devices that are provided and managed by DIT. Access from other devices, networks and Internet is limited by the security policy.

User responsibilities are defined by the Instruction No. 47 of 28 October 2003 on the use of the Council of Europe's Information System[15].

Users are fully responsible for managing their passwords, for example non-disclosure, timely renewal, etc.

[12] The confidentiality level of a data or information asset must be set by the asset owner or guardian and in accordance to the Council of Europe guidelines: link

[13] Council of Europe access policy: link

[14] Council of Europe standards: link

[15] Council of Europe Instruction No. 47 of 28 October 2003: link

9. Use of data and information

Information is made available to staff members for executing their duties – it is not for private use. For example, a report compiled by a staff member belongs to the Organisation. The staff member must not copy the report and keep it in his/hers archive outside the Organisation's I&T systems.

Data and information assets that need to be communicated outside the Organisation must be first cleared (authorised) by setting the appropriate security clearance of the asset (for example public, restricted or secret).

Each staff member authoring a data or information asset, has the responsibility for following and applying the security classification and rules of declassification of information as decided by the authoring entity.

The public (or individual members of the public, organisations, institutions, etc.) can use the information published on the Council of Europe websites or information directly communicated to them. They must respect the copyright and disclaimers accompanying the information as published on the Council of Europe official website.

10. Data protection

All users of Council of Europe data and information need to understand and observe the principles of data protection.

a. Personal data shall be processed fairly and lawfully.

b. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

c. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

d. Personal data shall be accurate and where necessary, kept up to date.

e. Personal data processed for any purposes shall not be kept longer than is necessary for that purpose or purposes.

f. Personal data shall be processed in accordance with the rights of data subjects under the data protection regulation.

g. Appropriate information and technology and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

h. Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

11. Disposal and destruction of data and information

Disposal and destruction of files is done in compliance with the archival policy[16]. Media destruction is done centrally by DIT. If there is a need for decentralised destruction (for instance at a field office), instructions and clearance for the secure destruction of the assets must be requested from DIT.

[16] Archival policy: link