Direction générale de l'administration
Direction des technologies de l'information

Strasbourg, 14 octobre 2013

DGA/DIT(2013)02

Politique de Gestion de l'Information et des Données du Conseil de l'Europe

Contenu

1. Introduction

La présente politique s'inscrit dans le projet de mise en place d'un système complet de gestion de l'information et des données au Conseil de l'Europe. Elle réaffirme le principe selon lequel l'information est une ressource clé du Conseil de l'Europe, ressource qui peut (et doit) être continuellement mise en valeur pour remplir le mandat et assurer le succès de l'Organisation. Les principes et le cadre opérationnel de cette politique concernent l'ensemble de l'Organisation.

La Cour Européenne des Droits de l'Homme (DH Cour) et la Direction Européenne de la Qualité du Médicament et soins de santé (DEQM) ont leurs propres politiques de gestion de l'information, qui répondent aux principes adoptés à l'échelle de l'Organisation, dans la mesure où ceux-ci conviennent à leurs missions spécifiques. Dans le contexte des services fournis de manière centralisée sous la responsabilité de la Direction des Technologies de l'Information (DGA-DIT), la DH Cour et la DEQM veilleront directement à la conformité de leurs procédures avec la présente politique de gestion de l'information et des données.

La Politique de Gestion de l'Information et des Données s'applique à l'ensemble des agents du Conseil de l'Europe et du personnel assimilé (contractants, experts, consultants, stagiaires, etc.).

2. Valeur de l'information

L'information est un atout clé pour atteindre les objectifs du Conseil de l'Europe, depuis la conduite d'activités sur le terrain jusqu'au fonctionnement efficace de l'administration. Toutes les Grandes Entités Administratives (MAE) créent et utilisent des données et des informations :

- Les données sont collectées ou créées ; elles retiennent les faits et forment un ensemble organisé.
- Les informations sont le fruit de l'interprétation des données. Nous les utilisons pour prendre des décisions, constater des faits, appréhender un contexte, etc.

En conséquence, les données ont un coût et les informations ont une valeur (figure 1). Pour que cette valeur puisse être reconnue, maintenue et préservée, les informations doivent être fournies en temps utile, disponibles et d'une qualité suffisante :

- Les informations et les données sont la propriété du Conseil de l'Europe tout comme les valeurs et bénéfices résultant de leur utilisation dans l'ensemble des activités. La seule exception à cette règle concerne les données personnelles (date de naissance, adresse du domicile, etc.)[1].
- Les agents sont les « gardiens » des données et des informations qu'ils importent ou qu'ils créent dans l'exercice de leurs fonctions, en veillant à leur actualité, à leur disponibilité, à leur qualité et à leur protection. Les informations archivées et les records et documents historiques relèvent de la responsabilité des Archives Centrales à la DIT.

La Direction des Technologies de l'Information fournit et applique les éléments suivants :

- La présente Politique de Gestion de l'Information et des Données.
- Le cadre opérationnel nécessaire à la mise en œuvre de cette politique.
- des services de conseil et de formation visant à assurer la meilleure utilisation possible de l'information et des données.
- Les systèmes et les processus nécessaires à la gestion de l'information tout au long de son cycle de vie.

[1] STE 108 - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel - lien

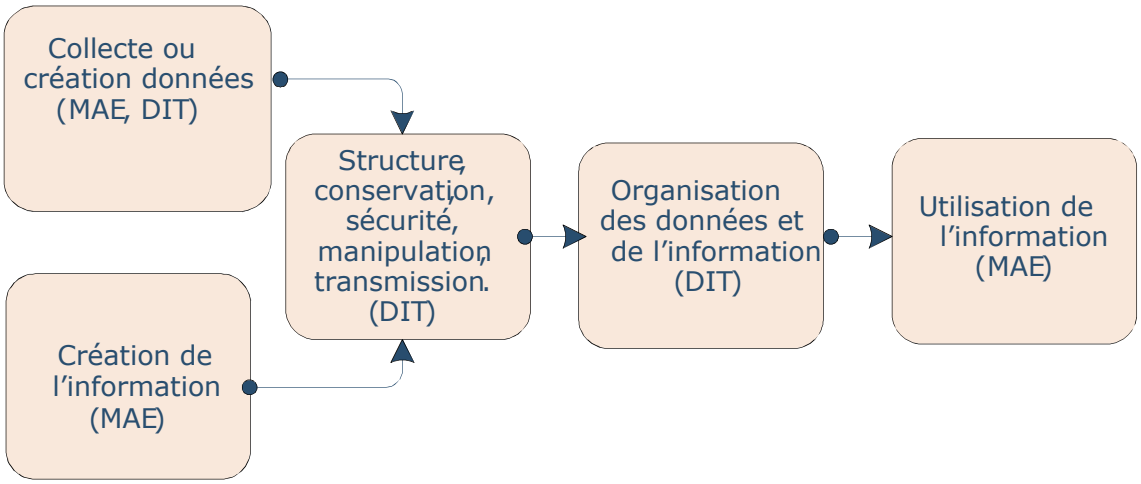

Figure 1. Chaîne de valeur de l'information et des données.

3. Gestion de l'information[2]

La Gestion et Gouvernance de l'Information du Conseil de l'Europe définit le cadre et les responsabilités au sein du système ; elle est composée de personnes, de processus, de règles et de solutions en technologies de l'information (TI). Son objectif est d'assurer la gestion efficace et efficiente de l'information pour permettre à l'Organisation d'atteindre ses objectifs stratégiques, et de mener à bien ses programmes et activités métier et administratifs.

Sa mise en œuvre s'appuie sur les éléments suivants :

- Le Comité directeur de la gestion des connaissances :
  Le comité adresse au Secrétaire Général, des recommandations concernant l'adoption de normes en matière de gestion de l'information, à l'échelle de l'Organisation.

- Les Grandes Entités Administratives, qui exercent les responsabilités suivantes :

  - Comprendre la nécessité de définir les niveaux requis de qualité des données.
  - Comprendre la valeur de l'information détenue par le Conseil de l'Europe en utilisant l'information de manière appropriée.
  - Appliquer la présente politique de gestion et les bonnes pratiques ; répondre aux exigences réglementaires énoncées dans le manuel administratif et dans les pages intranet correspondantes (DIT, pages consacrées à la gestion de l'information, etc.).
  - Créer et gérer l'information et les données comme une ressource du Conseil de l'Europe.
  - Définir les modes d'accès à l'information et aux données qu'elles produisent et gèrent.
  - Appliquer les règles de conservation et de destruction[3] fixées avec les grandes entités administratives.
  - Gérer les métadonnées associées et les maintenir à jour.
  - Assurer une coordination avec la DIT pour approbation de toute question concernant l'acquisition, le développement et l'installation de nouveaux systèmes ou processus relevant des technologies de l'information[4].
  - Respecter la législation nationale et internationale concernant l'utilisation et la diffusion des informations et données (par exemple, lois sur les droits d'auteur).

[2] La gestion de l'information traite l'information comme une ressource organisationnelle. Elle couvre les définitions, l'utilisation, la valeur et la distribution de toutes les informations et données au sein d'une organisation, soumises ou non à un traitement informatique. Elle évalue les types de données/informations dont une organisation a besoin pour fonctionner et se rapprocher de ses objectifs de manière efficace.
[3] Règles de conservation et de destruction : lien
[4] Liste de logiciels non conformes : lien

- Les Correspondants Informatiques et Correspondants Archives[5] :
  Ces groupes assurent une liaison entre les entités et la DIT. Leur rôle est défini dans les documents « Rôle et légitimité du Correspondant Informatique »[6], RAP-INF(2001)6 et DGAL 136 Politique d'archivage[7].

- La Direction des Technologies de l'Information :

  - Fournit les outils, les services[8] et les moyens techniques (systèmes TI) et organisationnels (processus et méthodes) permettant d'exécuter, de manière efficace, les tâches relatives à la gestion de l'information et des données.
  - Héberge les ressources humaines nécessaires aux activités TI de l'Organisation.
  - Offre un service de conseil et définit les normes relatives à la gestion de l'information.
  - Gère les données de référence communes (« common master data » utilisées dans toute l'Organisation).
  - Fournit un service d'archivage de longue durée et de conservation des records et des archives ; les entités doivent utiliser les outils et les procédures recommandés par la DIT pour créer les records.
  - Assure l'accès aux archives historiques.
  - Gère le budget (budget d'investissement et budget ordinaire) de toutes les activités de l'Organisation relevant des technologies de l'information. Toute exception doit être justifiée par la MAE concernée et approuvée par la DIT ; l'affectation de ressources TI fait l'objet d'un accord fondé sur un cas d'affaire[9] (business case) et une analyse des besoins métier[10] (business requirements).
  - Veille au respect de la présente politique de gestion par les utilisateurs et les MAE.

4. Collecte et création de l'information et des données

1. Collecte et création :

- Création : elle s'effectue en utilisant les systèmes de l'Organisation mis en place par la DIT en fonction des besoins métier déclarés par les MAE.
- Collecte : elle s'effectue par l'importation depuis des sources externes, au moyen de liens directs ou par transfert de fichiers. S'il est nécessaire d'utiliser un système spécifique, celui-ci doit être mis en place et validé par la DIT.

2. Qualité :

- Il incombe aux MAE de définir le niveau de qualité des données adapté à leurs besoins. Le niveau minimal comprendra les éléments suivants :
  - le niveau de précision nécessaire ;
  - le nom de la source ;
  - la date de création (et non la date d'acquisition) ;
  - la durée de validité (avec date d'expiration de la validité) ;
  - le gardien des données au sein de l'Organisation – la personne qui a importé les données ;

  Le niveau de qualité ainsi défini doit être indiqué dans les propriétés du fichier qui contient les données. Le gardien des données doit : soit entretenir la ressource (ensemble de données ou informations), soit la figer (créer un record), soit la détruire si elle n'a plus d'utilité.

[5] Rôle et légitimité du Correspondant archives : lien
[6] Rôle et légitimité du Correspondant informatique : lien
[7] Politique d'archivage : lien
[8] Catalogue de services de la DIT : lien
[9] Modèle de cas d'affaire (business case, en version anglaise uniquement) : lien
[10] Modèle d'analyses des besoins métier : lien

5. Stockage de l'information et des données

La DIT assure le stockage approprié de l'information et des données en format numérique de manière à :

- permettre l'accès, le partage, la recherche et la réutilisation des éléments conservés, à brève échéance et durablement ;
- appliquer des critères pertinents en matière de sécurité et de droits d'accès ;
- assurer la préservation des contenus numériques ;
- assurer la protection de l'information et des données en cas de sinistre ou de catastrophe.

Description succincte :

- les informations et données temporaires à caractère personnel sont conservées sur les lecteurs P:\ et dans les messageries des utilisateurs. La capacité de ces deux équipements est limitée ;
- les informations et données à caractère professionnel sont conservées dans les dossiers publics (public folders), les espaces partagés (shared drives) et les espaces collaboratifs. Les informations et données finalisées doivent être conservées sur ces supports ;
- les informations et données validées sont conservées dans l'espace WCD (Web Cube Documentaire), sur les sites web et dans les dossiers publics ;
- les records sont conservés exclusivement dans le système de records management ;
- la communication d'informations ou de données se fait à l'aide du courrier électronique ou des dispositifs intégrés dans le site web. Il est rappelé aux utilisateurs qui doivent communiquer des informations ou des données par d'autres moyens (CD, DVD, clé USB, etc.), qu'ils sont tenus de respecter les règles de confidentialité et de sécurité.

Les tableaux 1 et 2 décrivent plus en détail les modalités de traitement par la DIT, des informations conservées sur différents supports.

Le cycle de sauvegarde est organisé comme suit[11] :

- Les données sont enregistrées quotidiennement sur bande magnétique et conservées pour une durée d'un mois ; les enregistrements effectués en fin de semaine sont conservés pour une durée de deux mois. L'archivage est assuré par la DIT conformément à la Politique d'Archivage du Conseil de l'Europe.

La procédure de sauvegarde ne doit pas être considérée comme un mode de conservation permettant d'accéder aux données et aux informations sauvegardées. Son utilisation est strictement réservée à des fins de sécurité et de continuité de l'activité.

Le stockage de l'information et des données est une activité qui connaît une évolution technologique rapide, par exemple dans le domaine des systèmes de gestion documentaire et de records management. La Politique de Gestion de l'Information et des Données sera modifiée en conséquence pour s'adapter aux politiques opérationnelles ; les utilisateurs seront tenus informés de ces évolutions par l'intermédiaire de l'intranet de l'Organisation.

6. Conservation de l'information et des données

La conservation consiste à assurer la disponibilité de l'information et des données pertinentes, pour consultation et réutilisation, pendant une durée déterminée. En effet, une partie seulement des données et des informations doit être conservée pour des besoins opérationnels ou administratifs futurs. Les ressources dont la conservation n'est pas nécessaire doivent être détruites.

Les tableaux de gestion des MAE indiquent quelles sont les ressources à conserver, et pendant quelle durée. Ils sont approuvés conjointement par la MAE concernée et par la DIT. Les éléments non

[11] Une sauvegarde est une reproduction exacte des données actives, destinée à permettre la reprise d'activité après une catastrophe (gestion des risques à court terme) ; les sauvegardes se distinguent des archives, qui doivent assurer l'accès aux informations importantes de manière continue et sur une longue durée (plus de cinq ans).

mentionnés dans ces tableaux sont conservés pour une durée de cinq ans après leur dernière modification.

La DIT fournit les outils de gestion de la conservation et élimine les ressources inutiles conformément aux procédures convenues.

L'archivage de longue durée des ressources numériques est assuré, exclusivement, au moyen du système central de records management.

7. Sécurité de l'information et des données

La DIT fournit le matériel et les procédures de sécurité, pour l'ensemble de l'Organisation et de ses activités, comme suit :

- Le réseau du Conseil de l'Europe, routeurs, switch TCP/IP.
- Le centre informatique.
- La messagerie électronique.
- Les ordinateurs de bureau, ordinateurs portables, téléphones portables, tablettes et médias de stockage amovibles.

La responsabilité en matière de sécurité couvre les points suivants :

- La disponibilité des ressources TI, physiques ou non physiques.
- L'intégrité, la confidentialité[12] et la traçabilité des informations et des données.

En conséquence, les utilisateurs ne sont pas autorisés à connecter des équipements ni à installer des logiciels sur le réseau du Conseil de l'Europe sans l'accord formel de la DIT. Dans les bâtiments de l'Organisation, tous les lieux de rencontre ouverts au public sont équipés par la DIT de points de connexion Wi-Fi, à l'intention des visiteurs et des agents du Conseil de l'Europe ayant besoin d'une connexion internet sur place.

Les informations ou données dont la classification (niveau de confidentialité) n'est pas clairement établie ou définie par le propriétaire/gardien se voient attribuer le niveau de sécurité standard du système d'information de l'Organisation (accès interne uniquement). Le niveau de confidentialité est établi au moyen des métadonnées des ressources.

Les propriétaires/gardiens des données et informations doivent savoir qu'ils sont tenus de garder ces ressources dans le périmètre couvert par la présente politique de gestion. Le fait, par exemple, de transférer des ressources sur des médias amovibles (clé USB, CD, DVD, etc.) ou des sites de stockage en ligne (Gmail, DropBox, etc.) est contraire à la présente politique de gestion, à moins que les ressources n'aient fait l'objet d'un cryptage approuvé par la DIT. A cet égard, une attention particulière doit être accordée aux pièces jointes des courriers électroniques.

8. Accès à l'information et aux données

L'accès à l'information est régi par les textes en vigueur[13] et par des accords spécifiques conclus avec les services auteurs. Les modalités d'accès sont fixées dans les tableaux de gestion de chaque entité (normes actuelles[14]). La DIT gère une base de données des règles d'accès aux documents du Conseil de l'Europe (www.transparency.coe.int).

La DIT assure l'accès intégral au contenu de l'intranet depuis les équipements qu'elle fournit et gère. L'accès depuis d'autres équipements, d'autres réseaux ou par internet est soumis aux restrictions prévues par la politique de sécurité.

Les responsabilités des utilisateurs quant à l'utilisation du Système d'Information du Conseil de l'Europe, sont définies dans l'instruction n° 47, du 28.10.2003[15].

---

[12] Le niveau de confidentialité d'une ressource constituée d'un ensemble de données ou d'informations doit être défini par le propriétaire ou le gardien de la ressource, conformément à la réglementation interne : lien

[13] Politique d'accès aux documents du Conseil de l'Europe : lien

[14] Normes du Conseil de l'Europe : lien

[15] Instruction n° 47 : lien

Les utilisateurs sont pleinement responsables de la bonne utilisation de leur mot de passe (non-divulgation, renouvellement périodique, etc.).

9. Utilisation de l'information et des données

L'information est mise à la disposition des agents aux fins de l'exercice de leurs fonctions ; elle n'est pas destinée à un usage privé. Par exemple, les rapports établis par les agents sont la propriété de l'Organisation et ne doivent pas être copiés ni conservés sur des supports en dehors de l'infrastructure informatique de l'Organisation.

Les ressources qui doivent être communiquées à l'extérieur de l'Organisation feront préalablement l'objet d'une validation (autorisation) au moyen du niveau de sécurité approprié à la ressource (par exemple : accès public, restreint ou secret).

Tout agent auteur d'un ensemble de données ou d'informations est tenu de suivre et d'appliquer les règles relatives à la sécurité et à la déclassification de l'information établies par l'entité auteur.

Tout membre du public (particuliers, organisations, institutions, etc.) peut utiliser les informations qui sont publiées sur les sites web du Conseil de l'Europe ou qui lui sont communiquées directement. Dans ce contexte, les droits d'auteur et les clauses de non-responsabilité qui accompagnent les informations sur le site officiel du Conseil de l'Europe doivent être respectés.

10. Protection des données

Tous les utilisateurs de l'information et des données du Conseil de l'Europe doivent comprendre et observer les principes de la protection des données :

a. Les données personnelles doivent être traitées loyalement et licitement.
b. Les données à caractère personnel doivent être obtenues uniquement pour une ou plusieurs finalités déterminées et licites et ne doivent pas être traitées ou communiquées d'une manière incompatible avec cette ou ces finalités.
c. Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités poursuivies.
d. Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour.
e. Les données à caractère personnel, traitées pour une ou plusieurs finalités ne doivent pas être conservées plus longtemps que nécessaire au regard de la ou des finalités poursuivies.
f. Les données personnelles sont traitées conformément aux droits conférés aux personnes concernées par la règlementation sur la protection des données.
g. Les mesures techniques et d'organisation appropriées doivent être prises contre tout traitement non autorisé ou illicite, contre toute perte ou destruction accidentelle ou contre toute altération de données à caractère personnel.
h. Les données à caractère personnel ne doivent pas être transférées vers un pays ou territoire situé en dehors de l'Union européenne à moins que ce pays ou territoire n'assure un niveau de protection adéquat aux droits et libertés des personnes concernées en matière de traitement des données à caractère personnel.

11. Suppression et destruction d'informations et de données

La suppression et la destruction de fichiers sont assurées conformément à la politique d'archivage[16]. La destruction de médias est assurée centralement par la DIT. S'il est nécessaire de procéder à une destruction décentralisée (dans un bureau extérieur par exemple), les instructions et une validation doivent être obtenues auprès de la DIT, afin de garantir la destruction des ressources en toute sécurité.

[16] Politique d'archivage : lien