La numérisation des archives en CPAS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Laura CERRATO

Data Breach Case Officer

10/10/2023 – En ligne - UCMW

Axe 2 – Un cadre juridique

Dans un contexte archivistique

- Aperçu des lois principales sur la rétention et authenticité des données
- Retour sur la question de la substitution numérique
- RGPD et la gestion de l'information

Les archives

Quelle est la question ?

Les archives posent

- une question d'authenticité de l'information archivée
- une question de rétention (longue) de l'information archivée

Les obligations d’authenticité

« Authenticité »

De l'objet ? Du contenu ? Garantir la force probante ?

Ces dimensions de la donnée s'imposent:

- tant de la version papier à sa version numérique (« substitution»)
- tant dans sa version numérique ontologique (ex: signature numérique)

→ e-IDAS répond aux enjeux de la sécurité de l'information numérique sur le plan de l'intégrité et la non-répudiation des données numériques et numérisées

→ Le Digital Act belge organise le cadre légal de la substitution (Livre XII, titre 2 du C.D.E.) à des fins d'archive électronique.

Pour l'heure, il n'existe encore aucun service d'archivage qualifié actif reconnu au niveau national (la « trusted list » gérée par le SPF Économie).

Attention – ceci n'a rien a voir avec les données authentiques. Régime légal propre.

Seulement un service « Qualifié »?

- 2 Concepts issu d'eIDAS: service de confiance dit *qualifié* et *non-qualifié*
- Doit-on obligatoirement passer par un service dit qualifié ?
    - 3 conditions cumulatives pour recourir *de facto* au service qualifié (source: SPF Economie)
        - l'utilisateur doit opter pour la voie électronique
        - l'obligation n'existe que si « un texte légal ou réglementaire prévoit une exigence expresse » d'archivage, de recommandé ou de datation
        - par application du principe général de droit « lex specialis derogat legi generali », l'obligation ne s'applique que si une disposition légale ou réglementaire spécifique ne prévoit pas une autre solution.
- 2 définitions existent dans la loi: « service d'archivage électronique » (service de confiance tel que définit par eIDAS) et « service d'archivage électronique qualifié ». Ces définitions enseignent que les services d'archivage électronique peuvent être **soit** fournis par un prestataire de services de confiance au profit du public **soit** exploités par un organisme du secteur public ou une personne physique ou morale pour son propre compte. Pour le second, il existe des dérogations à l'article XII.28, §2 du CDE en vertu de 2 conditions.

Art. XII.28. [1 § 1er. Un prestataire de service d'archivage électronique qualifié et un organisme du secteur public ou une personne physique ou morale qui exploite pour son propre compte un service d'archivage électronique qualifié satisfont aux dispositions du règlement 910/2014 applicables au prestataire de services de confiance qualifié et aux exigences visées par le présent titre et son annexe I.

§ 2. Par dérogation au paragraphe 1er, un organisme du secteur public ou une personne physique ou morale qui exploite pour son propre compte un service d'archivage électronique qualifié est dispensé des exigences visées aux articles 20, paragraphe 1, 21 et 24, paragraphe 2, a), d) et i) du règlement 910/2014 ainsi que de celles visées aux e), i), j) et k) de l'annexe I du présent titre. Néanmoins, il est tenu de communiquer à l'Organe de contrôle, avant le début de l'exploitation du service, les informations suivantes:

1° son nom ou dénomination sociale;

2° l'adresse géographique où il est établi ou domicilié;

3° les coordonnées permettant de le contacter rapidement, y compris son adresse de courrier électronique;

4° son numéro d'entreprise;

5° un rapport d'évaluation, effectué à ses frais, par un organisme d'évaluation de la conformité, confirmant le respect des exigences du règlement 910/2014, du présent titre et de son annexe I.

L'Organe de contrôle lui délivre un récépissé dans les cinq jours ouvrables suivant la réception des informations. L'Organe de contrôle peut, s'il le juge utile notamment sur la base du rapport d'évaluation, procéder à un contrôle.

§ 3. Sans préjudice de l'article 34, paragraphe 2, du règlement 910/2014, le Roi peut déterminer les numéros de référence des normes applicables au service d'archivage électronique qualifié. Le service d'archivage électronique qualifié qui respecte ces normes est présumé satisfaire à tout ou partie des exigences du présent titre et de son annexe I. Le cas échéant, le Roi spécifie les exigences présumées satisfaites.]1

Les obligations de préservation

Rétention

- **Finalité primaire -** objectif opérationnel
- **Finalité secondaire -** objectif archivistique pour l'intérêt public, la recherche historique/scientifique et statistiques

→ Impositions légales – déclinaison multiple (EU, Fédérale , Région, Commission communautaire, Fédération, Province, Administrations locales ...) et sectorielles.

→ En absence de loi qui précise une rétention particulière (maximale) tant en finalité primaire que secondaire, le responsable de traitement/le propriétaire des données doit en déterminer le temps de préservation nécessaire a ses fins.

Un petit dernier: le RGPD

D’autres considérations ?

Les données personnelles sont traitées en ligne avec

1. Le principe de licéité
2. le principe de nécessité
3. le principe de proportionnalité
4. le principe de minimisation (quantité de données, temps de rétention de la donnée, accès aux données)
5. le principe de transparence
6. le principe de sécurité

→ **ces principes doivent être intégrés dans le cycle de vie de la donnée personnelle (directe et dérivée, finalité primaire et secondaire)**

→ le RGPD ne parle pas d’authenticité mais d’exactitude des données personnelles

→ Le RGPD s’applique tant au numérique qu’au support papier

Une dérogation : Art. 89, considérant 158

Cette dérogation

- concerne 3 domaines différents (avec des contraintes propres a prendre en considération)
- pose des limites aux droits des personnes
- peut aller à l'encontre du principe de minimisation (quantité de données, temps de rétention)
- et en même temps impose que des mesures [de sécurité] techniques et organisationnelles soient respectées pour garantir ce même principe de minimisation (accès aux données)

« Les autorités publiques ou les organismes publics ou privés qui conservent des archives dans l'intérêt public devraient être des services qui, en vertu du droit de l'Union ou du droit d'un État membre, ont l'obligation légale de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur, de diffuser des archives qui sont à conserver à titre définitif dans l'intérêt public général et d'y donner accès. »

Une gouvernance des données

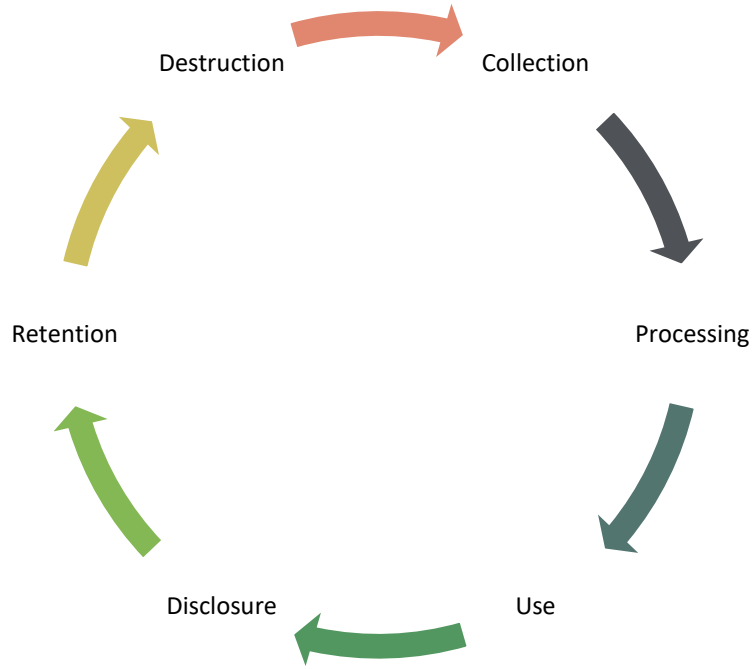
Le point de depart

Il est important de connaitre le **cycle de vie de la donnée** (personnelle) afin de **connaitre ses données** (“know your data”).

→ Outils à developer pour realiser cet objectif: **Inventaire de données** et **flux de données**

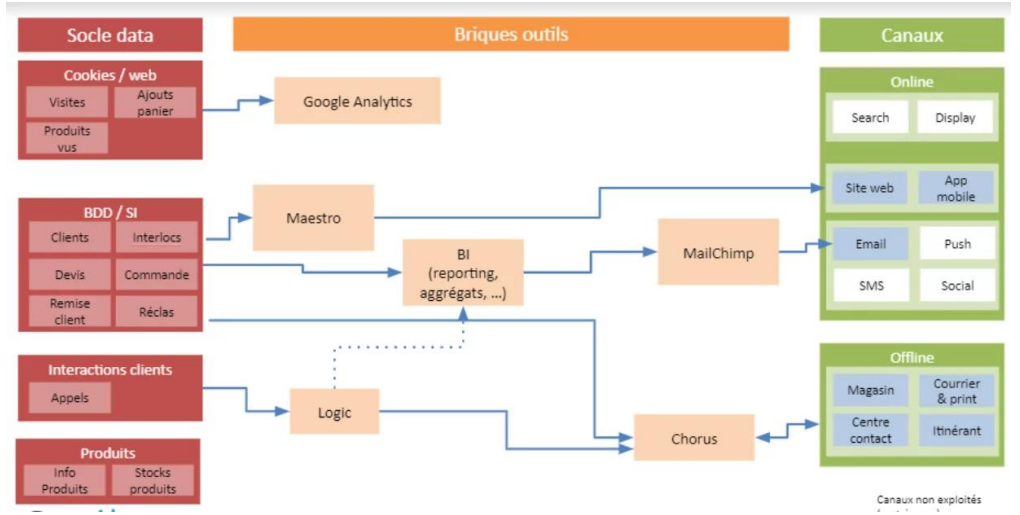
→ Ces outils permettront **é**galement d’identifier et realiser les principes suivants:

- archive by design
- privacy by design
- security by design
- risk assessment by design
- data subject’s right by design
- …



Par ou commencer ?

- Il n’y a pas une et seule recette pour démarrer un inventaire
- Vous pouvez démarrer l’exercice
  - Par département (ses processus)
  - Par outil existant
  - Par projet
- Le développement et la maintenance de ces instruments s’inscrivent dans un processus de contrôle itératif et continu.
- Cet exercice a plus qu’un seul avantage



Données sources

#	Source	Type de données	Type d'outil (SAAS, custom)	Volume	Fréquence de MAJ	Intégration possible (API, CSV, ...)	Commentaires
1	Cabestan	Données personnelles, de comportement email, de ciblage, ...	SAAS	5K users opt-ins. M envois emails/mois	Quotidienne	N/A	- 2 scénarios : Bienvenue / Anniv - 1 à 2 campagnes par mois - Alimenté en batch quotidien par
2	Caisse	Données de ventes et de consommation	Sequoiasoft / On-premise	Sur l'ensemble des restaurants : > M de commandes/mois > M de lignes de commandes consommés/mois	Quotidienne (à minima)	WebServices possibles	Si perte de connexion, alors un rattrapage est fait entre les serveurs locaux et celui consolidant les données de tous les restaurants au siège.
3	Wifi	Données de profiling anonymes (MAC)	Weblib	Dans une 20taine de restaurants.	N/A	Oui, API ou batch quotidien	Uniquement un volume de restaurants réduits. Pas d'interconnexion de données à ce jour vers le SI
4	Axis/Ingenico (paiement CB)	Token CB et données de paiement	Terminal de paiement électronique (TPE)	Entre M de règlements/mois	?	?	Mise en oeuvre finalisée à fin mai 2019. Dissocié du système de caisse.
5	Site web	Données personnelles ( )	Drupal	inscriptions NL / mois visiteurs / mois	-	Oui (détail à obtenir)	
6	P	Données de paiement en ligne quand on utilise le Click & Collect du site web	SAAS	15zaine de restaurants participent au click&collect. Une 40taine de commandes/semaine sur les	N/A	Oui (détail à obtenir)	Pas d'interconnexion de données à ce jour vers le SI

Liens intéressants

Lectures

- https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/276-1.pdf
- https://commission.europa.eu/system/files/2018-10/eag_draft_guidelines_1_11_0.pdf
- SPF Economie
- https://commission.europa.eu/system/files/2023-06/Whitepaper%20AbD_en.pdf
- https://www.arch.be/index.php?l=fr&m=fonctionnaire&r=terminologie-et-sujets&sr=legislation
- https://www.merak.be/be-fr/centre-de-connaissance/delais-legaux-de-conservation-des-archives

Lois

- CDE: http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&la=F&cn=2013022819&table_name=loi&&caller=list&F&fromtab=loi&tri=dd+AS+RANK&rech=1&numero=1&sql=(text+contains+(‘’))
- E-IDAS: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.FRA&toc=OJ:L:2014:257:TOC

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority