Publié dans MesInfos le 24/05/2017 (dernière mise à jour le 24/05/2017)
Tags : Uncategorized
http://reseau.fing.org/blog/view/169242/restituer-les-donnees-ca-veut-dire-quoi-1er-mode-d%E2%80%99emploi-pour-les-organisations
Page générée le 18/09/2019 à 00:04

Restituer les données, ça veut dire quoi ? 1er mode d'emploi pour les organisations

Que signifie pour une organisation se lancer dans le Self Data ? Comment faire pour restituer des données personnelles à ses clients ou usagers ? Une année de travail dans le cadre du pilote MesInfos nous a permis de documenter le process, les écueils, les leviers, les étapes… de la restitution des données, pour un détenteur qui souhaiterait se lancer dans le Self Data.

Nous avons identifié 4 questions clés pour les organisations qui souhaitent lancer un projet de Self Data. Mais une partie de ces enseignements peut aussi nourrir les projets de mise en oeuvre de la portabilité, telle que définie par le GDPR (Règlement Européen de Protection des Données Personnelles).

Ces éléments ont vocation à s'enrichir au fil de l'année, mais nous espérons qu'ils pourront d'ores et déjà nourrir les réflexions des uns et des autres !

"Je souhaite engager mon organisation dans la restitution des données personnelles, mais je ne sais pas par où commencer. Quels collaborateurs associer en interne ? Quel est le premier chantier ?"

La restitution des données personnelles aux clients ou aux individus est de fait un projet très transverse. Différents services et plusieurs personnes seront à associer à un moment ou à un autre du projet : innovation, marketing, DSI, services juridiques, métiers… un bon point de départ est de commencer par identifier des interlocuteurs, afin de présenter le projet en interne à plusieurs de ces collaborateurs, éventuellement en associant des acteurs de l'écosystème Self Data (Fing ou acteurs similaires, plateformes Self Data, etc.).

Quelles étapes pour la restitution des données à proprement parler ? Comment mettre cela en oeuvre ?

On peut décrire le processus avec les phases suivantes.

1. Formuler une liste des données : établir une liste de ce qu'il y a dans vos systèmes d'information en termes de données, que vous envisagez de transmettre aux individus qu'elles concernent (idéalement en mobilisant des collaborateurs de la DSI – voire de la gouvernance de la donnée – des métiers, habitués à travailler avec ces données au quotidien, et de la relation client / marketing)

2. Initier une procédure d'approbation de l'initiative, du principe et des modalités de transmission des données, et de la liste des données par votre organisation.

Tous les partenaires qui transmettent des données en 2016 dans le pilote MesInfos ont dû passer par là. Ces procédures internes étaient dans chaque cas différentes, mais en général assez longues, et demandant de porter le message en interne dans différents services. Ici encore, associer des acteurs extérieurs peut être opportun.

3. Formaliser la liste des données, en commencer la documentation. Cela permettra notamment de l'ajouter dans un outil indispensable au pilote : http://mesinfos.fing.org/cartographies/datapilote/. Cet outil est un support d'échange clé avec les acteurs du projet, et permet de faciliter l'appropriation des données par des ré-utilisateurs (cela mobilisera la DSI et ses métiers pour élaborer la documentation précise).

4. Préparer un système de transmission : nous penchons vers des éléments automatiques, mais pour l'instant cela reste des solutions assez légères, dimensionnées pour les quelques milliers de testeurs du pilote.

Ici, les questions à traiter (qui mobiliseront principalement la DSI) :

- identification : comment relier l'individu qui demande ses données, à son identifiant client dans le SI (et ainsi à ses données) ?
- authentification : comment s'assurer que la personne qui demande ses données est bien celle qu'elle prétend être ?
- transmission : comment transmettre de manière sécurisée les données ?

De quelles données parle-t-on ? Quel format, quel standard ? Quelles possibilités de visualisation ?

On trouve en général différentes catégories de données personnelles :

- Les données administratives et sur la relation client (CRM) : fiche client, données de segmentation, facturation, contrat, … On les retrouve dans toutes les organisations, souvent avec quelques spécificités. Elles amènent des cas d'usages assez administratifs. Par exemple, le cas d'usage de mise à jour automatique de ces données, de l'individu vers l'organisation, souvent évoqué comme une perspective intéressante par les organisations.

- Des données transactionnelles souvent très liées et spécifiques au métier de l'organisation. Ce sont les relevés de consommation d'énergie (des compteurs connectés), les relevés de comptes, les sinistres (assurances), le journal d'appel, … Elles offrent souvent un regard et un point de vue objectif à l'individu sur des actions dont il n'a pas forcément pleinement conscience. Ce sont ces données qui ouvrent le plus les potentiels de cas d'utilisation, et la valeur d'usage des services sur les Self Data.

- Des traces et des communications et points de contact entre l'organisation et son client, tels que les horodatages de connexion sur l'espace client Web, les dossiers de suivi du service client… On imagine immédiatement une exploitation partagée de ces données par l'organisation et l'individu, tant la transparence et l'efficacité sont précieuses dans ces moments pour les deux parties.

Les modèles de données et formats sont peu challengés, mais font l'objet d'une traduction dans la plateforme (Cozy), afin de les rendre plus cohérents, d'un point de vue transsectoriel.

Quelle responsabilité pour le détenteur de données ?

De manière relativement simple, une société détentrice de données personnelles, qualifiée de responsable du traitement au regard de la loi « Informatique et Libertés », n'est plus responsable des données une fois que :

- Celles-ci ont été transférées à la personne concernée ;

- Et qu'elle n'opère plus de traitement sur lesdites données (ce qui exclut tout traitement, y compris par une application fournie par le détenteur sur le cloud privé).

En d'autres termes, la responsabilité de traitement du détenteur s'arrête au moment où il n'a plus la maîtrise des données (en termes de finalité d'usage et de moyens de traitement) dans la mesure où il transmet ces dernières à la personne concernée.

Par ailleurs, de manière plus générale, la transmission des données est sans incidence, d'un point de vue juridique, sur les obligations du détenteur quant au traitement initialement opéré sur les données.

Mais alors, quel lien entre le pilote MesInfos et le GDPR ?

Quel lien peut-on faire avec l'évolution de la réglementation européenne concernant les données personnelles, notamment au regard de l'article sur le droit à la portabilité du GDPR (General Data Protection Regulation) ?

Le périmètre de ce droit, tel que défini notamment par la CNIL et le G29, est large. Il comprend toutes les données personnelles qu'un individu donné a fourni ("provided") au détenteur de données/responsable de traitement (voir question suivante).

L'article 20 du GDPR engage dans tous les cas les organisations à rendre ce droit à la portabilité effectif dans les deux années qui viennent (d'ici mai 2018).

Ainsi, **le pilote MesInfos est une manière pour les partenaires de réfléchir à ce droit** ; une occasion de déterminer les manières de se mettre en conformité avec le règlement et donc d'appliquer le règlement le plus vite possible, pour prendre un temps d'avance et créer pour eux comme pour leurs clients de la valeur autour de ce nouveau droit. Pour le dire autrement ce droit n'a jamais été mis en pratique ; en ce sens, le pilote MesInfos est une manière d'expérimenter des réponses techniques et juridiques. Il sera l'occasion de lister les questions et d'explorer des pistes qui permettent aux partenaires du pilote d'alimenter le travail des juristes dans les entreprises, en vue de l'implémentation du droit à la portabilité.

Quelles données sont concernées par ce droit ?

Le périmètre des données restituées dans le cadre du pilote MesInfos (qui correspond, en quelque sorte, à une mise en pratique du droit d'accès) ne sera probablement pas identique à celui du droit à la portabilité.

En effet, la mise en oeuvre du droit à la portabilité ne concerne pas toutes les données concernées par le droit d'accès. Le règlement fait références aux données "fournies" par l'utilisateur d'un service ; le périmètre est ainsi évidemment plus large que les seules données de formulaire, fournies par un utilisateur à l'inscription. Ces données "fournies" par l'individu couvrent à la fois (1) des données fournies proactivement (par exemple, adresse mail, âge, nom, etc.) et (2) des données "fournies" passivement par l'individu qui utiliserait un service. Ce second cas concerne par exemple des données d'historique de recherche, de géolocalisation, de trafic, ou d'autres données "brutes" telles que les mesures effectuées par des capteurs, objets ou applications (par exemple "nombres de pas" dans le cas du quantified self, données de consommation des compteurs communicants, etc.).

NB : Il peut y avoir des impossibilités justifiées de rendre ce droit à la portabilité pour certaines données (impossibilité technique, etc.), mais les motifs qui peuvent être invoqués sont très limités.

Qui est le responsable de traitement lorsque les données sont portables ?

La cascade de responsabilité est encore à définir. Mais globalement, la responsabilité d'un détenteur de données A s'éteint à partir du moment où il y a transfert des données vers un détenteur B.

Article importé:
http://mesinfos.fing.org/restituer-les-donnees-ca-veut-dire-quoi-1er-mode-demploi-pour-les-organisations/?utm_source=rss&utm_medium=rss&utm_campaign=restituer-les-donnees-ca-veut-dire-quoi-1er-mode-demploi-pour-les-organisations
Par: Marine Albarède
Publié: May 24, 2017, 4:27 pm