BANQUE CARREFOUR D'ÉCHANGE DE DONNÉES

COMPRENDRE LES PRISES DE TRACES ET D'INSCRIPTION : IMPACTS ET PROCÉDURES

TABLE DES MATIÈRES

1. Introduction 3
2. Le processus de prise de traces 4

2.1. Définition générale 4
2.2. Le processus 5

2.2.1. Vue globale 5
2.2.2. Proportionnalité de la prise de trace et responsabilité des acteurs 6
2.2.3. Rôles et responsabilités des différents acteurs : 7
2.2.4. Cas spécifique : prise de trace via BCED-WI 8
2.2.5. Quelques caractéristiques des traces 8
2.2.6. L'accompagnement de la BCED dans la prise de traces 8

3. Le processus des inscriptions 9

3.1. Définition générale 9
3.2. Cycle de vie des inscriptions 10

3.2.1. Les 4 opérations 10
3.2.2. Les mutations 10

3.3. Processus d'inscription 11

3.3.1. Principes de base 11
3.3.2. Publier, étendre et clôturer une inscription 12

4. Conclusion 16

1. Introduction

De manière globale, l'échange de données authentiques peut être défini comme une interaction entre un producteur de données (la source authentique) et un consommateur de données (une/ des administration(s) située(s) en Région Wallonne et/ou en Fédération Wallonie Bruxelles). Dans le cadre de sa mission, le consommateur va consulter une ou plusieurs données provenant du fournisseur. Techniquement parlant, la plupart des échanges s'opèrent via des web services[1]. C'est l'ESB[2] (Enterprise Service Bus) de la BCED qui se charge des échanges de données entre systèmes distants. La toute grande majorité des échanges de données concernant des données à caractère personnel, cela implique le respect strict de certaines règles afin d'être en conformité avec le RGPD[3].

L'objectif de ce document est donc de présenter et expliquer les principes à prendre en considération, fonctionnellement et techniquement, lors du développement des applications métiers afin de pouvoir contribuer à la conformité avec le RGPD lors du traitement opérationnel des données.

Nous aborderons les deux grandes notions fondamentales dans l'échange de données authentiques à savoir la « prise de traces » et le concept « d'inscription ». On peut très rapidement définir l'inscription comme le mécanisme permettant de matérialiser le fait qu'une administration possède un « dossier » sur un citoyen. Dès lors, dans le cadre de ce dossier, elle consulte des données afin de réaliser sa mission. La prise de trace quant à elle, consiste justement à enregistrer les consultations de données effectuées dans le cadre du dossier.

Ce contenu est destiné aux analystes fonctionnels et chefs de projets, qui doivent obligatoirement inclure dans leur éventuel cahier des exigences les recommandations en la matière. Il est également destiné aux développeurs, qui doivent prendre en compte ces principes lors de tout développement visant un traitement de données à caractère personnel.

---

[1] Un webservice en informatique est une application ou un service accessible via Internet qui permet à différents systèmes de communiquer entre eux. Il utilise des protocoles standard comme HTTP pour échanger des données, souvent au format XML ou JSON. En résumé, c'est un moyen pour des applications de s'interconnecter et de partager des informations de manière automatisée.

[2] L'ESB (Enterprise Service Bus) est un composant d'une architecture logicielle qui permet de connecter différentes applications au sein d'une entreprise et d'interfacer des applications externes à l'entreprise. Il facilite la communication et l'échange de données entre ces applications en utilisant des protocoles standardisés et des services intermédiaires pour transformer, acheminer et gérer les messages. Cela permet une intégration plus flexible et évolutive des systèmes informatiques.

[3] RGPD : Règlement Général sur la Protection des Données. Le texte complet du Règlement peut se trouver sur le site de l'UE :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

2. Le processus de prise de traces

2.1. Définition générale

Le terme de « **trace** » en informatique (« log » en anglais) désigne le mécanisme permettant de stocker des informations sur des évènements survenus sur un serveur, un ordinateur ou une application[4].
Nous pouvons en distinguer deux sortes :

1. Les **logs applicatifs :** Ces logs fournissent des informations sur le déroulement des processus applicatifs, ce qui est particulièrement utile pour le débogage. Il ne sera pas question de traiter ces dernières ici.

2. Les **Security (ou Privacy) logs** (ou traces légales) : ces logs permettent de savoir QUI a consulté QUOI, QUAND et POURQUOI. Ces traces sont obligatoires en vertu du Règlement Général sur la Protection des Données (« RGPD ou GDPR »)[5] qui oblige le responsable du traitement à :
   - Mettre en œuvre les mesures techniques et organisationnelles pour protéger les données (limiter les accès aux personnes autorisées, utiliser les données pour une finalité déterminée, minimisation et proportionnalité, etc...),
   - Communiquer une information à la personne concernée sur l'utilisation qui est faite de ses données.

Étant donné que les SECURITY LOGS contiennent des données à caractère personnel, seule une personne autorisée (DPO, CSI) peut y accéder. La prise de trace légale doit être effectuée à plusieurs niveaux :

1. Au niveau du consommateur de données.
2. Au niveau de l'intégrateur de service. (BCED, CIVADIS, BCSS, BOSA, ...).
3. Au niveau du fournisseur de données (Source Authentique).

Il est à noter que la prise de trace peut également être auditée par le CSI ou le DPO du responsable de traitement. La BCED, en tant qu'intégrateur de services, peut également effectuer des contrôles des traces auprès d'un consommateur de données.

---

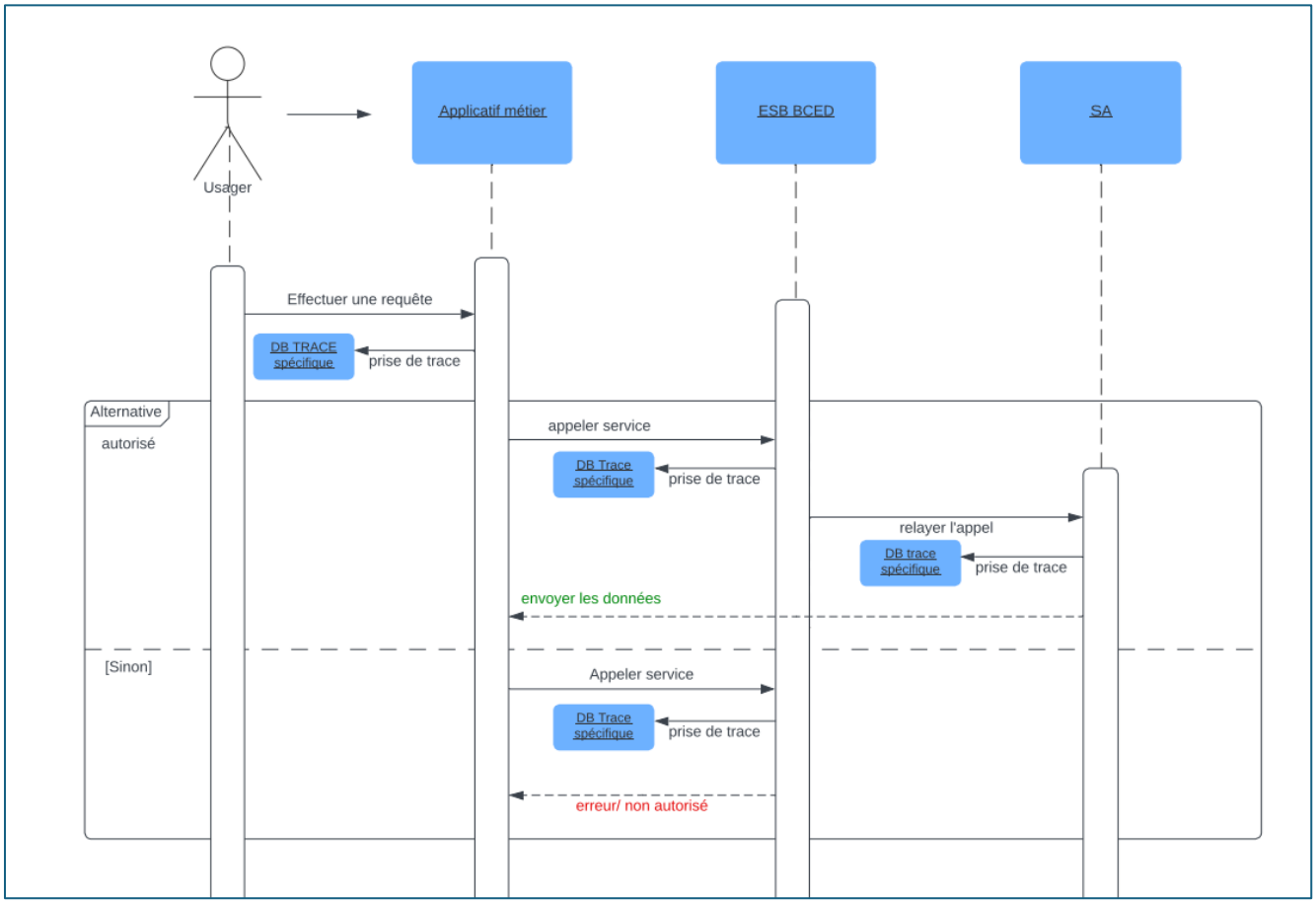
[4] https://blog.hubspot.fr/website/fichier-log

[5] Le *Règlement Général sur la Protection des Données* (RGPD) est une législation européenne entrée en vigueur le 25 mai 2018. Il vise à renforcer et unifier la protection des données personnelles des individus au sein de l'Union européenne. Le RGPD impose des obligations strictes aux entreprises et organisations concernant la collecte, le traitement et le stockage des données personnelles. Les principales exigences incluent le consentement explicite des utilisateurs, le droit à l'oubli, la portabilité des données, et la notification des violations de données. Le texte est consultable dans son intégralité à l'adresse suivante :
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

2.2. Le processus

2.2.1. Vue globale

Le diagramme de séquence ci-dessous, vous présente une vue globale du processus de la prise de traces.



Cette séquence peut être résumée de la manière suivante :

1. Un utilisateur effectue une requête dans son application métier pour consommer des DACP (« Données à Caractère Personnel »).
2. L'applicatif va réaliser la requête en appelant les données via le service adéquat.
3. À ce moment, une première prise de trace doit être effectuée et stockée au niveau de l'application consommatrice.
4. La BCED va réceptionner l'appel et va le relayer ensuite auprès de la source authentique.
5. Une prise de trace aura lieu au niveau de la BCED.
6. La Source authentique relayera les données réclamées via l'appel de l'application consommatrice[6].
7. Une prise de trace aura lieu à ce niveau également.

[6] Cet aspect ne sera pas détaillé mais il est bien évident qu'au préalable, le consommateur doit être autorisé à accéder aux données dont il demande la consultation.

Scénario alternatif :

1. En cas d'erreur ou d'accès non autorisé, l'appel est directement renvoyé avec un code erreur.

2.2.2. Proportionnalité de la prise de trace et responsabilité des acteurs

Comme exposé dans la section précédente, il importe de comprendre que la prise de trace constitue un **processus proportionné**. Il s'agit d'ailleurs d'une notion[7] centrale au sein RGPD.

Concrètement, cela signifie que l'ensemble de toutes les informations ne peut pas être en possession d'un seul acteur. Ceci ayant pour but d'éviter qu'un acteur puisse travailler individuellement sur toutes les données. Cela implique par conséquent deux choses :

1. **Chaque acteur ne doit stocker qu'une partie de la trace**. Ce principe vaut également pour des raisons de sécurité, par exemple en cas de compromission.

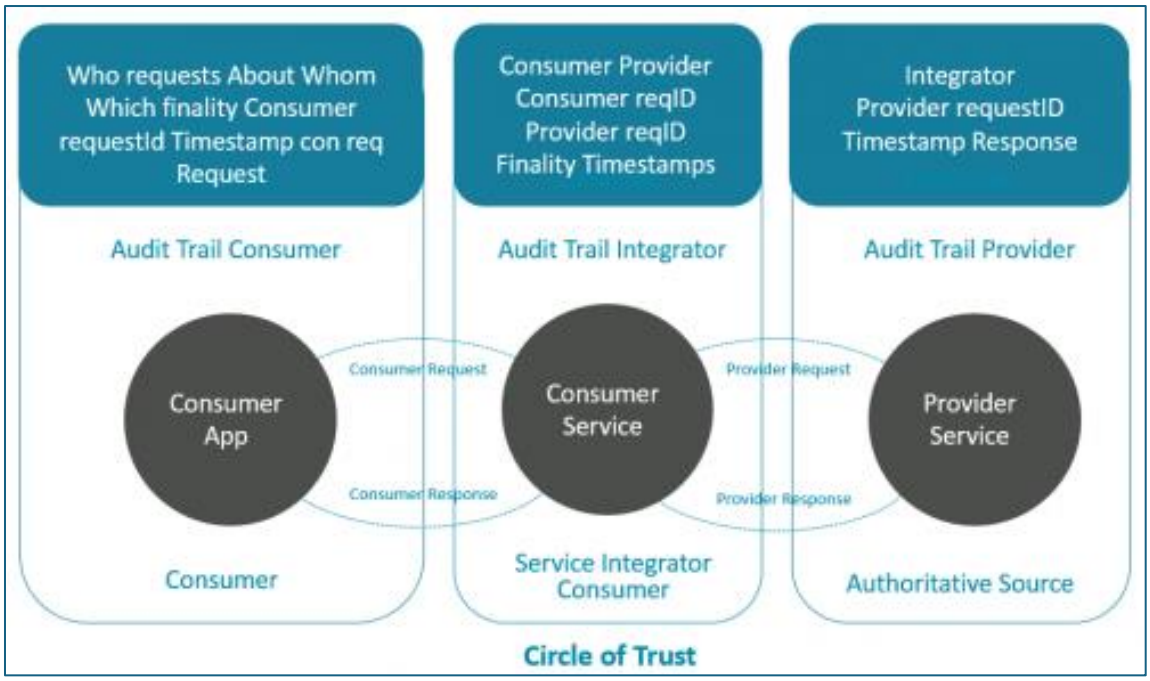
2. **Chaque partie de trace doit permettre de remonter au maillon précédent** ou faire le lien avec le suivant, de façon à pouvoir reconstituer l'ensemble de la trace (trace de bout-à-bout). Dans le cas spécifique de la BCED, nous devons donc être capable de remonter à l'application ayant appelé le service. Il est donc important de saisir que dorénavant, en tant que consommateur, vous avez la responsabilité d'opérer vous-même la prise de traces et de pouvoir par exemple remonter jusqu'à l'agent traitant[8]. La BCED peut éventuellement vous accompagner lors de cette étape pour s'assurer que la prise de trace dans votre applicatif est fonctionnelle.

Le SPF BOSA a d'ailleurs défini ce principe avec les notions de « Privacy audit trail » et de « Circle of trust ». Sur leur site internet, [9]on peut d'ailleurs trouver la représentation suivante :

[7] Il s'agit du principe en vertu duquel on ne peut traiter que des données personnelles adéquates, pertinentes et non excessives au vu de la finalité pour laquelle elles ont été obtenues. (Source : Autorité de protection des données, 19-11-24.)

[8] Le service TRACES que l'on peut proposait précédemment a en effet été décommissionné. Cela résulte d'une volonté de responsabiliser les consommateurs sur la prise de traces également à leur niveau.

[9] https://dtservices.bosa.be/fr/faq/07-generalites-quest-ce-quun-privacy-audit-trail-et-quelle-est-la-part-de-responsabilite-de-mon



2.2.3. Rôles et responsabilités des différents acteurs :

Nous avons brièvement évoqué le fait que les traces devaient servir à répondre aux questions « QUI/QUOI/QUAND/POURQUOI ».

Dans le tableau ci-dessous, nous indiquons en détail ce que chaque acteur doit être en mesure de fournir pour pouvoir répondre à chacune de ces questions.

	QUI	QUOI	QUAND	POURQUOI
Consommateur (Vous)	Agent traitant ou responsable de traitement (la personne, pas juste un identifiant qui pourrait disparaître en 10 ans)	Service et opérations appelées Identification de la donnée accédée	Date et heure de l'appel	Justification de la consultation particulière en lien avec un dossier ou un traitement
Intégrateur(s) (La BCED)	Application appelante et organisation autorisée	Service et opérations appelées Identification de la donnée accédée	Date et heure de l'appel	Contexte légal
Source Authentique (RN, BCE, DIV, …)	Intégrateur ou application appelante	Service et opérations appelées Identification de la donnée accédée	Date et heure de l'appel	

2.2.4. Cas spécifique : prise de trace via BCED-WI

La BCED dispose de sa propre interface web, BCED-WI, permettant de consulter des données provenant de sources authentiques[10], essentiellement destinée aux utilisateurs ne disposant pas d'un applicatif métier.

Dans ce contexte, en tant que consommateur, vous ne devez pas mettre en œuvre un mécanisme de prise de traces : la BCED s'en charge pour vous.

2.2.5. Quelques caractéristiques des traces

Les traces légales doivent répondre à certaines caractéristiques précises qui vous sont présentées et explicitées dans le tableau ci-dessous. Étant donné que vous devez gérer vous-mêmes la prise de trace à votre niveau, il est important de bien intégrer ces notions :

Caractéristiques	Définition
Une trace doit être proportionnelle	Définie au point précédent, cette caractéristique signifie que la prise de trace par un acteur de la chaine ne doit stocker que les informations essentielles à son rôle et ses responsabilités
Une trace doit être inaltérable	Une trace ne peut être ni effacée ni modifiée ou un appel ne peut pas être dissimulé
Une trace doit être confidentielle	L'accès doit être restreint et tout accès aux traces doit être stocké

2.2.6. L'accompagnement de la BCED dans la prise de traces

La BCED peut vous accompagner pour la rédaction des cas de test et déterminer ce que doit contenir les traces au minimum. De manière plus globale, la BCED vous accompagne à chaque étape de votre projet d'échanges de données : depuis la détermination du besoin jusqu'à la consultation des données en passant par l'autorisation de la source authentique.

[10] https://labced.be/home/nos-expertises/change-et-acces-aux-donnees/bced-wi.html

3. Le processus des inscriptions

3.1. Définition générale

Le concept « d'inscription » est utilisé pour matérialiser le fait qu'une administration possède ou a possédé un dossier sur une personne physique dans le cadre d'une finalité particulière et qu'une récupération d'informations peut avoir lieu au travers des services de la BCED.

Cette inscription est nécessaire pour :

- Contrôler la conformité des accès aux principes du RGPD : l'inscription est un préalable à la consultation de données à caractère personnel pour une finalité particulière[11].On ne peut en effet consulter les données d'une personne que si cela est justifié au regard de l'autorisation obtenue [12].

- L'information du citoyen[13] : l'inscription permet d'apporter une meilleure information au citoyen sur les administrations qui possèdent des données le concernant (actuellement seuls les dossiers faisant appel à une récupération de données à caractère personnel via la BCED sont soumis aux inscriptions).

En premier lieu, il s'agit de définir une période comprenant une date de début et une date de fin. Le respect de la proportionnalité en matière de traitement de données à caractère personnel impose qu'on consulte les données uniquement durant la durée de traitement du dossier. Donc, la durée de l'inscription doit être identique à la durée de traitement du dossier. En effet, lorsque le dossier d'une personne est clôturé, l'administration n'a plus de raison légale de consulter ses données ni de recevoir ses mutations[14]. C'est donc à vous de veiller à définir la durée de l'inscription en s'assurant que celle-ci n'excède pas la durée de traitement.

Ensuite, dans le cadre des inscriptions, le concept de dossier se rapporte au dossier administratif ouvert concernant le sujet. Il s'agit uniquement d'un élément interne au métier qui permet au responsable de traitement d'ajouter toute information utile qui lui faciliterait ses recherches en cas d'enquête vis-à-vis des consultations réalisées par son service concernant une personne particulière. Les données du dossier (au-delà du NRN/NISS) n'ont donc de signification que pour le métier qui les a créées (pas pour les intégrateurs de service ou le fournisseur). Une inscription est dès lors sensée avoir une relation 1-1 avec le dossier (1 inscription pour 1 dossier spécifique).

---

[11] Attention toutefois que ce contrôle ne peut être opéré que si le NISS (ou l'identifiant du sujet) est fourni en requête.
[12] Voir l'article 5 du RGPD qui énonce les principes de bases : licéité, finalité déterminée, minimisation des données, données exactes et à jour et enfin limitation de la durée.
[13] Art. 12 et suivants du RGPD
[14] Une mutation est une modification d'une donnée dans une source authentique (ex : changement d'adresse). La réception des mutations permet d'avoir une base de données à jour et d'être informé d'un type de changement permettant le déclenchement d'un traitement métier. Les mutations sont générées et communiquées quotidiennement par la SA au travers de la BCED. La demande de réception de mutations est liée à un (ou plusieurs) contexte légal spécifique. Une administration demande donc à obtenir les mutations sur base des personnes inscrites sous un certain contexte légal. (Source : Glossaire BCED). L'obtention des mutations doit faire l'objet d'une demande spécifique auprès de la SA.

3.2. Cycle de vie des inscriptions

Cette section présentera les quatre opérations du service inscription, formant en quelque sorte le « cycle de vie » des inscriptions.
Ensuite, il s'agira d'évoquer également les mutations de données et leurs interactions avec les inscriptions.

3.2.1. Les 4 opérations

Le processus des inscriptions s'articule autour de quatre opérations. Le tableau ci-dessous les présente avec une brève explication. Elles seront davantage développées plus loin dans le document.

Opération	Explication
Publish Inscription	- Déclare un nouveau dossier pour un identifiant n'ayant pas encore d'inscription non annulée. - Date de fin optionnelle ()
Extend Inscription	- Etend la date de début d'inscription dans le passé - Etend la date de fin d'inscription dans le futur
Close Inscription	- Met la date de fin d'inscription à « maintenant »
Cancel Inscription	- Annule une inscription qui serait effectuée par erreur. - Ceci doit constituer une exception[15]

Il est important de mentionner qu'aucune inscription n'est effacée. Qu'elle soit clôturée ou annulée, elle reste existante dans nos systèmes.

3.2.2. Les mutations

Une mutation consiste en une modification d'une donnée dans une source authentique (ex : changement d'adresse). La réception des mutations permet donc d'avoir une base de données à jour et d'être informé d'un type de changement permettant le déclenchement d'un traitement métier. Les mutations sont générées et communiquées quotidiennement par la source authentique au travers de la BCED. La demande de réception de mutations est liée à un (ou plusieurs) contexte légal spécifique. Ce lien entre inscription et mutation vous permet de recevoir les mutations uniquement pour la durée de traitement du dossier. **Autrement dit, il est interdit de recevoir des mutations en dehors d'une période d'inscription.**

[15] En effet, l'opération cancel est uniquement prévue pour annuler en cas d'erreur. Il ne s'agit pas de publier une inscription, consulter puis annuler.

3.3. Processus d'inscription

3.3.1. Principes de base

Le processus d'inscription n'est pas spécialement complexe mais il faut veiller à respecter certains principes lorsque vous procédez à l'inscription.

1. Avant d'appeler un service qui traite des données à caractère personnel, le consommateur doit procéder, via son application, à une inscription préalable. Si cela n'est pas fait, la consultation sera refusée[16].
2. Vous devrez également prévoir, dans votre processus, de clôturer les dossiers. La durée de l'inscription doit aller de pair avec le temps de traitement moyen d'un dossier. Par exemple, si un dossier de bourse d'études est systématiquement clôturé en fin d'année scolaire, la durée de l'inscription ne pourra être démesurément plus longue qu'un an.

➔ **Il s'agit d'une obligation basée sur le principe de minimisation de la durée[17].**

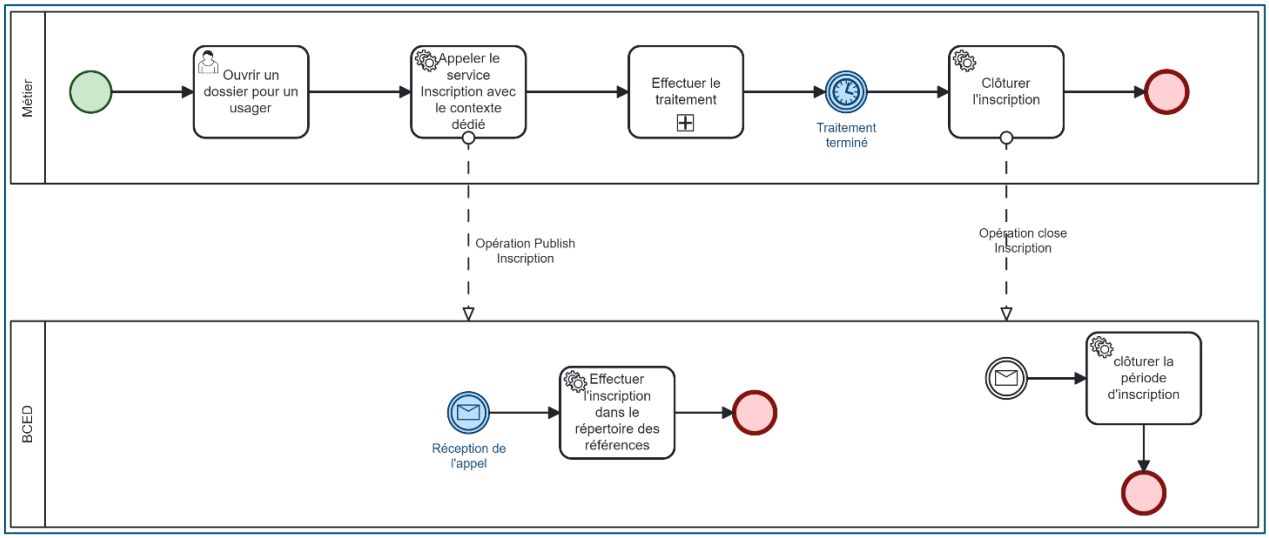
3. Si un dossier dure plus longtemps que ce qui est prévu (par exemple, toujours dans un contexte scolaire ; en cas de recours), il est possible d'étendre l'inscription (=allonger la durée) via l'opération *extendInscription*. Précisons que l'extension peut être effectuée sur un dossier clôturé ou expiré, par exemple dans le cadre d'une réouverture.
4. Si le traitement métier est terminé avant la fin de la période d'inscription vous devrez obligatoirement clôturer proactivement l'inscription au moment où le dossier est clôturé via l'opération *closeInscription*. Il ne s'agit donc pas « d'attendre » la date de fin définie en amont.

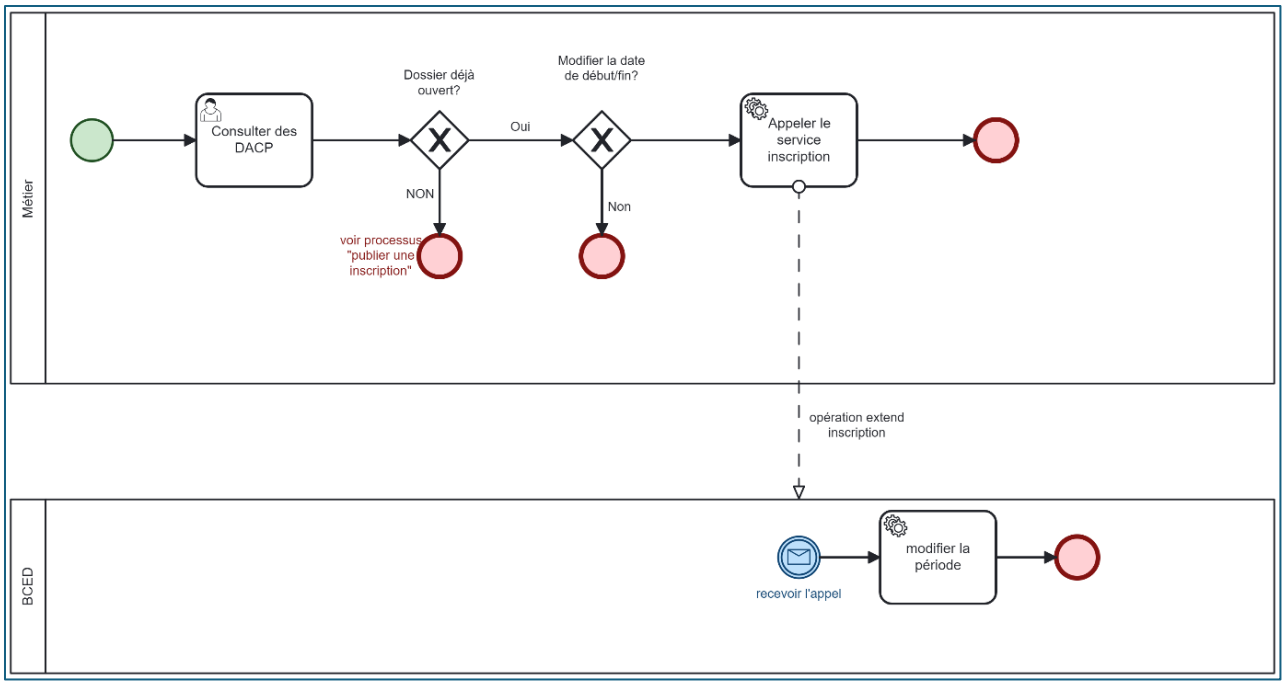
[16] À note que l'appel de certaines opérations offertes par certains web services ne nécessite pas d'inscription préalable. Par exemple, lorsqu'une recherche phonétique est effectuée pour retrouver le NISS d'une personne, l'administration va cibler son action non pas sur l'ensemble des NISS mais bien sur la personne souhaitée.
[17] Art. 5, 1, c) et e) du RGPD

3.3.2. Publier, étendre et clôturer une inscription

3.3.2.1.1 PUBLIER UNE INSCRIPTION

Le diagramme ci-dessous résume le processus de prise d'une inscription.

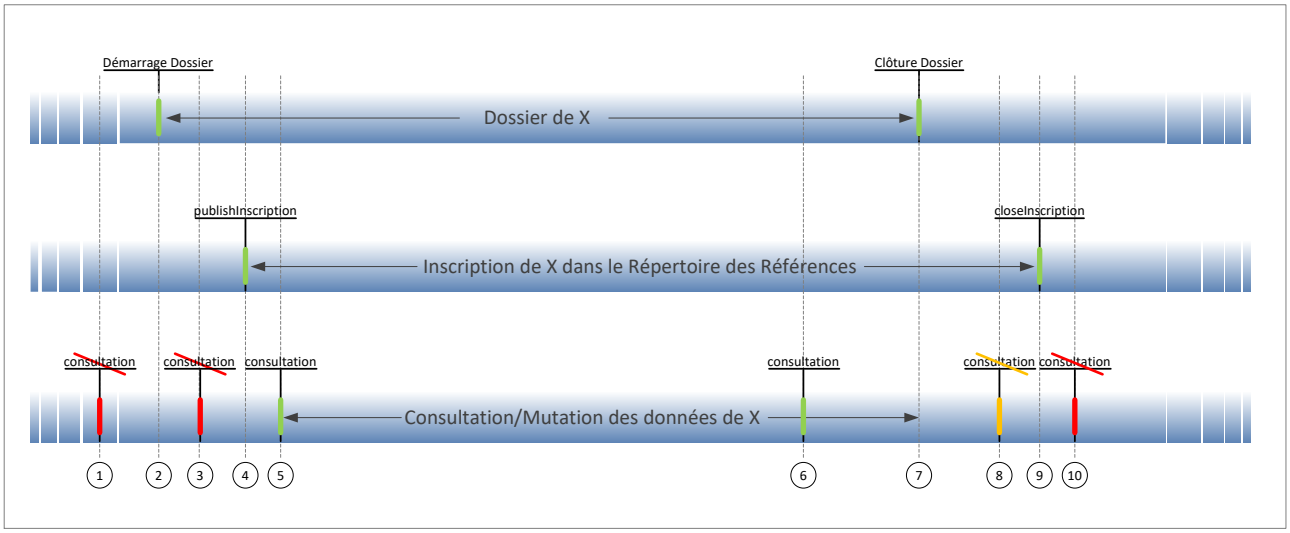




Commentaires :

1. Un usager va effectuer une requête dans le dossier d'un citoyen. Cette requête via son applicatif métier traite de DACP.
2. L'applicatif va publier une inscription (via l'opération « publish_inscription ») dans le répertoire des références. Ensuite, il s'agira d'appeler le webservice correspondant.
3. La BCED intègrera l'inscription dans le répertoire des références.
4. La BCED relayera l'appel à la SA pour génération de la réponse.

En cas de souscription aux mutations, le processus est identique.
Le schéma ci-dessous présente une autre vue, plus détaillée, de la durée de vie d'un dossier et d'une inscription.



Commentaires :

1. La consultation a lieu avant la période d'inscription, elle est refusée car impossible.
2. Une administration a ouvert un dossier[18] pour X et a défini une période correspondant à la durée de traitement.[19].
3. Tant que l'inscription n'est pas effective, la consultation de DACP pour X n'est pas possible. Bien que le dossier soit ouvert côté métier, l'inscription n'étant pas faite à la BCED on ne peut pas consulter les données au travers de nos services.
4. L'inscription est créée au travers d'un appel au service inscription via l'opération *publish_inscription*.
5. Les données peuvent être consultées.
6. La consultation des données est toujours possible, malgré le long délai avec l'étape 5 car nous sommes encore dans la période de « durée de vie » définie du dossier.
7. L'administration a terminé de traiter le dossier, elle le clôture.

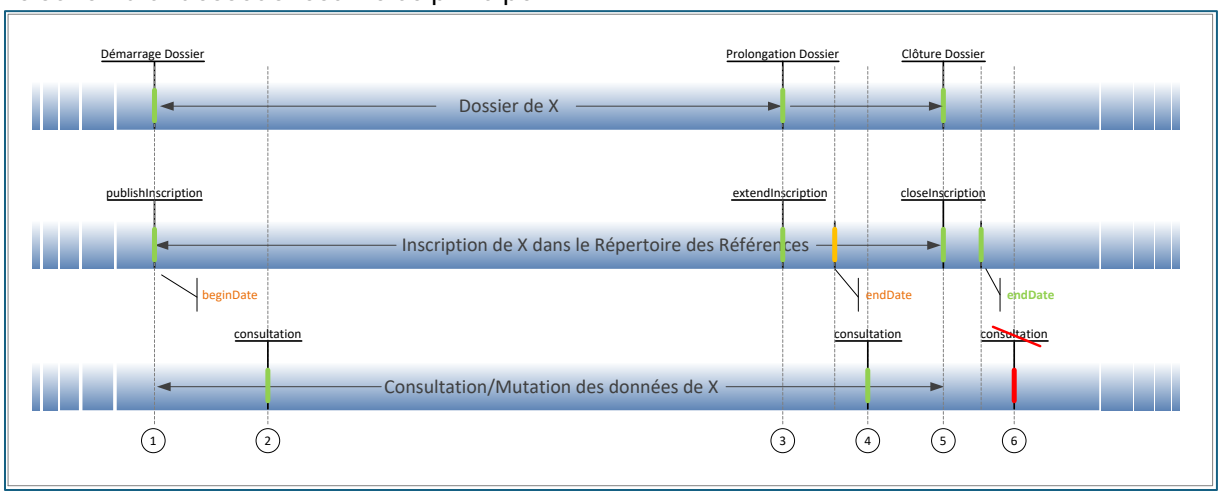
[18] La notion de dossier est à considérer au sens large. Il peut s'agir en effet d'un dossier dans un applicatif (BO) ou bien un dossier papier, un fichier Excel, ...
[19] Voir page11, avec la définition de l'inscription. La durée de l'inscription est du ressort du métier qui doit la déterminer en tenant compte de la durée de traitement.

8. La consultation est encore possible techniquement (car l'inscription n'est pas encore clôturée) mais ne devrait plus l'être car le traitement est terminé.
9. L'inscription est clôturée via l'appel au service inscription (opération *close_inscription :).*
10. La consultation n'est plus possible car l'inscription est clôturée.

3.3.2.1.2 ÉTENDRE UNE INSCRIPTION

Comme nous l'avons vu, si le traitement du dossier devait prendre plus de temps que prévu, il est possible d'étendre la durée de l'inscription. En effet, pour rappel, la durée de l'inscription est déterminée en amont et doit en principe, correspondre à la durée de traitement moyen. Si celle-ci est plus longue qu'estimée, l'appel au service inscription doit être effectué (opération extendInscription) pour « prolonger » la durée de vie du dossier et permettre de continuer à consulter les DACP.

Le schéma ci-dessous résume ce principe :



Commentaires :

1. Les étapes 1 et 2 sont identiques à la section précédente.
2. L'étape 3 matérialise la prolongation du dossier via l'opération *extend*.
3. Une nouvelle date de fin est dès lors définie permettant de consulter les données pour une période plus longue (étape 4)
4. Lorsque le traitement est terminé, l'inscription est également clôturée (étape 5).
5. La consultation n'est plus possible en raison de la clôture du dossier et de l'inscription (étape 6).

3.3.2.1.3 CLÔTURER UNE INSCRIPTION

Comme évoqué précédemment, la clôture d'une inscription est obligatoire : Le RGPD impose en effet le principe de n'avoir recours aux données que pour la stricte durée de traitement[20].

Par conséquent, outre cet élément, dès lors que la durée de traitement est plus courte que celle définie en amont, l'inscription doit également être clôturée. Il n'est en effet pas légal de

[20] Art.5, 1, c) et e) du RGPD

pouvoir consulter des données ou recevoir des mutations pour un dossier dont le traitement est terminé.

3.3.2.1.4 ANNULER UNE INSCRIPTION

Une opération spécifique (*cancel)* permet d'annuler une inscription réalisée. Il convient d'être particulièrement prudent quant à celle-ci. En effet, l'annulation ne peut avoir lieu uniquement lorsqu'il s'agit d'une erreur. Par exemple, une inscription réalisée dans un mauvais dossier dont on n'a pas besoin de consulter les données. Cette opération est et doit donc rester une exception. Rappelons cependant que même si l'inscription est annulée, celle-ci ne sera pas effacée pour autant : la BCED stockera en effet l'information dans ses systèmes.

4. Conclusion

On l'aura compris : consulter des données provenant de source authentique ne se fait pas « n'importe comment ». Des règles strictes sont d'application et le non-respect de celles-ci peut entrainer des sanctions tant au niveau du responsable de traitement qu'au niveau de l'agent.

Parmi ces exigences, les notions d'inscriptions et de traces constituent le fondement afin de pouvoir toujours vérifier et le cas échéant, justifier la consultation de données à caractère personnel.

En tant que consommateur de données, vous êtes un maillon essentiel de la chaine et il est de votre responsabilité de mettre en œuvre les mécanismes explicités dans le présent document.

La BCED est à votre disposition pour vous guider et vous accompagner à chaque étape du processus.

081/40.98.10

support@labced.be

https://labced.be