MARCEAU AVOCATS
Avocats au Barreau de Paris

AmbiCio
L'AMBITION CENTRÉE CLIENT

L'anonymisation, un moyen d'alléger les obligations liées au RGPD

Sous-traitance - Projet - Archivage

Avis d'un avocat spécialisé et d'un expert en système d'information

Marceau Avocats
71 avenue Marceau
75016 PARIS
www.marceau-avocats.com

AmbiCio
67 Av. André Morizet
92100 Boulogne-Billancourt
www.ambicio.fr

Sommaire

1. Un point sur l'actualité
2. Pourquoi anonymiser ?
3. Comment anonymiser?
4. Quand anonymiser ? 3 cas pratiques
    1. Cas pratique 1: Faire appel à un sous-traitant
    2. Cas pratique 2: Conserver mes données à des fins statistiques
    3. Cas pratique 3: Environnements études et projets

Copyright 2018

CNIL.

1. Un point sur l'actualité

- **7 millions** de visites sur le site de la CNIL
- **130 000** téléchargements de l'outil PIA
- **1000** notifications de violations, soit 7/jour
- **9700** plaintes contre 7200 en 2017
- **345** plaintes transfrontalières

2. Pourquoi anonymiser?

Échapper à l'application de la règlementation sur les données à caractère personnel

Considérant 26 du RGPD

Attention: d'autres règlementations peuvent s'appliquer!

3. Comment anonymiser?

3.1 Les clés d'une anonymisation réussie (1/2)

- Pas de définition de l'anonymisation
- Traitement de données à caractère personnel dans le but d'empêcher **irréversiblement** l'identification de la personne concernée.
- Importance des **éléments contextuels**: prendre en compte l'ensemble des moyens susceptibles d'être raisonnablement utilisés à des fins d'identification par le responsable du traitement ou par un tiers. (coût, technologies disponibles, temps nécessaire…)

  Quel risque de réidentification ? Réévaluer la fiabilité de la technique régulièrement.

- Approche différente en droit français
- Sources: Considérant 26 du RGPD; Avis du G29

Copyright 2018

3.1 Les clés d'une anonymisation réussie (2/2)

- Pas de techniques reconnues comme « valables »
- Lignes directrices du G29
- Prendre en compte 3 types de risques:
  - INDIVIDUALISATION: La possibilité d'isoler un individu dans un ensemble de données
  - CORRELATION: la possibilité de relier entre eux deux enregistrements
  - INFERENCE: possibilité de déduire des informations de l'ensemble des données.

Copyright 2018

3.2 Pseudonymiser ses données ne suffit pas

- Remplacer une donnée (généralement unique / directement identifiante) par un pseudonyme, un code propre à chaque individu.

- Exemples:
  - Choix d'un pseudonyme et génération d'une table de correspondance
  - Chiffrement
  - Hachage?

- Les personnes peuvent toujours être identifiées indirectement. Exemple: AOL, 2006

Copyright 2018

Des précisions s'imposent…

MARCEAU AVOCATS
Avocats au Barreau de Paris

AmbiCio

François → Hachage → b3140f50db8520403a6e38adf50648

b3140f50db8520403a6e38adf50648 → ✗

Obsolètes

- MD5
- SHA-1
- SHA-2 de 128bits

Conseillés

- ✓ SHA-2 > 256bits
- ✓ SHA-3

François5d4D → Hachage → f38f69672045f2a56b658b683280

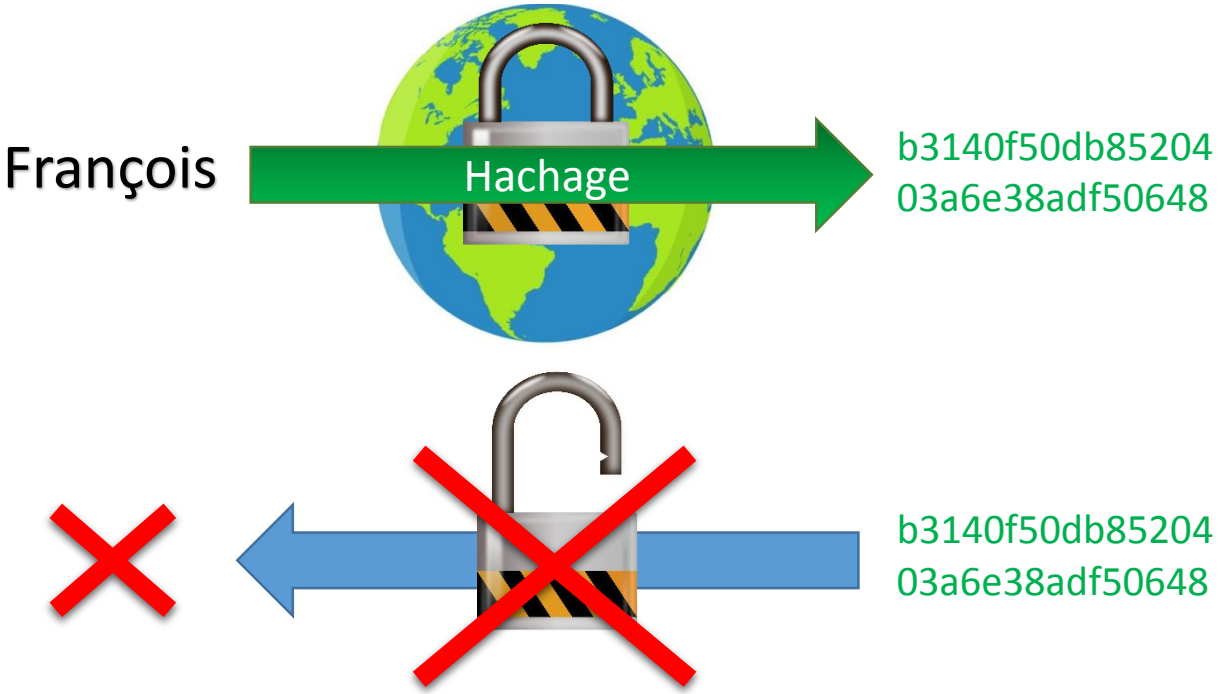
f38f69672045f2a56b658b683280 → ✗

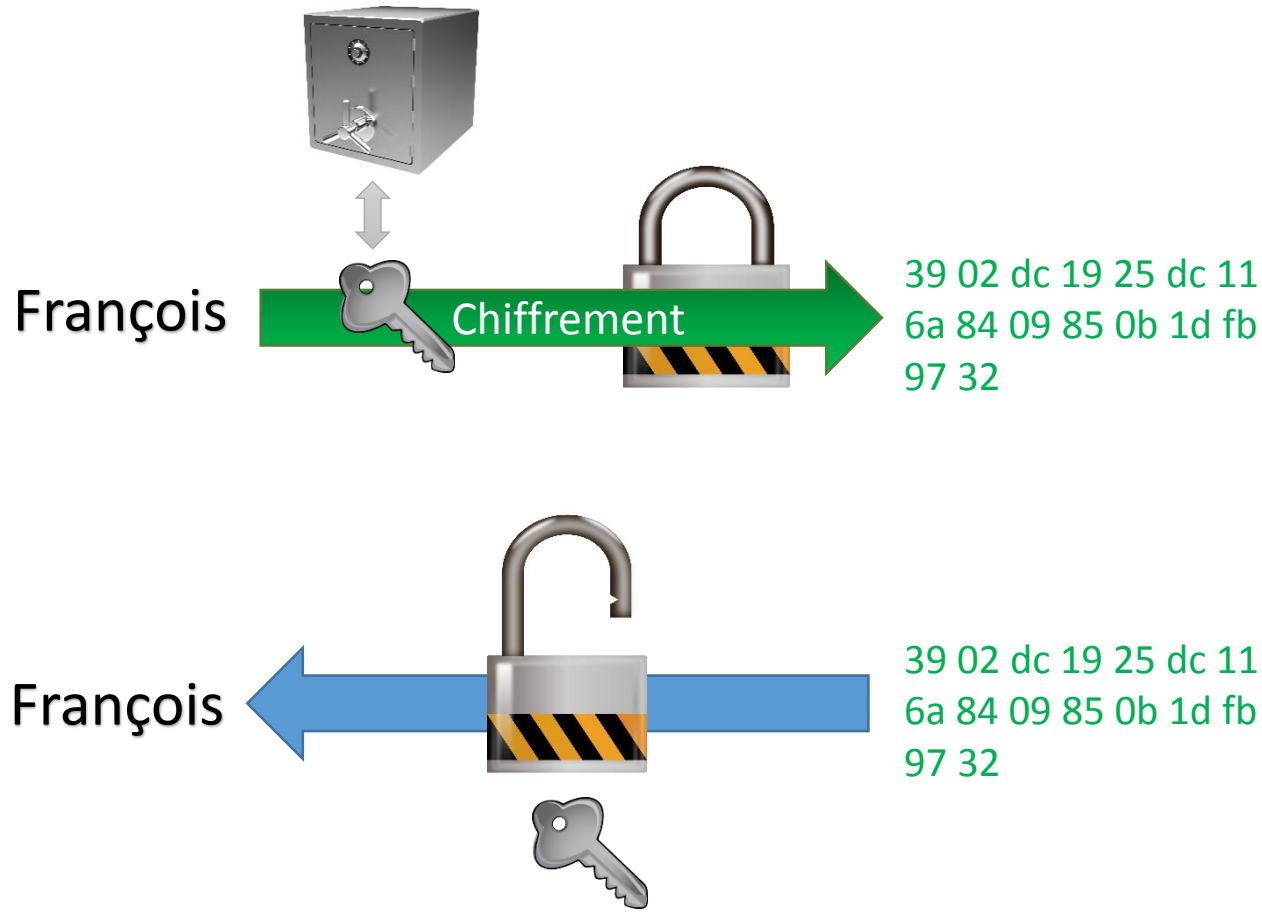
Les modalités de salage doivent être validées et protégées.

Des précisions s'imposent…

MARCEAU AVOCATS
Avocats au Barreau de Paris

AmbiCio





Obsolètes

- MD5
- SHA-1
- SHA-2 de 128bits

Conseillés

- ✓ SHA-2 > 256bits
- ✓ SHA-3

Obsolètes

- 3DES

Conseillés

- ✓ AES
- ✓ RSA

3.3 Les procédés d'anonymisation

La randomisation

Ajout de bruit

- Diminuer la précision des données en ajustant leurs valeurs selon une fourchette pertinente
- Taille, âge, montants…

Permutation

- Mélange des données entre les enregistrements
- Adresse,

Confidentialité différentielle

- Notion de confidentialité applicable aux bases statistiques

La généralisation

Agrégation/dilution de l'information

- Plusieurs enregistrements sont agrégés
- Par tranche d'âge, par segment,…
  - k-anonymisation
  - l-diversité
  - t-proximité

❖ **Exploitation de métadonnées**

La revue du besoin

Copyright 2018

Nom : **LeChasseur**
Prénom : **François**
Pseudo : **Lecha123**
Date de naissance : **05/08/1978**
Age : **40 ans**
ID : **0001 176 34**

Mail : **f.lechasseur@live.fr**
Num. Port : **06 54 12 78 21**
Num. Fix : **04 73 65 05 10**

N° & Rue : **1 place du panthéon**
CP : **63 240**
Ville : **Le Mont-Dore**
Pays : **France**

Relevé d'Identité Bancaire

IBAN
➢ **FR76 3043 8001 0026 0050 4289 541**
BIC
➢ **AMBCFR21XXX**
Dom
➢ **BNPPARIBAS PARIS HAUSSMANN**

Num : 4970 1012 3458 7890
Exp. : 12/18
CVV : 296

Exemple - Avant

Nom : **LuhasCseser**
Prénom : **François**
Pseudo : **3a1Lceh2**
Date de naissance : **05/08/1978**
Age : **40 ans**
ID : **0001 176 34**

Mail : **f.luhascseser@live.fr**
Num. Port : **06 76 89 32 43**
Num. Fix : **04 54 12 67 09**

N° & Rue : **5 rue Pasteur**
CP : **63 240**
Ville : **Le Mont-Dore**
Pays : **France**

Relevé d'Identité Bancaire

IBAN
➢ **FR23 8734 2398 2367 0080 7643 317**
BIC
➢ **MLSCFR34TRE**
Dom
➢ **BNPPARIBAS PARIS HAUSSMANN**

Num : 8723 2843 3458 7890
Exp. : 12/18
CVV : 789

Exemple - Après

Copyright 2018

3.4 Comparatif - Délibérations de la CNIL

2 exemples de collectes d'adresses MAC pour mesurer l'efficacité de campagnes publicitaires

Projet JCDecaux à la Défense

Délibération 2015-255 – CE 8 février 2017

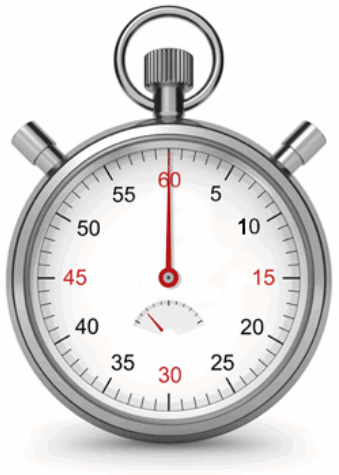
- Technique
  - Hachage + salage avec sel propre à JC Decaux
  - Possibilité de réidentification
- Finalité
  - Compter le nombre de personnes + le nombre de fois où une même personne repasse sur l'esplanade + déterminer les parcours susceptibles d'être réalisés d'un mobilier publicitaire à un autre
  - les objectifs mêmes de la collecte des données par la société JCDecaux France étaient incompatibles avec une anonymisation des informations recueillies. CORRELATION et INFERENCE

Projet Retency à la gare de Dijon

Délibération 2017-145

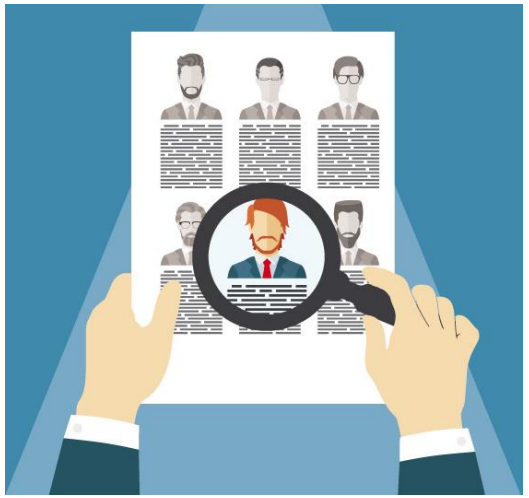
- Technique
  - Hachage + sels renouvelés tous les 15 jours
  - Aucun accès possible aux données collectées via les boitiers
  - Aucune possibilité de réidentification
- Finalité
  - Comptage du nombre de personnes, sans pour autant qu'un parcours individuel ne puisse être établi

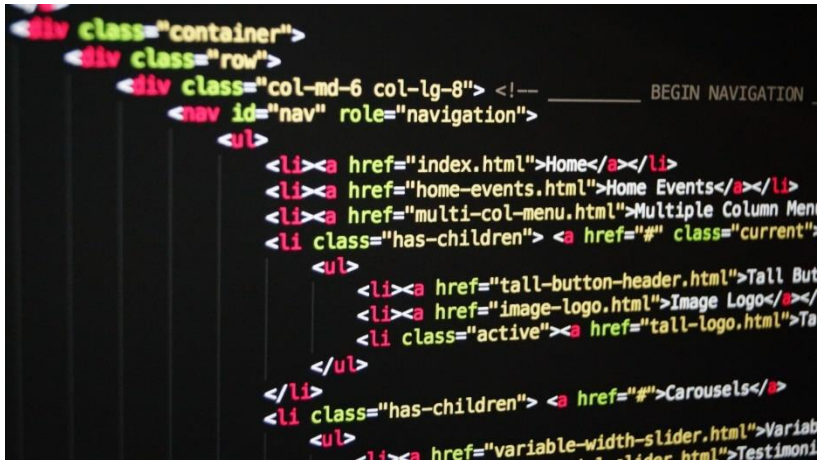
Copyright 2018



4. Quand anonymiser ?

4.1 Faire appel à un sous-traitant (1/3)





Copyright 2018

4.1 Faire appel à un sous-traitant (2/3)

Sans anonymiser

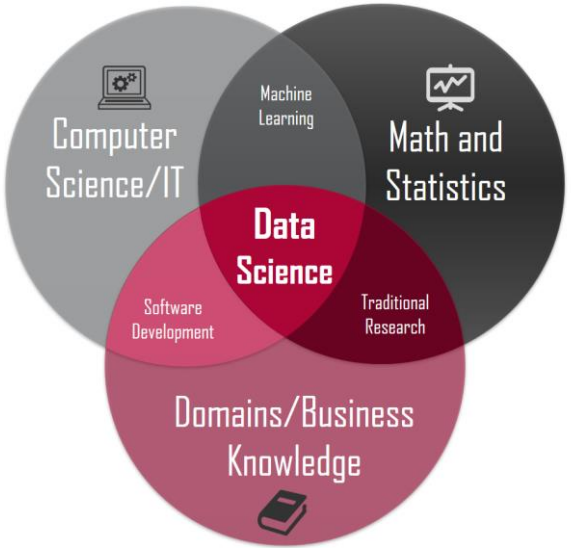
- Contrat de sous-traitance avec les mentions obligatoires de l'article 28 RGPD
- Informations des personnes
- Transferts hors UE règlementés
- Recenser les caractéristiques du traitement sous-traité dans un registre
- Mesures de sécurité à adopter (exemple: pseudoynmisation)

En anonymisant

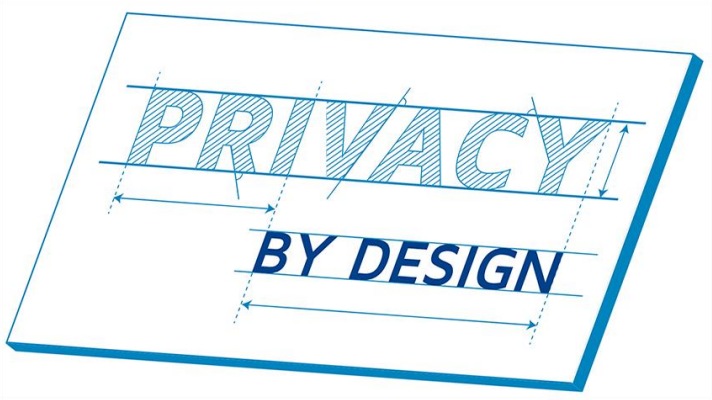
- Hors champs RGPD, mais attention aux règlementations spécifiques
- Réévaluer régulièrement la fiabilité de la technique d'anonymisation

Copyright 2018

4.1 Faire appel à un sous-traitant (3/3)



Ne pas oublier la sécurisation des transferts de données



Copyright 2018

4.2 Cas pratique 2: conserver mes données à des fins statistiques

Rappel sur les durées de conservation

Les données à caractère personnel doivent être conservées « *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ». (article 5 RGPD)

A prendre aussi en compte:

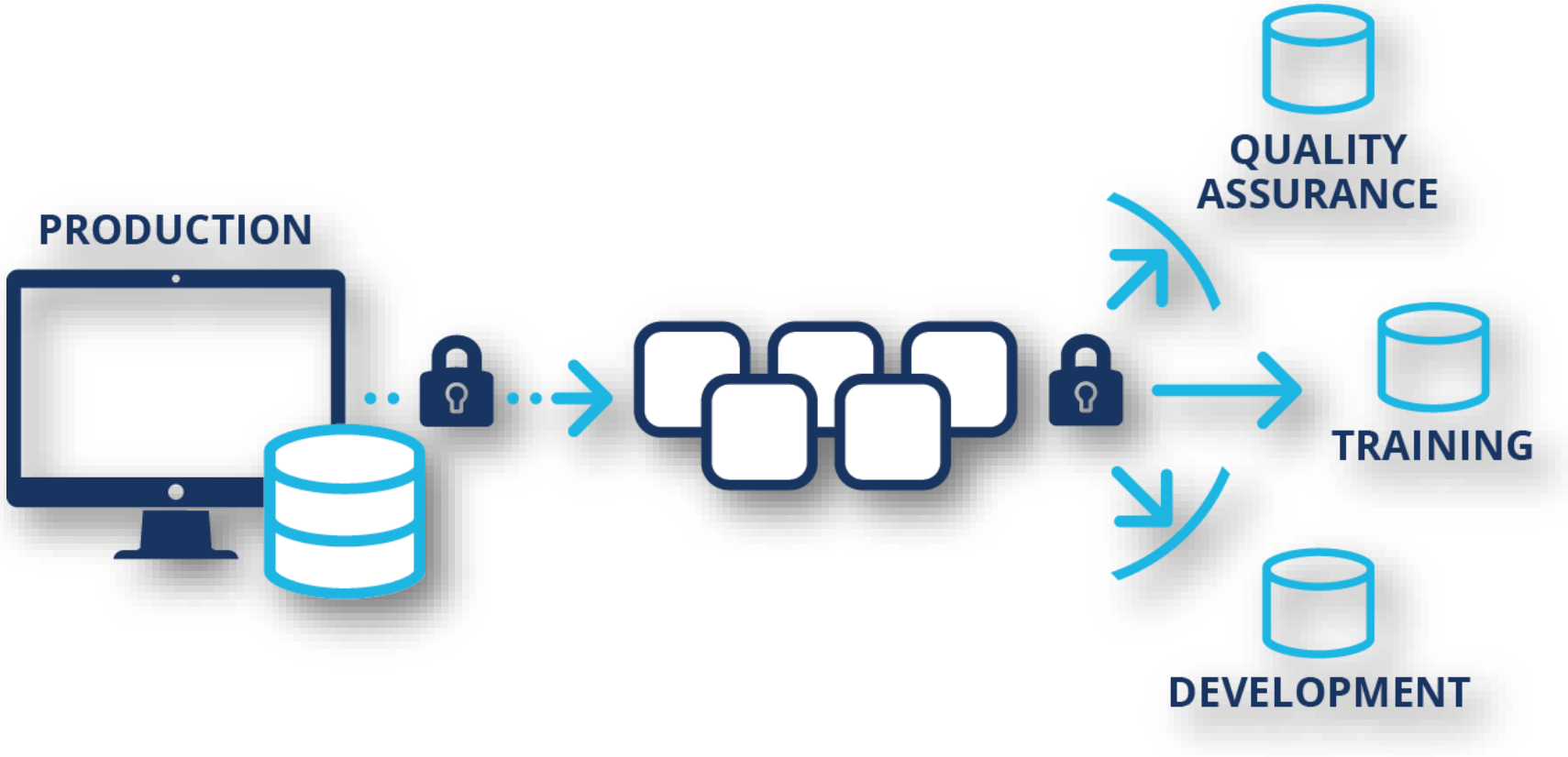
- la durée de prescription applicable.
- Les durées de conservation obligatoires. Exemple, factures: 10 ans (Article L.123-22 du Code de commerce)

Quelques bonnes pratiques:

- Candidat à un emploi non retenu: 2 ans à compter du dernier contact (bonne pratique, Délibération n°02-017 du 21 mars 2002)
- Salarié: pendant la période d'emploi + prescription
- Données clients à des fins de prospection commerciale: 3 ans à compter de la fin de la relation commerciale (Norme simplifiée NS-048)

Copyright 2018

4.3 Cas pratique 3: Environnements études et projets



Copyright 2018

Conclusion

MARCEAU AVOCATS
Avocats au Barreau de Paris

AmbiCio

Stratégie Conseillée

01 Situation

Analyser le contexte juridique (acteurs, licéité)

02 Risques

Etudier les risques et au besoin, réaliser un PIA

03 Stratégie

Définir quelle stratégie à adopter pour chaque donnée

04 Gouvernance

Adopter une gouvernance Globale en anticipant des failles liées à des combinaisons d'informations.

05 Documentation

Documenter la démarche, garder une trace des opérations réalisées

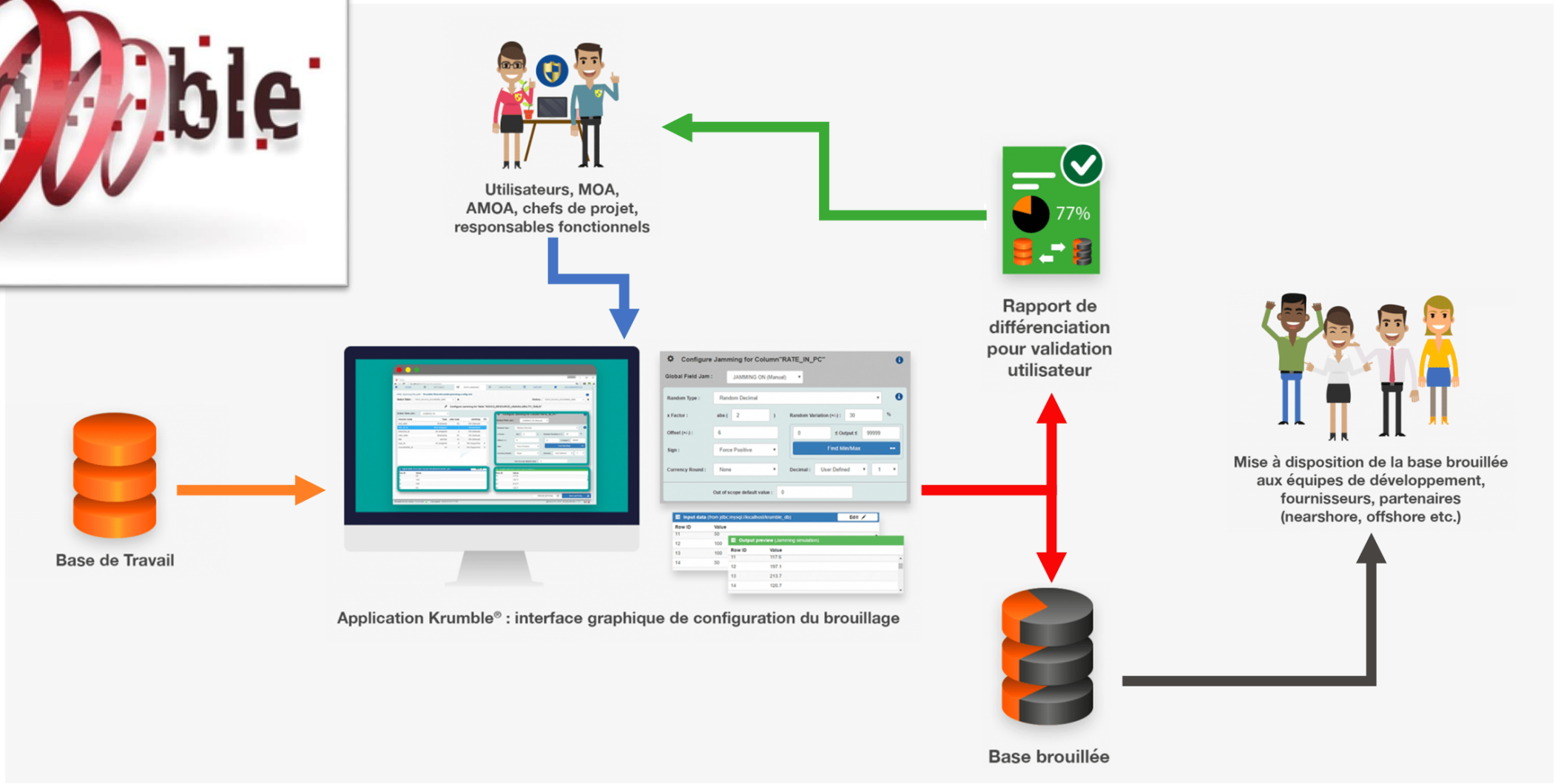
06 Conformité

Contrôler le bon déroulement des opérations (audit qualité).

Copyright 2018

Copyright 2018

Et si nous parlions outil ?



Copyright 2018

Démo

Copyright 2018

3.3 Exemple - Avant

Nom : **LeChasseur**
Prénom : **François**
Pseudo : **Lecha123**
Date de naissance : **05/08/1978**
Age : **40 ans**
ID **: 0001 176 34**

Mail : **f.lechasseur@live.fr**
Num. Port : **06 54 12 78 21**
Num. Fix : **04 73 65 05 10**

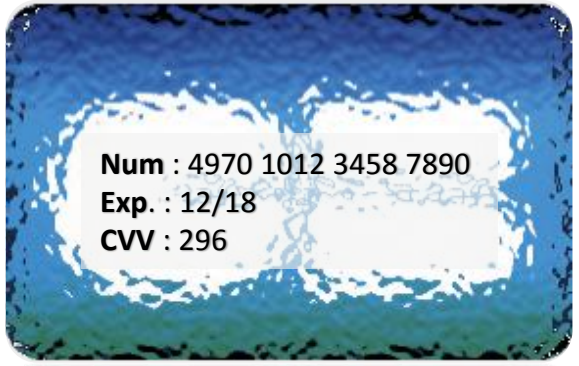
N° & Rue : **1 place du panthéon**
CP : **63 240**
Ville : **Le Mont-Dore**
Pays : **France**

Relevé d'Identité Bancaire

IBAN
- **FR76 3043 8001 0026 0050 4289 541**

BIC
- **AMBCFR21XXX**

Dom
- **BNPPARIBAS PARIS HAUSSMANN**



Le 20/11/18
à 17h

Le 12/10/18
à 17h

3.3 Exemple - Après

Nom : **LuhasCseser**
Prénom : **François**
Pseudo : **3a1Lceh2**
Date de naissance : **05/08/1978**
Age : **40 ans**
ID **: 0001 176 34**

Mail : **f.luhascseser@live.fr**
Num. Port : **06 76 89 32 43**
Num. Fix : **04 54 12 67 09**

N° & Rue : **5 rue Pasteur**
CP : **63 240**
Ville : **Le Mont-Dore**
Pays : **France**

Relevé d'Identité Bancaire

IBAN
- **FR23 8734 2398 2367 0080 7643 317**

BIC
- **MLSCFR34TRE**

Dom
- **BNPPARIBAS PARIS HAUSSMANN**

Le 20/11/18
à 17h

Le 12/10/18
à 17h