L’administration numérique

Dématérialisation,

Certificats électroniques,

R.G.P.D.

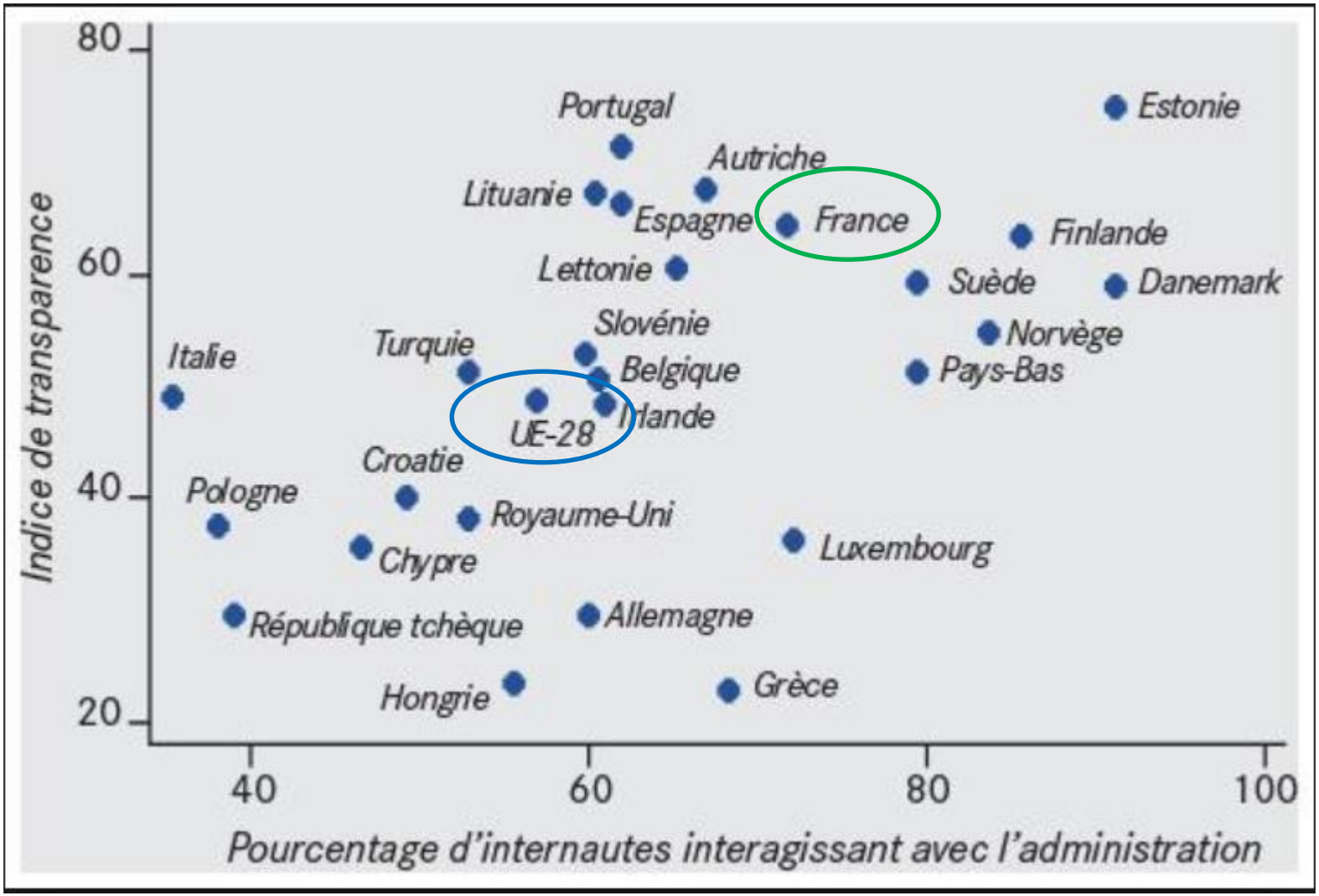
Sommaire

- La dématérialisation
  - Contexte général
  - Contexte de la dématérialisation des finances (baromètre)
  - Calendrier de la dématérialisation
  - Focus sur la dématérialisation des marchés publics
- Certificats électroniques
  - Qu'est ce que c'est ?
  - A quoi ça sert
  - L'évolution avec EIDAS
- RGPD
  - Contexte réglementaire
  - LE DPD (DPO)
  - Comment mettre en œuvre ?

L’administration numérique

Contexte général

Où nous situons nous dans l'UE ? (07/2016)



Source Eurostat 2016

L'administration numérique : contexte général

- *Les français attendent un service public renouvelé*
  - *Un service public accessible et plus personnalisé*
    - *Dématérialisation des démarches administratives (encore plus fort chez les jeunes)*
    - *Des démarches intuitives et qui s'adaptent sans cesse*
    - *Mais aussi une présence physique dans les territoires*
  - *Des services publics plus réactifs qui tiennent mieux compte de l'avis des usagers*
    - *Signaler un problème de voirie par Internet*
    - *Evaluer le service rendu*
    - *Attente d'une réactivité forte des pouvoirs publics*
  - *La possibilité de participer à la production du service*
    - *Start up utilisant les données en OPEN DATA*
    - *Covoiturage local...*
    - *Civi techs : engagement dans l'Education, la santé*

L'administration numérique : contexte général

- Orientation de l'Etat : transformer le service public CAP 2022
  - Proposition 3 : « Investir dans le numérique pour offrir un service public augmenté, plus efficient et qui réinvente ses relations avec les usagers »
  - *Programme* « 100 % des procédures en ligne pour les citoyens »

- *Echanges avec les collectivités via :*
  - *Association d'élus, de collectivités, de structures mutualisantes*
  - *DCANT : association des collectivités au développement de l'administration numérique*

- Pour les collectivités locales :
  - Processus inévitables :
    - Intégrer les projets numériques de l'Etat
    - Répondre aux besoins des usagers locaux
    - Se créer une image et identité territoriale numérique

Calendrier de la dématérialisation

- Calendrier de 2016 à 2022
  - Calendrier complet en ligne
    - https://www.cogitis.fr/blog/grands-rendez-de-dematerialisation-communes/
  - Quelques dates :
    - 7 novembre 2016 : Saisine par Voie Electronique (SVE)
    - 25 mai 2018 : entrée en vigueur du RGPD
    - 1er octobre 2018 : dématérialisation des procédures de marchés
    - Novembre 2018 ou novembre 2022 : Dématérialisation des demandes de permis de construire et des Déclarations d'Intention d'Aliéner (DIA).
    - 1er janvier 2019 : transmission électronique pour le Répertoire Electoral Unique (REU)
    - 1er janvier 2020 : facturation électronique pour toutes les entreprises

L’administration numérique : le contexte de la dématérialisation des finances

- Accélération de la dématérialisation des flux comptables
  - Volumes de factures déposées
  - Taux d’utilisation de la dématérialisation par les collectivités
- Démarrage du DUME
- Dématérialisation des marché publics

Dématérialisation des finances : Chorus Pro

(statistiques source DGFIP)

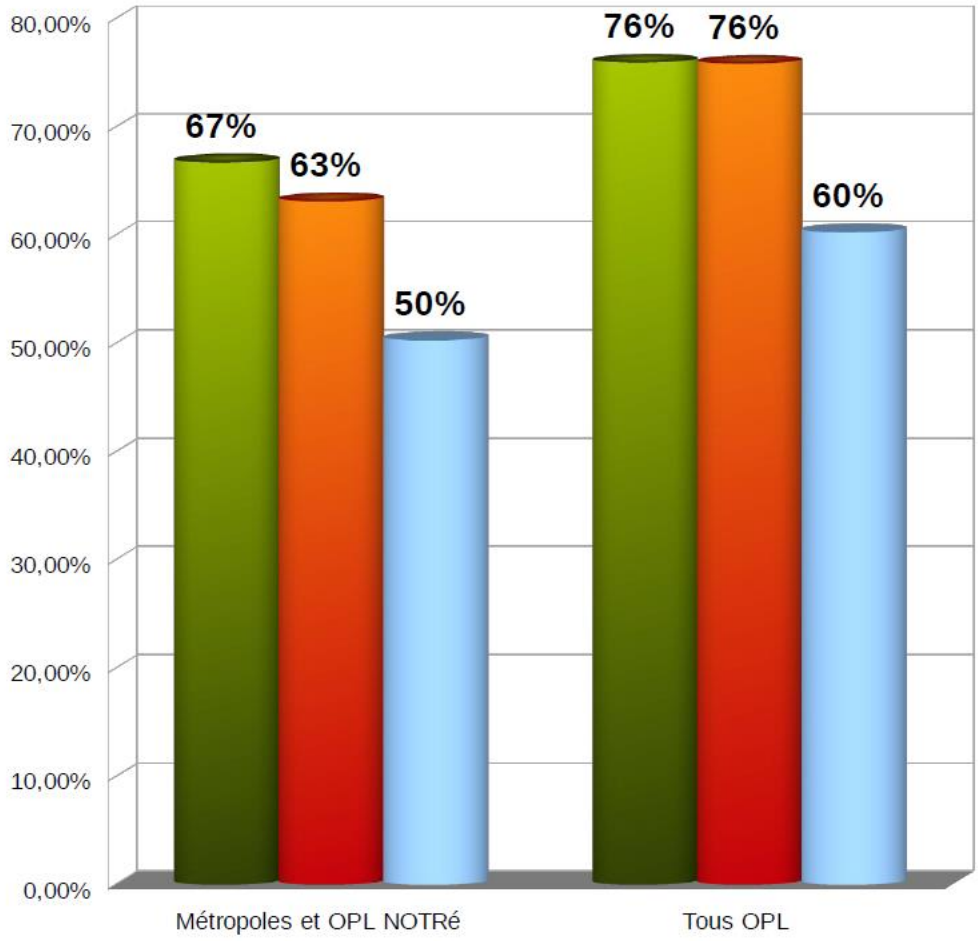
Novembre 2017

- 83 722 structures privées
  - Dont 15 % de grandes entreprises émettent 74 % des factures
- 80 503 entités publiques ont déjà reçu au moins une facture
- 8 millions de factures échangées

Juin 2018

- 200 788 structures privées
  - Dont 7 % de grandes entreprises émettant 47 % des factures et 7 % d'ETI émettant 37 % des factures
- 85 196 entités publiques ont déjà reçu au moins une facture
- Plus de 9 millions de factures échangées en 2018 (et au cumul plus de 20 millions)

Dématérialisation des factures
(source DGFIP)



numérateur : nombre de mandats ayant donné lieu à paiement / nombre de titres ayant donné lieu à encaissement accompagnés de pièces justificatives dématérialisées (ou de liens vers des pièces dématérialisées précédemment transmises) ;

dénominateur : nombre de mandats / de titres ayant donné lieu à paiement ou encaissement

Démarrage du DUME
(source DGFIP)

Les statistiques DUME remontées quotidiennement proviennent :
/ Des profils d'acheteur raccordés au Service DUME (Atline, AWS, Achatpublic.com et Atexo)
/ Du portail web Service DUME de l'AIFE (Utilitaire)

1986 DUME créés

634 Entreprises

489 Acheteurs

1101
DUME A

885
DUME OE

1 591
DUME créés sur l'utilitaire Service DUME

395
DUME créés sur les profils d'acheteurs

*Les statistiques présentées tiennent compte des DUME créés entre le **30/03/18 et le 205/06/18.***

Dématérialisation des marchés publics

- Rappel des dates clés :

  - 1er avril 2018 : Obligation d'accepter le DUME (Document Unique de Marché Européen) par voie électronique (eDUME)

  - 1er Octobre 2018 :
    - Obligation de dématérialisation des procédures de passation de marchés (>= à 25 000 €)
    - Publication des données essentielles
    - Tout marché peut être signé électroniquement

  - 1er janvier 2020 : obligation de signature électronique des marchés

Quelques sites Internet

- REAP (Recensement Economique de l'Achat Public) : permet d'alimenter l'OECP (Observatoire Economique de la Commande Publique).
  - Obligatoire depuis le 1er janvier 2018 pour les marchés > 90 000 €
  - Les marchés notifiés en 2018 pourront être déclarés jusqu'en mars 2019
  - Convergence des données de recensement et des données essentielles prévue en 2022
  - https://www.reap.economie.gouv.fr/reap/servlet/authentificationAcheteur.html
- ETALAB : plate-forme Open Data de l'Etat
  - https://www.data.gouv.fr/fr/
- SERVICE DUME : Création de DUME
  - https://dume.chorus-pro.gouv.fr

LE DUME

- DUME : est une déclaration sur l'honneur harmonisée au niveau européen basée sur un formulaire qui est utilisé dans les procédures de passation des marchés publics, à la fois par les acheteurs publics (pouvoirs adjudicateurs ou entités adjudicatrices) et les opérateurs économiques de l'Union Européenne.

LE DUME

- Le DUME comprend 6 parties :
  - Information sur l'acheteur
  - Sa procédure
  - L'opérateur économique (OE)
  - Les motifs d'exclusion
  - Les critères de sélection
  - La déclaration sur l'honneur de l'OE

- Certaines données peuvent être pré-remplies par l'acheteur

- Remplace le DC1 et DC2

- Possibilité pour l'OE d'éviter des ressaisir à chaque consultation. Modèles de DUME. Récupération des informations connues des autres administrations (attestations sociales et fiscales…)

SERVICE DUME

- SERVICE DUME : service dématérialisé de l'Etat pour la création de DUME, il permet :
  - aux entreprises de prouver de manière simple, et conformément au droit, qu'elles remplissent les critères de sélection d'une offre et n'entrent pas dans un cas prévu par les interdictions de soumissionner.
  - de ne plus avoir à fournir un document lorsque celui-ci a déjà été transmis à une administration, allégeant ainsi la procédure.
  - https://dume.chorus-pro.gouv.fr

DUME et profil acheteur

CHORUS PRO
SERVICE DUME

PLATE-FORME
MARCHÉS

SI ETAT &
ADMINISTRATIONS

Acheteurs publics

Publication

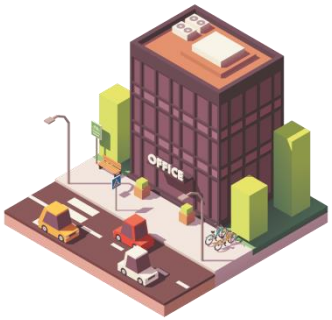
DUME A

Dépôt des plis

DUME

ATTESTATIONS

Fiscales,
Sociales…



Entreprises

Candidature &
réponse

DUME OE

Publication des données essentielles

- A partir du 1er octobre 2018
- Pour les procédures supérieures ou égales à 25 000 €
- Les données essentielles sont définies dans l'arrêté du 14 avril 2017 (modifié par l'arrêté du 2 juillet 2018 (numéro de marché, date de notification, nom de l'acheteur…)
- Elles sont mises à disposition 2 mois après la date de notification sur le profil acheteur
- Elles sont maintenues pendant une durée minimale de 5 ans
- Accessibles gratuitement en consultation et en téléchargement (format JSON et XML)

Le profil acheteur

- Plate-forme de dématérialisation d'achats publics
- Publication électronique des documents de la consultation
- Il Garantit :
  - La confidentialité des candidatures et des offres
  - Assure l'intégrité des données
  - Conformité au Référentiel Général de Sécurité
- Fonctionnalités et exigences minimales définies par l'arrêté du 14 avril 2017
- Nécessité de s'équiper d'un profil acheteur :
  - A l'acte auprès des éditeurs
  - De façon individuelle (fort volume de marchés)
  - Avec d'autres acheteurs auprès de structures publiques mutualisantes

Caractéristiques minimales du profil acheteur

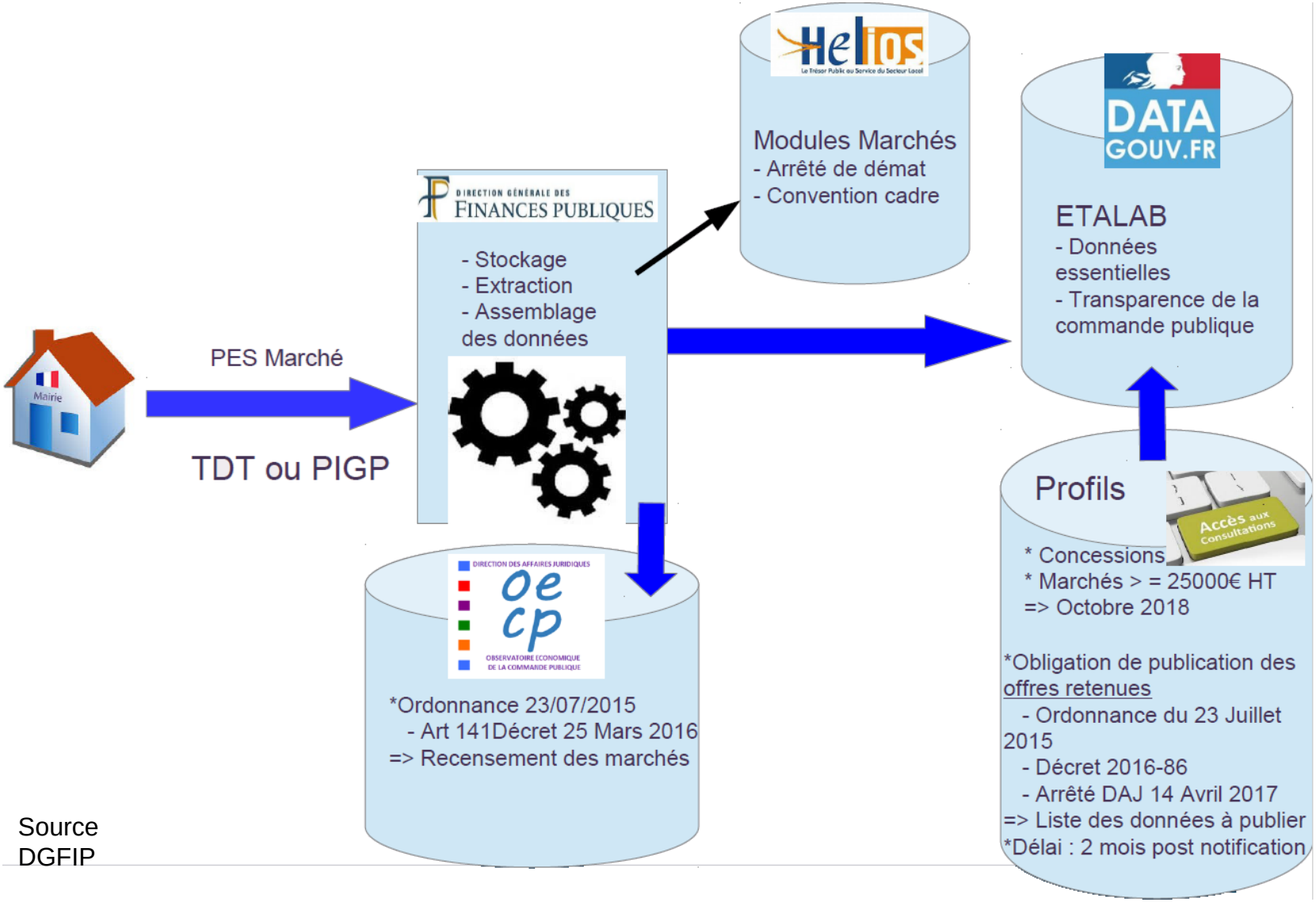
Acheteurs

1. S'identifier et s'authentifier
2. Publier des avis d'appel à la concurrence et leurs éventuelles modifications
3. Mettre à disposition les documents de la consultation
4. Réceptionner et **conserver** des candidatures y compris si elles se présentent sous la forme du document unique (DUME)
5. Réceptionner et conserver des offres, y compris hors délais
6. **Compléter** un formulaire nécessaire à la publication des données essentielles (open data) prévues par l'arrêté du 14 avril 2017 : marchés > 25.000 €HT
7. Accéder à un service de courrier électronique au sens de l'article 1 de la loi n° 2004-575 du 21 juin 2004
8. Accéder à un historique des évènements permettant l'enregistrement et la traçabilité des actions ayant eu lieu sur le profil acheteur notamment le retrait et le dépôt de documents
9. Répondre aux questions soumises par les entreprises
10. Obtenir les documents justificatifs et moyens de preuve lorsque ceux-ci peuvent être directement obtenus auprès d'autres administrations

Opérateurs économiques

1. S'identifier et s'authentifier
2. Connaître les prérequis techniques et les modules d'extension nécessaires pour utiliser le profil acheteur
3. Accéder à un espace permettant de tester que la configuration du poste de travail utilisé est en adéquation avec les prérequis techniques du profil d'acheteur
4. Effectuer une recherche permettant d'accéder notamment aux avis d'appel à la concurrence, aux consultations
5. Consulter et télécharger en accès gratuit, libre, direct et complet les documents de la consultation, les avis d'appel à la concurrence et leurs éventuelles modifications
6. Accéder à un espace permettant de simuler le dépôt de documents
7. Déposer une candidature y compris si elle se présente sous la forme du document unique de marché européen électronique constituant un échange de données structurées
8. Déposer des offres, y compris les dépôts successifs quand la procédure le requiert et les offres signées électroniquement
9. Solliciter une assistance ou consulter un support utilisateur permettant d'apporter des réponses aux problématiques techniques
10. Formuler des questions à l'acheteur
11. **Consulter et télécharger les données essentielles** conformément aux dispositions de l'arrêté du 14 avril 2017 relatif aux données essentielles

PES marché (Schéma cible)



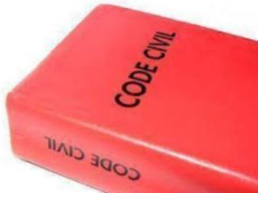
Source DGFIP

Signature électronique et certificat électronique

Signature et certificat électroniques
Plan du chapitre

- Qu'est ce que c'est ? A quoi ça sert ?
- Comment ça fonctionne ?
- Les fondements juridiques
- Les utilisations
- La notion d'original et de copie
- Evolution du RGS vers EIDAS
- La délégation

La signature Qu'est ce que c'est ?
Définition Code civil Article 1316-4



- La signature manuscrite que vous connaissez identifie celui qui l'appose. Elle manifeste le consentement

- La signature électronique, permet de garantir **l'identité du signataire** et **l'intégrité de l'acte**

Qu'est ce que c'est ?
Plus en détail

- En informatique : une signature électronique est fabriquée au moyen d'un certificat électronique et d'une application informatique

- Une signature confirme que **les informations proviennent du signataire et que le document signé n'a pas été modifié**
  - Le **certificat électronique**, représente une preuve d'identité de son possesseur (en général contenu sur une clé USB ou carte à puce)
  - Pour être valide ce certificat doit être délivré par une Autorité de Certification agréée (CCI, Greffe, Notaire…)

A quoi ça sert ?
A garantir des propriétés essentielles

- Garanties associées à la signature électronique
  - **Authenticité** : Le signataire est confirmé en tant que tel (Son identité et sa qualité dans la collectivité)

  - **Intégrité** : Le contenu de la pièce signée n'a pas été modifié ou falsifié depuis sa signature numérique

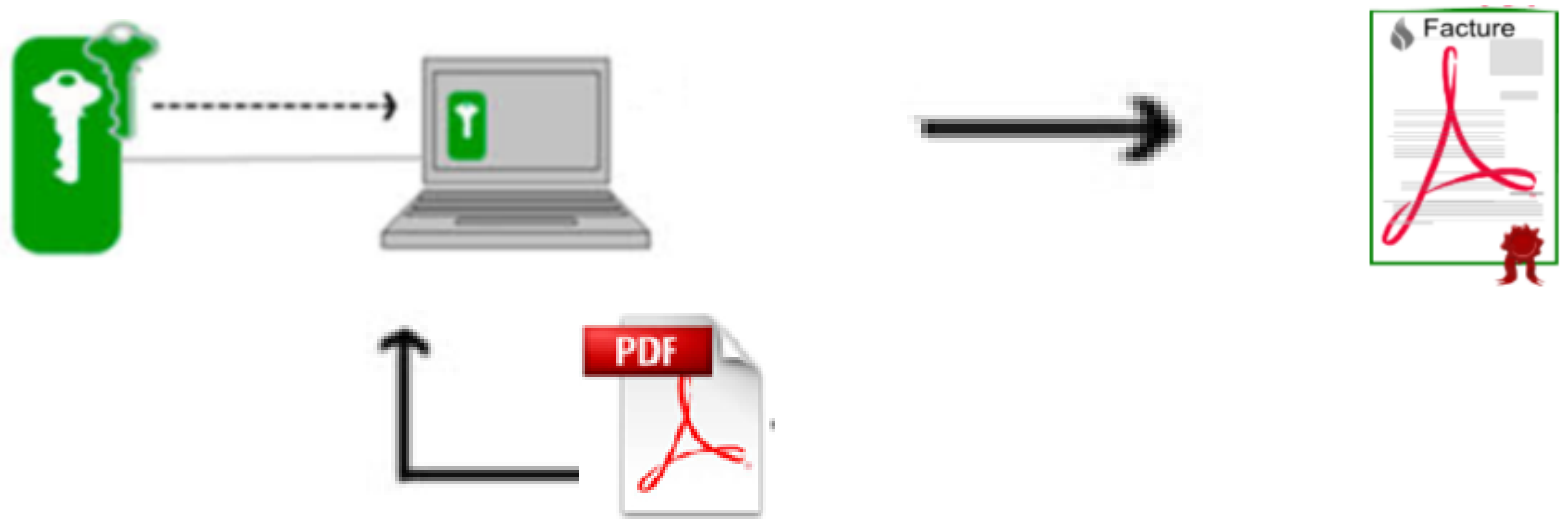
  - **Non-répudiation** : Prouve à toutes les parties l'origine du contenu signé. Le terme répudiation fait référence à l'acte d'un signataire qui rejette tout lien avec le contenu signé

  - **Notarisation** : La signature qui est horodatée par un serveur d'horodatage sécurisé, a dans certaines circonstances, une valeur de notarisation

Comment ça fonctionne ?

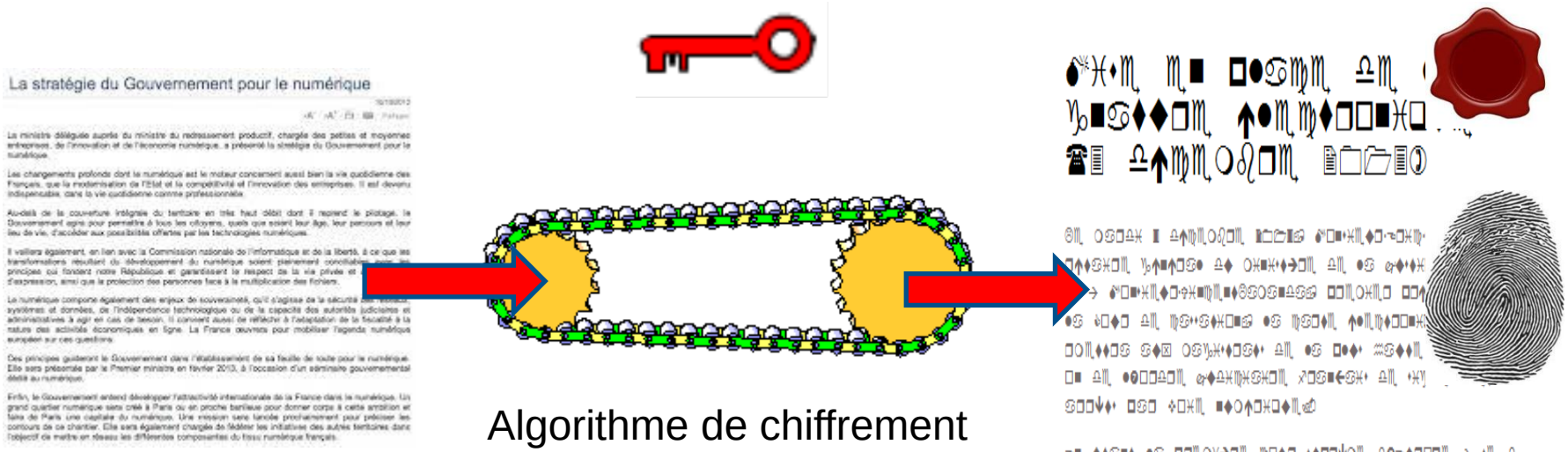
- Quand vous signez électroniquement vous apposez (au moyen d'un outil informatique (Acrobat, Outlook, Word, Parapheur électronique, Profil acheteur…) au document votre signature électronique

- Le document électronique devient un « original » (donc signé)



Comment ça fonctionne ?
En théorie

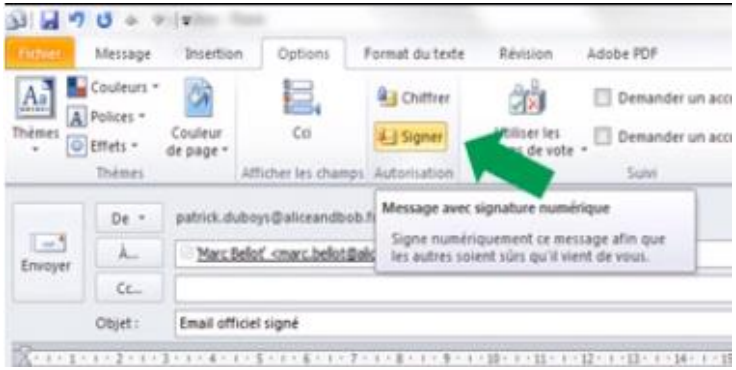
- En informatique, votre marque personnelle, c'est une clé de chiffrement. Pour signer un document, vous le chiffrez.

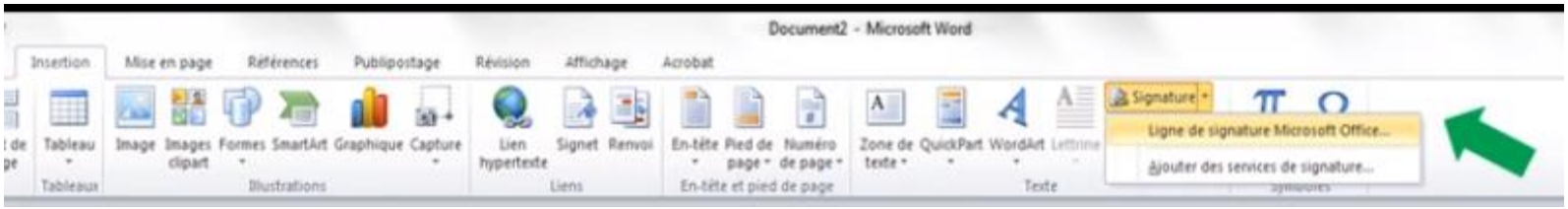


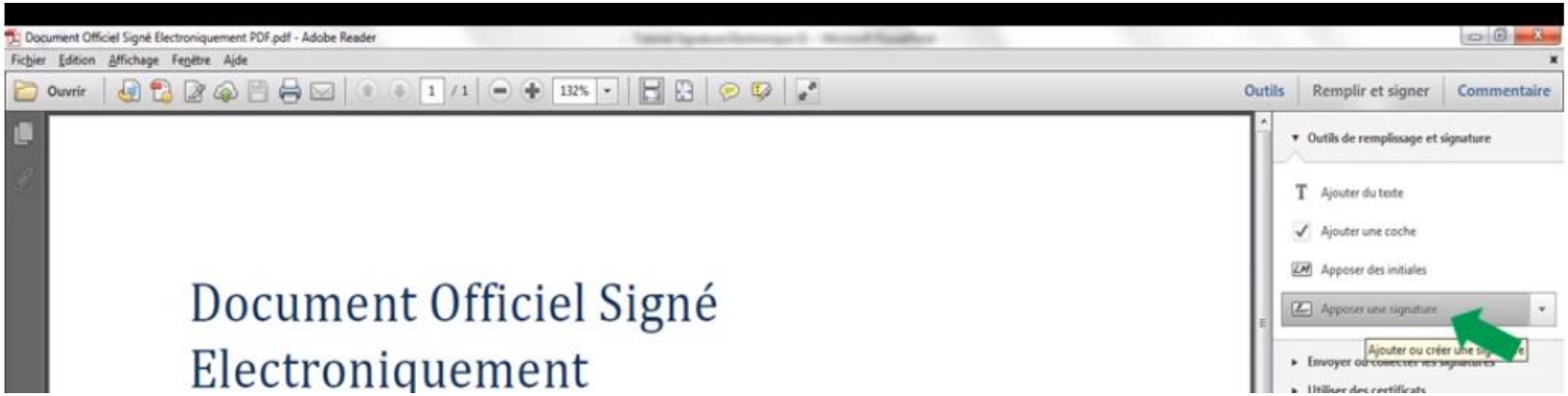
Algorithme de chiffrement

- L'action de signature électronique a :
  - Demandé votre consentement → Assure la **non répudiation**
  - Produit un condensé du message → Assure le contrôle de **l'authentification** et la **notarisation**
  - Chiffré le condensé → Assure **l'intégrité**

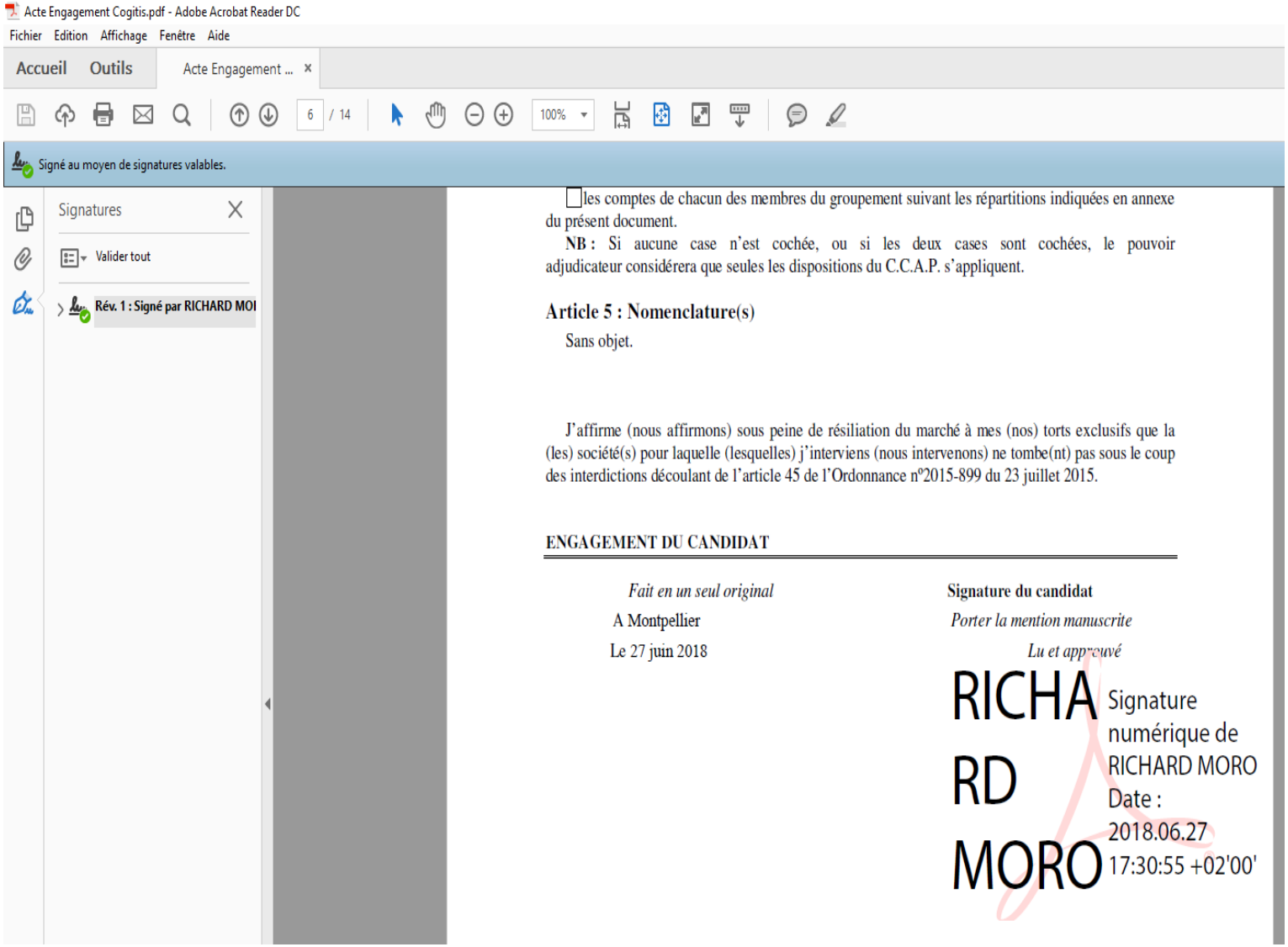
Comment ça fonctionne ?
Dans les outils







Comment ça fonctionne ?
Le résultat…



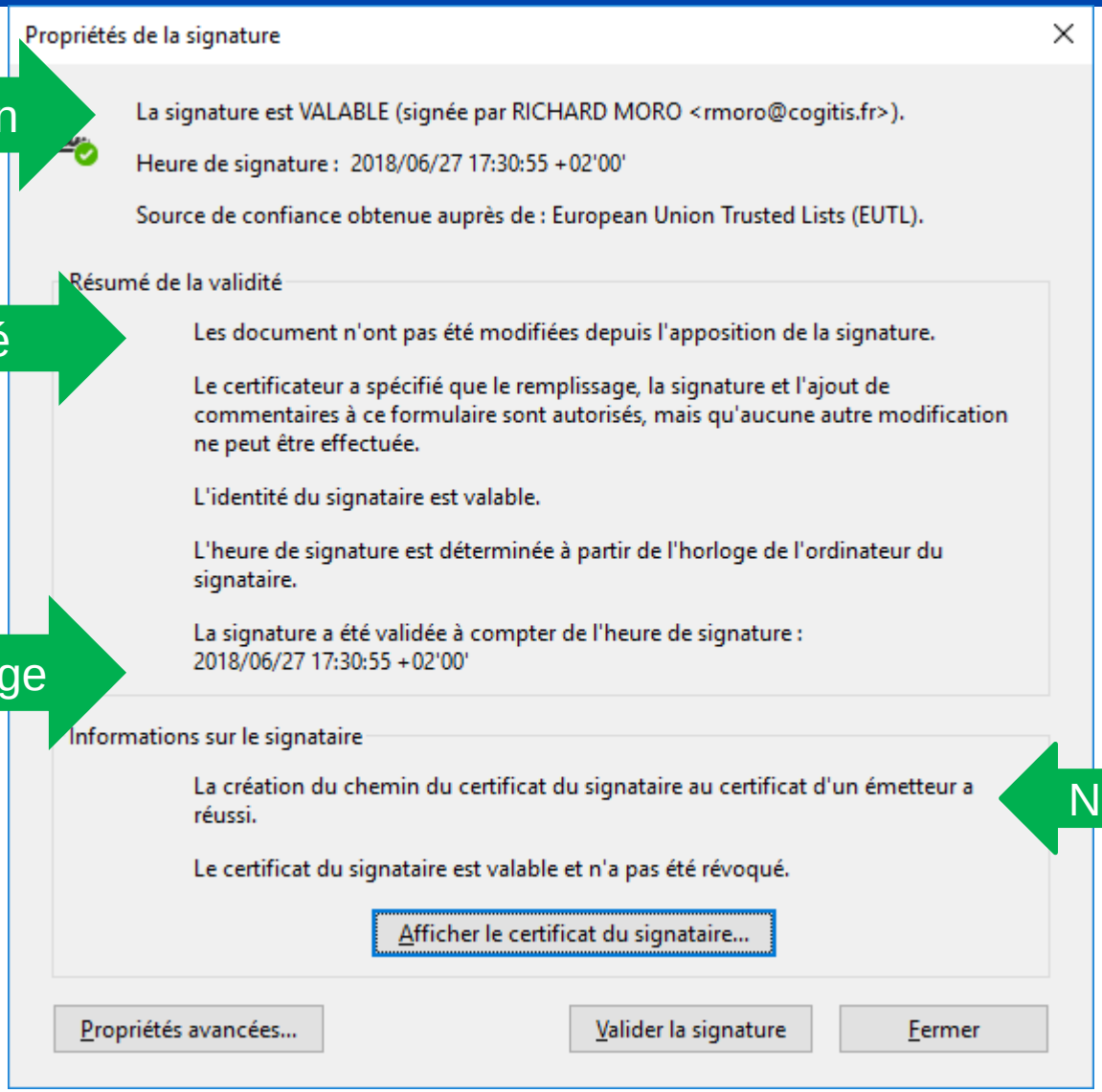
Comment ça fonctionne ?
La vérification…

Authentification

Intégrité

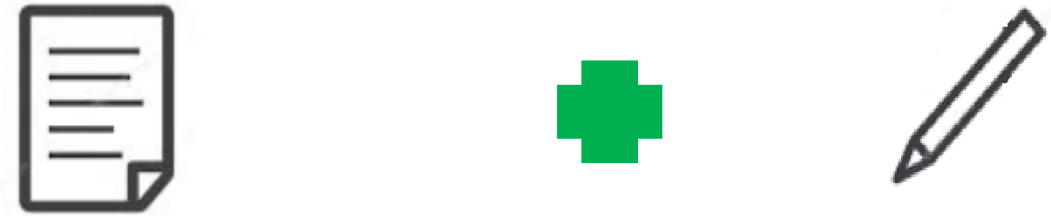
Horodatage

Non répudiation



En résumé, comment créer un original ?

- Traditionnel, vous connaissez…



Création d'un original signé

Soumis à règles d'archivages

- Numériquement, c'est très semblable

De nombreuses utilisations

ACTES - Authentification du service expéditeur

Marchés publics (x2)

Réseau privé de la Justice

Prodou@ne

HELIOS - Authentification du service expéditeur

COMEDEC

Réseau des experts comptables

HELIOS- Signature des Bordereaux Journaux

Actes notariés

Contrats Inter-Pro (B to B)

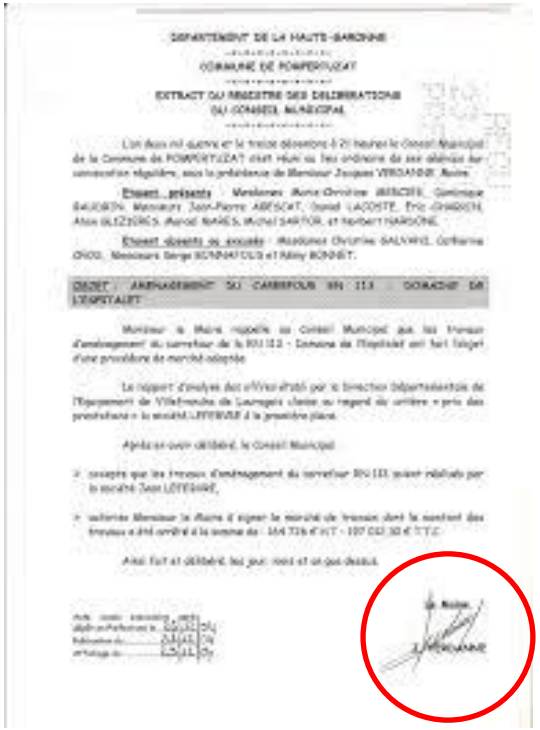
Certaines opérations bancaires

TRACFIN / ERMES

Les familles de signature

- Signature scannée
- Signature manuscrite sur tablette
- Signature à la volée
- Signature électronique avec ou sans *
- Signature par identification en ligne

Signature scannée insérée dans un document numérique



DEPARTEMENT DE LA HAUTE-GARONNE

COMMUNE DE POMPERTUZAT

EXTRAIT DU REGISTRE DES DELIBERATIONS DU CONSEIL MUNICIPAL

L'an deux mil quatre et le treize décembre à 21 heures le Conseil Municipal de la Commune de POMPERTUZAT était réuni au lieu ordinaire de ses séances sur convocation régulière, sous la présidence de Monsieur Jacques VERDANNE, Maire.

Etaient présents : Mesdames Marie-Christine ARSCOTE, Dominique BAUDEIN, Messieurs Jean-Pierre ARESCAT, Daniel LACOSTE, Eric CHABOSY, Alain GLEIZORGS, Marcel MARES, Michel SARTOR, et Norbert NARDONE.

Etaient absents ou excusés : Mesdames Christine SALVANI, Catherine CROS, Messieurs Serge SCHWARTZLO et Rémy BONNET.

OBJET : AMENAGEMENT DU CARREFOUR RN 113 - DOMAINE DE L'HOPITALET

Monsieur le Maire rappelle au Conseil Municipal que les travaux d'aménagement du carrefour de la RN 113 - Domaine de l'Hopitalet ont fait l'objet d'une procédure de marché adaptée.

Le rapport d'analyse des offres établi par la Direction Départementale de l'Equipement de Villefranche de Lauragais classe au regard des critères « prix des prestations » la société LEFEBVRE à la première place.

Après en avoir délibéré, le Conseil Municipal

- accepte que les travaux d'aménagement du carrefour RN 113 soient réalisés par la société Jean LEFEBVRE,
- autorise Monsieur le Maire à signer le marché de travaux dont le montant des travaux a été arrêté à la somme de : 164 726 € HT - 197 051,30 € TTC.

Ainsi fait et délibéré les jour, mois et an que dessus.

Le Maire,

J. VERDANNE

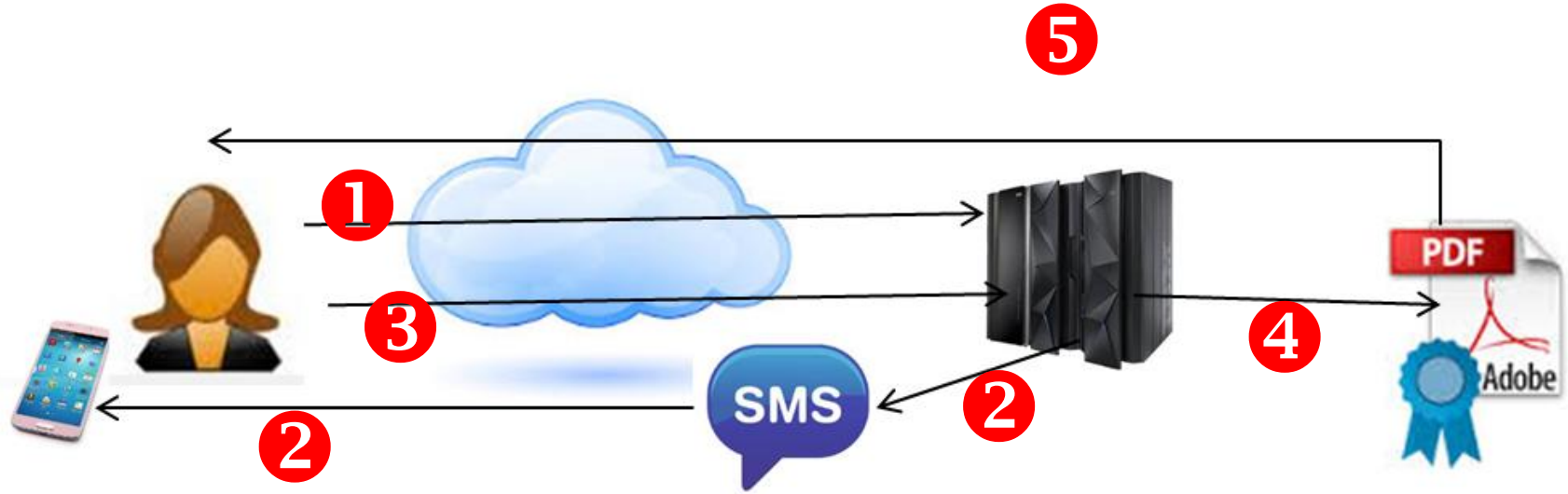
- Valeur juridique : **aucune car non signé**, n'importe qui peut scanner un courrier du Maire ou du Président et le coller dans un document numérique quelconque…

Signature manuscrite sur tablette

- La signature électronique manuscrite est un processus reconnu et accepté qui témoigne d'un accord volontaire.

- Valeur juridique : **plus ou moins forte** à condition de :
  - **Mettre en place une piste d'audit fiable :**
    - Enregistrement des coordonnées GPS
    - Capture du tracé et du temps d'exécution
    - Pression
    - Photographie…
  - **Respecter la sécurité**
    - Transfert crypté et sécurisé de la signature et des informations d'audit

Signature à la volée



- Valeur juridique : **début de preuve** à condition de :
  - **Mettre en place une piste d'audit fiable :**
    - Conservation des traces de l'opérateur véhiculant le SMS
  - **Respecter la sécurité**
    - Echanges sécurisés entre les parties

Signature électronique RGS 1/2/3 * ou eIDAS

- Signature classique telle que vous commencez à la connaître dans vos collectivités.

- Nécessite l'usage d'un outil spécifique (Acrobat, Outlook, Parapheur électronique, Profil acheteur, Word…),

- Le niveau de signature dépend de vos besoins :
  - Sans * : gratuite sur Internet, sans grande valeur juridique (début de preuve)
  - 1* : permet d'authentifier des machines, Actes par exemple
  - 2* : permet de signer des marchés, des bordereaux Hélios
  - 3* : permet de s'authentifier avec un haut niveau de protection technique et juridique, inverse la charge de la preuve

Signature par identification en ligne

- Actuellement, le plus grand projet est celui de l'Etat plateforme porté par « France Connect ».
- France Connect est un système d'identification et d'authentification offrant un accès universel à l'ensemble des administrations en ligne.
- Les usagers choisissent leur fournisseur d'identité (La Poste, Améli, Les impôts, Mobile connect et moi (Orange)…).
- France Connect identifiera les utilisateurs selon 3 niveaux (faible, substantiel ou fort) qui seront alignés eIDAS.
- Pour le citoyen usager, 2 promesses :
  - Une identification/authentification unique.
  - Un espace personnalisé dans lequel il disposera de toutes les données nécessaires à sa démarche, récupérées avec son accord auprès des autres administrations.

En résumé

Type de signature électronique	Appellation RGS/ eIDAS	Valeur juridique	Utilisation
Scannée		Aucune	Pas de besoin juridique : Invitation aux vœux…
Manuscrite sur tablette		Début de preuve --> Valeur probatoire	La plupart des actions en ligne ayant un enjeu financier ou juridique faible L'organisme ayant réalisé la procédure de signature doit prouver que le procédé est fiable
Signature à la volée			
RGS 1* / eIDAS N1	Elémentaire /Simple	Début de preuve	
RGS 2* / eIDAS N2	Standard /Avancée	Valeur probatoire	Signature administrative (Hélios, MP, prochainement Actes)
RGS 3* / eIDAS N3	Renforcée /Qualifiée	Inversion de la preuve	Signature ayant un enjeu juridique fort Acte notarié, Connexion COMEDEC
Signature par identification en ligne		Valeur probatoire	Identification des citoyens sur les portails des collectivités

La Règlementation

Référentiel - Général - de Sécurité

eIDAS

Les principales obligations

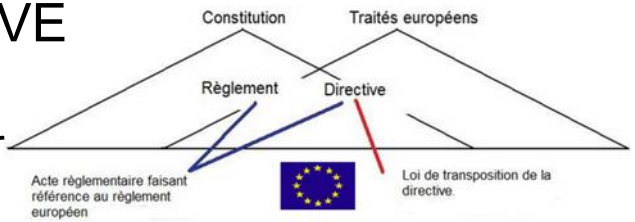
- Gérées par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI - Service à compétence nationale, rattaché au Premier ministre).
- L'ANSSI maintient à jour le Référentiel Général de Sécurité (RGS) qui s'impose à toutes les administrations en matière de sécurité des systèmes d'information.

- Actuellement le RGS
  - Objectif : confiance dans les échanges au sein de l'administration et avec les citoyens.
  - RGS v2 applicable depuis le 1er juillet 2014.
  - Version 3 en cours de réflexion qui prendra en compte la règlementation européenne eIDAS.
  - Exemple : Pour leurs échanges avec d'autres administrations ou avec les usagers, les collectivités doivent accepter les certificats électroniques conformes au RGS.

eIDAS 1/3, ce qu'il faut retenir !

- C'est bien un REGLEMENT et pas une DIRECTIVE

  Il vise à développer une confiance accrue dans les transactions électroniques au sein du marché intérieur de l'Union Européenne.



- Il s'impose à tous les Etats de l'UE et a engendré des modifications sur de nombreuses lois et règlements (RGS)

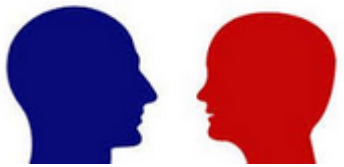
- Un nouvel objet juridique : la signature électronique de personne morale (Art. 3) ou « cachet électronique »

eIDAS 2/3, ce qu'il faut retenir !

- Des services de confiance européens (signature, horodatage…) (Art.20)

- Des listes de confiance tenues par les Etats (Art. 22)

- Maintien du face-à-face (Art. 24)



- Harmonisation européenne de la signature électronique (Art. 25) et des identifications électroniques (Art. 6)

eIDAS 3/3
ce qu'il faut retenir !

- La présentation d'un service de conservation des signatures électroniques (Art. 34)

- L'horodatage introduit au niveau européen (Art. 41)

- Un document électronique est une preuve (Art. 46)

- → Maintient des anciens certificats jusqu'à leur expiration

La délégation de signature

La délégation

- Comme pour les délégations classiques, la personne qui va signer de manière électronique doit :
  - Etre en charge de l'administration (Maire, Président) de par son statut (CGCT Article L2122-18).
  - Avoir reçu une délégation par arrêté pour une mairie, une délégation de signature (CGCT Article L2122-19) permet de déléguer aux :
    - *Elus (si délégation de fonction)*
    - *DGS et DGA, DG et Directeur des services techniques*
    - *Responsables des services communaux*
- La mise en place de la signature électronique doit **anticiper** cette « possibilité » afin de prendre les arrêtés nécessaires et déclencher les achats de certificats électroniques.
- Rappel : le certificat de signature électronique est **INDIVIDUEL** : pas de communication du code PIN à un autre agent

Automne 2018

Conseil d’achat d’un certificat de signature électronique

Achat d'un certificat de signature électronique, quelques conseils pour 2018

- Acheter un certificat certifié RGS (Qualifié par LSTI et ANSSI) et eIDAS
- Taille de la clé publique : RSA 2048 bits minimum
- Algorithme de « hashage » : SHA-256
- Durée de validité entre 1 et 3 ans (dépend de votre contexte)
- Paramètres à revoir tous les 2 à 3 ans

Achat d'un certificat : exemple ChamberSign RGS 2*-eIDAS

Le certificat AUDACIO RGS est dorénavant remplacé par le certificat Eurodacio répondant aux normes eIDAS pour toutes vos télé-procédures et autres usages.**

Le certificat Eurodacio est le dernier né de la gamme de produits de ChamberSign France.

Il est qualifié RGS et répond à la réglementation européenne eIDAS.

Véritable carte d'identité électronique professionnelle certifiée par un tiers de confiance, **le certificat Eurodacio** permet une authentification forte conforme au RGS** et la signature de document conforme à la réglementation européenne eIDAS.

Il permet de générer une signature avancée avec certificat qualifié conformément à **l'arrêté du 12 avril 2018 relatif à la signature électronique dans la commande publique.**

DESCRIPTION | CARACTÉRISTIQUES | CIRCUIT DE COMMANDE | PIÈCES À FOURNIR | FAQ | **PRÉ-REQUIS**

LES TARIFS :

	Paiement annuel par tacite reconduction	Tarif sérénité 3 ans	+ Support clé OBLIGATOIRE
EURODACIO	80€ HT	73,33€ HT/an soit 220€ HT	50€ HT

Eurodacio permet une révocation rapide et simple, avec une mise à jour journalière de la liste de révocation permettant de vérifier la validité d'un certificat.

Ce certificat doit obligatoirement être livré sur une clé USB cryptographique répondant aux normes de sécurité demandées par eIDAS et l'ANSSI.

Le certificat est remis à son titulaire lors d'un rendez vous dans le bureaux d'enregistrement de son choix.

Achat d'un certificat : exemple Certidemat RGS 3*-eIDAS

CERTIFICATS EIDAS / RGS***

Accueil / Certificat eIDAS / RGS***

PRODUITS

- RGS***
- RGS**

SIGNATURE ÉLECTRONIQUE EIDAS / RGS***

Lorsque vous commandez un certificat ID Pack eIDAS / RGS***, il est délivré obligatoirement sur un support de type carte à puce ou clé cryptographique au format USB. Nous devons également effectuer un face-à-face physique avec le futur porteur afin de vérifier son identité.

Quels sont les usages possibles?

- Authentification
- Chiffrement
- Signature
- Signature de mail
- Signature de documents avec inversion de la preuve
- TRACFIN / ERMES
- COMEDEC
- Toutes les autres utilisations nécessitant un certificat RGS * et **

Commander | Demande de devis

Pack eIDAS / RGS*** remis en Face à Face dans toute la France (déplacement en sus sur devis uniquement en Ile de France)		
Durée	Tarif € HT	Tarif € TTC
1 an	290 €	348 €
2 ans	370 soit 185 € / an	444 €
3 ans	430 soit environ 137 € / an	516 €

Le RGPD

Sommaire RGPD

- Actualité
- Principes
- Règlement européen
- Droits des citoyens
- Données personnelles, données sensibles
- Enjeux pour les collectivités
- LE DPD (DPO)
  - Rôle, Missions...
  - Nomination
  - Possibilité de mutualiser
- Comment mettre en œuvre ?
  - Méthode CNIL en 6 étapes

Ce « qu'ils » savent de nous
(d'après une présentation de « Le point » du 25/01/2018)

Finances
Solvabilité, investissements
Produits achetés, recherchés...

Identité
(nom, prénom, âge, n° ss, e-mail...)

Vie privée
Origine, religion, orientation sexuelle...

Evènements de la vie
Grossesse, naissance, mariage, retraite...

Comportement d'achat
Sommes dépensées, produits achetés, moyens de paiement...

90 % de l'ensemble des données aujourd'hui disponibles ont été crées au cours des deux dernières années

« Data broakers »
Acheteurs/vendeurs
de données

Santé
Fumeur ou non, maladies et traitements recherchées, achat et ordonnances en lignes...

Véhicules
Immatriculation, type, assurance...

Voyages
Lieux, dates, fréquences, budgets...

Réseaux sociaux
Identités, familles, photos, vidéos, liens, like...

En 1 minute

900.000 connexions

4 millions vidéos vues

21 millions de messages

Sources : rapport US Trade commission / SMILE

RGPD, quelques principes

- RGPD : **Règlement** Général de la Protection des données
  - Directement applicable dans toute l'UE depuis le 25 mai 2018.
  - Quelques principes fondamentaux :
    - « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental ».
    - « Toute personne a droit à la protection des données la concernant ».

- Mise en application :
  - Logique de conformité sous la responsabilité des acteurs.
  - Renforcement du rôle de la CNIL (Conseil, Contrôle et Sanction).

RGPD : objectifs visés

- Augmenter la confiance

- Renforcer le droit des personnes même en dehors de l'UE
  - Portabilité des données personnelles
  - Droit au recours collectif par le biais d'associations de consommateurs
  - Dispositions propres aux personnes mineures

- Responsabiliser les acteurs traitant des données
  - Editeurs et sous-traitants
  - Responsables de traitements de données personnelles

- Crédibiliser la régulation
  - Renforcement des sanctions
  - Harmonisation et unification de la législation au sein de l'UE

→ Pour la France, simplifier les démarches (déclarations CNIL)

Droits individuels des citoyens

Portabilité
Récupérer au format numérique les données communiquées à une plateforme et les transmettre à un autre (réseau social, fournisseur d'accès internet…)

Transparence
Savoir comment les données sont utilisées et exercer ses droits plus facilement (droit d'accès, droit de rectification)

Droits des mineurs
Obtenir pour les services en ligne le consentement des parents des mineurs de moins de 16 ans avant leur inscription

Guichet unique
Pouvoir s'adresser en cas de problème à l'autorité de protection des données de son pays quel que soit le lieu d'implantation de l'entreprise qui traite mes données

Sanctions
Avoir des sanctions pour l'entreprise responsable jusqu'à 4 % du chiffre d'affaires mondial en cas de violation des droits

Droit à l'oubli
Demander qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à la vie privée

Source CNIL – Dessins Martin Vidberg

Données personnelles
Données sensibles

Une donnée personnelle

- « Toute information qui permet d'identifier une personne physique directement ou indirectement »

Une donnée personnelle sensible

- « Toute information concernant **l'origine raciale** ou **ethnique**, les **opinions politiques**, **philosophiques** ou **religieuses**, **l'appartenance syndicale**, **la santé** ou **la vie sexuelle** »

Les changements pour les collectivités
Enjeux

- Modernisation de l'action publique par **l'e-administration et** l'usage grandissant des **technologies du numérique** par les collectivités doit s'accompagner de vigilance et contrôle
- Augmentation des **cyberattaques**
- Préoccupation grandissante des citoyens sur l'utilisation de leurs **données personnelles**
- Exigence élevée sur la **protection et la sécurité** des données pour mériter la **confiance des administrés**

Les changements pour les collectivités
Impacts

- Changement de culture
  - Logique de contrôle → Logique de responsabilisation
  - Les études d'impact sur la vie privée (EIVP) !
  - La notification de failles de sécurité (aux autorités et personnes concernées) !
- Mise en conformité permanente et dynamique
  - Mesures techniques et organisationnelles
  - L'adhésion à des codes de conduite
- Niveau optimal permanent de protection des données
  - Suivi des actions sur le matériel et les logiciels
  - Mise en place dès la conception d'un produit
  - Intégration de la conformité au RGPD dans les marchés publics
  - Tenue d'un registre des traitements !
- Désignation d'un(e) Délégué(e) à Protection des Données !

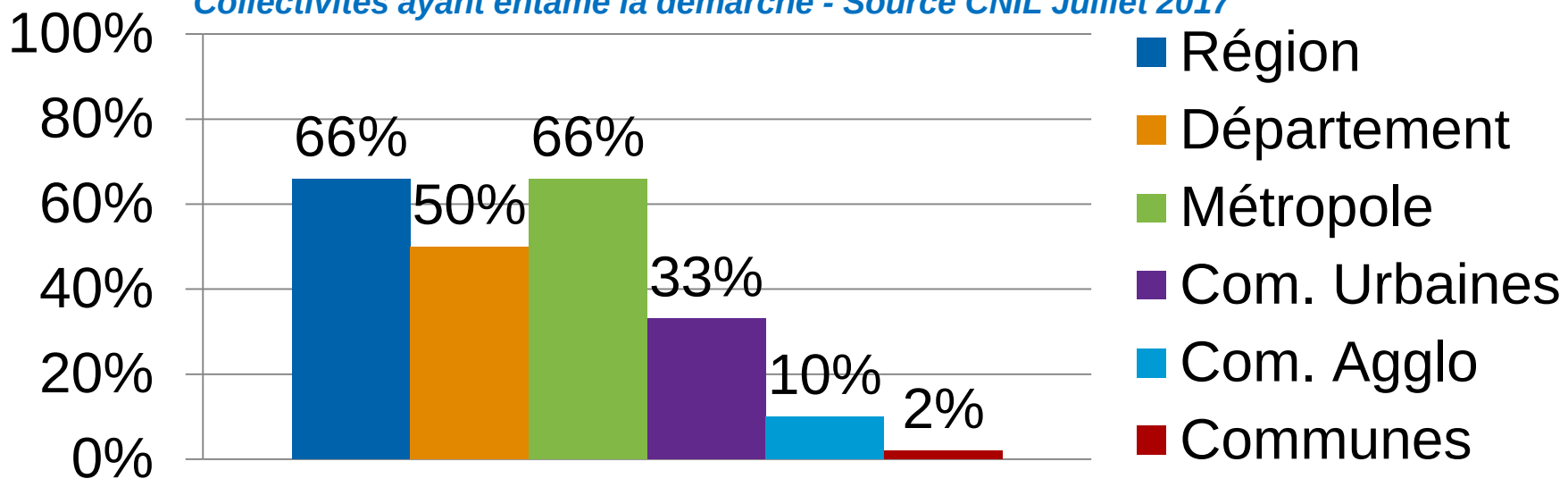
! obligatoire

Les changements pour les collectivités le DPD (ou DPO en version anglaise)

- Missions
  - Diffuser une culture au sein de la collectivité
  - Informer et conseiller les agents, le responsable métier, le sous-traitant
  - Conseiller la collectivité sur la réalisation d'analyse EIVP
  - Etre associé à l'ensemble des questions informatiques et libertés
  - Contrôler le respect du règlement et du droit national en matière de protection des données
  - Rendre compte directement au niveau le plus élevé de la hiérarchie
  - Etre le contact avec la CNIL et coopérer avec elle
- Comment et qui choisir ?
  - Désigner hors des conflits d'intérêts, avoir une liberté d'action
  - Une personne (interne ou externe à la collectivité) qui ait des connaissances du droit et des pratiques en matière de protection des données

Les changements pour les collectivités
Collectivité ayant désigné un DPD

Collectivités ayant entamé la démarche - Source CNIL Juillet 2017



- Mutualisation du DPD, avec qui ?
  - Structure de mutualisation informatique
  - Centre de gestion
  - EPCI
- Travail collaboratif entre collectivités sans DPD mutualisé

Et si on ne faisait rien ?

Les sanctions

- Sanctions administratives
  - Avertissement
  - Mise en demeure
  - Limitation temporaire ou définitive d'un traitement
  - Suspension du flux des données
  - Ordre de satisfaire à l'exercice des droits des personnes
  - Ordre de rectifier, limiter ou effacer des données

- Amendes administratives
  - Selon la catégorie de l'infraction
    - Montant maximum 10.000.000 € (jusqu'à 2 % du CA pour une entreprise)
    - Montant maximum 20.000.000 € (jusqu'à 4 % du CA pour une entreprise)
  - Exemples
    - 07/06/2018 Optical center 250.000 € : sécurité insuffisante du site web client
    - 28/06/2018 l'association ADEF 75.000 € : sécurité insuffisante du site web client

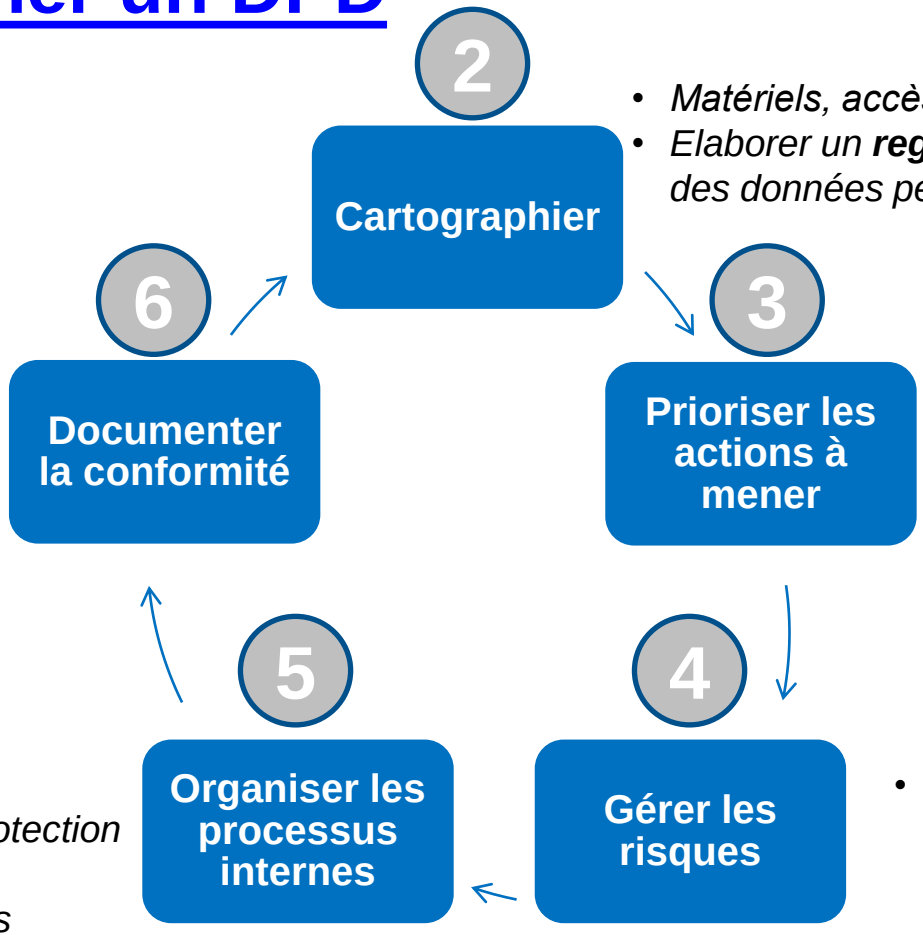
La méthodologie préconisée par la CNIL

CNIL.

La méthodologie préconisée par la CNIL

CNIL.

1 Désigner un DPD



- *Matériels, accès, sauvegardes…*
- *Elaborer un **registre des traitements** des données personnelles*

- *Identifier les actions à mener en fonction du registre des traitements*
- *Prioriser les actions au regard des risques sur les droits des personnes*

- *Mener une analyse d'impacts (AIPD) sur les traitements à risque pour les droits et libertés*

- *Mettre en place des procédures pour la protection des données*
- *Prendre en compte les évolutions*

- *Prouver la conformité au règlement*
- *Contrôler et actualiser régulièrement*

CONCLUSION : Réussir son administration numérique

Les éléments de base

Le site Internet

- La brique essentielle : un site Internet que l'on maîtrise (même si prestataire)
- Prise en compte du SVE/SVA : une fiche contact
- Une adresse mail professionnelle, un nom de domaine
- Compatible RGPD, RGS, RGA
- Point d'entrée pour les habitants de la commune pour toute leurs procédures : locales et nationales

Autres briques…

- Profil acheteur : obligatoire dès le 1er octobre 2018… Demain !
- Signature électronique : authentification numérique
- Une politique de protection des données : pragmatisme et bon sens
- L'archivage électronique sera à prévoir
- Une organisation :
  - De vos délégations
  - De vos circuits de gestion des demandes
  - Des processus internes dématérialisés

Des obligations mais aussi des opportunités…

- Se concentrer sur ce qui est obligatoire !
- Politique des petits pas mais on avance !
- Mais n'hésitez pas à créer des procédures dématérialisées pour vos usagers locaux : Signalisation de problème de voirie, pb d'éclairage, signalisation de voisin en difficulté…
- Une opportunité pour la commune de créer un nouveau canal de contact avec les habitants.

Merci de votre attention

Annexe

Aspect juridique : les textes fondateurs… 20 ans déjà !

- 1999 : Directive Européenne 1999/93/CE : cadre communautaire pour les signatures électroniques
- 2000 : Loi n°2000-230 du 13 mars 2000 : Prise en compte de la signature électronique dans le code civil
- 2001 : Décret n° 2001-272 du 30 mars 2001 : Transposition de la Directive Européenne 1999/93/CE
- 2002 : Décret n° 2002-535 du 18 avril 2002 : Attribution du rôle de certificateur à l'ANSSI (ex DCSSI)
- 2002 : Arrêté du 31 mai 2002 : Attribution du rôle d'accréditeur au COFRAC, pour l'évaluation des prestataires de certification électronique
- 2004 : Loi du 21 juin 2004 sur la confiance dans l'Economie Numérique (dite LCEN)
- 2004 : Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation
- 2005 : Ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives
- 2010 : Décret du 2 février 2010 (dit "décret RGS")
- 2010 : Arrêté du 6 mai 2010 portant approbation du RGS et précisant les modalités de mise en œuvre
  2014 : Arrêté du 13 juin 2014 portant approbation du RGS v2
- 2014 : Règlement européen « eIDAS » (Electronic Identification and Signature - Electronic Trust Services) adopté le 23 juillet et publié au journal officiel de l'Union européenne (JOUE référence 910/2014/UE) le 28 août, (abroge la directive 1999/93/CE) applicable depuis 01/07/2016
- 2016 : Ordonnance 2016-131 du 10 février 2016 a transféré les dispositions correspondantes au nouvel article 1367 du Code civil
- 2017 : Décret n° 2017-1416 du 8 septembre 2017 reconnaît désormais en droit civil français la fiabilité de la signature électronique qualifiée conforme à la norme européenne eIDAS
- 2018 : Arrêté du 12 avril 2018 relatif à la signature électronique dans la commande publique