DOSSIER

Règlement Général sur la Protection des Données

QUE FAUT-IL SAVOIR ?

Croissants de l'APREF

apref
ASSOCIATION DES PROFESSIONNELS DE LA RÉASSURANCE EN FRANCE

13/06/2017

INTRODUCTION

SOMMAIRE

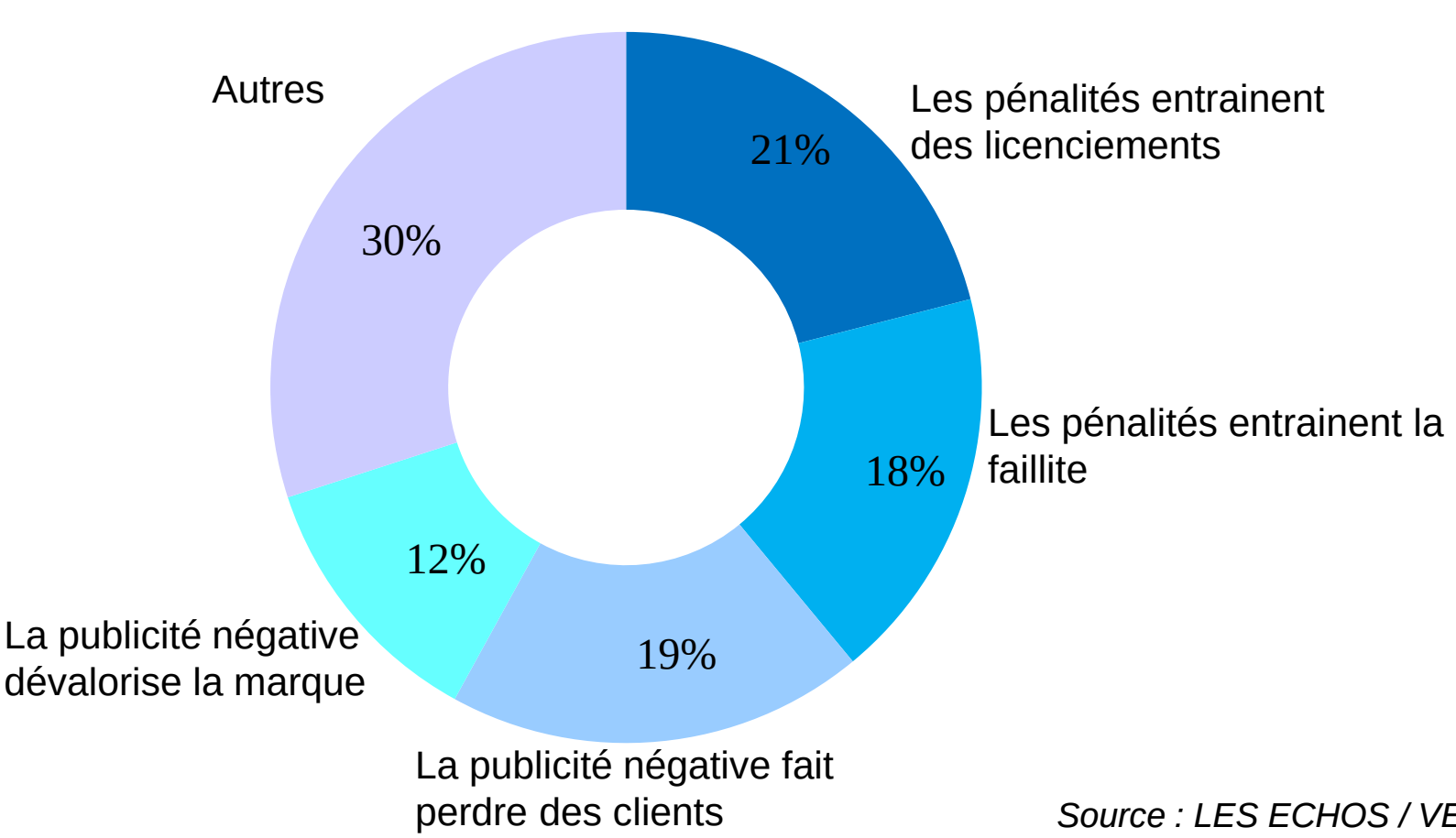
SOMMAIRE

Champ d'application du RGPD

Ce nouveau texte s'appliquera, en principe, à toutes les données personnelles :

- **des personnes physiques résidants dans l'UE ou**
- **dès qu'une étape du traitement se déroule sur le territoire européen.**

Les plus grosses préoccupations des dirigeants d'entreprise sur la conformité au RGPD



Source : LES ECHOS / VERITAS

Le GT data protection de l'APREF:

- **8 réassureurs**
- **11 représentants**
- **11 réunions**
- **1 note de synthèse**

La note :

- **explique le texte (origine de la DP, nouvel écosystème),**
- **n'est pas un guide pratique d'implémentation de la nouvelle réglementation (texte à venir de la CJ de l'APREF).**

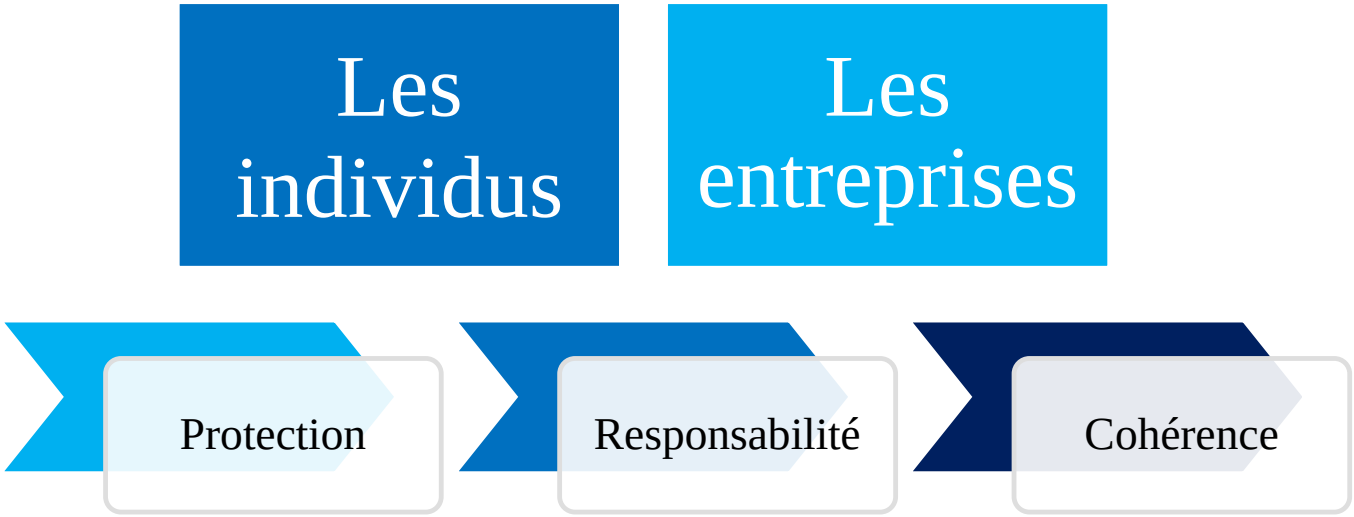
Les membres du GT présents :

- Jean Modry – Chief Risk & Compliance Officer – Hannover Re
- Marvin Dewkurun – Référent Juridique – SCOR
- Marie Schallier - Directeur Général Adjoint – Mut Re
- Xavier Debras – Client Manager – Swiss Re

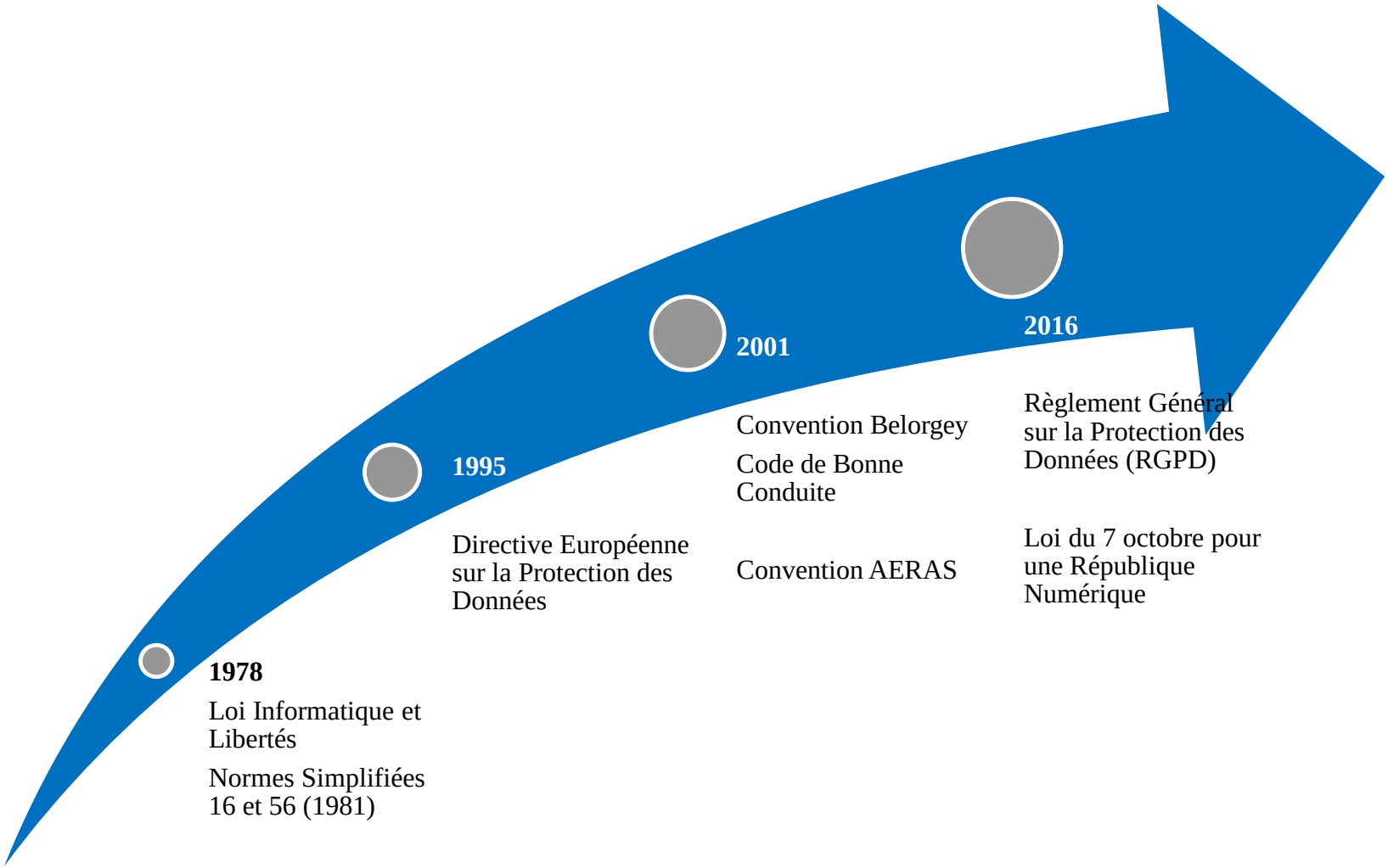
SOMMAIRE

“L’humanité produit autant d’informations en deux jours qu’elle ne l’a fait en deux millions d’années”

Gabriel Siméon, Libération, “Données le vertige” - 3 décembre 2012



Une histoire ancienne…



5 principes issus de la Loi de 1978

Les objectifs du RGPD

- Harmoniser le droit de l'UE
- Renforcer les droits des personnes concernées
- Responsabiliser les acteurs traitant les données
- Crédibiliser la régulation

Calendrier

2016

Mai
Publication du RGPD

2017

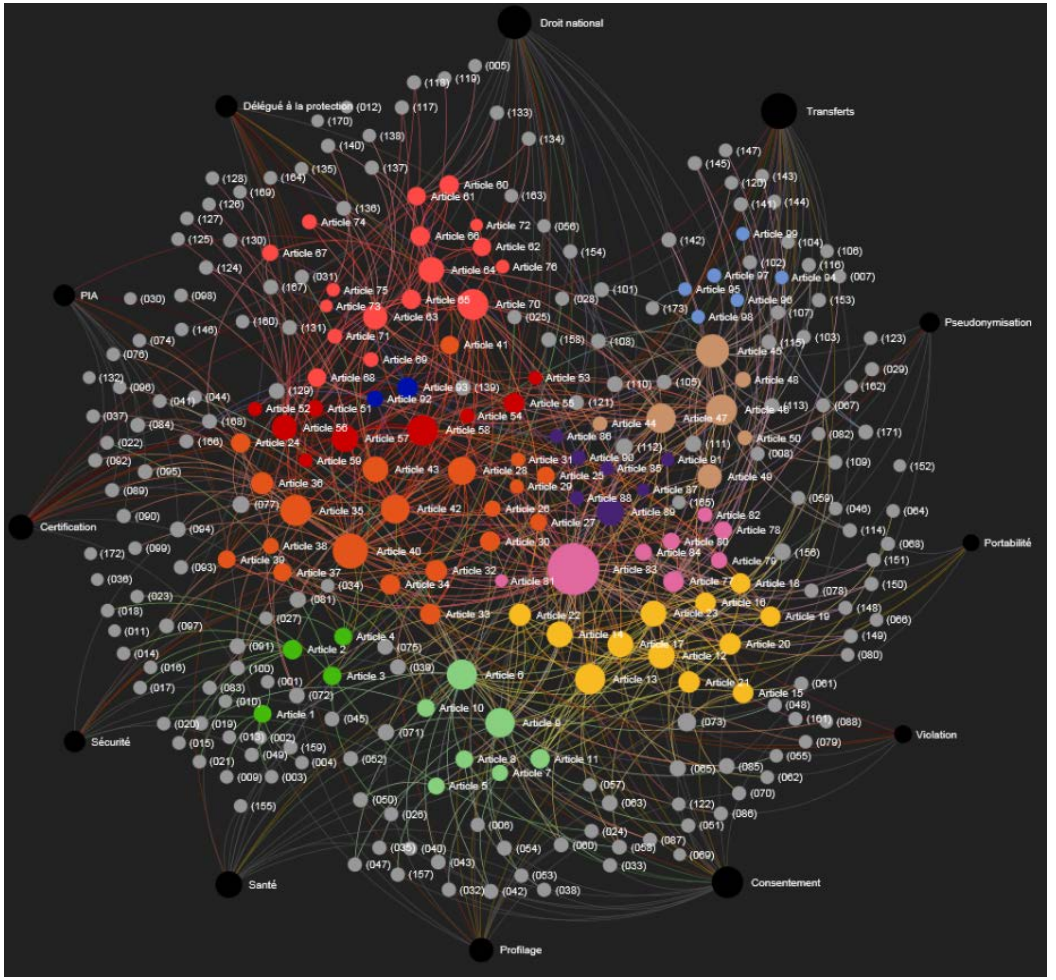
Mise en conformité

2018

25 mai
Application du RGPD

99 articles résumés par la CNIL.

en DataViz



SOMMAIRE

3 Le nouvel écosystème

- **Modification dans la relation commerciale**
- Modification dans la gestion interne des données
- Modification dans la relation avec le régulateur

Modification dans la relation commerciale (1)

1. Le consentement renforcé

Les 4 piliers du consentement

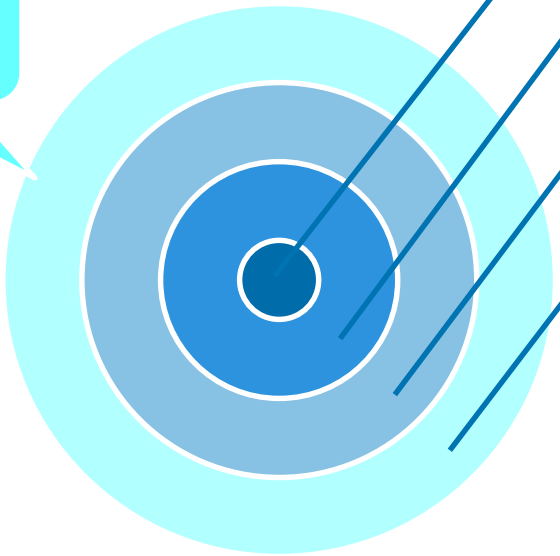
Recueil obligatoire	Peut être retiré à tout moment	Information claire et intelligible de la **finalité** du traitement	Charge de la preuve: responsable de traitement

Modification dans la relation commerciale (2)

2. Périmètre de données potentiellement élargi

Nouveau

- données de localisation
- identifiant en ligne



Données santé / médicales

- Art L.1111-8 CSP

Données santé

- Art 4 (15°) du règlement européen

Données sensibles

- Art 8 Loi I&L
- Art 9 du règlement européen

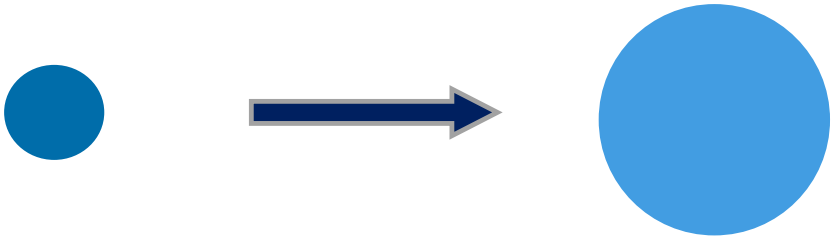
Données à caractère personnel

- Art 2 de la Loi I&L (2°)
- Art 4 (1°) du règlement européen

Modification dans la relation commerciale

2. Périmètre de données potentiellement élargi

- **Univers plus large pour les données de santé?**



I&L

- Loi I&L art 8: « Données **relatives à la santé** » (pas de définition explicite des données de santé dans la Loi I&L)
- Données médicales Art L.1111-8 CSP « données recueillies à l'occasion **d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social** »

RGPD

- Règlement européen art 4: « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la **prestation de services de soins de santé**, qui révèlent des informations sur l'état de santé de cette personne »

Modification dans la relation commerciale

3. De nouveaux droits pour le client

Droits confirmés	Droits renforcés	Nouveaux droits
• Accès • Rectification • Opposition • Interrogation	• Information en cas de violation des données • Réparation du dommage matériel ou moral	• Effacement (oubli numérique) • Limitation du traitement • Portabilité

3 Le nouvel écosystème

- Modification dans la relation commerciale
- **Modification dans la gestion interne des données**
- Modification dans la relation avec le régulateur

Gestion interne des données (1)

Différents éléments sont à prendre en compte dans la gestion interne des données :

Privacy by default et Privacy by design

- Prise en compte de la **protection des données** à la fois **dès la conception du produit ou du service** et s'assurer de ne collecter par défaut **que les données strictement nécessaires**

Accountability

- Plus de déclaration systématique mais le responsable du traitement doit être capable **de justifier de la légalité** du traitement à tout moment

Gestion interne des données (2)

- **L'élaboration d'Études d'Impact sur la Vie Privée (EIVP)** pour les traitements à risque.

Contexte, délimitation et description

↓

Mesures pour assurer la sécurité

↓

Risques associés

↓

Validation formelle en interne des solutions apportées

Gestion interne des données (3)

Un registre détaillé de **tous les traitements** doit être tenu par le responsable et comporter les informations suivantes:

- identité du responsable
- les finalités de chaque traitement
- catégorie des personnes concernées
- détails des données détenues
- détails des destinataires
- détails des éventuels transferts
- détails des mesures de sécurité
- détails des délais prévus pour l'effacement

Gestion interne des données (4)

- **Nomination d'un Délégué à la Protection des Données (ou DPO- Data Protection Officer)**
- **L'élaboration de codes de bonne conduite**
- **Mesures techniques et organisationnelles**
  - pseudonymisation
  - chiffrement
  - systèmes I.T sécurisés, disponibles et résilients
  - continuité d'activité et protection
  - tests et revues
  - formation des salariés
  - …

3 Le nouvel écosystème

- Modification dans la relation commerciale
- Modification dans la gestion interne des données
- **Modification dans la relation avec le régulateur**

Modification dans la relation au Régulateur

- **Les associations professionnelles sont autorisées à concevoir des codes de bonne conduite spécifiques à leur activité:**
  - **Ces codes doivent être approuvés par le régulateur.**
- **La création de Certification et de Labels de Conformité au règlement est également possible.**

Le Délégué à la Protection des Données

Responsable de la conformité des traitements

- Principe d' « accountability »
- Principe du Privacy by Default
- Principe du Privacy by Design
- Le registre des traitements
- Les études d'impact (Privacy Impact Assessment)
- La sécurité des données

➢ **Notification des violations**

- Au régulateur sous 72h
- Aux personnes concernées dans certains cas

➢ **Informations à fournir**

- Nature de la violation
- Nbre de personnes concernées
- Conséquences probables
- Les mesures prises

➢ Faire des enquêtes
➢ Arrêter des décisions contraignantes
➢ Infliger des sanctions:

- **Sanctions administratives** (plafonds)
  - 20 M€ ou dans le cadre d'une entreprise : 4% du CA mondial
- **Sanctions pénales**
  - Sanctions pénales possibles, au choix des Etats Membres

Le Régulateur

- Le guichet unique
- Le mécanisme de cohérence

SOMMAIRE

Les points d'attention :

1. **Nommer un DPO et prévoir une gouvernance**

2. **Faire (ou affiner) une cartographie des risques de conformité « data protection » :**
   - le registre détaillé
   - les analyses d'impact par traitement

3. **Définir un plan d'action de conformité « data protection » :**
   - modifier l'existant (par ex. ne plus collecter la profession si superflue)
   - prévoir les nouvelles obligations (droit à l'effacement, accès et modifications, …)

Les membres participants à la Note APREF :

- Arnaud VERREY, CCR
- Jean-Pierre MLYNARCZYK, GEN RE
- Johann LAUNAY, HANNOVER RE
- Jean MODRY, HANNOVER RE
- Marie SCHALLIER, MutRé
- Medhi HIMEUR, PARTNER RE
- Gurvan LE RHUN, RGA
- Marvin DEWKURUN, SCOR
- Delphine LABOJKA, SCOR
- Benoît AUDOYE, SWISS RE
- Xavier DEBRAS, SWISS RE

Et Merci de votre attention !

POUR PLUS D'INFORMATIONS SUR L' APREF & LA RÉASSURANCE

Notre site internet : www.apref.org

Notre Situation : 26, Boulevard Haussmann (6ème étage)

Notre compte Twitter : @Apref_Reass