econocom

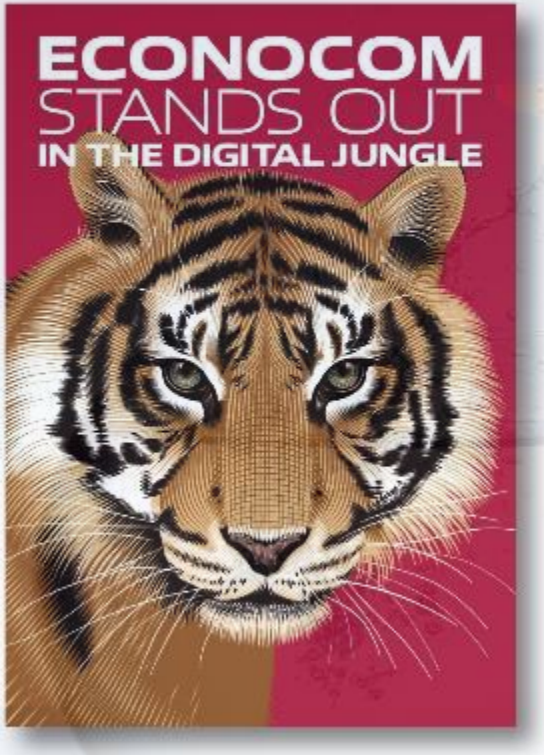
Notre démarche de mise en conformité au RGPD

ANDSI 14/11/2017

Au programme

- Petit rappel de ce qu'est Econocom
- Rapide retour sur le RGPD
- Le plan d'action d'Econocom
- Les points d'attention
- Conclusion
- Q&R

UN ACTEUR EUROPÉEN ENGAGÉ DANS LA TRANSFORMATION DIGITALE



2,5 milliards d'euros de chiffre d'affaires en 2016

40 ans d'expérience

19 pays

7 millions d'actifs technologiques gérés

10000 collaborateurs

«ONE GALAXIE»: UN BUSINESS MODEL UNIQUE POUR CONNECTER ET ORCHESTRER TOUTES NOS FORCES, AU PROFIT DE NOS CLIENTS

UNE PLANÈTE

AVEC 3 MÉTIERS HISTORIQUES & COMPLÉMENTAIRES:

> LES PRODUITS & SOLUTIONS DIGITALES
> LES SERVICES NUMÉRIQUES
> LE FINANCEMENT DES PROJETS

90%

part du CA de la Planète dans le CA du groupe en 2016

8000

collaborateurs

DES SATELLITES

AVEC DES COMPÉTENCES POINTUES INCARNÉES PAR DES PME EXPERTES & AUTONOMES:

> IoT
> CLOUD
> CYBER SÉCURITÉ...

10%

part du CA des Satellites dans le CA du groupe en 2016

2000

collaborateurs

Rapide retour sur le RGPD

- Applicable à toutes entreprises traitant des DCP de citoyens européens
- Règlement entrant en vigueur au 25 mai 2018
- 3 objectifs :
  - Renforcer les droits des personnes
  - Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants)
  - Crédibiliser la régulation

Le plan d'action d'Econocom

1. Piloter
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser les processus internes
6. Documenter

Le plan d'action d'Econocom - **Piloter**

- En phase projet
  - Sous responsabilité de la direction juridique
  - AMOA confiée à notre entité Digital Security
  - Prestation externe d'assistance à la mise en conformité
- Un livrable incontournable :
  - La Politique de protection des données

Le plan d'action d'Econocom - **Piloter**

- En run
  - Rôle de DPO est attribué à une juriste spécialisée de la protection des données à caractère personnel
    - ↪ contrôler le respect du règlement
    - ↪ de conseiller sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
    - ↪ de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.
  - Elle devrait être rattachée à la direction juridique

Le plan d'action d'Econocom - **Cartographier**

- Obligation de tenir une documentation interne complète des traitements de données à caractère personnel recensant :
  - Les différents traitements de données à caractère personnel,
  - Les catégories de données personnelles traitées ;
  - Les objectifs poursuivis (les finalités) ;
  - Les acteurs (internes ou externes) qui traitent ces données ;
  - Les flux en indiquant l'origine et la destination des données.

Feuille de calcul
Microsoft Excel

- Qui ?, Quoi ?, Pourquoi ?, où ?, jusqu'à quand ? et comment ?

Le plan d'action d'Econocom - **Cartographier**

- Démarrage « from scratch »
- Une première cartographie a été faite en 2016 visant à contrôler le niveau de conformité des traitements déclarés à la CNIL
- Capitalisation sur cette première cartographie pour évaluation de la conformité au RGPD

Le plan d'action d'Econocom - **Prioriser**

- Premier périmètre sur la France
- Priorisation en accord avec les métiers et selon les données traitées
- Arbitrage sur les Satellites par le COMEX suite à une étude de responsabilité

Le plan d'action d'Econocom – **Gérer les risques**

- PIA : Privacy Impact Assessment
- Analyse des risques axée vers les droits et les libertés des personnes
- Elément fondamental pour démontrer le respect du règlement

Le plan d'action d'Econocom – **Gérer les risques**

- Outil disponible sur le site de la CNIL (ici)
- Méthode similaire à une approche ISO 27005 ou EBIOS
- 3 critères à évaluer :
  - Accès illégitime aux DCP
  - Modification non désirée des DCP
  - Disparition des DCP

Le plan d'action d'Econocom – **Gérer les risques**

- Capitalisation des analyses des risques faites dans le cadre de notre certification ISO 27 001

- Etude de l'intégration de ces analyses à notre outil Risk'n TIC

Le plan d'action d'Econocom - **Organiser**

- Pour les projets : questionnaire en amont :
  - Pour prévenir des potentiels risques sur les DCP à l'instar de ce que nous faisons pour la sécurité de l'information
  - Prévoir le recueil du consentement si nécessaire

- Sensibiliser/Former les collaborateurs avec un plan de communication. Sur ce point nous pouvons capitaliser sur les mesures mise en œuvre pour notre certification ISO 27 001

Le plan d'action d'Econocom - **Organiser**

- Traiter les réclamations et les demandes (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) :
  - les acteurs et les modalités
  - NB : l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen)
- Anticiper les violations de données
  - la notification à CNIL doit être faite dans les 72 heures
  - aux personnes concernées dans les meilleurs délais.

Le plan d'action d'Econocom – **Documenter**

- La documentation relative aux traitements
  - Le registre des traitements
  - Les PIA
  - Les contrats ou cadres régissant les éventuels transferts hors UE

Le plan d'action d'Econocom – **Documenter**

- Concernant le devoir d'information des personnes
  - Les mentions d'information
  - Les modèles de consentement des personnes
  - Les procédures de mise en œuvre des droits des personnes

Le plan d'action d'Econocom – **Documenter**

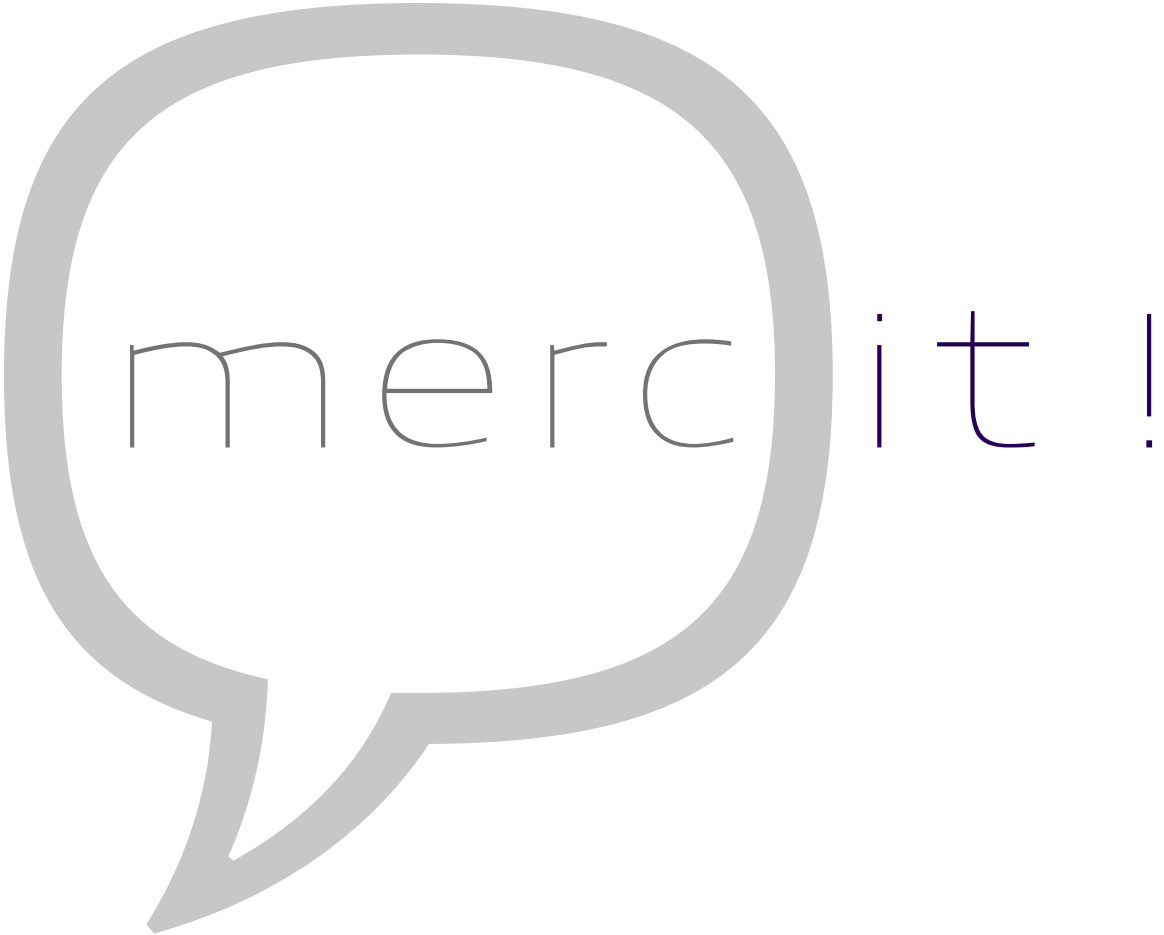
- Concernant les rôles et responsabilités
  - Les contrats de sous-traitance
  - Les procédures de gestion de crise en cas de violation des DCP
  - Les preuves de consentement

Les points d'attention

- Ne collecter que le strict nécessaire
- Les éventuels bases juridiques applicables au traitement
- Le consentement préalable à tout traitement (ou presque)
- Réviser régulièrement les documentations
- Mettre en place un suivi des sous-traitants et des contrats
- Bien anticiper l'exercice des droits des personnes
- Contrôler régulièrement les mesures de sécurité

Conclusion

- Le RGPD n'est pas une révolution mais est important sur 4 sujets :
  - le consentement préalable
  - le renforcement des droits des personnes
  - la coresponsabilité
  - La notification en cas d'incident
- Une démarche PDCA pour les DCP
- Les autorités de contrôle sont conscientes que 100% de conformité au 25 mai 2018 est illusoire. **En revanche, il faut un plan et que celui-ci soit démarré**


merc it !

econocom