

LES DONNÉES SENSIBLES DANS UN ENVIRONNEMENT HYBRIDE

Florent DELLA VALLE (CNIL)
David PASSANI (ANSSI)

Quelles sont mes données sensibles ?

Identification et catégorisation – hors données classifiées SECRETS, TRES SECRETS

Ce que dit la réglementation

- Doctrine d'utilisation de l'informatique en nuage **par l'État** du 31 mai 2023 [R9] – SREN article 31
- IGI1300 du 9 août 2021 : Diffusion Restreinte
- RGPD du 25 mai 2018 : Données à caractère personnel
- II 901 du 28 janvier 2015 : Diffusion Restreinte

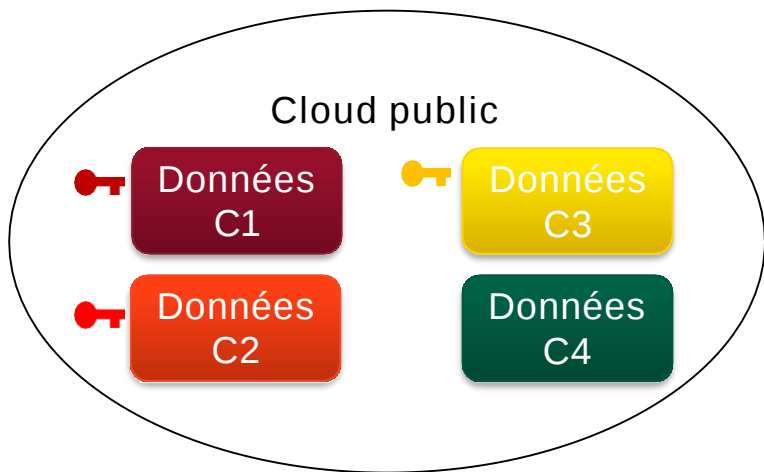
Mais il y a d'autres critères de sensibilité (ex. : secrets d'affaires, industriels, etc.)

Ce que vous devez faire

- Une échelle d'impact (humain, juridique, financier, opérationnel ou DIC)
- Des niveaux de sensibilité (critique, grave...) associés aux risques
- Un inventaire des données
- Une correspondance de la donnée avec un niveau de sensibilité et l'application des protections

Comment se protéger

L'illusion de la protection



- 🔑 Clé gérée dans votre organisation
- 🔑 Clé gérée par un tiers de confiance
- 🔑 Clé gérée par votre CSP

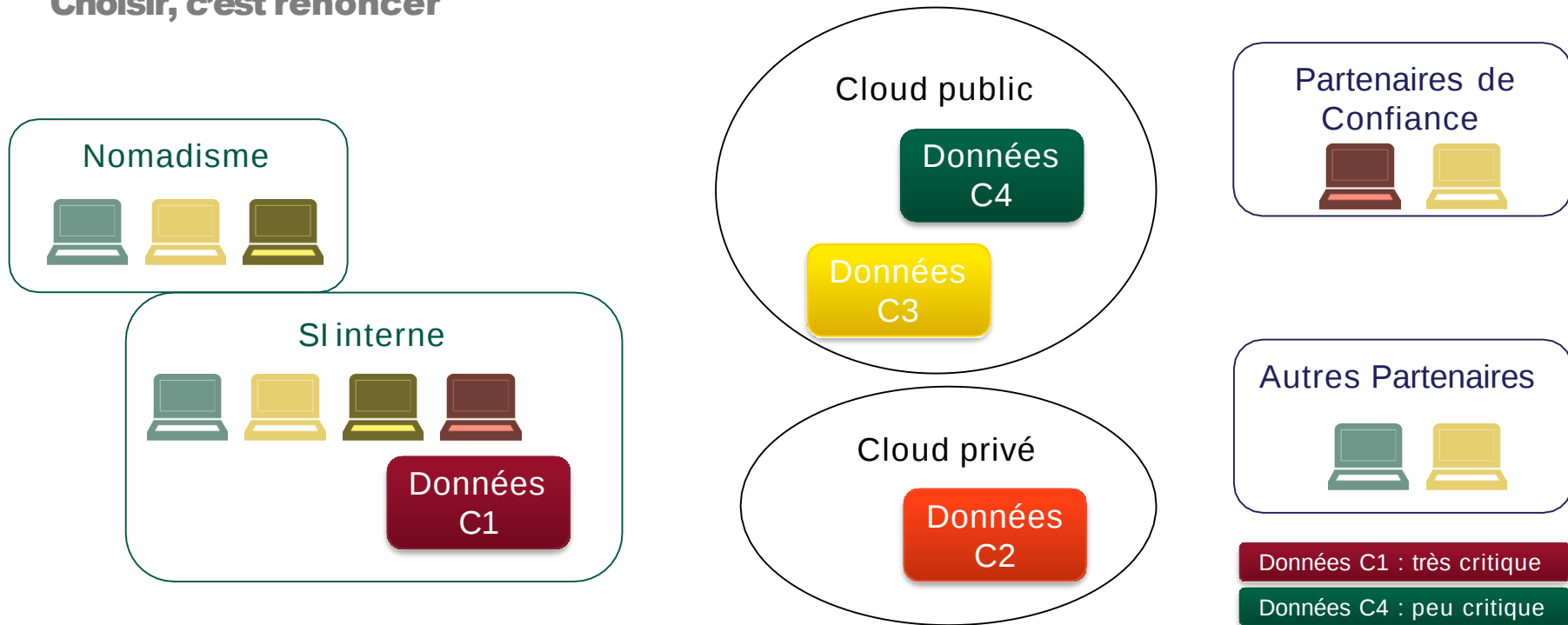
Données C1 : très critique

Données C4 : peu critique

Importance de l'analyse de risque et de l'évaluation du
risque après application des mesures de sécurité

Les données sensibles dans une infrastructure hybride

Choisir, c'est renoncer



Nos convictions

S'interroger au plus vite

Dans l'objectif d'avoir des SI

- **conformes aux réglementations**
- **à coûts maîtrisés**
- **résistants aux menaces**
- **en adéquation avec les besoins métiers**

1. **Ma gouvernance** en place est-elle satisfaisante ?
2. **Ma gestion des risques** est-elle à jour ?
3. **Mon organisation** est-elle à maturité ?
4. **La chaîne de mes sous-traitants** est-elle maîtrisée ?
5. **La relation avec mes tiers** est-elle sécurisante ?
6. **Ma gestion des incidents et de crise** est-elle opérationnelle ?

Mes mesures de sécurité sont-elles efficaces ?

Pour aller plus loin

La méthode EBIOS Risk Manager

<https://cyber.gouv.fr/la-methode-ebios-risk-manager>

Données et traitements sensibles

<https://cyber.gouv.fr/publications/donnees-traitements-sensibles>

Se protéger des fuites de données

<https://cyber.gouv.fr/publications/se-protger-des-fuites-de-donnees>

Recourir à des solutions cloud

<https://cyber.gouv.fr/recourir-des-solutions-cloud>

Sauvegarde des systèmes d'information

<https://cyber.gouv.fr/publications/sauvegarde-des-systemes-dinformation>

<https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation>

Recommandations relatives à l'authentification multifacteur et aux mots de passe

<https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe>

Donnée sensible : définition du RGPD

<https://www.cnil.fr/fr/definition/donnee-sensible>

Sécurité dans le cloud (fiche pratique)

<https://www.cnil.fr/fr/securite-cloud-informatique-en-nuage>

Chiffrement dans le cloud

<https://www.cnil.fr/fr/les-pratiques-de-chiffrement-dans-linformatique-en-nuage-cloud-public>

Outils de sécurisation d'applications dans le cloud et enjeux RGPD

<https://www.cnil.fr/fr/les-outils-de-securisation-dapplications-web-dans-linformatique-en-nuage-cloud>

Cloud et violation de données : un cas typique

<https://www.cnil.fr/fr/violation-du-trimestre-les-defauts-de-configuration-des-espaces-de-stockage-dans-le-cloud-public>



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

VOS QUESTIONS