THALES
Building a future we can all trust

DPO FORUM

# RGPD & Schrems-II = Souveraineté et protection de données

DPO Forum – Paris 5 April 2022
https://dpo-forum.eu/conferences-fr-2022/

Romain Deslorieux
Director, Strategic Partners
Thales – Cloud Protection division
Certified DPO PECB DATA PROTECTION OFFICER

cpl.thalesgroup.com

## Aujourd'hui, nous parlerons de

- lien entre souveraineté et protection de données
- mesures de protection spécifiques aux clouds

# Avec le cloud, protection des données et souveraineté sont intimement liées

# Souveraineté?

# La souveraineté et le RGPD

## DoctoLib

- Décision du Conseil d'Etat


## Google Analytics

- Décision du DPA Autriche
- Confirmé par la CNIL




Sources:
https://www.conseil-etat.fr
https://www.data-protection-authority.gv.at/
https://www.cnil.fr

# La souveraineté numérique est une problématique sociétale

**Governance**

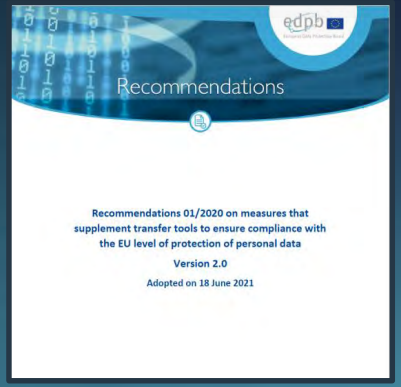
Gaia-X Data Sovereignty
+ Sovereign Cloud initiatives


**Risk**

US Executive Order on
**Nation's Cybersecurity**


**Compliance**

EU data privacy requires
User control over cloud assets




edpb.europa.eu/
whitehouse.gov/
gaia-x.eu/
thalesgroup.com/

# Pour faciliter sa mission, le DPO doit s'appuyer sur les challenges de souveraineté

# *Souveraineté numérique*, **qu**'èsaco?

# Souveraineté numérique & GRC - Gouvernance

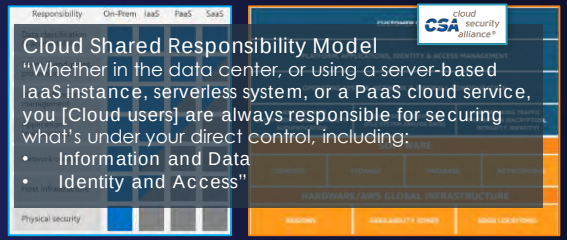
→ la Protection des Données s'inscrit dans une décision stratégique d'adoption et gouvernance du cloud

Cloud = ordinateur de quelqu'un d'autre

## Modèle de responsabilité partagée

Data & Access Security
=Users

CSP=
Infra/plt Security




Cloud Shared Responsibility Model
"Whether in the data center, or using a server-based IaaS instance, serverless system, or a PaaS cloud service, you [Cloud users] are always responsible for securing what's under your direct control, including:
- Information and Data
- Identity and Access"

# Souveraineté numérique & GRC - Risque

→ la Protection des Données est inhérente à une stratégie de sécurité dans le cloud (au-delà de la conformité)

Cloud = « peut induire des risques pour le SI et les données »

*ANSSI, Risques de l'Infogérance*

## Risques liés à la perte de contrôle

- Risque pour la confidentialité des données ;
- Risque juridique à cause de l'incertitude sur la localisation des données (en particulier pour les données à caractère personnel, le patrimoine scientifique et technique) ;
- Risques liés à la perte de maîtrise du système d'information (forte dépendance au prestataire quant aux choix techniques, incapacité à déceler et gérer les incidents) ;
- Risque de captati[illegible]

## Cyber assurance

Utilisation d'authentification forte vs ransomware


Data sovereignty
"Cryptographic products that implement encryption or tokenization are critical components for growing data residency risks"

Operational sovereignty
"CDPG is increasingly important to help reduce these risks by restricting access to data to specific staff, as well as potentially blocking access by the CSP."

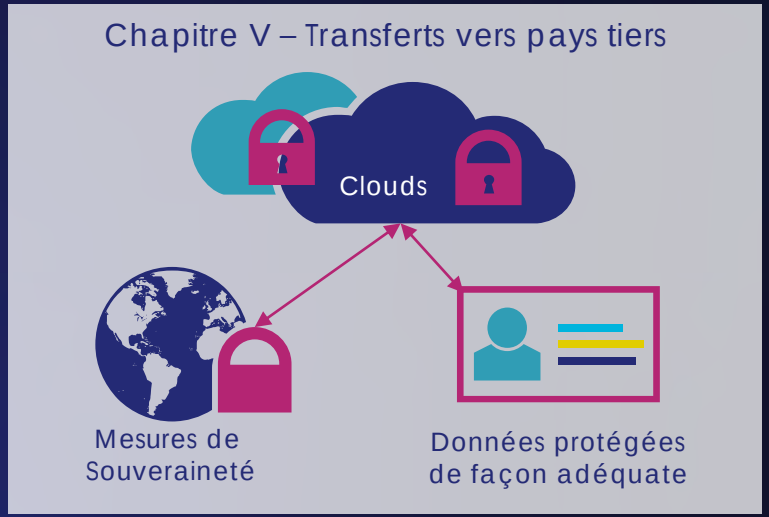
# Souveraineté numérique & GRC - Conformité

→ Le RGPD lui-même inclut des articles liés à des problématiques de souveraineté

"Privacy Shield Decision invalid on account of invasive US surveillance"

*EU, "Schrems-II"*

## Conformité & mesures de souveraineté

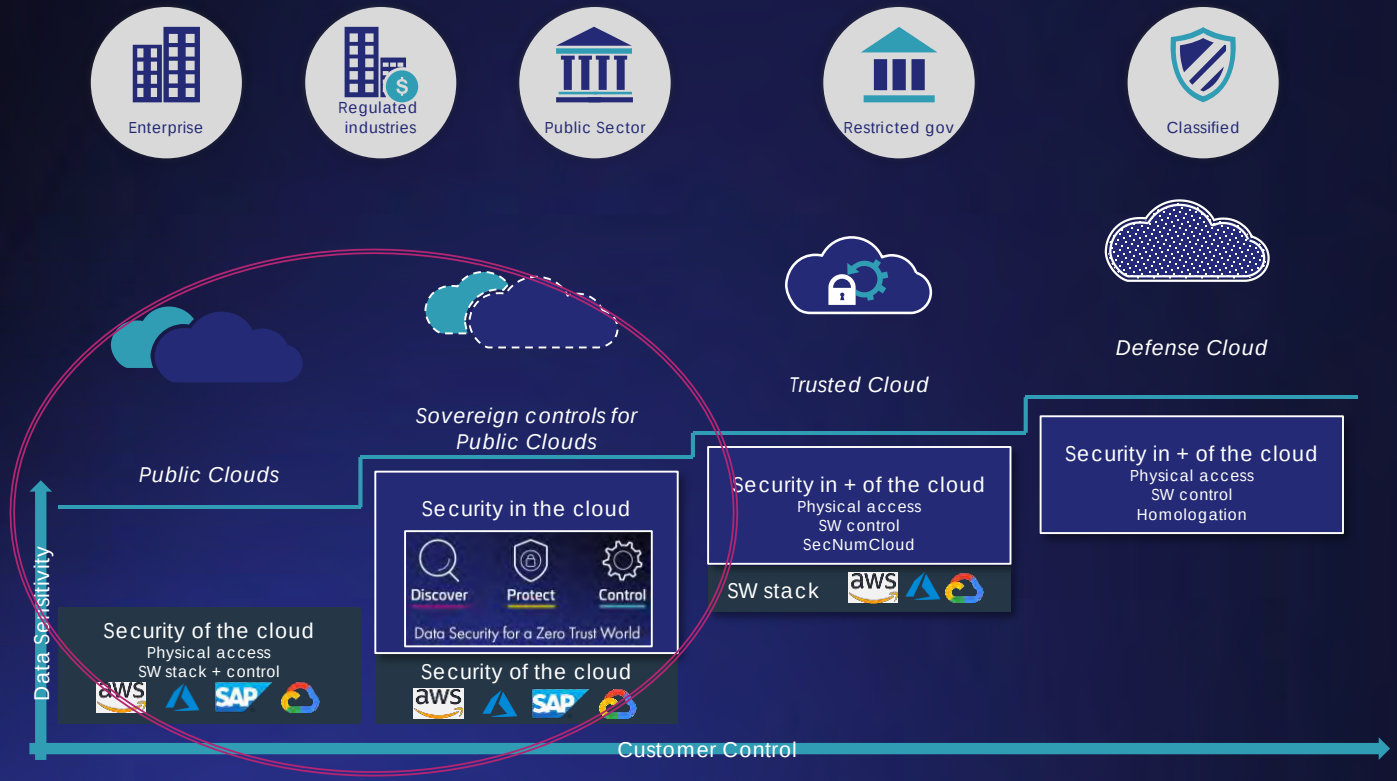


# Cloud, souveraineté, protection des données… quelles solutions?

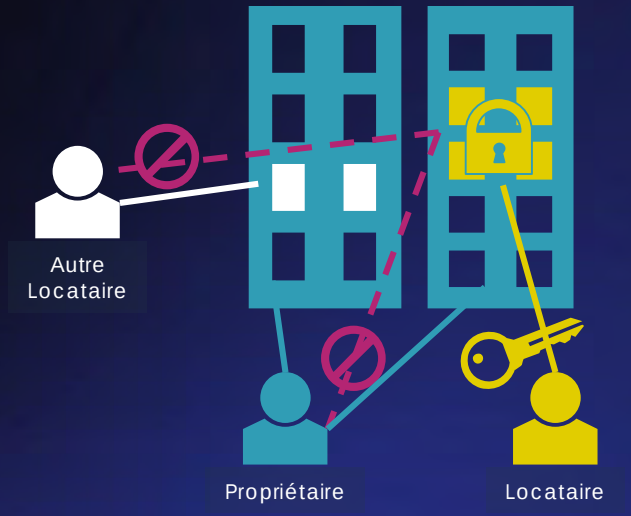


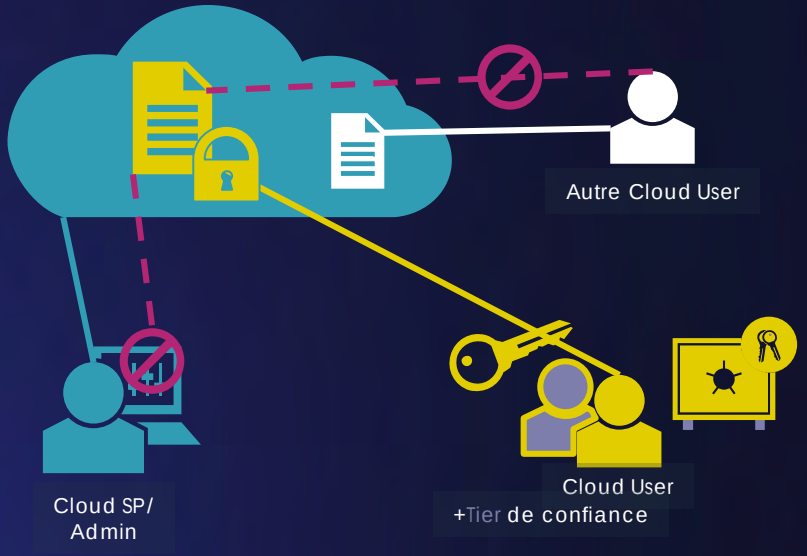
THALES
Building a future we can all trust

# Cloud & souveraineté – différents modèles

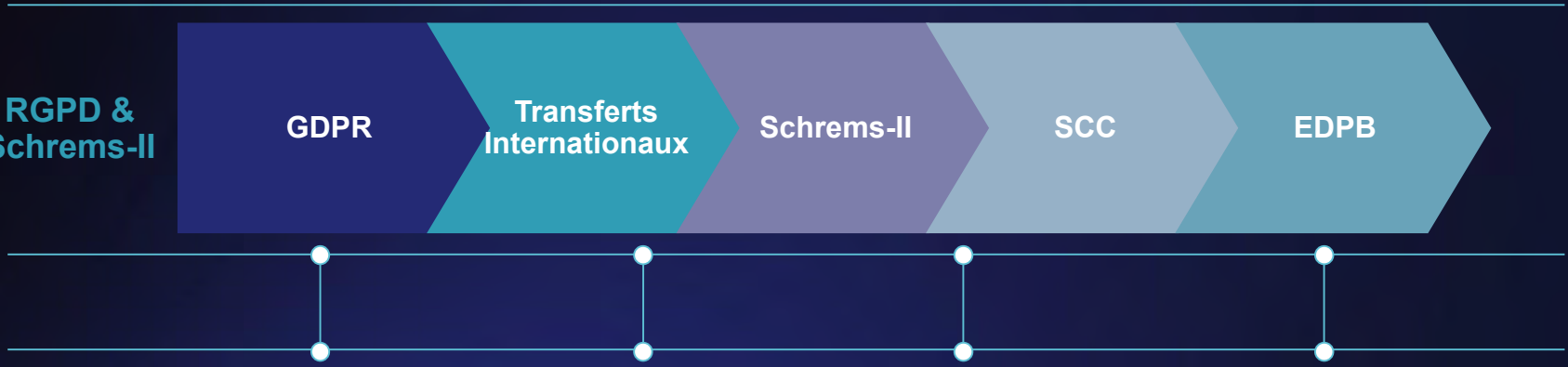


# Qu'est-ce qu'une "mesure tech. et org. de souveraineté"?



# RGPD et “Schrems-II” en 5 étapes




**En bref**

Les traitements doivent être évalués (Art 35), connus (Art 30). Les données doivent être protégées en termes de confidentialité, intégrité et disponibilité (Art 32).

Les transferts hors UE sont régulés (Chap V) et demandent des mesures supplémentaires pour des pays sans adéquation (Art 46).

Privacy Shield invalidé pour Art 46.2.a
Nouvelles SCC pour l’Art. 28, et mesures supplémentaires nécessaires pour transferts hors EU validées par autorité de contrôle (Art 46.2.d).

EDPB Recommandations pour l’Art46.2.d:

- 6 étapes dont:
- Déployer des mesures supplémentaires de protection

# Trans-Atlantic Data Privacy Framework

THE WHITE HOUSE

BRIEFING ROOM

FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework

MARCH 25, 2022 • STATEMENTS AND RELEASES

The United States and the European Commission have committed to a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union when it struck down in 2020 the Commission's adequacy decision underlying the EU-U.S.

European Commission - Press release

European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework

Brussels, 25 March 2022

The European Commission and the United States announce that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the *Schrems II* decision of July 2020.

The new Framework marks an unprecedented commitment on the U.S. side to implement reforms that will strengthen the privacy and civil liberties protections applicable to U.S. signals intelligence activities. Under the Trans-Atlantic Data Privacy Framework, the United States is to put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and

signals intelligence activities to ensure compliance with limitation

The Trans-Atlantic Data Privacy Framework reflects ma

between the U.S. and E.U. led by Secretary of Co

Justice Didier Reynders. It will provide a dur

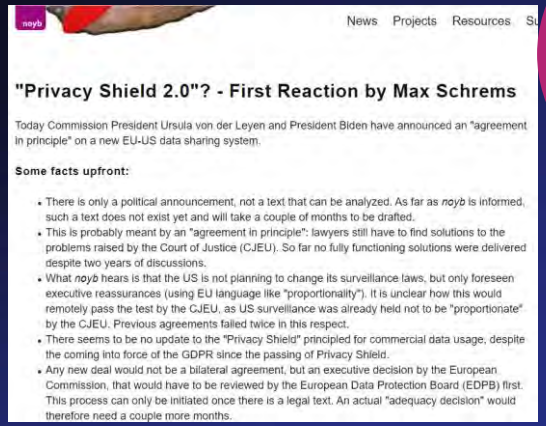
to protecting citizens' rights and enabli

including for small and medium ente

framework will promote an inclusi

companies of all sizes from all

- "The European Commission and the United States announce that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework"
- "It will address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020."



noyb News Projects Resources Su

"Privacy Shield 2.0"? - First Reaction by Max Schrems

Today Commission President Ursula von der Leyen and President Biden have announced an "agreement in principle" on a new EU-US data sharing system.

**Some facts upfront:**

- There is only a political announcement, not a text that can be analyzed. As far as *noyb* is informed, such a text does not exist yet and will take a couple of months to be drafted.
- This is probably meant by an "agreement in principle": lawyers still have to find solutions to the problems raised by the Court of Justice (CJEU). So far no fully functioning solutions were delivered despite two years of discussions.
- What *noyb* hears is that the US is not planning to change its surveillance laws, but only foreseen executive reassurances (using EU language like "proportionality"). It is unclear how this would remotely pass the test by the CJEU, as US surveillance was already held not to be "proportionate" by the CJEU. Previous agreements failed twice in this respect.
- There seems to be no update to the "Privacy Shield" principled for commercial data usage, despite the coming into force of the GDPR since the passing of Privacy Shield.
- Any new deal would not be a bilateral agreement, but an executive decision by the European Commission, that would have to be reviewed by the European Data Protection Board (EDPB) first. This process can only be initiated once there is a legal text. An actual "adequacy decision" would therefore need a couple more months.

?

- announcement, not a text that can be
- d solutions to the problems raised by the ). So far no fully functioning solutions were
- o years of discussions."
- not use a deal until it is formally passed, which nths."
- A decision can quickly be challenged with the European Court of Justice."
- "noyb expects to be able to get any new agreement that does not meet the requirements of EU law back to the CJEU within a matter of months"



Sources:
ec.europa.eu/commission/
whitehouse.gov/
nyob.eu/

# GDPR & EDPB – European Data Protection Board

GDPR Art 32 & Art 4

«**pseudonymisation**», pour que les données ne puissent plus être attribuées à une personne sans des **informations supplémentaires**, pour autant que ces informations supplémentaires soient **conservées séparément** et soumises à des **mesures techniques** et **organisationnelles**. »

Recommandations EDPB pour le transfert de données

"Vous devez **connaître où les données exportées** sont stockées ou traitées par le sous-traitant (plan des destinations)"

"les données sont **traitées avec du chiffrement** avant transmission, et l'**identité** du sous-traitant est vérifiée"

"les données sont chiffrées de bout en bout au niveau applicatif, avec des **méthodes de chiffrement à l'état de l'art**"

"Les clés sont **gérées de manière fiable** (générées, administrées, stockées, **liées à des identités** autorisées, et révoquées)

"les clés restent **sous contrôle du seul responsable** du traitement"


Connaître vos données

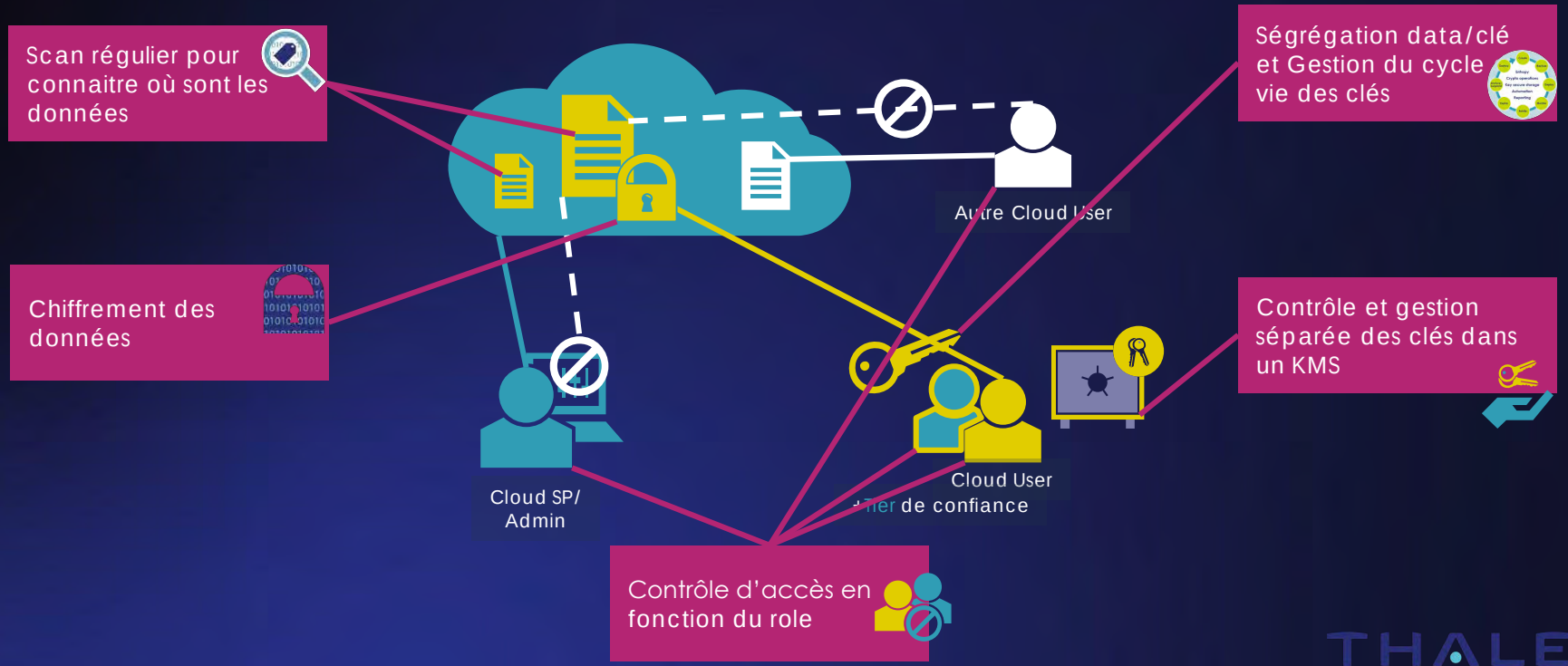

Chiffrer vos données


Appliquer des règles **d'accès basées sur l'Id**


Gérer le cycle de vie des clés


Garder seul le contrôle des clés

# EDPB: mesures techniques et organisationnelles de souveraineté



# Illustration / Jurisprudence

## DoctoLib / Conseil **d'Etat**

- application directe de l'EDPB
- DoctoLib peut utiliser AWS grâce à des mesures supplémentaires techniques de protection des données, telles que recommandées par l'EDPB



**Conseil d'Etat / DoctoLib**

« Doctolib a également mis en place un dispositif d
**sécurisation des données** hébergées par la socié
AWS Sarl reposant sur un tiers de confiance situé e
France afin d'empêcher la lecture des données par
des tiers. »

## Google Analytics / DPA Autriche

- Application directe de l'EDPB
- Google Analystics ne peut plus être utilisé car les clés de chiffrement, sous contrôle de Google, sont donc aussi soumis à FISA
- confirmé par la CNIL en France


**'Etat / DoctoLib**

le a adopté des mesures supplémentaires,
e suffisent pas à exclure la possibilité
es services de renseignements américains
à ces données. »

Sources:
https://www.conseil-etat.fr
https://www.data-protection-authority.gv.at/
https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure

# Souveraineté & GDPR – Entreprise, DPO, RSSI

| Challenges de souveraineté pour **l'entreprise** | Challenges RGPD pour le DPO (entre autres!) | Mesures techniques et organisationnelles. Actions avec le RSSI |
|---|---|---|
| **Gouvernance/Gestion des risques**<br>Limiter impact en cas de brèche.<br>• Impact financier: amendes, rançons, assurance cyber<br>• Image de marque/relation client<br><br>**Souveraineté opérationnelle**<br>• ZeroTrust<br>Architecture cyber appliquée sur les actifs digitals (données, app) et basée sur l'identitéplutôt que l'infra/réseau/cloud.<br>• Shadow IT<br>Maitriser l'utilisation de ressources IT dans le cloud.<br><br>**Souveraineté des données**<br>• Cloud Shared Responsibilty Model<br>Dans le cloud, la protection des données et le contrôle d'accès et d'identités est la resp de l'utilisateur, pas du CSP | **Approche systématique:**<br>Protection par chiffrement pour CIA des données, tout le temps et qqsoit l'infrastructure.<br>Art 25 – Sec par conception & défaut<br>Art 30 – Registre<br>Art 32 – Sécurité du traitement<br>Art 35 – Analyse d'impact<br>Art 45/6 – Transferts<br><br>**Gestion d'une brèche:**<br>Impact réduit fortement si mesures tech et org auditables, rendant les données « incompréhensibles » et/ou inaccessibles.<br>Art 33 – Notif au régulateur<br>Art 34 – comm aux personnes<br>Art 83 – amendes | **Connaitre les données et traitements**<br>• Les data dans le cloud sont-elles automatiquement scannées et systématiquement rapportées? (« data discovery & classification »)<br><br>**Protéger les données**<br>• Les data sont-elles chiffrées dans le cloud? (« BYOE »)<br>• Les clés sont-elles dans un gestionnaire de clés (key manager) externe/séparé? (« BYOK »)<br>• L'accès aux data/clé est-il basé sur l'identité? pour meilleur traçage et granularité?<br>• L'accès aux applications cloud notamment est-il protéger par de l'authentification forte (« MFA »)? |

GDPR Art 4.5 et Art 32- Pseudonymisation vs Chiffrement?
La **pseudonymisation** est l'objectif.
Le **chiffrement** avec séparation des clés, la **tokenisation** avec séparation du vault de tokens, sont des *mesures techniques* pour y parvenir.

# Résumé

Contactez nous!
Romain.Deslorieux@thalesgroup.com
linkedin.com/in/romaindeslorieux/

THALES
Building a future we can all trust

Discover Protect Control

Data Security for a Zero Trust World

## Souveraineté & Cloud

Souveraineté des données et opérationnelle GRC du cloud Gestion des risques

## GDPR & Cloud

Know your data

Encrypt your data


Manage key life cycle

Full control of keys

Identity-based access control

## Thales: contrôles de souveraineté

- Connaitre vos data et transferts
  - CipherTrust Data Discovery and Classification
- Protéger vos data
  - CipherTrust Data Encryption and Tokenisation
  - High Speed Encryptor
- Contrôler vos data et vos clés
  - CipherTrust Manager
  - CipherTrust Cloud Key Manager
  - Luna Hardware Security Module
  - Safenet Trusted Access

# References

European Institutions
European Council = heads of EU member states
European Commission = the government of the EU, selected by EU Parliament
European Parliament = the elected assembly of the EU
European Court of Justice = the court of justice of the EU

## References to European Institutions

- Ref A: GDPR official text (general data Protection Regulation)
  - Source: European Parliament and Council of Europe
  - https://eur-lex.europa.eu/eli/reg/2016/679/oj
- **Ref B : Concept of "adequacy"** for transfer of data to international organisations
  - Source: European Commission
  - https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- Ref C: Schrems-II decision of the CJEU
  - Source: Court of Justice of the European Union
  - https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1292116
- Ref D: EDPB recommendations
  - Source: European Data Protection Board (overall EU data privacy supervisory authority)
  - https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
- Ref E: Standard Contractual Clauses (SCC)
  - Source: European Commission
  - https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

## Thales literature for further reading

- Thales Cloud Security solutions
  - https://cpl.thalesgroup.com/resources/thales-data-protection-portfolio-brochure
- Thales GDPR & Schrems-II microsite and eBook
  - https://cpl.thalesgroup.com/compliance/emea/schrems-ii
  - https://cpl.thalesgroup.com/resources/compliance/data-security-compliance-and-regulations-ebook