



FEDERALE OVERHEIDSDIENST
MOBILITEIT EN VERVOER



Mobilité autonome en confiance : Privacy & Cyber comme leviers d'innovation ?

Oya Tanil



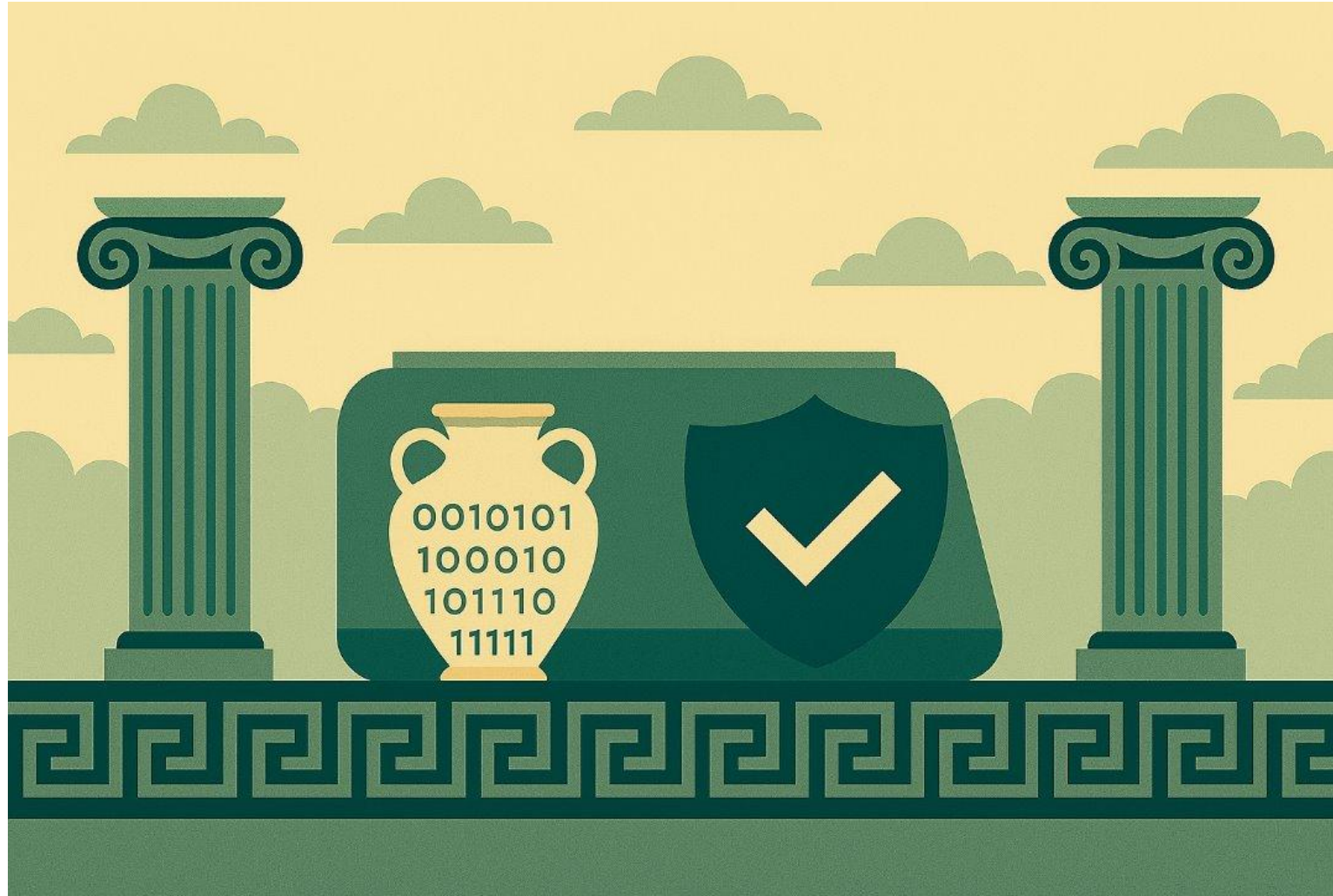
Au programme

- Petite histoire en guise d'introduction
- Flux de données dans les véhicules autonomes
- Risques en matière de cyber et privacy
- Mesures de protection & Mitigation
- Conclusion & Recommandation





Petite histoire d'Olympe numérique



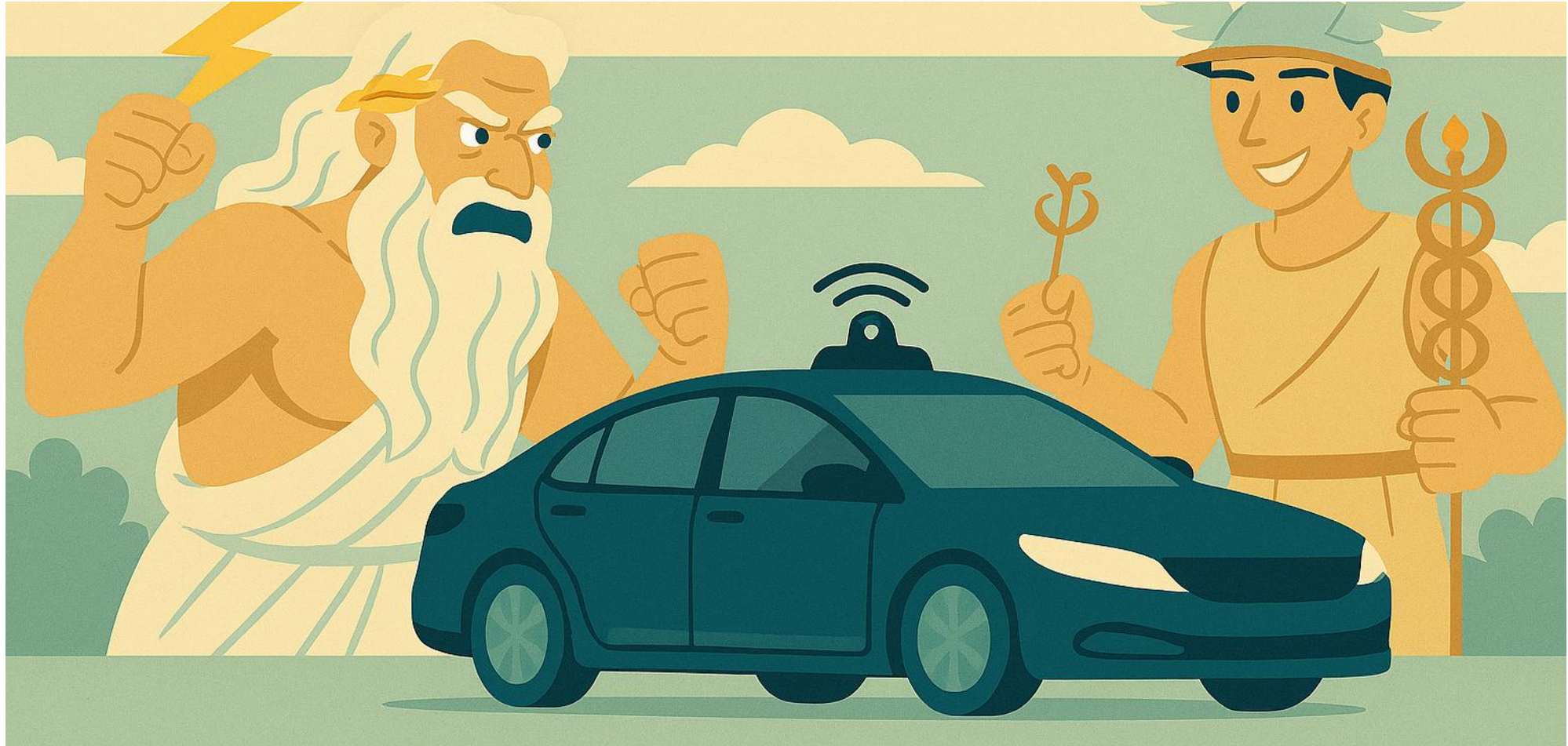


Chapitre 1: Les dieux descendent sur Terre





Chapitre 2: Les tentatives de sabotage





Chapitre 3: La bataille des données





Chapitre 4: Le pacte de l'Olympe numérique







Liste non exhaustive de flux des données

Capteurs et actionneurs

Networks et protocoles

Algorithmes

Composants de confort

Fonctions du véhicule

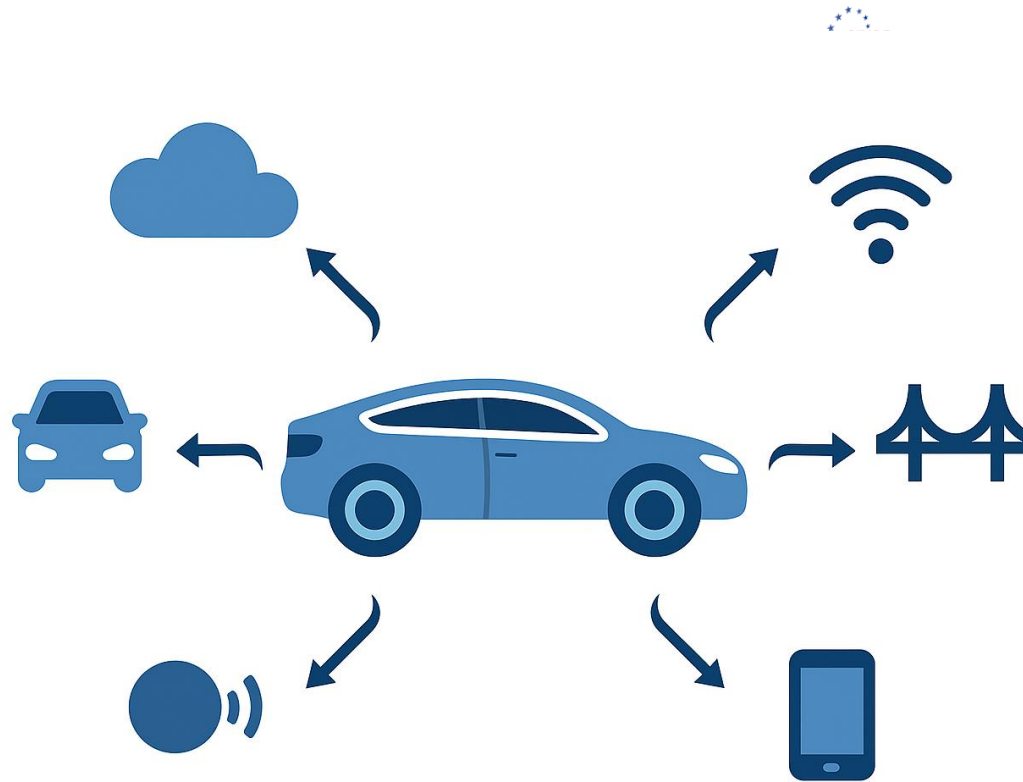
Composants externes

Cloud computing

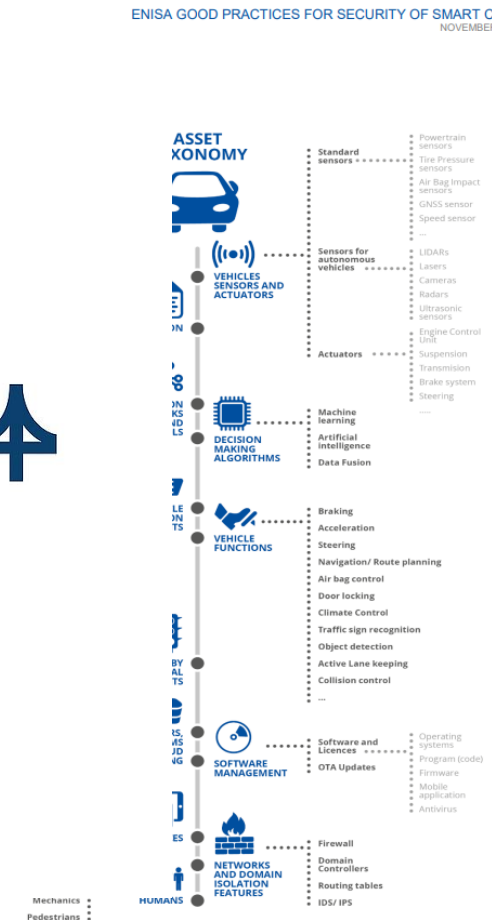
Software management

Device management

Facteur humain







ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS
NOVEMBER 2019





Liste des risques cybersécurité/sécurité

Menaces	Risques de cybersécurité
Attaque <i>Man in the middle</i>	Interception ou modification des messages entre le véhicule et l'infrastructure
Divulgation ou altération d'information	Trajets, paramètres ou données internes rendus visibles ou modifiés
Manipulation des données serveurs / Perturbation des communications	Le véhicule reçoit des informations essentielles (trafic, mises à jour...)
<i>Data replay</i>	Anciennes données réinjectées pour tromper le véhicule
Vulnérabilités chez le constructeur	Empêchement des mises à jour de sécurité
Dommages involontaires	Composants logiciels remplacés par erreur
Changement involontaire de données/composants	Composants logiciels remplacés par erreur
DDOS	Services de communication indisponibles
Manipulation des données	Services de communication indisponibles
 Véhicule malveillant	Services de communication indisponibles
 <i>Spoofing</i> des capteurs	Services de communication indisponibles
 Brouillage radio	Services de communication indisponibles
 GPS <i>spoofing</i>	Services de communication indisponibles
Pannes de service	Services de communication indisponibles
Sabotage des panneaux ou unités routières	Services de communication indisponibles
Altération de système de back-up	Services de communication indisponibles
Vol ou usurpation d'identité	Services de communication indisponibles

N'oublions pas le contexte géopolitique 😊



Risques concernant la protection des données personnelles

Exemples de risques privacy

Suivi des déplacements

Profilage comportemental

Surveillance accrue par capteurs

Risque de fuite ou vol de données personnelles

Utilisation secondaire des données au-delà des finalités

Corrélation avec d'autres bases de données

Partage de données excessif et abusif, notamment vidéos enregistrées (à l'extérieur)

Les risques varient en fonction des cas d'usage.

Notamment en cas de traitement de données biométriques



Mesures de protection en fonction de risques

Mesures techniques

Outils d

Seg

Security by design
Privacy by design

S

Ge

Monitoring et test

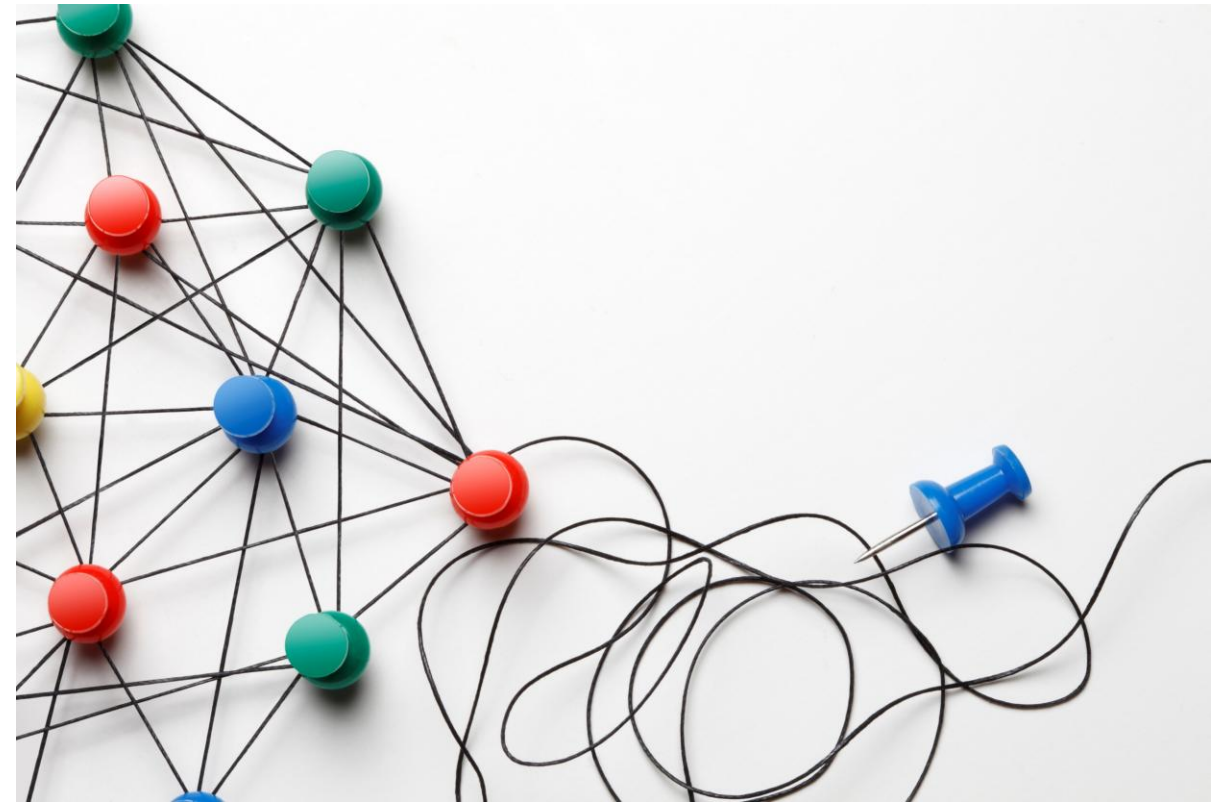
Anonymisation & Pseudonymisation





Rôle des autorités publiques ?

- Importance de l'analyse des risques et des mitigations
- Monitoring des rapports et des analyses de risques
- Sensibilisation des parties prenantes
- Responsabilisation des parties prenantes
- Intégration et promotion des principes « dès la conception et par défaut » de sécurité de l'information
 - Privacy by design
 - Security by design
- Conformité au cadre réglementaire existant: GDPR, NIS2, ITS, etc.
- Impact (potentiel) de nouvelles législations
 - CRA + CSA + Data Act + Data Gouvernance Act

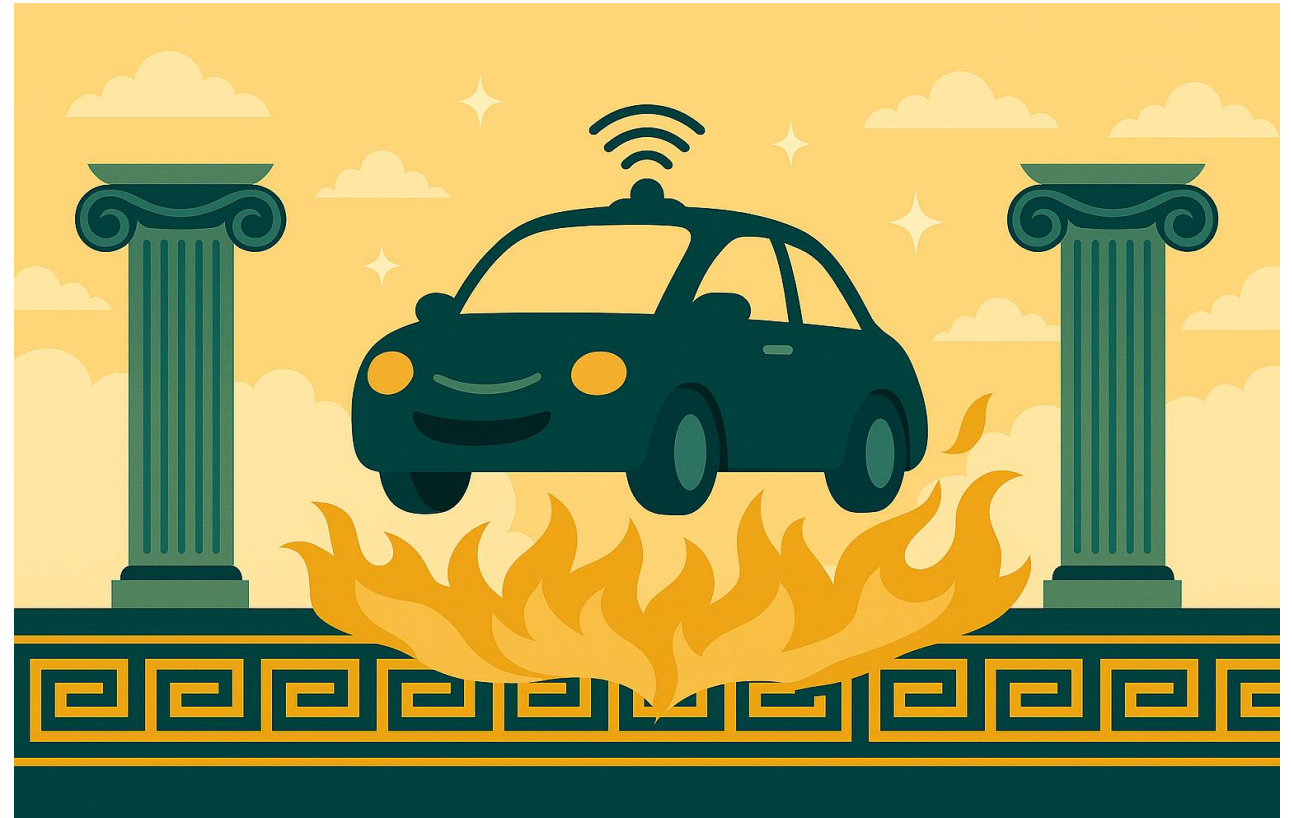




Conclusion

La cybersécurité et la *privacy* donnent la confiance nécessaire à l'innovation pour prendre de l'élan.

Ne faisons pas de la conformité une case à cocher, mais un levier pour sécuriser, améliorer et innover.





Merci pour votre attention

