L'utilisation de services basés sur le cloud

Points d'attention au regard des règles de protection des données personnelles

Conférence organisée par la Chambre de commerce de Luxembourg, 24 avril 2023

Mickaël Tome
Togouna & Tome Avocats

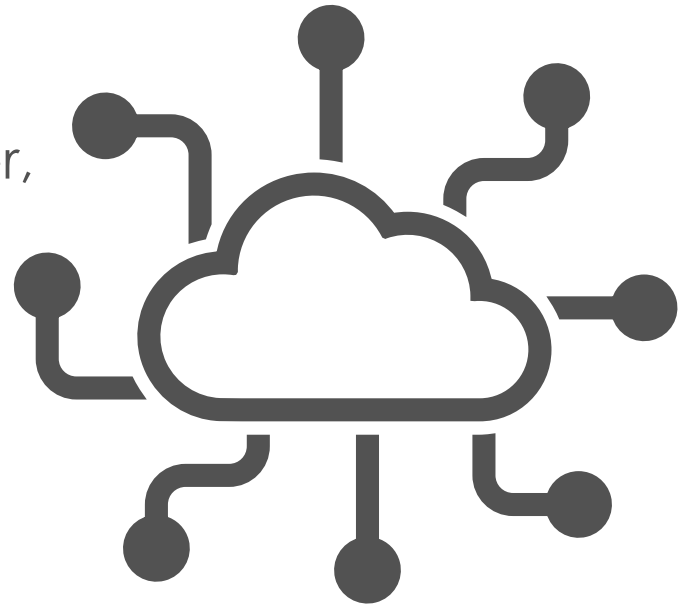
ENJEUX ET RISQUES LIÉS AU CLOUD

- Un outil essentiel pour gagner en efficacité et en coûts
  - Une transformation des opérations informatiques (digitalisation, externalisation)
  - Un instrument privilégié de la transformation numérique des entreprises

- Dépendance des organisations aux systèmes d'information et aux données personnelles

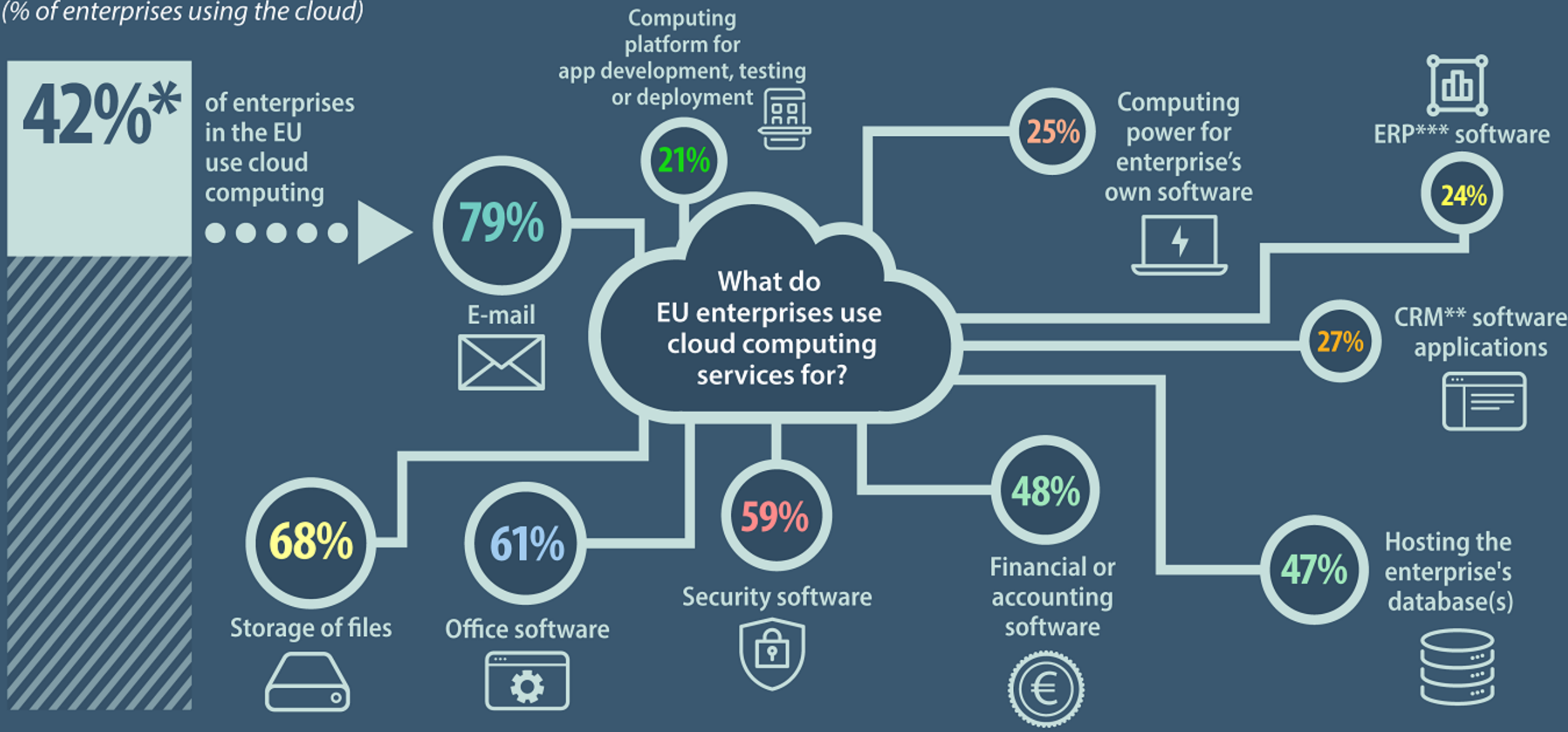
- Cyber-risque

- Environnement réglementaire complexe
  - Protection des données personnelles
  - Règlementations sectorielles (cybersécurité, secteur financier, communications électroniques…)



Use of cloud computing services in EU enterprises in 2021, by type of service

(% of enterprises using the cloud)



*Poland: data temporarily not available. As a result, the EU aggregate has been estimated.

**Customer Relationship Management (CRM)

*** Enterprise Resource Planning (ERP)

DÉFIS CONTEMPORAINS

- Analyse d'impact
- Rôle des parties
- Négocier des contrats sur mesure
- Chaîne de sous-traitance
- Transferts internationaux
- Accès par des gouvernements étrangers
- Télémétrie
- Audit

Pour plus de détails
cf. CEPD, *Coordinated Enforcement Framework Report, Use of cloud-based services by the public sector*, 17 janvier 2023

QUELLES PRÉCAUTIONS PRENDRE?

DONNEES & TRAITEMENTS

Identifier clairement les données et les traitements qui passeront dans le cloud

SECURITE TECHNIQUE & JUR.

Définir ses propres exigences de sécurité technique et juridique.

ANALYSE DES RISQUES

Conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise

CHOIX DU CLOUD PERTINENT

Identifier le type de Cloud pertinent pour le traitement envisagé

CHOIX DU PRESTATAIRE

Choisir un prestataire présentant des garanties suffisantes

SECURITE ORGANISATIONNELLE

Revoir la politique de sécurité interne

EVOLUTIONS

Surveiller les évolutions dans le temps

CONTRAT

Eléments essentiels devant figurer dans un contrat de prestation de services de cloud

Pour aller plus loin

- CNIL, Recommandations 'Cloud computing', 2012
- A29WP, Avis 05/2012 sur le Cloud computing', WP 196, 2012

SÉLECTION DU PRESTATAIRE DE CLOUD ET ANALYSE DES RISQUES

- Une obligation pour l'organisation responsable du traitement qui souhaite recourir aux services d'un prestataire de cloud

- Lorsqu'un traitement doit être effectué pour le compte de l'organisation responsable du traitement, faire uniquement appel à des sous-traitants qui présentent des garanties suffisantes (mesures techniques et organisationnelles, protection des droits des personnes)

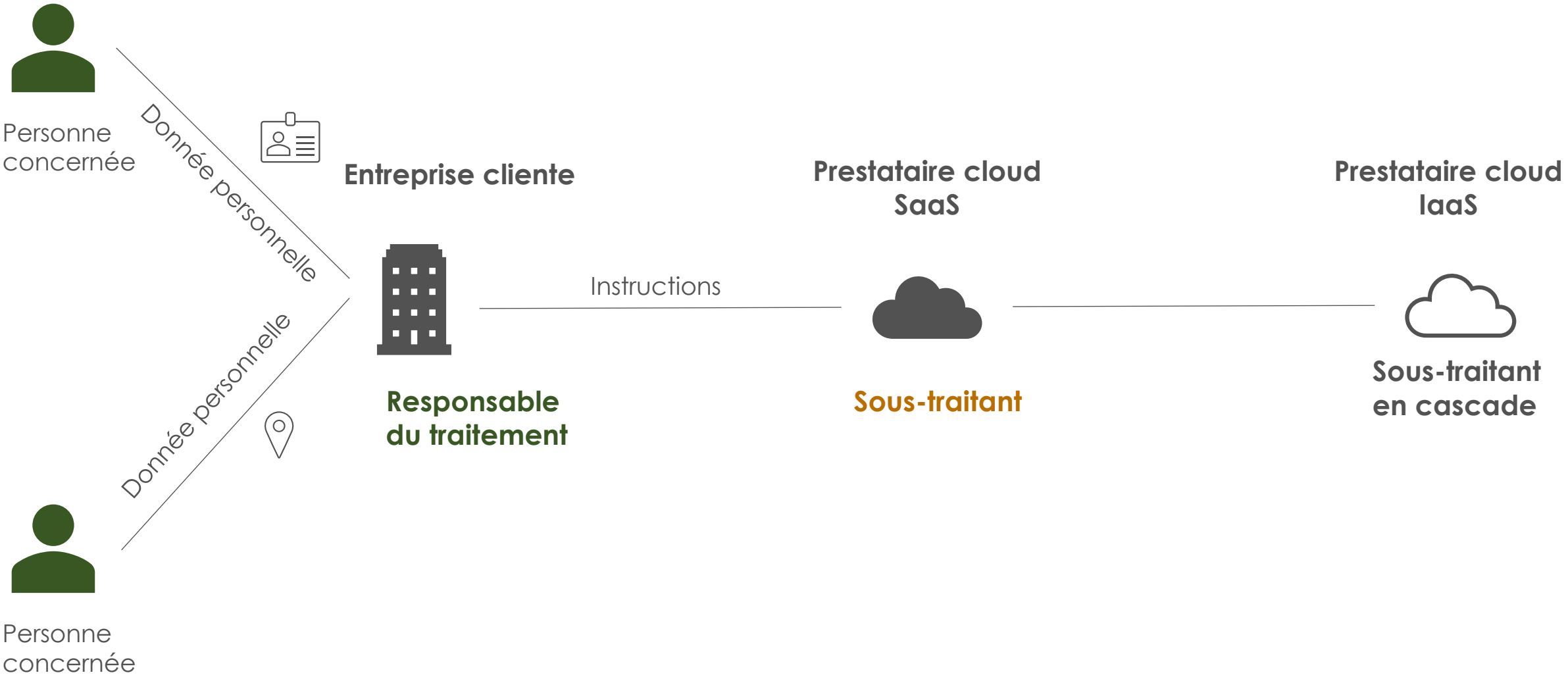
→ Evaluer les risques en tenant compte du type de traitement confié au sous-traitant

En pratique

L'organisation responsable du traitement doit gérer les risques liés à l'intervention des prestataires de cloud:

- Définir des exigences en matière de protection des données
- Vérifier le niveau de protection des données et de sécurité offert par un potentiel prestataire de cloud (en amont)
- Définir et suivre une procédure d'exécution des contrats avec ces prestataires
- Définir et mettre en œuvre un processus d'évaluation des risques de protection des données liées au prestataire de cloud

RÔLES ET RESPONSABILITÉS



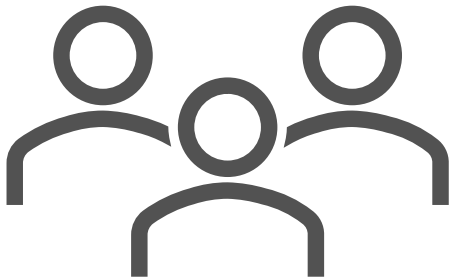
DÉTERMINER CLAIREMENT LES RÔLES ET RESPONSABILITÉS

- S'agissant des traitements pour lesquels le prestataire de cloud agit en sous-traitant:
  - ➢ s'assurer qu'il agit uniquement pour le compte et conformément aux instructions documentées du responsable de traitement
  - ➢ s'assurer que l'on peut s'opposer efficacement à ce qu'il recourt lui-même à d'autres sous-traitants (maîtriser la chaîne de sous-traitance)
  - ➢ s'assurer que la procédure d'engagement de prestataires envisage déjà toutes les exigences permettant d'être conforme au RGPD
  - ➢ Analyser minutieusement le contrat et si nécessaire renégocier

- Identifier tout traitement que le prestataire de cloud effectue en qualité de responsable de traitement indépendant

En pratique

- Certaines situations de déséquilibre des pouvoirs
- Les qualifications retenues dans les contrats peuvent être trompeuses
- Risques d'incertitudes entre les parties → étendue de l'assistance apportée par le sous-traitant (exercice des droits, analyse d'impact…), capacité à faire face à des cas violations de données personnelles



ÉVALUER LE NIVEAU DE PROTECTION ASSURÉ PAR LE PRESTATAIRE DE CLOUD

- Obligation pour les sous-traitants de mettre à disposition toutes les informations nécessaires pour permettre au responsable du traitement de démontrer sa conformité

- L'organisation responsable du traitement est supposée connaître et maîtriser:
  - les traitements effectués par le prestataire de cloud
  - les garanties mises en œuvre par le prestataire
  - la localisation des données et les transferts éventuels
  - la sécurité des données
  - la chaîne de sous-traitance éventuelle (sous-traitance en cascade)

En pratique

- Insuffisance de transparence de la part des prestataires de cloud (condition de fourniture du service, sécurité, transferts…)
- Déterminer les mesures techniques et organisationnelles appropriées au terme d'une évaluation des risques préalable et ne pas se reposer uniquement sur les analyses de risques faites par les prestataires de cloud
- Privilégier les sous-traitants adhérant à des codes de conduite (CISPE, EU Cloud CoC) ou ayant obtenu une certification pertinente

QUELLES SONT LES OBLIGATIONS EN MATIÈRE DE SÉCURITÉ?

- Tendance: standardisation des offres de cloud (absence de cahier des charges particulier)

- Obligation pour le responsable du traitement de définir ses propres exigences de sécurité
  - Aspects techniques (interopérabilité avec un système existant…)
  - Aspects organisationnels (disponibilité, portabilité…)

- Des mesures techniques et organisationnelles appropriées déterminées en fonction des risques, ce qui peut inclure → pseudonymisation, chiffrement, authentification multi-facteur, contrôle d'accès des employés, audits périodiques…

- Hypothèses de violation de données
  - Organisation cliente (responsable de traitement): notifier au régulateur dans les meilleurs délais et si possible dans les 72h au plus tard (sauf en l'absence de risque)
  - Prestataire de cloud (sous-traitant): signaler toute violation de données à ses clients dans les meilleurs délais

UN ENCADREMENT CONTRACTUEL NÉCESSAIRE

- Un encadrement contractuel imposé
  - dans la majorité des cas, un contrat (des clauses) de sous-traitance (art. 28 du RGPD)
  - dans des situations plus exceptionnelles, un contrat de coresponsabilité (art. 26 RGPD)

- Une obligation pour le prestataire de cloud et ses clients

- En théorie, le contrat doit être négocié et taillé sur mesure par rapport aux opérations de traitement

En pratique

- Le contrat est souvent rédigé de manière unilatérale par le prestataire de cloud en tant que sous-traitant (contrat d'adhésion)…
- … mais l'organisation responsable du traitement n'est pas exemptée de sa responsabilité
- Un gage important de la conformité et de la maturité en matière de gestion de la protection des données
- Contractualiser avant la mise en œuvre du traitement

SUPERVISION DU PRESTATAIRE DE CLOUD

- Effectuer des vérifications sur le niveau de protection des données et de sécurité offert par les prestataires de cloud existants
  - Obligation pour les sous-traitants de permettre la réalisation d'audits
  - Vérifications de l'exactitude des informations fournies ou détenues par le prestataire de cloud
  - Vérifications de la conformité aux exigences définies dans le contrat
  - Contrôle de l'effectivité des mesures techniques que le prestataire de cloud s'est engagé à mettre en œuvre
- Définir et mettre en œuvre une procédure pour traiter les cas de non-conformité aux contrats
- Vérifier les risques nouveaux ou évolutifs en matière de protection des données liés aux contrats à long terme

LE DÉFI MAJEUR DES TRANSFERTS INTERNATIONAUX

- Un défi majeur depuis l'invalidation du *Privacy Shield* (*Schrems II*)

- Nombre de prestataires de cloud opère au-delà des frontières nationales et utilisent des infrastructures techniques dans de multiples *data centers*.

- Rappel des obligations
  - Recenser et tenir un inventaire des transferts
  - Documenter les mécanismes de transfert utilisé pour les transferts:
    - Décision d'adéquation
    - Garanties appropriées: clauses contractuelles types, règles d'entreprise contraignantes(*BCR*), respect d'un code de conduite/certification…
    - Dérogations de l'art. 49 RGPD (consentement, contrat…)
  - Évaluer l'efficacité du mécanisme de transfert envisagé par rapport à la loi du pays de destination et mettre en place des mesures supplémentaires si nécessaire

- Un choix difficile à opérer en pratique: quelles sont les options?

POINTS D'ATTENTION

Merci pour votre attention !

Mickaël Tome – Avocat à la cour
Togouna & Tome Avocats
mickael@togouna-tome.eu
(+352) 2820 8913