LE 4ÈME PRINTEMPS DU RGPD A LA REUNION

SHEO TECHNOLOGY
VOTRE PRESTATAIRE EN SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

MERCREDI 25 MAI 2022

Dina Morgabine

absys
Les données bien ordonnées

Le programme de cette matinée de partage

Accueil
Quelques chiffres importants de l'année 2021
Thématiques et contrôles CNIL
Comment démarrer son projet RGPD?
Le transfert de données dans la zone océan Indien
Le métier de DPO
Clôture

SHEO TECHNOLOGY
VOTRE PRESTATAIRE EN SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

absys
Les données bien ordonnées

Dina Morgabine

Chafik MOHAMED

- Consultant et formateur en sécurité informatique, cybersécurité et RGPD – RSSI et DPO externe
- 25 ans d'expériences dans l'IT (systèmes, réseaux, cloud)
- Membre de l'APAC, CLUSIR-OI
- Organisateur du Sheo-tech Days (évènement de sensibilisation à la sécurité Informatique, cybersécurité et RGPD): prochaine édition en octobre 2022
- Plusieurs certifications dans le Domaine de la sécurité info et protection des données

PECB Délégué à la protection des données certifié conformément au référentiel de certification des compétences du DPO de la CNIL

Microsoft 365 CERTIFIED SECURITY ADMINISTRATOR ASSOCIATE

PECB ISO/IEC 27001 Lead Implementer

PECB ISO/IEC 27001 LEAD AUDITOR

SHEO TECHNOLOGY

absys Les données bien ordonnées

Dina Morgabine

Quelques chiffres importants de l'année 2021

Prenez votre smartphone et allons sur:

https://kahoot.it/

SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Jean-François TARDIF

- **Consultant en protection des données / DPO externe / consultant SI ERP CRM**
- **Associé/Gérant d' ABSYS ORGANISATION CONSEIL (A.O.C)**

absys
Les données bien ordonnées

SHEO TECHNOLOGY

Dina Morgabine

Thématiques et stratégie de contrôle de la CNIL

absys
Les données bien ordonnées

SHEO TECHNOLOGY

Thématiques et stratégie de contrôle de la CNIL

- 2018 :
  - Les Traitements des données liées au recrutement;
  - Les Pièce justificatives demandées par les agences immobilières aux candidats à la location;
  - les traitements relatifs à la gestion des services de stationnements payants réalisés au moyen d'équipements connectés.
- 2019 : +
  - Le respect des droits des personnes;
  - Le traitement des données des mineurs;
  - La répartition des responsabilités entre responsable de traitements et sous-traitants.
- 2020 :
  - La sécurité des données de santé;
  - Mobilités et services de proximité, les nouveaux usages des données de géolocalisation;
  - Le respect des dispositions applicables aux cookies et autres traceurs.

SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Thématiques et stratégie de contrôle de la CNIL

- 2021 :
  - La cybersécurité du web français;
  - La sécurité des données de santé;
  - Le respect des règles applicables aux cookies et autres traceurs.
- 2022 : +
  - La prospection commerciale;
  - Les outils de surveillance dans le cadre du télétravail;
  - L'utilisation de l'informatique en nuage (cloud).

SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Thématiques et stratégie de contrôle de la CNIL

FOCUS SUR 2022

- La prospection commerciale;
  - la CNIL a publié, en février 2022, un nouveau référentiel « gestion commerciale », encadrant notamment la réalisation d'actions de prospection commerciale et qui était accompagné de nombreuses ressources pour guider les acteurs dans leur mise en conformité.
    - **La prospection commerciale par courrier postal et appel téléphonique**
    - **La prospection commerciale par courrier électronique**
    - **La prospection commerciale par SMS-MMS**
    - **La prospection commerciale par automates d'appel**
    - **La prospection vers les particuliers (B to C) quelles règles pour transmettre des données à des partenaires ?**
    - **La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial**
    - **Comment utiliser une liste repoussoir pour respecter l'opposition à la prospection commerciale**

SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Thématiques et stratégie de contrôle de la CNIL

FOCUS SUR 2022

- Les outils de surveillance dans le cadre du télétravail;
  - la période COVID19 à amené à aborder désormais le télétravail sous deux angles en période normal ou en période sanitaire
    - **Quelles sont les conditions de mise en place du télétravail**
    - **L'employeur peut-il contrôler l'activité des salariés en télétravail ?**
    - **L'employeur peut-il surveiller constamment ses salariés ?**
    - **Quelles précautions prendre en cas d'utilisation par les salariés de leur équipement personnel**
    - **Visioconférence : un employeur peut-il obliger un salarié à activer sa caméra lors d'une réunion ?**

- L'utilisation de l'informatique en nuage (cloud).
  - La thématique prioritaire du cloud s'inscrit également dans l'action du premier cadre d'application coordonné (coordinated enforcement framework en anglais) du Comité européen de la protection des données (CEPD). 22 autorités de contrôle vont, dans les prochains mois, lancer des investigations sur l'utilisation, par le secteur public, de services utilisant le cloud.
    - **Il s'agit d'une action clé de la stratégie du CEPD pour les années 2021-2023 qui vise à harmoniser l'application effective du RGPD et la coordination entre les autorités de contrôle.**
    - **Au niveau national, la CNIL assurera sa participation à ce groupe de travail européen au travers de procédures de contrôles visant cinq ministères.**

SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Thématiques et stratégie de contrôle de la CNIL

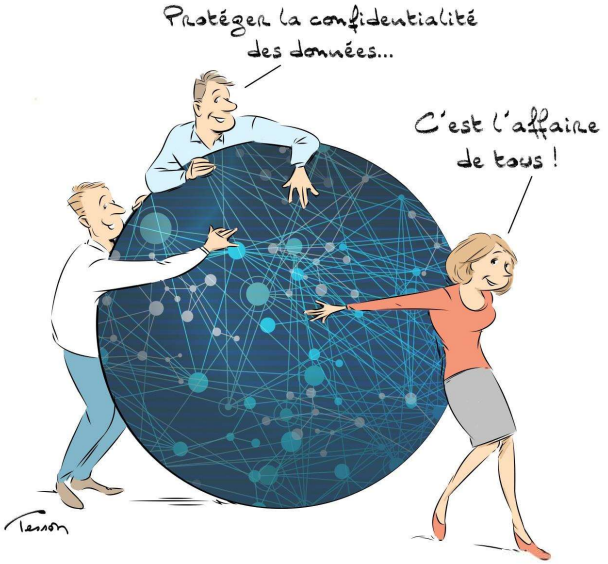
MOMENT D'ECHANGES

Comment démarrer son projet RGPD?

Ageris GROUP

absys
Les données bien ordonnées

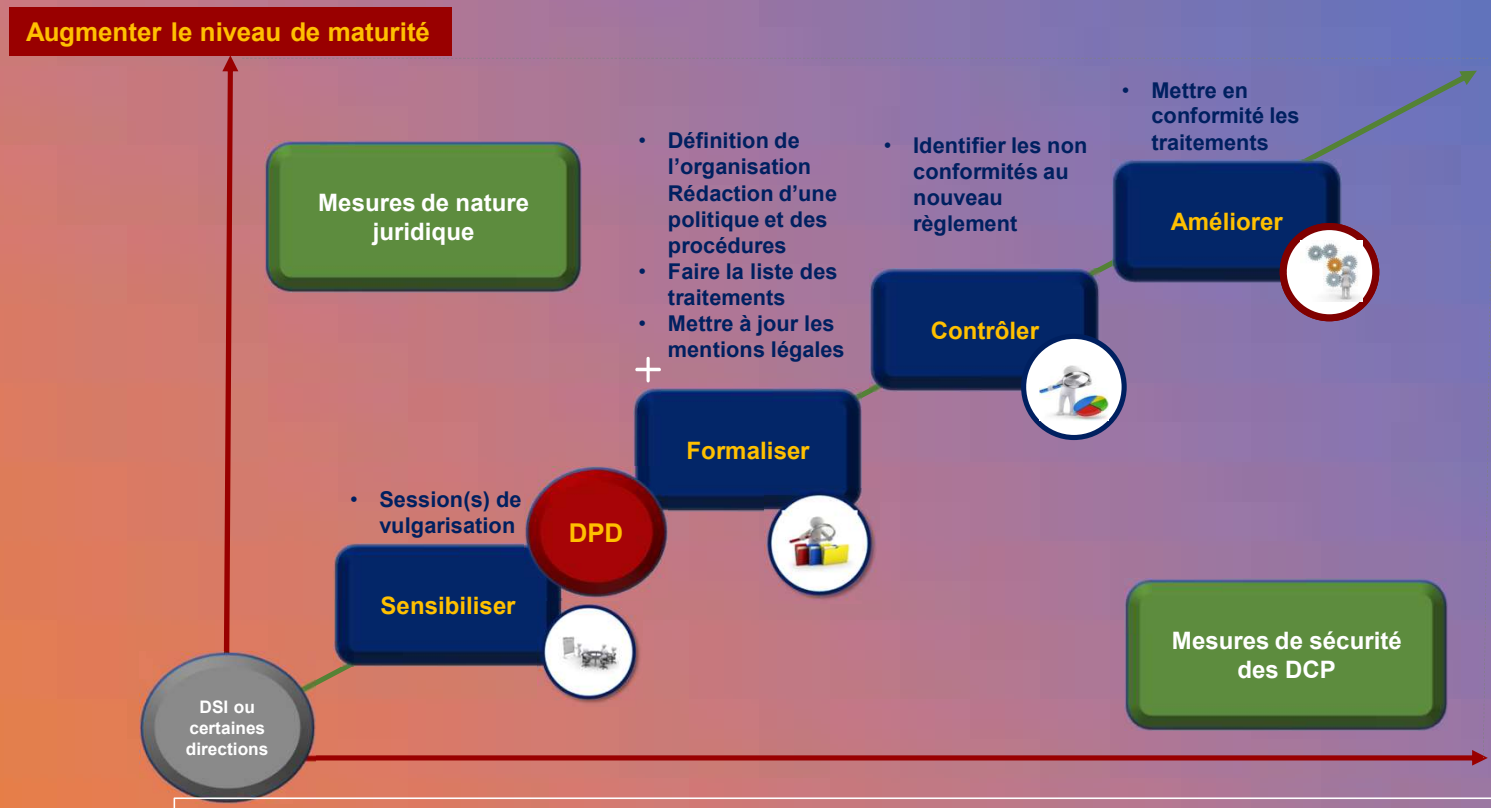
SHEO TECHNOLOGY
VOTRE PRESTATAIRE EN SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ



Protéger les données personnelles...

AFCDP

Comment démarrer son projet RGPD?



12 chantiers / 40 actions à prévoir

SHEO TECHNOLOGY

Ageris GROUP

absys

Dina Morgabine

Comment démarrer son projet RGPD?

Chantiers	Actions à prévoir
Mettre en place une organisation / gouvernance adaptée	1. Sensibiliser la Direction Générale sur les impacts du RGPD et son rôle 2. Sensibiliser les directeurs / chefs de service sur leurs responsabilités 3. Désigner un Délégué à la Protection des Données (DPD) (ou a minima un chef de projet en charge du suivi du plan d'actions) 4. Faire un état des lieux général sur la conformité au RGPD 5. Mettre en place des référents dans les directions et un comité de validation et de pilotage / validation et homologation
Faire la liste des traitements	6. Créer un registre des traitements et les fiches de collecte d'informations 7. Faire le recensement de tous les traitements (ateliers de travail avec les chefs de services) 8. Identifier les non-conformités et définir un plan d'actions correctifs par service concerné
Mettre à jour les mentions légales	9. Définir les mentions légales types 10. Recenser tous les formulaires de collecte 11. Organiser avec les services concernés la mise à jour des formulaires de collecte
Revoir les clauses contractuelles avec les sous-traitants	12. Recenser les sous-traitants concernés par le RGPD 13. Rédiger les clauses contractuelles types (modèle de la CNIL) 14. Organiser la mise à jour des contrats actifs (courrier, réunion de travail, ..) 15. Prévoir les clauses dans les nouveaux marchés

Comment démarrer son projet RGPD?

Chantiers	Actions à prévoir
Formaliser les directives internes et les procédures	16. Formaliser une politique interne de protection des données à destination des personnels cadres et non cadres
	17. Formaliser une politique externe (public) à destination des clients / tiers
	18. Mettre à jour la charte des utilisateurs (inclure des directives relatives à la protection des données et aux respects du RGPD) et continuer les actions de sensibilisation
	19. Mettre à jour la PSSI (intégrer les directives de la CNIL en matière de sécurité des données)
	20. Rédiger les procédures internes (gestion des réclamations, gestion des violations de DCP, alerte du RT, gestion des contrôles de la CNIL, …..) et préparer les registres associés (registre des réclamations, des violations, ..)
Mettre en place une démarche de gestion des risques pour la vie privée	21. Identifier les traitements soumis à obligation d'AIPD 22. Créer les référentiels permettant de mener les AIPD (outillage d'analyse) 23. Organiser un projet pilote sur un traitement sensible (en impliquant le service concerné et les mettre d'œuvre) 24. Renforcer les procédures et les moyens de traitements des incidents de sécurité (gestion des violations)
Engager une démarche de protection par défaut et lors de la conception	25. Auditer l'application des principes « Privacy By Default » dans les applications les plus sensibles et définir un plan d'actions correctifs 26. Intégrer la protection des données et le respect du RGPD dans les démarches projets (formation des chefs de projets, outillage, définition des livrables à chaque étape d'un projet, …)

Comment démarrer son projet RGPD?

Chantier	Actions à prévoir
Faire une veille sur les nouvelles directives de la CNIL	27. Surveiller la diffusion par la CNIL des modifications apportées à la loi « Informatique et Libertés » (ordonnances) et analyser les impacts pour l'organisme 28. Surveiller la diffusion par la CNIL des codes de conduite à appliquer 29. Adhérer à l'AFCDP (Association Française des Correspondants à La Protection des Données) ou association équivalente.
Rédiger un bilan de toutes les actions de conformité réalisé en cours d'année	30. Organiser la gestion des documents et des éléments de traçabilité 31. Rédiger un bilan annuel des actions réalisées à remettre au responsable des traitements
Sensibiliser tous les personnels	32. Définir et faire valider un plan de sensibilisation annuel 33. Organiser des actions de sensibilisation pour les nouveaux arrivants 34. Organiser des actions de sensibilisation pour les personnels en poste 35. Créer un espace intranet « RGPD » permettant la diffusion d'informations et la communications à l'ensemble du personnel
Anticiper les besoins en ressources et en moyens	36. Définir les besoins techniques pour renforcer la protection des données (voir l'article 32 du RGPD) 37. Définir les besoins humains pour assurer le maintien en condition opérationnelle des mesures techniques et organisationnelles mises en oeuvre
Auditer et améliorer	38. Conduire des audits périodiques 39. Mettre en œuvre les mesures correctives 40. Conserver les preuves

Comment démarrer son projet RGPD?

MOMENT+ D'ECHANGES

•

SHEO TECHNOLOGY

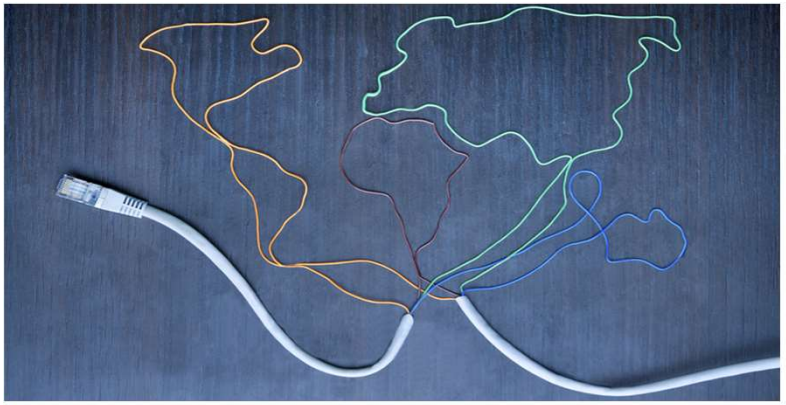
Ageris GROUP

absys
Les données bien ordonnées

Dina Morgabine

Transfert de données dans la zone Océan Indien

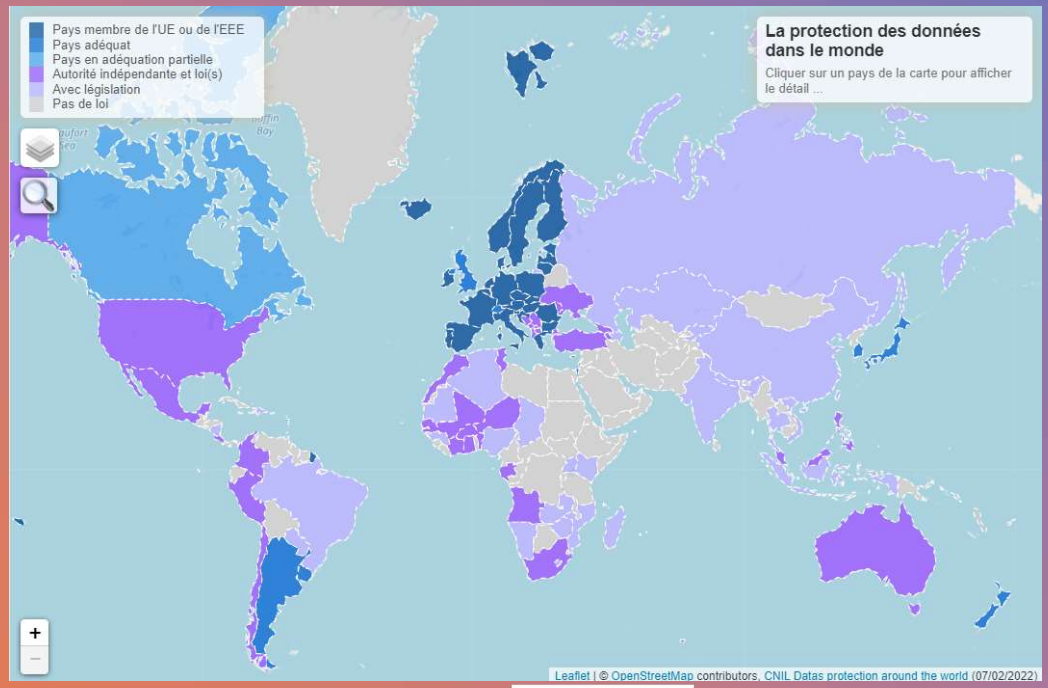
absys
Les données bien ordonnées



SHEO TECHNOLOGY

Transfert de données dans la zone Océan Indien

Les responsables de traitement et les sous-traitants peuvent transférer des données hors de l'Union européenne (UE) et de l'Espace économique européen (EEE) à condition d'assurer un niveau de protection des données suffisant et approprié. Ils doivent encadrer ces transferts en utilisant les différents outils juridiques définis au chapitre V du RGPD.



SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Transfert de données dans la zone Océan Indien

ZOOM SUR L'OCEAN INDIEN

Réunion

Niveau de protection : Pays membre de l'UE ou de l'EEE

La protection des données de ce pays est encadrée par la loi Informatique et Libertés Française.

Ce pays est membre de l'AFAPDP.

CNIL
3 Place de Fontenoy - TSA 80715 -
75334 PARIS CEDEX 07

Site Internet : https://www.cnil.fr

Mayotte

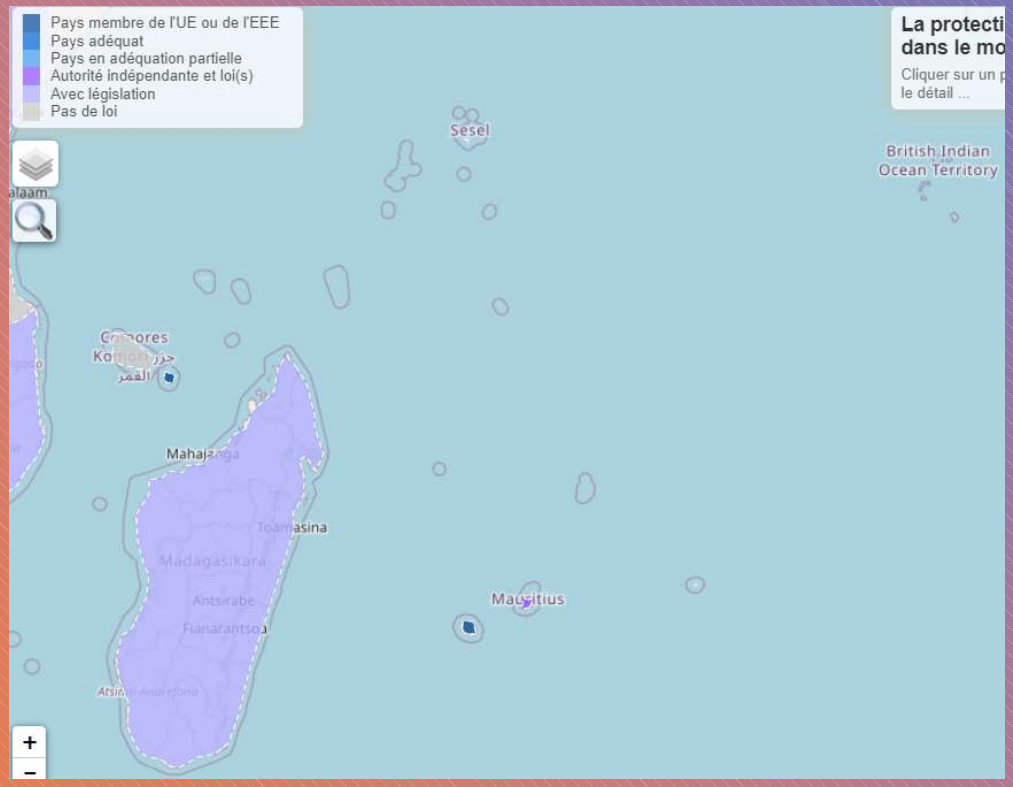
Niveau de protection : Pays membre de l'UE ou de l'EEE

La protection des données de ce pays est encadrée par la loi Informatique et Libertés Française.

Ce pays est membre de l'AFAPDP.

Commission nationale de l'informatique et des libertés (CNIL)
3 Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

Site Internet : https://www.cnil.fr



Madagascar

Niveau de protection : Avec législation

Existence d'une législation générale sur la protection des données personnelles ou des dispositions spécifiques.

Ce pays n'est pas reconnu comme adéquat par l'UE.

Les transferts de données personnelles vers ce pays nécessitent d'être encadrés par des outils de transfert.

En savoir plus sur l'encadrement des transferts de données...

Ce pays est membre de l'AFAPDP.

Commission malagasy de l'informatique et des libertés (CMIL) en cours d'installation

Comores

Niveau de protection : Pas de loi

Ce pays n'est pas reconnu comme adéquat par l'UE.

Les transferts de données personnelles vers ce pays nécessitent d'être encadrés par des outils de transfert.

En savoir plus sur l'encadrement des transferts de données...

Maurice

Niveau de protection : Autorité indépendante et loi(s)

Ce pays n'est pas reconnu comme adéquat par l'UE.

Les transferts de données personnelles vers ce pays nécessitent d'être encadrés par des outils de transfert.

En savoir plus sur l'encadrement des transferts de données...

Ce pays dispose d'une législation nationale en matière de protection des données personnelles et d'une autorité de protection des données reconnue par la conférence internationale des commissaires à la protection de la vie privée et des données personnelles.

Ce pays est membre de l'AFAPDP.

Data Protection Office
5th Floor
Happy World House
Corner Sir William Newton & SSR Streets
Port Louis
Republic of Mauritius

Site Internet :
https://dataprotection.govmu.org/Pages/About%20Us/About-the-Office.aspx

Inde

Niveau de protection : Avec législation

Existence d'une législation générale sur la protection des données personnelles ou des dispositions spécifiques.

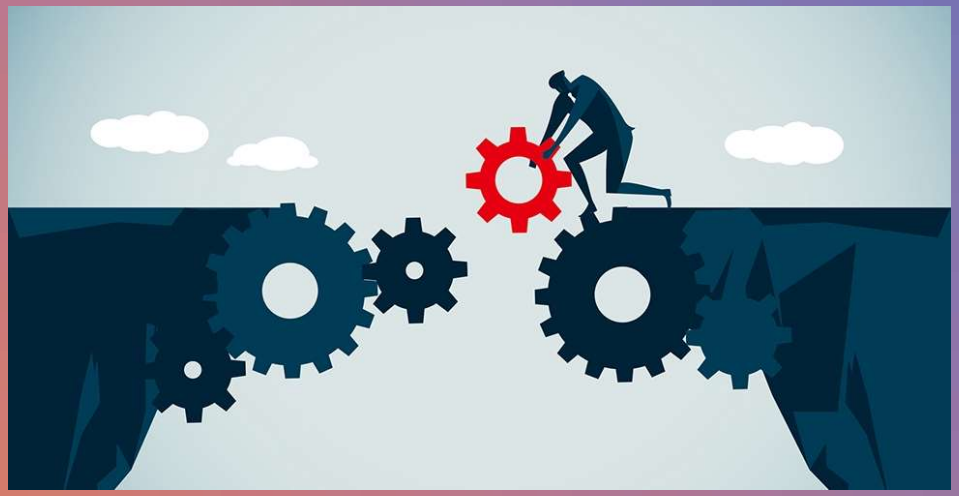
Ce pays n'est pas reconnu comme adéquat par l'UE.

Les transferts de données personnelles vers ce pays nécessitent d'être encadrés par des outils de transfert.

En savoir plus sur l'encadrement des transferts de données...

Transfert de données dans la zone Océan Indien

LES OUTILS NECESSAIRES



- CCT : Clauses contractuelles types
- BCR : Binding Corporate Rules ou les règles d'entreprises contraignantes

SHEO TECHNOLOGY

absys
Les données bien ordonnées

Dina Morgabine

Débat sur le métier de DPD/DPO

SHEO TECHNOLOGY
VOTRE PRESTATAIRE EN SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

absys
Les données bien ordonnées


MERCI À
TOUTES ET A
TOUS