RGPD

Passez à l'action !

Amphithéâtre de la CCISM

Vendredi 7 mars 2019

De 14h à 18h30

esci

CCISM
POLYNÉSIE FRANÇAISE

DGEN
DIRECTION GENERALE DE L'ECONOMIE NUMERIQUE

OPEN
Organisation des Professionnels de l'Économie Numérique

CLUSIR
TAHITI

TAHITI NUI FORTRESS

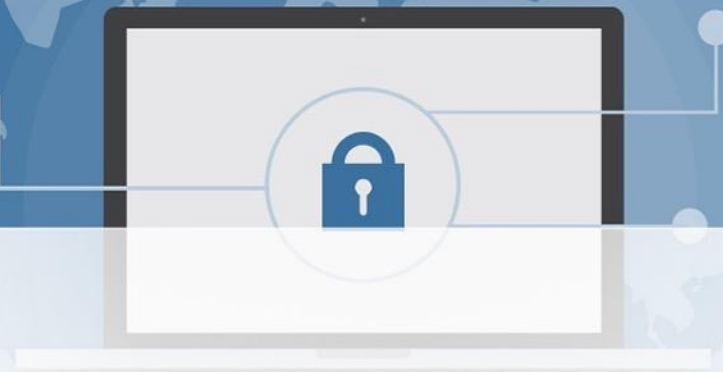
DT
DIGITAL TAHITI

SPILOG
Partner Consulting Services

ACTECIL
RGPD SOLUTIONS

IAORA systems
SERVICES ET INGÉNIERIE INFORMATIQUES

Intervention
De M. Jean-Claude HOEN



IAORA systems
VOTRE PARTENAIRE DIGITAL EN POLYNÉSIE

Acteur du numérique en Polynésie depuis 2001:

- Activité Editeur Logiciel
- Activité Conseil
  - **Accompagnement** à la mise en conformité RGPD
  - **Formation** et **sensibilisation** de vos équipes
  - **DPO externe** de sociétés polynésiennes

Une démarche pour entamer votre mise en conformité

R

G

P

D

PLAN D’ACTIONS

Une notion préalable

- Prouver votre conformité au RGPD à tout moment

(≠ ancienne loi I&L traitements déclarés à la CNIL)

CNIL

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

Plan de l’intervention

1

RECENSER

2

ELABORER
LE PLAN
D’ACTION

3

METTRE
EN OEUVRE

1er Objectif

RECENSER

1. Identifier les activités principales de votre entreprise
2. Lister l'ensemble de vos traitements
3. Constituer votre registre des traitements

1

Le registre

Qu’est-ce que le registre des traitements ?

- L’ensemble des fiches de registre d’activité
- Il est placé sous la responsabilité du dirigeant d’entreprise.

1

Comment procéder ?

- Identifier et désigner un responsable du projet (DPO)
- Identifier les personnes qui ont une connaissance globale des traitements et processus de l'entreprise : personnes ressources (**PR**)
- Organiser une sensibilisation de ces **PR** au RGPD (2 à 4 heures)

1

Comment procéder ?

- Organiser des entretiens avec ces **PR**
  - Identifier les traitements et les documenter
  - Collecter la documentation : procédures, contrats, formulaires de collecte, sites Internet

- Remplir une fiche de registre d'activité pour chaque traitement

La fiche de registre

Comment remplir une fiche de registre d'activité ?

1. Finalités
2. Fondement juridique
3. Informations et droits des personnes
4. Consentement
5. Catégories de personnes
6. Catégories de données collectées
7. Durées de conservation
8. Catégories de destinataires (internes/externes ou sous-traitant)
9. Flux de données (origine et destination des données)
10. Mesures de sécurités

1

Gestion de la paie:

Un exemple de fiche de traitement commun

1 - Objectifs poursuivis - Finalités

- Calcul et paiement des rémunérations et accessoires et des frais professionnels
- Déclarations et versements à l'administration fiscale (CST) et à la CPS
- Fourniture des informations permettant de satisfaire aux obligations légales (tenue du registre unique du personnel et la déclaration d'emploi de travailleurs handicapés).

2 - Fondement du traitement

- Exécution du contrat de travail

1

Gestion de la paie:

Un exemple de fiche de traitement commun

3 - Information des personnes (incluant les droits des personnes)

- Oui : par l'intermédiaire du contrat de travail et du règlement intérieur

4 - Consentement des personnes

- Non nécessaire

5 - Catégories de personnes concernées

- Salariés
- Apprentis, stagiaires

1

Gestion de la paie:

Un exemple de fiche de traitement commun

6 - Catégories de données collectées

- Etat-civil, identité, données d'identification, images, numéro de DN …
- Vie personnelle : Situation matrimoniale, enfants à charge …
- Vie professionnelle : Lieu de travail, date d'entrée dans l'entreprise, ancienneté, emploi occupé, nature du contrat de travail …
- Informations d’ordre économique et financier
- Congés et absences, frais professionnels, mode de règlement, identité bancaire ou postale …

1

Gestion de la paie:

Un exemple de fiche de traitement commun

- Des données sensibles sont-elles traitées ?
  Non
- Mode de collecte des données
  Directement auprès de la personne

7 - Durées de conservation des catégories de données

Exemple : Fiches de paie : 5 ans après le départ de l'employé

1

Gestion de la paie:

Un exemple de fiche de traitement commun

8 - Catégories de destinataires des données

- Destinataires internes
  - Services de la paie du personnel
  - Services chargés du contrôle financier dans l'entreprise
- Organismes externes
  - Caisse de Prévoyance sociale
  - Direction des Impôts et des Contributions Publiques (DICP)
  - Organismes intervenant dans la gestion des comptes de l'entreprise
- Sous-traitants

1

Gestion de la paie:

Un exemple de fiche de traitement commun

9 - Transferts des données hors UE

- Non

10 - Mesures de sécurité

- Contrôle d'accès des utilisateurs
  - Documents papiers rangés dans une armoire fermée à clé dans un bureau qui ferme à clé situé au service des ressources humaines
  - Logiciel de paie Apetahi accessible par un couple identifiant + mot de passe. Le DRH et le chargé de paie sont les seuls utilisateurs autorisés

1

Gestion de la paie:

Un exemple de fiche de traitement commun

- Mesures de traçabilité
  - Traçabilité des connexions avec date et heure de connexion
- Sauvegarde des données
  - Sauvegarde mensuelle automatique contrôlée par le service informatique
- Chiffrement des données
  - Mot de passe : Hachage SHA-3
- Contrôle des sous-traitants
  - Autres mesures

1

Félicitations !!!

vous avez créé votre registre des traitements

2ème objectif

Elaborer le plan d'actions

1. Les principes relatifs aux traitements des données
2. Les droits des personnes
3. Diagnostic de conformité au RGPD

2

Les principes à respecter

- Licéité, loyauté, transparence
- Limitation des finalités
- Minimisation des données
- Exactitude
- Limitation de la conservation
- Sécurité : Intégrité et confidentialité

Les droits des personnes

- Portabilité
- Accès
- Rectification
- Opposition
- Limitation
- Effacement

Les personnes ont des droits sur leurs propres données.

AFCDP

Comment faire ?

Diagnostic de conformité au RGPD

- Etudier votre registre des traitements et les documents collectés
- Détecter les écarts de conformité
- Identifier les procédures de bonnes pratiques à mettre en place
- Analyser les résultats obtenus

- Prioriser les actions selon vos critères

3ème OBJECTIF

Mettre en œuvre le plan d'actions

1. Les collaborateurs
2. Les sous-traitants
3. Les mesures diverses

Les collaborateurs

- Sensibiliser les collaborateurs
- Faire signer un engagement de confidentialité
- Revoir les procédures : charte informatique, procédures d’entrée et sortie

Les sous-traitants

- Faire signer un avenant RGPD au contrat de sous-traitance
- Mise en œuvres par le sous-traitants des mesures techniques et organisationnelle pour la protection des données

Les mesures diverses

- Les droits des personnes
  - Informer les personnes de leurs droits
  - Organiser l'exercice des droits des personnes
    Ex : Droit d'effacement ou « droit à l'oubli » (Art. 17)
    Exemple base de données pour soirées de dégustations de vin
- Gérer les durées de conservation de DCP
  - Minimiser la durée de conservation au strict minimum
    Exemple la gestion du recrutement
  - *Mettre en place la procédure et les outils permettant de réaliser ces actions*

Les mesures diverses

- Les zones de commentaires libres (**ZCL**):
  - Eviter si possible l'utilisation de ces zones
  - Auditer régulièrement les **ZCL**
    Exemple : « Client sourd, communiquer par e-mail »

- Réaliser les Analyses d'Impact relative à la Protection des Données (DPIA ou EIVP)

RGPD

En marche vers la conformité

Conclusion

- Etablir le registre des activités des traitements
- Créer un plan d'actions priorisées de mise en conformité
- Sensibiliser vos employés régulièrement
- Revoir les contrats avec vos sous-traitants
- Informer & organiser l'exercice des droits des personnes
- Sécuriser vos données
- Documenter votre conformité
- Maintenir et auditer votre conformité régulièrement

RESSOURCES

CNIL. https://www.cnil.fr/professionnel

ANSSI Agence nationale de la sécurité des systèmes d'information https://www.ssi.gouv.fr/

iaora systems http://www.iaora-systems.pf/RGPD

rgpd@ios.pf

dpo@ios.pf

- Guide de la Cnil : se préparer en 6 étapes
- Le texte officiel du RGPD (JO)
- Ordonnance no 2018-1125 du 12 décembre 2018
- Guide Cnil La sécurité des DCP
- Guide l'Anssi : Le guide d'hygiene informatique