ADEQUACY

DPO & RSSI

LES CLÉS D'UNE COLLABORATION RÉUSSIE POUR LA CONFORMITÉ RGPD

DPO FORUM

PARIS 2024

Alessandro FIORENTINO

ADEQUACY

- Product Owner de la plateforme Adequacy
- Responsable de la formation DPO certifié Afnor

PRIVACY TECH

- Vice-Président de l'association PRIVACY TECH

ISEP & Institut Mines Télécom

- Data Protection Management Senior Lecturer – Institut Mines-Télécom
- Personal Data Protection Lecturer - DPO Practices - ISEP
- Member of Scientific Board of Data Protection Management Master - ISEP

AU PROGRAMME

01 DPO & RSSI, À CHACUN SON RÔLE ET SES RESPONSABILITÉS

02 COMMUNICATION ET PARTAGE D'INFORMATION : LES PILIERS D'UNE RELATION SOLIDE

03 EVALUATION ET AMÉLIORATION CONTINUE POUR UNE SÉCURITÉ ET UNE CONFORMITÉ PÉRENNE

04 LES OUTILS POUR UNE PARFAITE SYNERGIE

05 NIS2, QUAND CYBERSÉCURITÉ ET RGPD SONT LIÉS

06 INTELLIGENCE ARTIFICIELLE, ADOPTER UNE POSTURE COMMUNE.

DPO & RSSI
À CHACUN SON RÔLE ET SES RESPONSABILITÉS

RSSI, Un métier en évolution depuis 30 ans

Il pilote la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation

Rôle de chef d'Orchestre

Il définit les politiques de sécurité la politique de sécurité, Il a pour objectif de garantir la confidentialité, la disponibilité, l'intégrité du système d'information et la traçabilité des actions.

Rôle d'assistance

Le RSSI aide à chaque étape de la politique de sécurité informatique de l'organisation.

Rôle d'information, de sensibilisation et de formation

Le RSSI informe, sensibilise, responsabilise et forme toutes les équipes et tous les services aux risques encourus par la sécurité informatique.

Rôle d'alerte

Il revient au RSSI d'alerter aussi bien les responsables que le personnel face aux risques inhérents au manque de sécurité des données et des applications.

Rôle d'interface

Le RSSI joue le rôle d'interface entre les exploitants et les chefs de projets, mais aussi entre les experts et les intervenants extérieurs pour les problèmes de sécurité du système d'information.

DPO, Un métier consacré par le RGPD

Il pilote la démarche de conformité au sein de l'organisation tant dans le cadre de sa construction que de son maintien.

Rôle de chef d'Orchestre

Il assure le suivi du programme de conformité, il définit les procédures relatives à la protection des données personnelles, Il a pour objectif de garantir la confidentialité, la disponibilité, l'intégrité des données personnelles d'assurer l'accountability de l'organisation.

Rôle d'assistance

Le DPO assure un fonction support auprès des différentes directions de l'organisation.

Rôle d'information, de sensibilisation et de formation

Le DPO informe, sensibilise, responsabilise et forme toutes les équipes et tous les services aux risques encourus par la protection des données personnelles.

Rôle d'alerte

Il revient au DPO d'alerter aussi bien les responsables que le personnel face aux risques inhérents au manque de respect de la réglementation.

Rôle d'interface

Le DPO joue le rôle d'interface entre les personnes concernées et l'organisation et entre l'autorité de contrôle et l'organisation.

Le DPO et le RSSI ne sont pas concurrents, bien au contraire.

Deux métiers pour deux périmètres

Le DPO est responsable de la conformité de l'entreprise aux règlementations en cours sur la protection des données personnelles.

Le RSSI doit quant à lui veiller à la protection des données informatiques de son entreprise.

Communication et partage d'information

Comme dans tout travail collaboratif, la communication entre les acteurs est essentielle.

Elle doit être rapide, afin de pouvoir réagir rapidement en cas de début de crise.

Elle doit aussi être régulière afin que DPO et RSSI sachent chacun s'ils respectent bien l'évolution des contraintes légales en vigueur.

COMMUNICATION ET PARTAGE D’INFORMATIONS

LES PILIERS D’UNE RELATION SOLIDE

Seul, on va plus vite. Ensemble, on va plus loin

DPO et RSSI doivent cultiver une étroite collaboration pour travailler ensemble.

Pour cela, ils peuvent mettre en place des points réguliers au cours desquelles ils pourront échanger sur les mesures de sécurité à prendre pour tel ou tel point spécifique et coordonner leurs efforts.

Cette coordination régulière leur permettra également de prévoir des actions de sensibilisation du personnel et du management aux problématiques de sécurité.

Collaboration DPO – RSSI : Les chantiers communs

- La gestion des incidents et des violations de données personnelles
- La réalisation des Analyses d'Impact relatives à la Protection des Données
- Sensibilisation du personnel et de la Direction.
- Contrôle régulier des mesures de sécurité.

Collaboration DPO – RSSI : Les erreurs à éviter

- Faire du RSSI, le sous-traitant du DPO
- Faire du RSSI, le responsable du DPO

Ils devraient tous les deux être rattachés à la direction générale.

EVALUATION ET AMÉLIORATION CONTINUE POUR UNE SÉCURITÉ ET UNE CONFORMITÉ PÉRENNE

ISMS et PIMS

- La norme ISO 27001 implique la mise en place d'un Information Security Management System,
- La norme ISO 27701 implique quant à elle la mise en place d'un Personal Information Management System

C'est deux démarches suivent la même méthodologie.

La norme ISO 27701, publiée en août 2019, se base sur deux normes ISO de sécurité de l'information et les étend pour intégrer la protection des données personnelles :

l'ISO 27001, qui certifie un système de management de la sécurité informatique ;

l'ISO 27002, qui détaille les bonnes pratiques pour la mise en œuvre des mesures de sécurité nécessaires.

Lorsque cette démarche est mise en œuvre le PIMS est dépendant des bonnes pratiques pour la mise en œuvre des mesures de sécurité.

LES OUTILS POUR UNE PARFAITE SYNERGIE

UNE COUVERTURE FONCTIONNELLE ADAPTÉE AUX BESOINS

DPO

- Registre des activités
- Exercice des droits
- Gestion des Contrats
- Mentions d'information
- Bilan DPO
- Médiathèque
- Gestion des Tiers

SYNERGIE

- AIPD
- Incidents et Violations
- DBIA
- Formation
- Evaluation
- Plan d'action

RSSI

- Cartographie applicative
- Politiques
- Recensement des mesures
- Audits Applicatifs

NIS2, QUAND LA CYBERSÉCURITÉ ET RGPD SONT LIÉS

NIS 2
LES ATTENDUS DE L'ARTICLE 21

01 LES POLITIQUES RELATIVES À **L'ANALYSE DES RISQUES** ET À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

02 **LA GESTION DES INCIDENTS**

03 LA CONTINUITÉ DES ACTIVITÉS, PAR EXEMPLE LA GESTION DES SAUVEGARDES ET LA REPRISE DES ACTIVITÉS, ET LA GESTION DES CRISES

04 LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT, Y COMPRIS LES ASPECTS LIÉS À LA SÉCURITÉ CONCERNANT LES RELATIONS ENTRE CHAQUE ENTITÉ ET SES FOURNISSEURS OU PRESTATAIRES DE SERVICES DIRECTS

05 LA SÉCURITÉ DE L'ACQUISITION, DU DÉVELOPPEMENT ET DE LA MAINTENANCE DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION, Y COMPRIS LE TRAITEMENT ET LA DIVULGATION DES VULNÉRABILITÉS

06 **DES POLITIQUES ET DES PROCÉDURES POUR ÉVALUER L'EFFICACITÉ DES MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSÉCURITÉ**

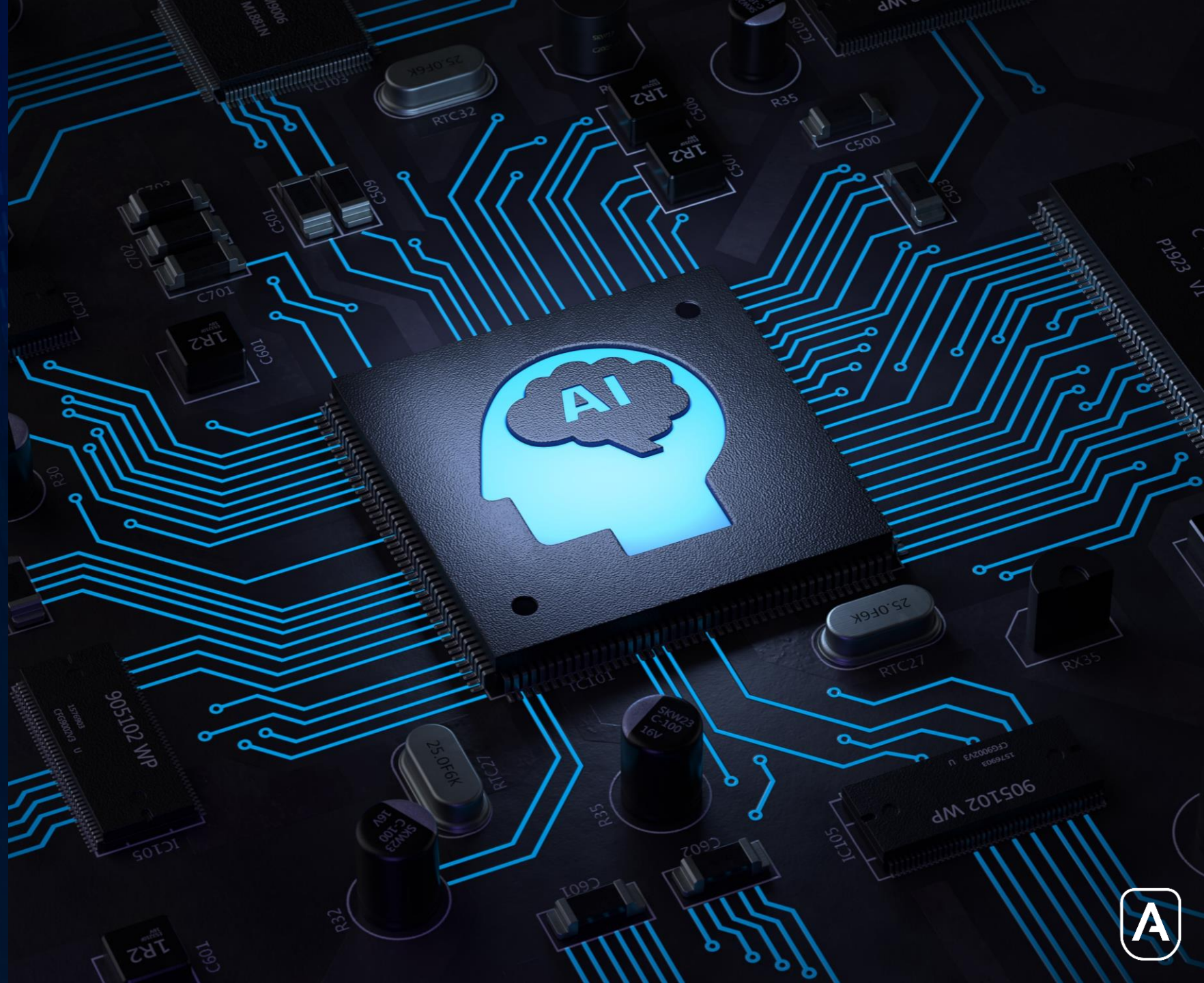
07 LES PRATIQUES DE BASE EN MATIÈRE DE CYBERHYGIÈNE ET **LA FORMATION À LA** CYBER**SÉCURITÉ**

08 **DES POLITIQUES ET DES PROCÉDURES** RELATIVES À L'UTILISATION DE LA CRYPTOGRAPHIE ET, LE CAS ÉCHÉANT, DU CHIFFREMENT

09 LA SÉCURITÉ DES RESSOURCES HUMAINES, **DES POLITIQUES DE CONTRÔLE D'ACCÈS ET LA GESTION DES ACTIFS**

10 L'UTILISATION DE SOLUTIONS D'AUTHENTIFICATION À PLUSIEURS FACTEURS OU D'AUTHENTIFICATION CONTINUE, DE COMMUNICATIONS VOCALES, VIDÉO ET TEXTUELLES SÉCURISÉES ET DE SYSTÈMES SÉCURISÉS DE COMMUNICATION D'URGENCE AU SEIN DE L'ENTITÉ, SELON LES BESOINS

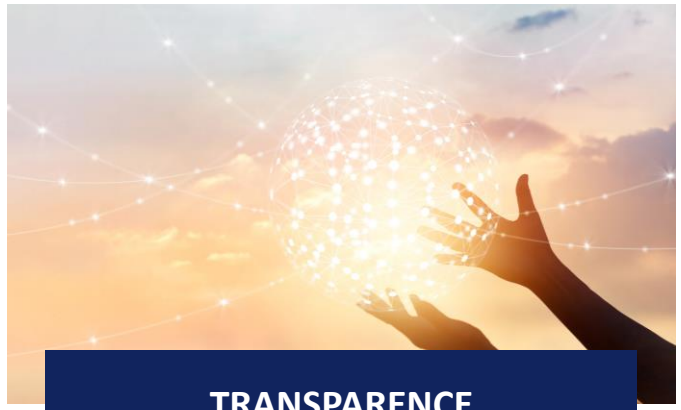
INTELLIGENCE ARTIFICIELLE, ADOPTER UNE POSTURE COMMUNE



DES PRINCIPES CLÉS À GARANTIR

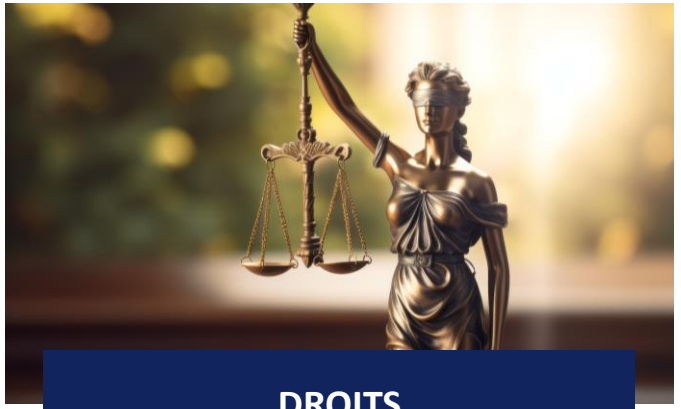
L'INFORMATION

EXPLICABILITÉ

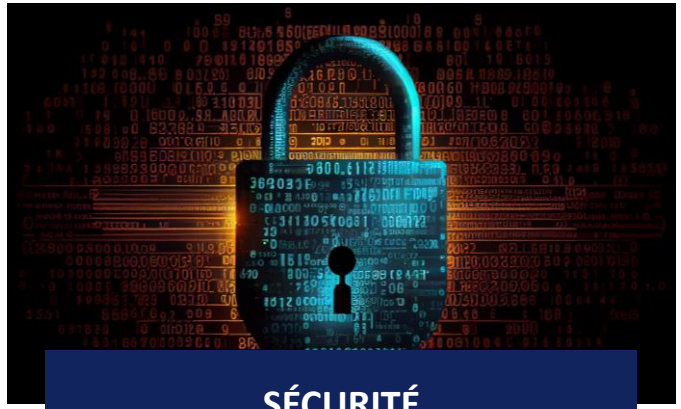


TRANSPARENCE

GARDER LA MAITRISE



DROITS



SÉCURITÉ

MERCI
DE VOTRE PARTICIPATION

Alessandro FIORENTINO
afiorentino@adequacy.app

ADEQUACY