Luxgap

DATA PRIVACY PARTNER

MISE EN CONFORMITÉ RGPD :

Approche proposée

Sommaire

FORMATION

1
Proposer une formation générale

2
Proposer des formations ciblées pour chaque métier

3
Former et sensibiliser les équipes de manière régulière

Encadrer et donner les formations, données soit sur place par un formateur de Luxgap ou donnés via notre plate-forme e-learning. Par exemple des micro-formations de 3 à 5 minutes pour sensibiliser aux nouvelles politiques implémentées.

ANALYSE DES DONNÉES

Identifier les données personnelles traitées au sein des différents départements/ services

Établir un registre des traitements et une politique de conservation des données

Réaliser une évaluation de l'intérêt légitime si nécessaire

Réaliser le registre des traitements et valider les bases légales.

Il y a un registre par département. Le registre permet de définir les bases légales, d'identifier les données personnelles, d'identifier les besoins d'analyse d'impact et de cibler les finalités de chaque traitement.

TRANSPARENCE ET INFORMATION

Rédiger une politique générale de protection des données personnelles

Informer ses équipes du traitement de leurs données personnelles et de leurs droits

Informer les clients / prospects du traitement de leurs données personnelles et de leurs droits

Etablir les documents qui concernent la transparence : La notice d'utilisation du site internet, la notice aux candidats à l'embauche, la notice pour les employés, la notice pour d'éventuelles caméras. Chaque fois qu'il y a traitement de données personnelles une notice doit expliquer ce que l'article 12 impose.

SÉCURITÉ DES DONNÉES PERSONNELLES

Accompagner à la montée en maturité selon la norme ISO27001. L'article 32 du RGPD impose des mesures techniques et organisationnelles en ligne avec le risque.

Dès lors nous allons identifier la situation actuelle et apporter des mesures et techniques que nous allons décrire dans une liste nommée TOMs. Un plan assurance qualité sera également créé où nous documentons et expliquons ces mesures afin de démontrer notre conformité auprès des partenaires qui le demandent.

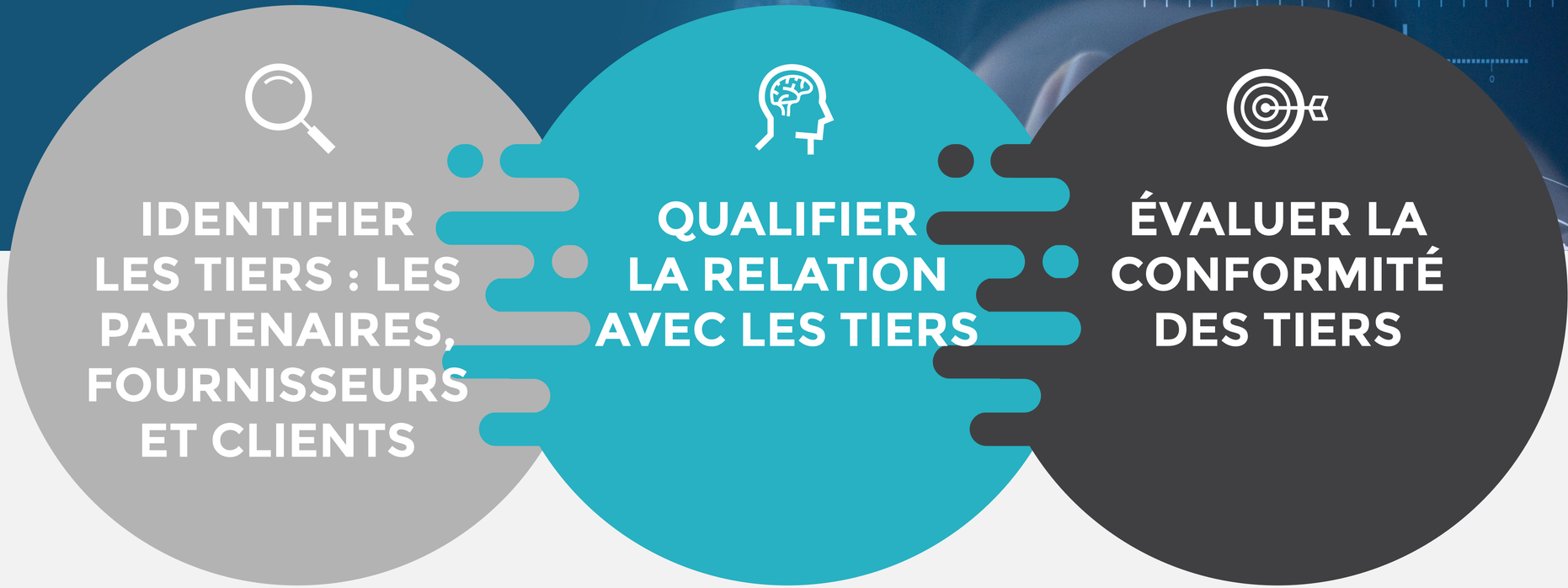
Passer en revue les mesures de sécurité existantes et les tester **1**

Évaluer les risques existants **2**

Il s'agit ici de réduire le risque d'attaque informatique via les vulnérabilités techniques et humaines.

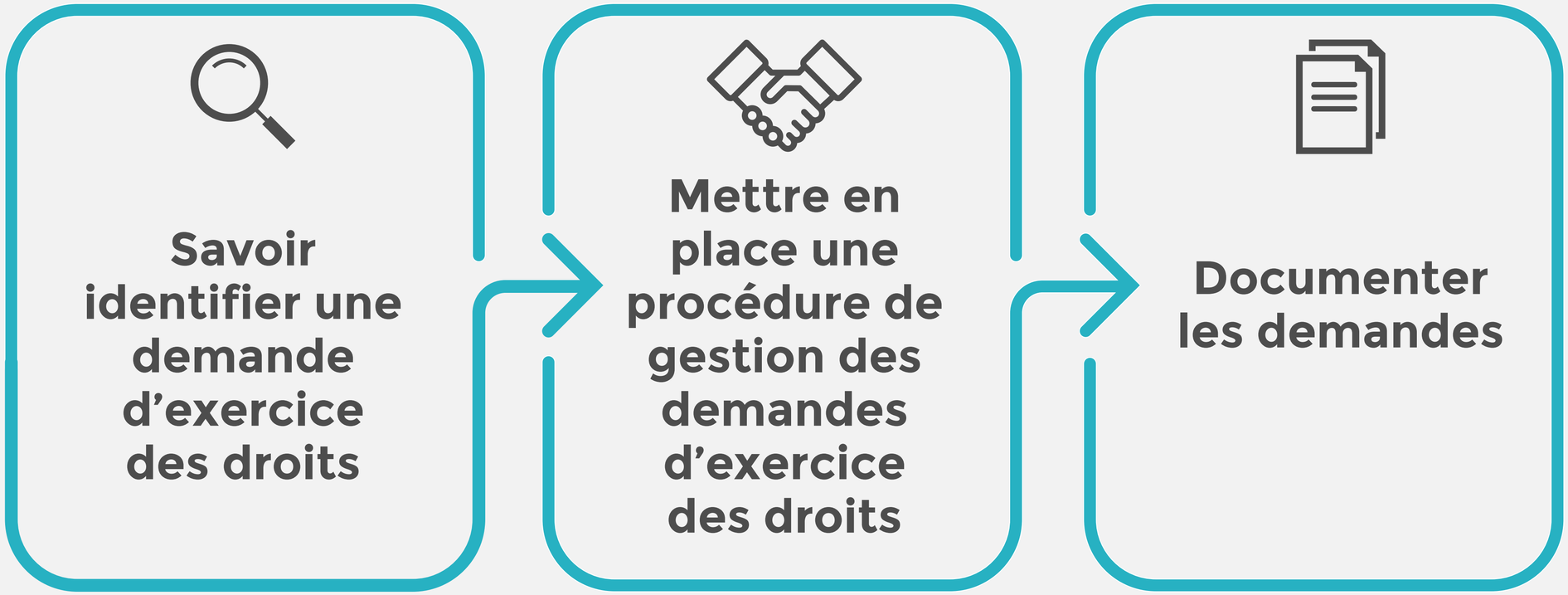
Proposer des mesures organisationnelles et techniques adéquates basées sur les risques et mettre en place les procédures nécessaires **3**

ACTEURS DU TRAITEMENT :
RESPONSABLES DU TRAITEMENT ET SOUS-TRAITANTS



Analyser tous les contrats avec les tiers qui manipulent des données personnelles. L'article 28 du RGPD nous impose cela. En cas de doute sur la conformité, par exemple technique si la société fourni des services informatiques, Notre équipe spécialisée en sécurité de l'information vont aller plus loin et analyser le niveau de risque du prestataire. S'il n'est pas conforme, celui-ci devra réaliser une liste d'actions pour se conformer. En cas de refus nous conseillerons un changement de prestataire.

DROITS DES PERSONNES



Encadrer le respect du droit des personnes : Soit le public dont on collecte les données personnelles, soit les employés. Nous rédigerons les procédures expliquant comment répondre à ces demandes, et on y répondra ou accompagnerons les personnes en charge de ces réponses pour garantir que cela soit fait de manière sécurisée et dans les délais imposés par la loi.

VIOLATION DES DONNÉES

Mettre en place une procédure de gestion des violations de données

01

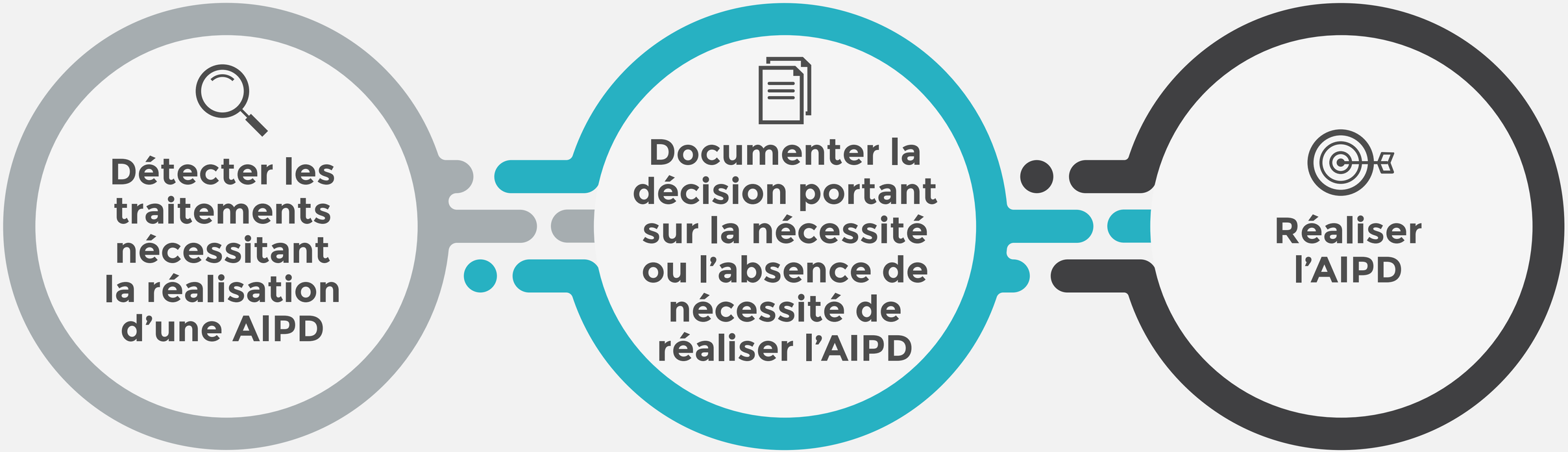
Documenter les incidents

02

Encadrer et se préparer à une éventuelle fuite de données. Tous les incidents sont documentés en cours d'année.

En cas d'incident grave, nous sommes préparés à la gestion des incidents, nous pouvons alors intervenir sur site le jour même afin d'épauler les équipes à une bonne réaction suite à une attaque.
Un plan de continuité d'activité peut être créé lors de la deuxième année de mandat DPO externe. Ce dernier optimise la réaction face aux crises.

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)



Les AIPD sont des analyses de risque sur les personnes. Le besoin s'active si deux des 9 critères définis par la loi sont concernés. Nous utilisons un outil que nous avons développé sur mesure afin de permettre de réaliser plus facilement ce type d'analyse de risque.

TRANSFERTS INTERNATIONAUX DE DONNÉES

Pour les transferts internationaux, nous devons vérifier s'il y en a. Cela peut concerner des outils informatiques ou des technologies non européennes dont l'utilisation doit être encadrée et analysée.

Cela peut concerner des partenaires installés en dehors de l'UE/EEE.

Détecter les transferts de données personnelles en dehors de l'UE/EEE et les encadrer

01

Rédiger et mettre en place une procédure de transfert de données si nécessaire

02

EXEMPLE DE PLAN D'ACTION ET DE DOCUMENTATION

ACTIONS	DESCRIPTION
FORMATION	
Formation et sensibilisation des collaborateurs	Organiser une session de formation pour les collaborateurs
ANALYSE DES DONNEES	
Registre des traitements	Etablir un registre des traitements
Evaluation de l'intérêt légitime (LIA)	Réaliser une évaluation pour tous les traitements fondés sur l'interet légitime
Conservation des données	Définir des périodes de rétention et valider une politique de conservation des données
TRANSPARENCE ET INFORMATION	
Cadre général	Rédiger et valider une politique de gestion des données
Information des collaborateurs	Mettre à disposition une information est complète et à jour
Information des tiers (clients, fournisseurs, partenaires, etc.)	Mettre à disposition une information est complète et à jour
Information des visiteurs du site internet	S'assurer que l'utilisation des cookies est conforme
RESPONSABLES DE TRAITEMENT ET SOUS-TRAITANTS	
Identification et qualification des acteurs du traitement	Identifier et qualifier les prestataires / fournisseurs (registre des tiers)
Due diligence des prestataires	Evaluer les prestataires / fournisseurs
SECURITE DES DONNEES	
Mesures techniques et organisationnelles	Identifier les mesures actuellement en place et s'assurer de leur efficacité
Documentation	Rédiger et valider les politiques informatiques manquantes
Sensibilisation	Effectuer une campagne de phishing
Scans de vulnérabilité	Effectuer des scans de vulnérabilité hebdomadaires
DROITS DES PERSONNES	
Gestion des droits des personnes concernées	Rédiger er valider une procédure de gestion des demandes d'exercice de droits
VIOLATIONS DES DONNEES	
Gestion des violations de données	Rédiger er valider une procédure de gestion des violations de données
ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES	
Encadrement des AIPDs	Identifier les traitements nécessitant la réalisation d'une AIPD et la réaliser si nécessaire
TRANSFERTS INTERNATIONAUX	
Encadrement des transferts	Identifier les éventuels transferts et les encadrer si nécessaire

Luxgap

DATA PRIVACY PARTNER

LUXGAP.COM

MISE EN CONFORMITÉ RGPD :
Approche proposée