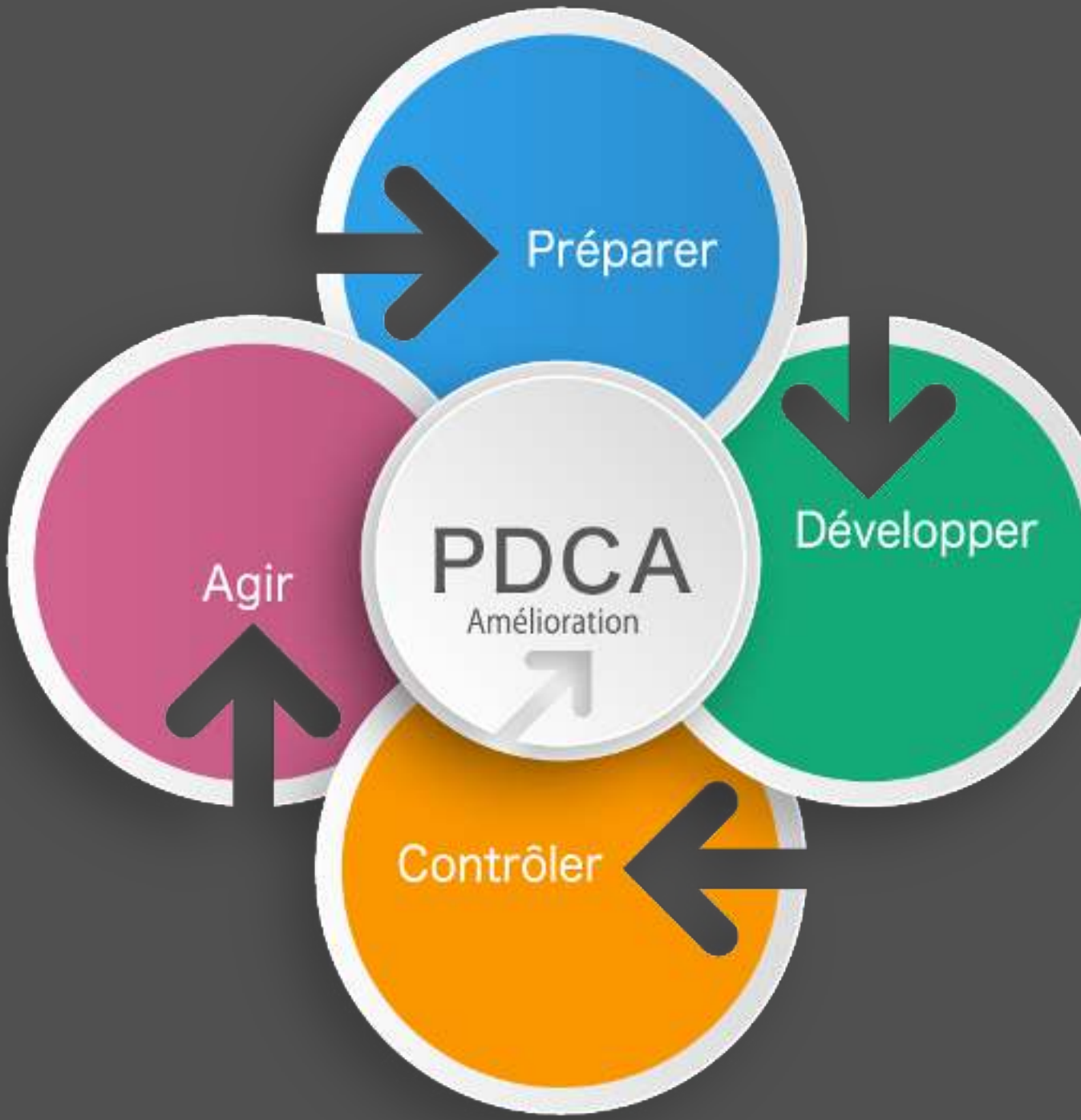

Contrôler ses processus
de mise en œuvre
du RGPD

conformité
dynamique
vs statique



Contrôler

S’assurer que :

⇒ Les outils et les méthodes de gouvernance des données personnelles en place traitent efficacement des exigences en matière de **transparence**, de **tenue de dossiers** et de **rapports.**

⇒ Les politiques et profils de protection des données fournissent un contrôle approprié aux personnes concernées et assurent un traitement conforme à la légalité.

⇒ Les **contrôles de sécurité** qui ont été mis en œuvre sont effectivement appliqués pour contrôler l'endroit où les données personnelles sont stockées et comment elles sont utilisées.

Agir et améliorer

⇒ Mettre en œuvre des mesures correctives sur les différences significatives entre les résultats réels et prévus

⇒ Analyser les différences dans les éléments de données personnelles qui nécessitent une révision en termes de classification, de politiques de protection / de divergences de profils, etc. pour déterminer leurs causes profondes

⇒ Déterminer où appliquer les modifications qui incluront les améliorations de l'ensemble du processus

Processus RGPD

- es traitements des onnées
- a prévention des risques
- es réponses aux droits des ersonnes
- a réponse à la violation de onnées
- rivacy by design et rivacy by default
- a sensibilisation des ersonnes

Le registre des activités de traitement

véritable outil de pilotage de votre conformité au RGPD

- Le registre doit être mise à jour régulièrement au gré des évolutions fonctionnelles et techniques des traitements de données.
- En pratique, toute modification apportée aux conditions de mise en œuvre de chaque traitement inscrit au registre (nouvelle donnée collectée, allongement de la durée de conservation, nouveau destinataire du traitement, etc.) doit être portée au registre.

Le registre des activités de traitement

Vérifier la pertinence de la cartographie des traitements

Procéder à des audits internes réguliers

⇒ Quelles données personnelles sont détenues

⇒ Comment elles sont utilisées

⇒ L'antériorité de ces données

⇒ Qui accède à ces données

- On réalise cette vérification sur la base des traitements recensés et présents dans le regis des activités de traitement et au delà.
- Les éventuels nouveaux traitements découver sont à intégrer dans le registre des activités d traitement.

La prévention des risques

Toute modification du traitement ou des données collectées et traitées doit provoquer un réexamen.

- Il convient de procéder à une **analyse de risques** sur la base des écarts constatés.
- Les actions correctrices seront vérifiées lors d'une prochaine itération du cycle PDCA, en fonction du délai de résolution accordé.
- Le Registre des traitements doit pouvoir être mis à disposition de l'autorité de contrôle à tout moment y compris durant une procédure d'audit.

La prévention des risques

- Vérifier l'efficacité des mesures de sécurité techniques et organisationnelles en place
- Ces vérifications concernent aussi bien le responsable de traitement que les sous-traitants

Les réponses aux droits des personnes

S’assurer que les réclamations et les demandes des personnes concernées quant à l’exercice de leurs droits sont **(bien) effectives.**

- Les procédures et les formulaires de demande de droits **sont accessibles** par les utilisateurs
- Toutes les requêtes sont prises en compte et traitées dans **des délais raisonnables**
- **Les droits sont effectivement appliqués**

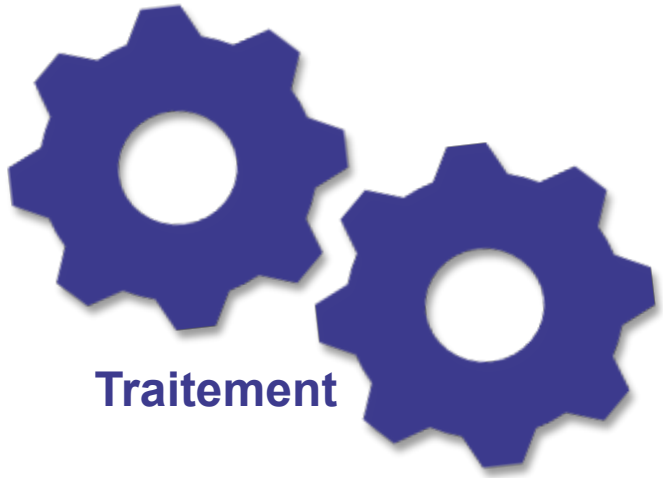
Réponse à la violation de données

Vérifier le niveau opérationnel du processus de notification de violation des données personnelles

- Planifier un exercice de simulation et s'assurer que toutes les parties prenantes peuvent être convoquées dans un délai court pour respecter les 72 heures et, en cas de dépassement de ce délai, d'être en mesure de le motiver.

Privacy by design
Privacy by default

ouveau
service,
ouvelle
lication



Traitement

Mesures techniques

Mesures organisationnelle

Privacy by design
Privacy by default

Mesures techniques

1. Mesures proactives et non réactives
2. Protection implicite de la vie privée
3. Protection de la vie privée dans la conception des systèmes et des pratiques
4. Fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
5. Sécurité pendant toute la période de conservation des données
6. Visibilité et transparence du système pour les utilisateurs
7. Respect de la vie privée des utilisateurs

La protection de la vie privée doit être envisagée par la responsable de traitement comme une valeur ajoutée à sa technologie et non comme un frein au développement de son activité commerciale.

Mesures organisationnelle

Le responsable de traitement doit mettre
place des mécanismes visant à garantir,
par défaut, que :

les données
ue finalité du
de minimisation) ;
pas conservées a
cessaire à ces

pas rendues
accessibles à un nombre indéterminé
personnes physiques.

Sensibilisation des personnes

Améliorer la prise de conscience et la collaboration en interne

⇒ **Sensibiliser** les collaborateurs aux enjeux de la prote de la vie privée

⇒ **Favoriser** les remontées d'information dans l'identifica et la cartographie des traitements de données personn

⇒ **Former** régulièrement les personnels concernés sur le standards de sécurité de l'entreprise qui régissent comment les données personnelles sont gérées, accédées, transférées et supprimées.

STITUT du RISK
COMPLIANCE

Merci pour votre attention

Corinne Plourde
corinne.plourde@4cysec.io

4CYSEC
CYBER SECURITY EXPERT

e préparer aux audits

s points de vigilance à prendre en compte

Le registre des traitements de données à caractère personnel

Le respect des formalités préalables à la mise en œuvre d'un traitement

Les **principes juridiques** contrôlés par la CNIL : e respect des principes de **licéité des raitements**, la **durée de conservation des lonnées**, le **respect des droits** des personnes concernées, les **transferts de données** en dehors le l'UE

Les **mesures de sécurité** contrôlées par la CNIL : es rôles et les responsabilités, la sous-traitance, la écurité physique et logique des équipements, la gestion des habilitations, les champs commentaires dans les applications, les outils de surveillance du réseau, la sécurité des données lans le cadre de nouveaux projets

CNIL

COMMISSION NATIONAL
INFORMATIQUE & LIBERTÉ

Préparer l'entreprise aux audits

- Le rôle de la Direction Générale
- Le rôle des responsables de services durant l'audit
- La préparation des personnels d'accueil
- Comment se comporter lorsque l'inspecteur de la CNIL nous interroge ?
- Les documents à prévoir

Ce qui se passe avant un contrôle de la CNIL

La décision de procéder à une mission de contrôle est prise par le Président de la CNIL, sur proposition du service des contrôles.

La décision de prévenir, ou non, le responsable de traitement est prise en opportunité. La convocation doit parvenir au moins 8 jours avant.

Il peut être demandé au responsable de traitement visé par un contrôle de communiquer préalablement des documents.

Lorsque le contrôle se fait sur place, le procureur de la République est informé de la date, de l'heure et de l'objet du contrôle 24 heures avant.

Lorsque le contrôle est effectué à la demande d'un homologue d'un Etat membre de l'UE, la CNIL en informe le responsable du traitement.

Les agents de la CNIL participant aux contrôles sont habilités dans les conditions prévues par la loi. Ils peuvent être assistés d'experts.

ne mission de contrôle vise
ritairement à obtenir copie du
maximum d'informations,
chniques et juridiques, pour
oprécier les conditions dans
uelles sont mis en œuvre des
traitements de données à
caractère personnel.

La délégation de la CNIL peut demander communication de tous documents nécessaires à l'accomplissement de sa mission, quel qu'en soit le support, et en prendre copie..

Les contrôleurs peuvent accéd
aux programmes informatiques
aux données, et en demander
transcription pour les besoins
contrôle.

La délégation peut demander copie de : contrats (ex.: contrats de location de fichiers, contrats de sous-traitance informatique), formulaires, dossiers papiers, bases de données, etc.

Un procès-verbal de fin de mission est établi à l'issue du contrôle, pour préciser notamment la liste des documents dont une copie a été effectuée.

e qui se passe **pendant** un contrôle
e la CNIL

Ce qui se passe **après** un contrôle de la CNIL

- A l'issue du contrôle, la CNIL examine les documents dont une copie aura été effectuée pour apprécier les conditions de mise en œuvre des dispositions de la loi informatique et libertés.
- Lorsque les constatations effectuées n'appellent pas d'observations particulières, le contrôle est clôturé par un courrier du président de la CNIL qui peut contenir des recommandations (ex. : modification des durées de conservation, des mesures de sécurité, etc.).
- Lorsque les manquements relevés sont sérieux, le dossier est transmis à la formation restreinte de la CNIL, qui peut prononcer les sanctions prévues par la loi. Cette transmission à la formation restreinte n'est pas exclusive d'une dénonciation au Parquet (article 40 du code de procédure pénale).

Lorsque la CNIL est empêchée de contrôler

Dans le cadre d'un contrôle sur place, lorsqu'un responsable des locaux contrôlés s'oppose à la visite de la délégation, le Président de la Commission peut demande l'autorisation de poursuivre le contrôle aup du juge des libertés et de la détention du Tribunal de Grande Instance.

La loi punit d'un an d'emprisonnement et de 15 000 € d'amende, l'entrave à l'action de la CNIL.

Le contrôle en ligne un nouveau pouvoir de la CNIL

Les agents de la CNIL sont habilités à réaliser des vérifications à partir d'un service de communication au public en ligne (par exemple, un site internet).

Ils permettent le traitement de thématiques identifiées telles que le **dépôt de cookies** et d'autres traceurs, **les mentions d'information** à l'attention des utilisateurs ou la **sécurité du site internet.**

Les contrôles en ligne s'effectuent au sein de la CNIL à partir d'une plateforme et d'une connexion internet dédiées.

Ces contrôles se limitent à la consultation des données librement accessibles ou rendues accessibles, y compris par imprudence, négligence ou du fait d'un tiers.

Le contrôle en ligne débouche sur la rédaction d'un procès-verbal de constatations. Une demande d'information complémentaire peut être demandée.

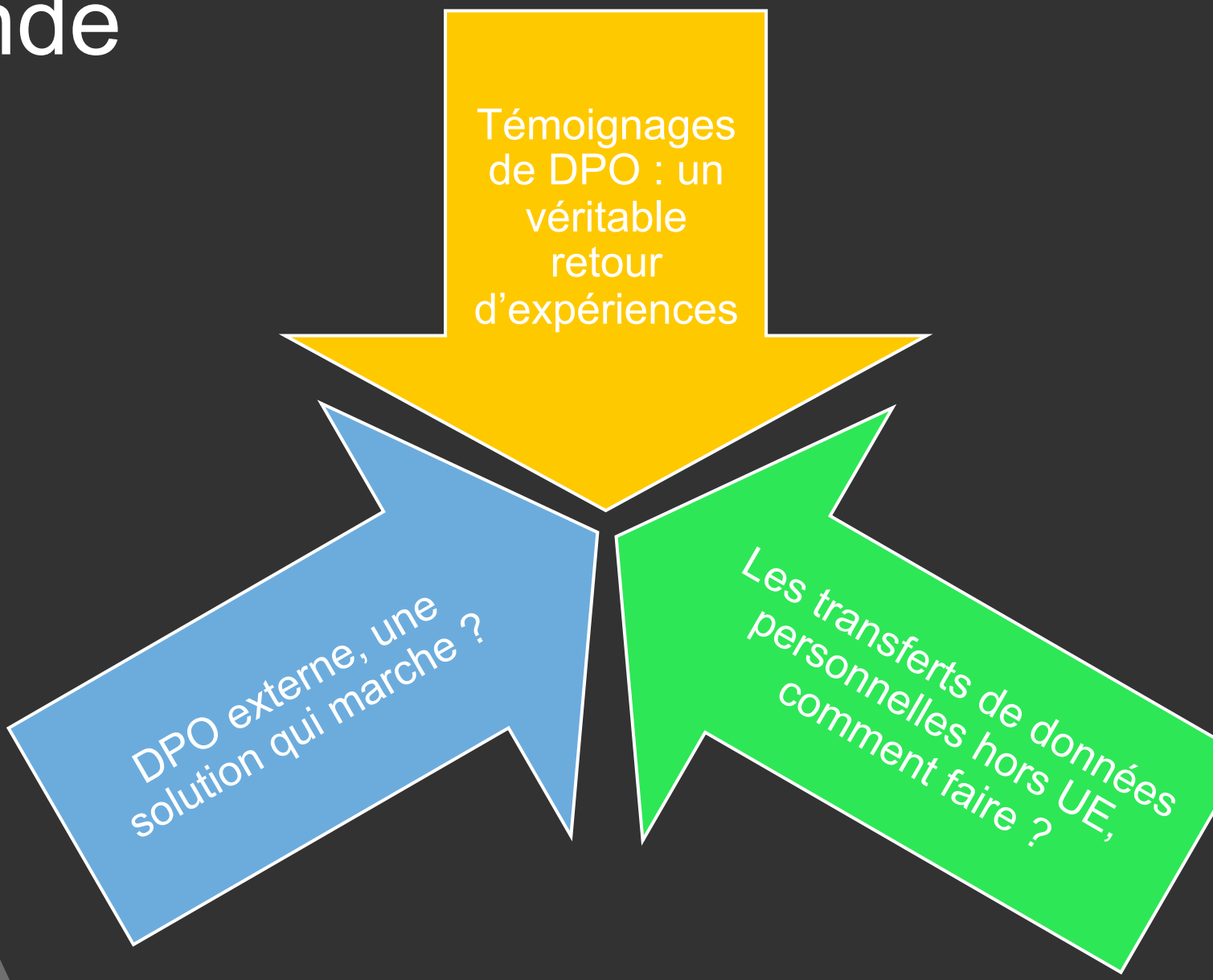
STITUT du RISK
COMPLIANCE

Merci pour votre attention

Corinne Plourde
corinne.plourde@4cysec.io

4CYSEC
CYBER SECURITY EXPERT

Table ronde



STITUT du RISK
COMPLIANCE