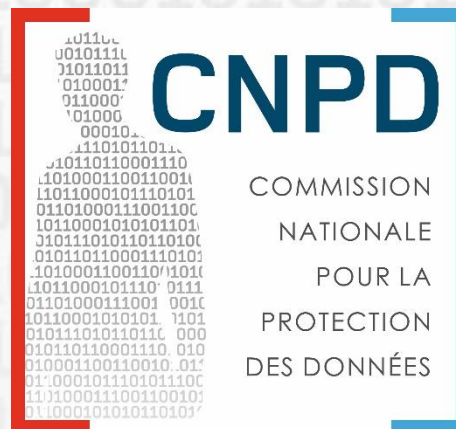


Règlement général sur la protection des données

Le contrôle de la conformité par la CNPD



14 mai 2018
Luxembourg

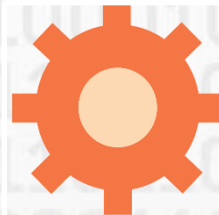
Christophe Buschmann
Membre effectif

Agenda



Missions,
pouvoirs

Approche



Les étapes
d'un contrôle

Conseils
pratiques



Missions et pouvoirs





Changement de paradigme

Pas de reporting régulier et obligatoire envers la CNPD

Contrôle à priori

Contrôle à postérieur

Mais: Le principe de la responsabilité nécessite une documentation et un reporting interne





Missions et pouvoirs

Article 57 Missions: Chaque autorité de contrôle, sur son territoire:

- **contrôle l'application** du présent règlement et veille au respect de celui-ci;
- **effectue des enquêtes** sur l'application du présent règlement, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique;
- **suit les évolutions pertinentes**, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, **notamment dans le domaine des technologies** de l'information et de la communication et des **pratiques commerciales**;
- ...

Article 58 Pouvoirs: Chaque autorité de contrôle dispose de tous les pouvoirs d'enquête suivants:

- mener des **enquêtes sous la forme d'audits** sur la protection des données;
- obtenir du responsable du traitement et du sous-traitant **l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires** à l'accomplissement de ses missions;
- obtenir **l'accès à tous les locaux** du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres.
- ...



Cooperation, mutual assistance, joint operations and consistency

Article 60 Coopération

- L'autorité de contrôle chef de file peut demander à tout moment aux autres autorités de contrôle concernées de se prêter mutuellement assistance en application de l'article 61 et peut mener des opérations conjointes en application de l'article 62, en particulier pour effectuer des enquêtes ou contrôler l'application d'une mesure concernant un responsable du traitement ou un sous-traitant établi dans un autre État membre.
- ...

Article 61 Assistance mutuelle

- ...L'assistance mutuelle concerne notamment les demandes d'informations et les mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables, les inspections et les enquêtes
- ...

Article 62 Opérations conjointes

- Les autorités de contrôle mènent, le cas échéant, des opérations conjointes, y compris en effectuant des enquêtes conjointes et en prenant des mesures répressives conjointes, auxquelles participent des membres ou des agents des autorités de contrôle d'autres États membres
- ...

Article 63 Mécanisme de contrôle de la cohérence

- Afin de contribuer à l'application cohérente du présent règlement dans l'ensemble de l'Union, les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission dans le cadre du mécanisme de contrôle de la cohérence établi dans la présente section.

Approche





Objectifs des contrôles

Identifier
des
problèmes
ponctuels et
récurrents

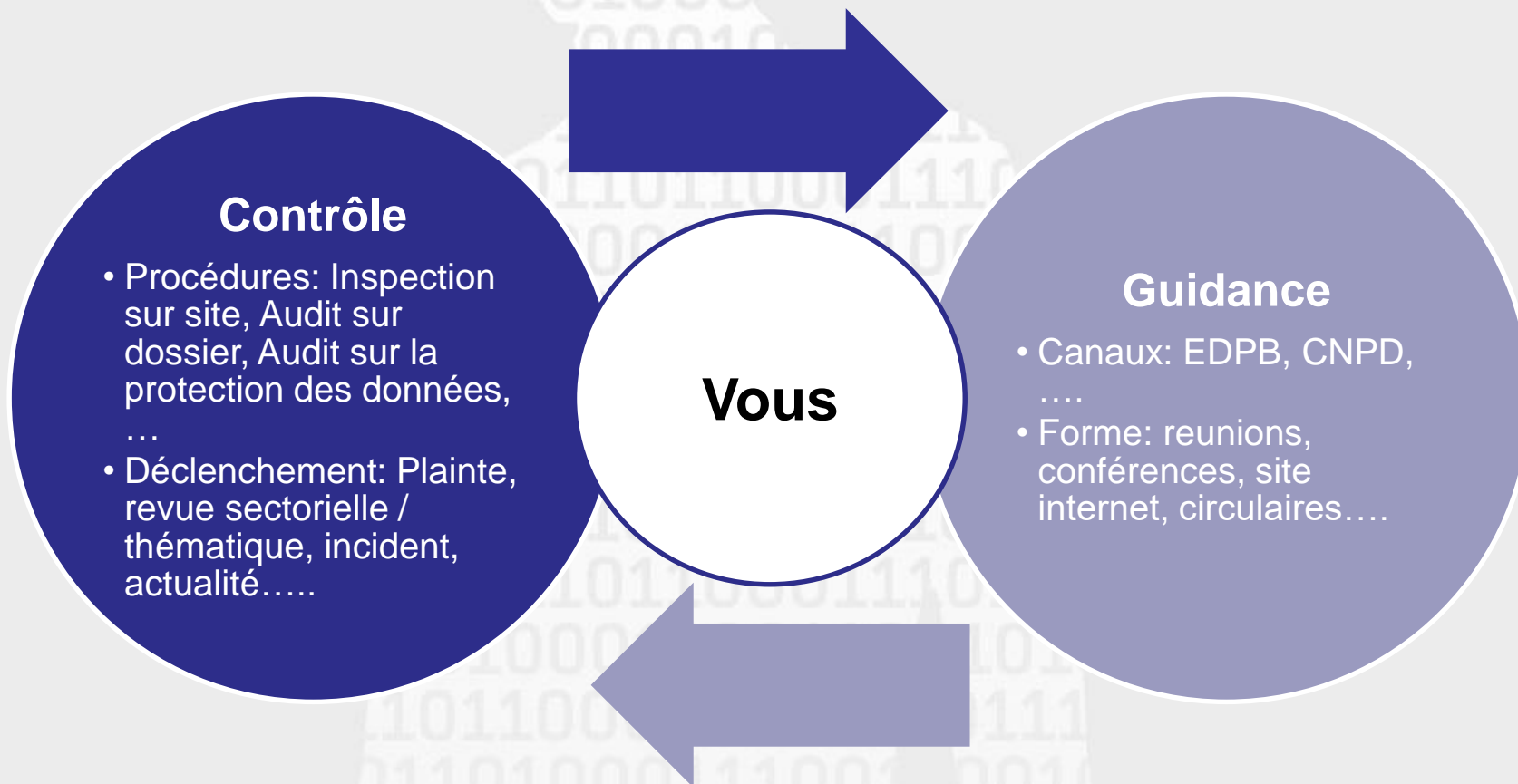
Vérifier
l'application
de guidance
fournie

Investigation
en cas de
problèmes
notifiés

Vérifier la
mise en
place de
mesures de
mise en
conformité

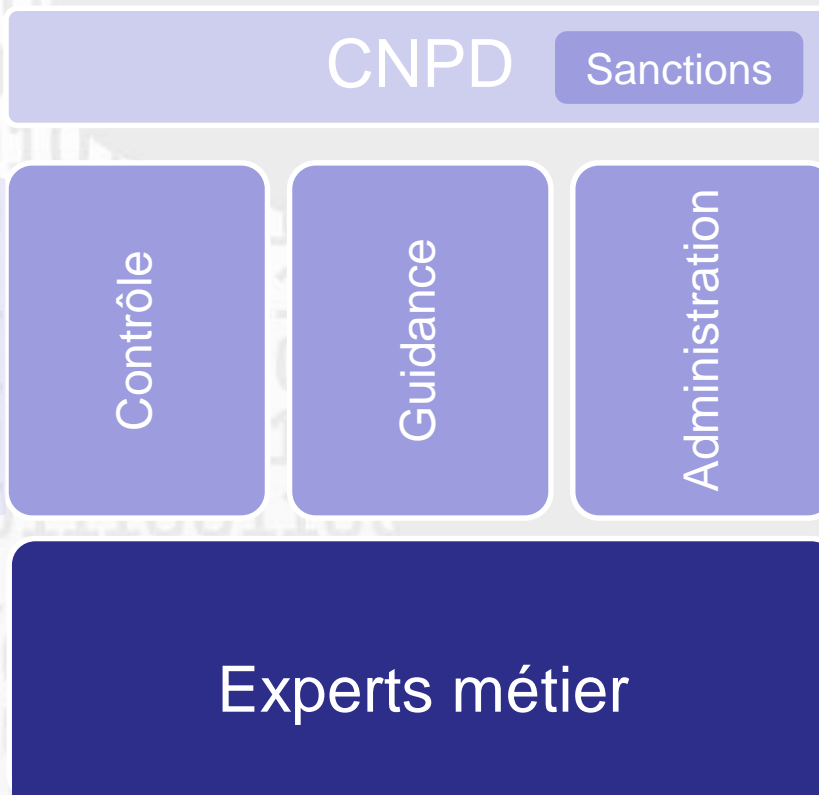
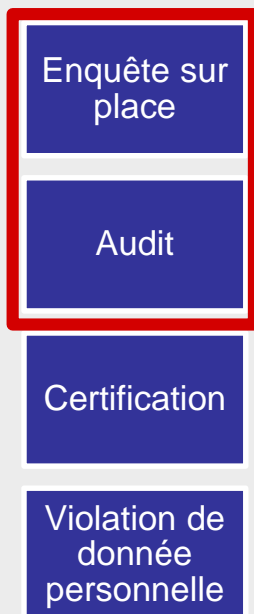


La bonne balance





Structure organisationnelle



Les intervenants



Collège



Chef d'enquête



Enquêteur



Expert



Coopération européenne

Types de contrôle

Enquête sur place

- Inspection sur site
- Périmètre ciblé
- Intervention ponctuelle

Enquête sur dossier

- Transmission d'un questionnaire
- Analyse des réponse / éléments fournis
- Adaptation de l'approche si nécessaire / utile

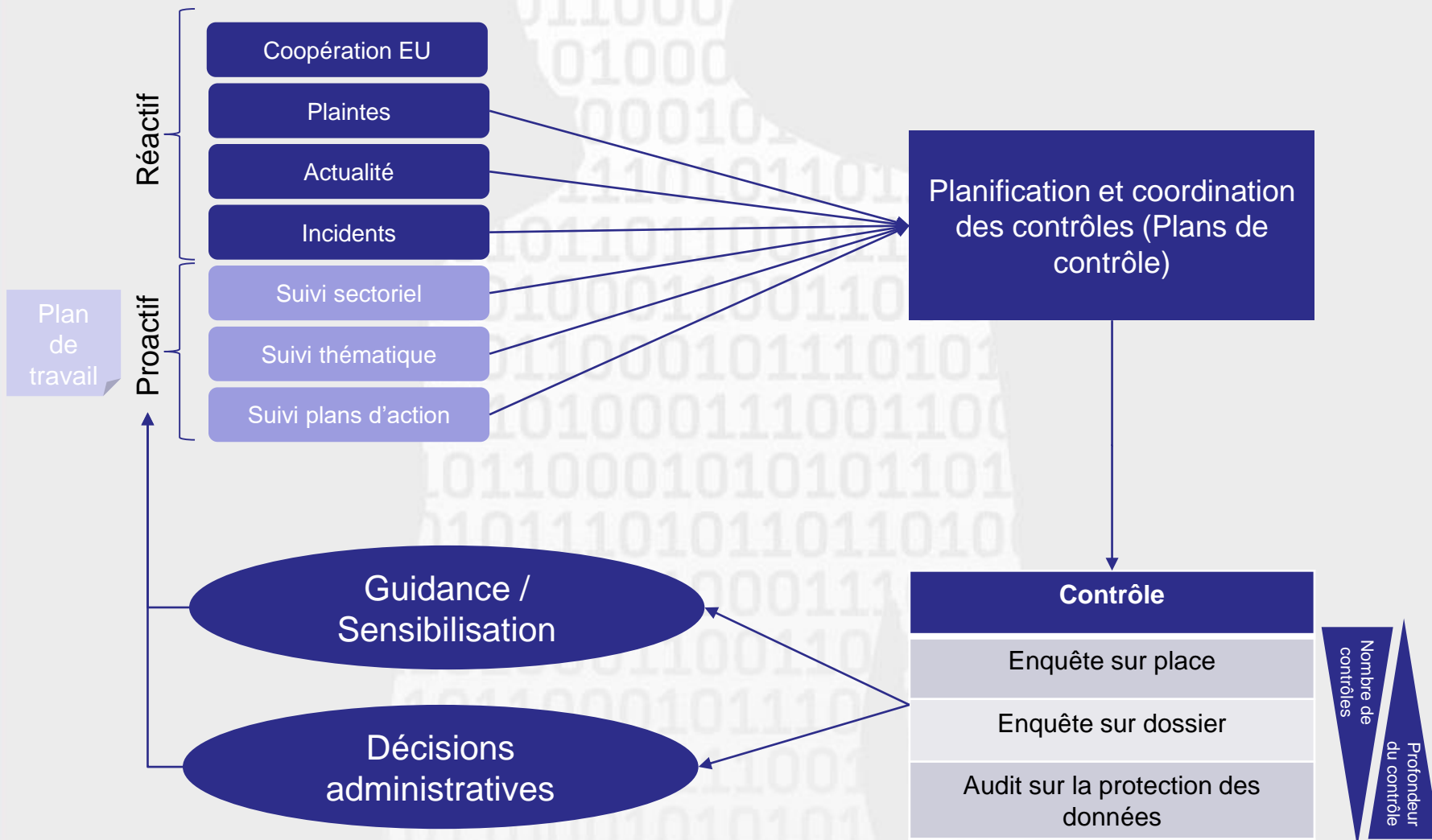
Audit sur la protection des données

- Revue plus approfondie
- Plusieurs échanges physiques et formels
- Périmètre plus large et adapté en fonction de l'évolution du dossier

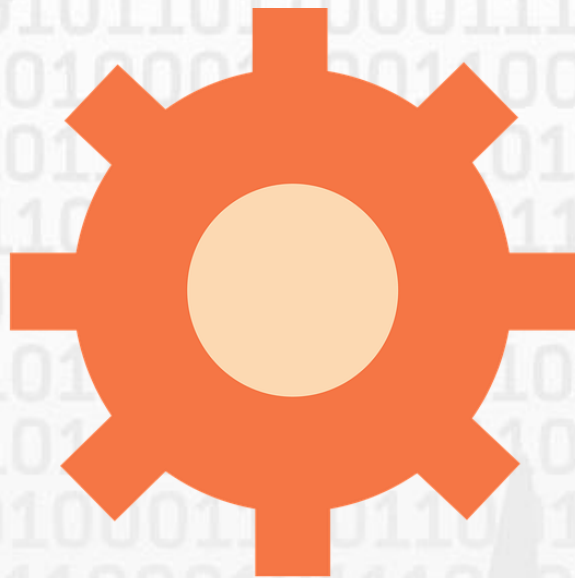




Référentiel de contrôle



Les étapes d'un contrôle





Les étapes d'un contrôle

Encadrement sur site:

Manipulations de systèmes IT à réaliser par vos soins. Accès physique avec votre présence.

Indépendance:

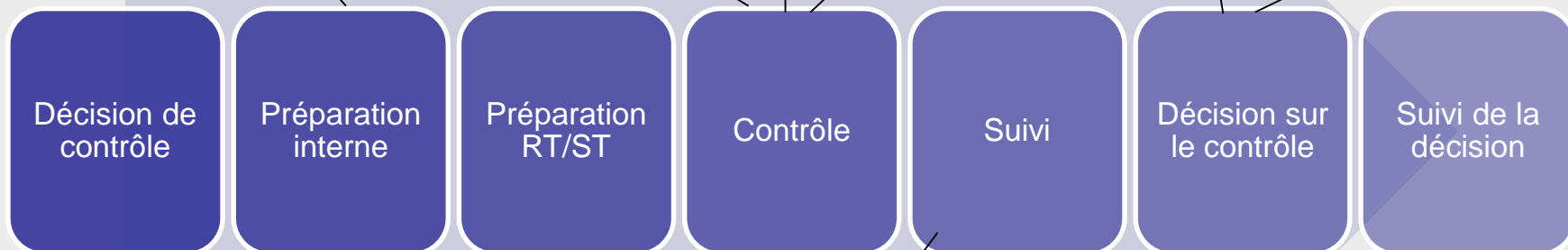
Pas de vote du chef d'enquête.

Annonce: Enquête sur place en règle général non annoncée. Audit annoncé.

Présentation sur site: Identification avec carte de légitimation. Possibilité de vérifier auprès de la CNPD.

Discrétion: Minimisation de l'impact sur votre métier

Formalisme: Décision administrative – pas nécessairement avec une sanction



Référentiel: Approche transparente et structurée

Documentation: Si applicable une liste des éléments à préparer / des préparatifs à assurer sera fournie

Formalisme: PV du contrôle, et le cas échéant un rapport d'audit - Email encrypté si souhaité

Interactions: Possibilité d'audition et ou autres échanges (formels)

Délais de réponse: Indication claire et adaptée au cas par cas – prévenir en cas de problèmes (absence de réponse)

Recommandations / mise en demeure: Pas de décision administrative – clarification de nos attentes

Recours: Délais de recours

Conseils pratiques





Avant le contrôle

Informez le personnel relevant de la possibilité de contrôle

Définissez au préalable une personne de contact interne disponible en cas de contrôle

Informez vous où se trouve la documentation – respectivement les personnes qui le savent

Impliquez le DPO si applicable dans la mise en place de ces procédures (si applicable)

Pour les enquêtes sur dossier et audits: impliquez les bonnes personnes dès le départ

Evitez des problèmes en premier lieu: Plaintes, incidents, plans de mitigation non suivis,....



Pendant le contrôle

Soyez transparent
coopératif et honnête

Vérifiez la qualité /
l'exactitude des
éléments que vous allez
nous fournir

Soyez spécifiques dans
les réponses – évitez
des malentendus

Si applicable – assurez
une disponibilité
d'éventuels experts
(p.ex. au niveau IT)

Assurez le respect
mutuel – politesse et
professionnalisme

Soyez proactifs si des
éléments
éventuellement
pertinents n'ont pas été
demandé explicitement

N'hésitez pas à poser
des questions



Après le contrôle

Vérifiez les PV transmis et faites nous part de vos commentaires

Respectez les délais

Restez joignables en cas de questions

Prenez en compte les éventuelles recommandations / mises en demeure indiquées

Informez nous des mesures déjà prises ainsi que des mesures que vous comptez mettre en place – avec un engagement et des délais

Assurez vous de la qualité et exactitude des informations et pièces transmises (notamment si une demande de préparation a été faite)

N'hésitez pas à communiquer avec nous lorsque vous avez des questions

Vous avez la possibilité de demander une audition – évitons les mauvaises compréhensions



Après la décision

Analysez la décision fournie – une décision ne comporte pas toujours une sanction

Soyez conscient des délais (de recours) qui courent

N'hésitez pas à nous contacter si vous avez des questions

Respectez les éventuels engagements sur les plans d'action que vous avez pris

Si applicable – vérifiez bien les actions que vous devez entreprendre (p.ex. interdiction de traitement,...)

Si applicable - Communiquez –nous toute impossibilité d'implémenter la décision.

Commission nationale pour la protection des données

Merci pour votre attention!

