

Protection des données au Luxembourg

Quelles nouveautés en matière de décisions et jurisprudences ?

Programme

I. Les règles procédurales devant la CNPD

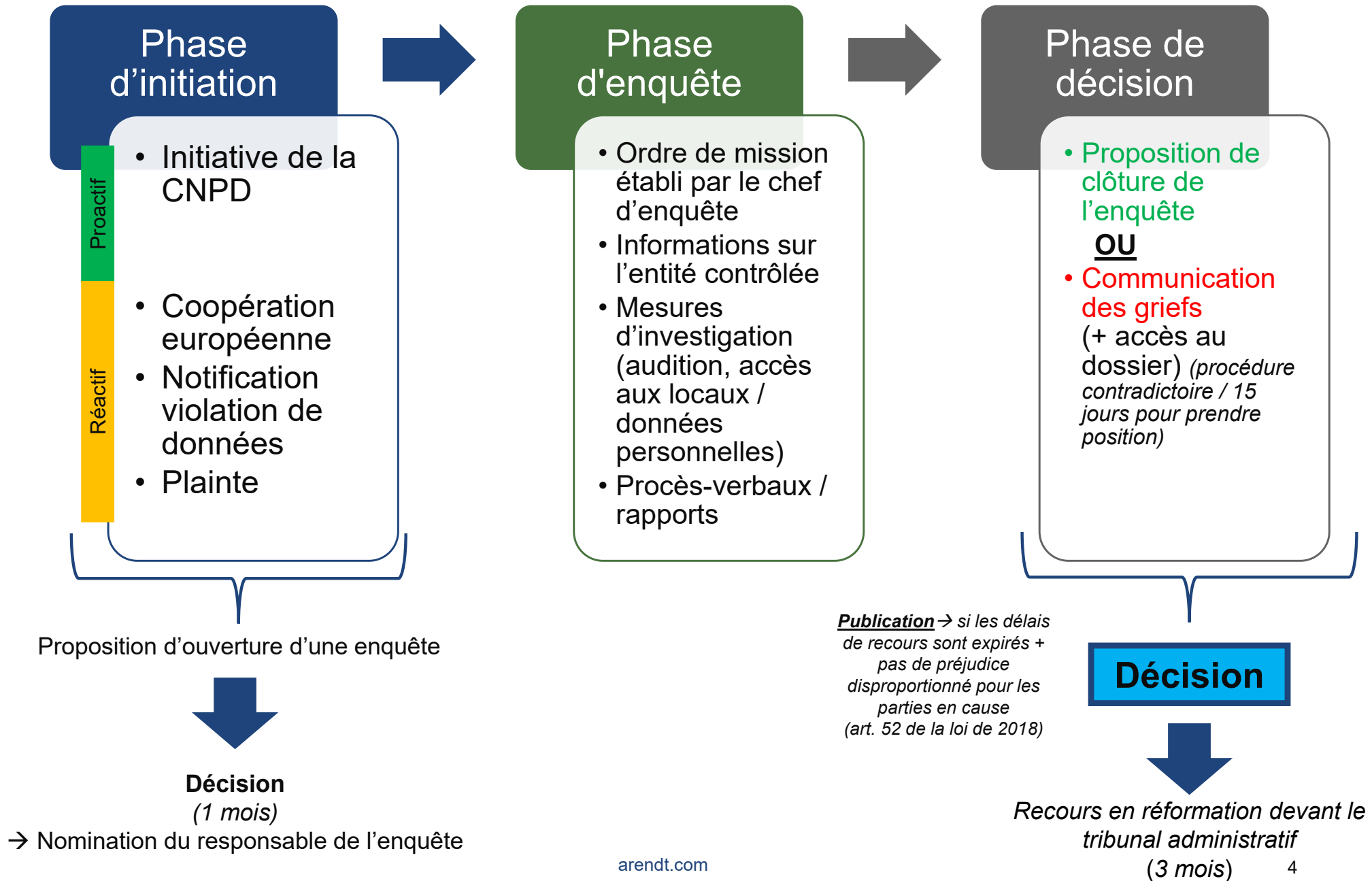
II. Les décisions de la CNPD

III. L'affaire Amazon

I. Les règles procédurales devant la CNPD

Différentes phases...

arendt



Quelques chiffres : Audits et enquêtes sur place de la CNPD

2018

- 25 **audits** concernant le DPO
- 12 **enquêtes sur place** sur la vidéosurveillance, la géolocalisation, la publicité et le marketing

2019

- 25 "**audits proactifs**" concernant le DPO
- 9 "**audits réactifs**" suite à des réclamations (droit d'accès, sécurité, recrutement, cookies, etc.)
- 33 **enquêtes sur place** concernant la vidéosurveillance, la géolocalisation, la publicité et le marketing

2020

- 6 **audits** concernant la "transparence" dans le secteur des communications électroniques
- 8 **enquêtes sur place** sur la vidéosurveillance et les traitements pendant Covid-19

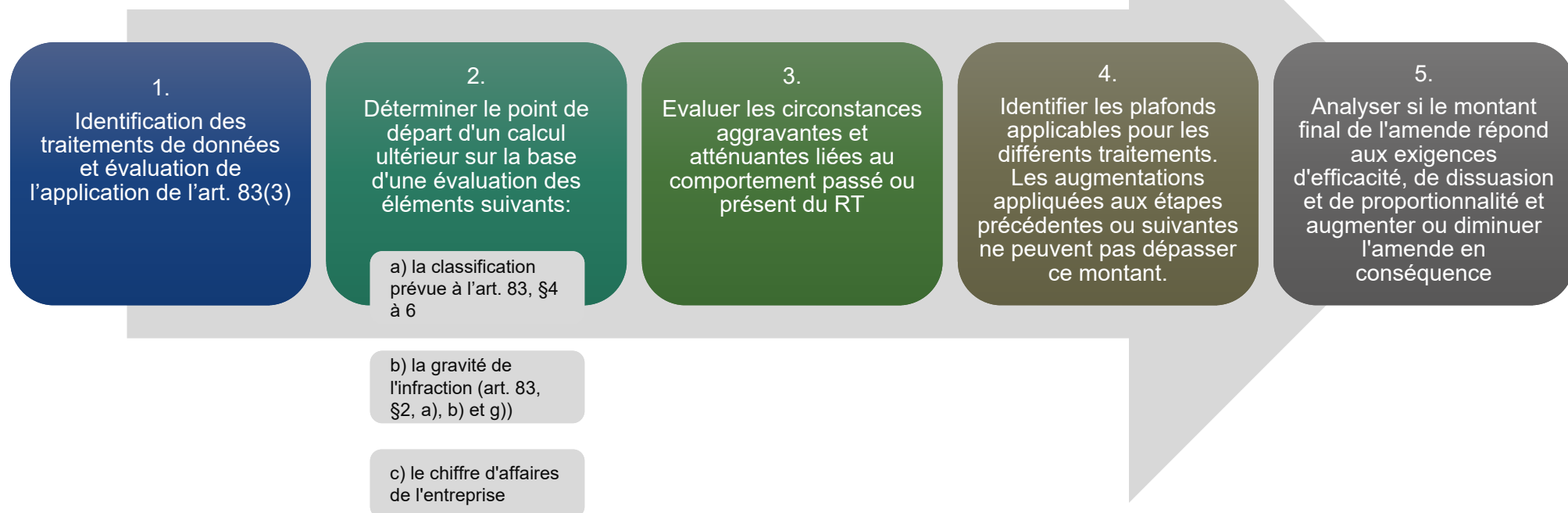
2021

- 6 **audits** concernant la "transparence" (responsabilisation) dans le secteur des services en ligne
- 18 **enquêtes sur place** principalement sur la vidéosurveillance



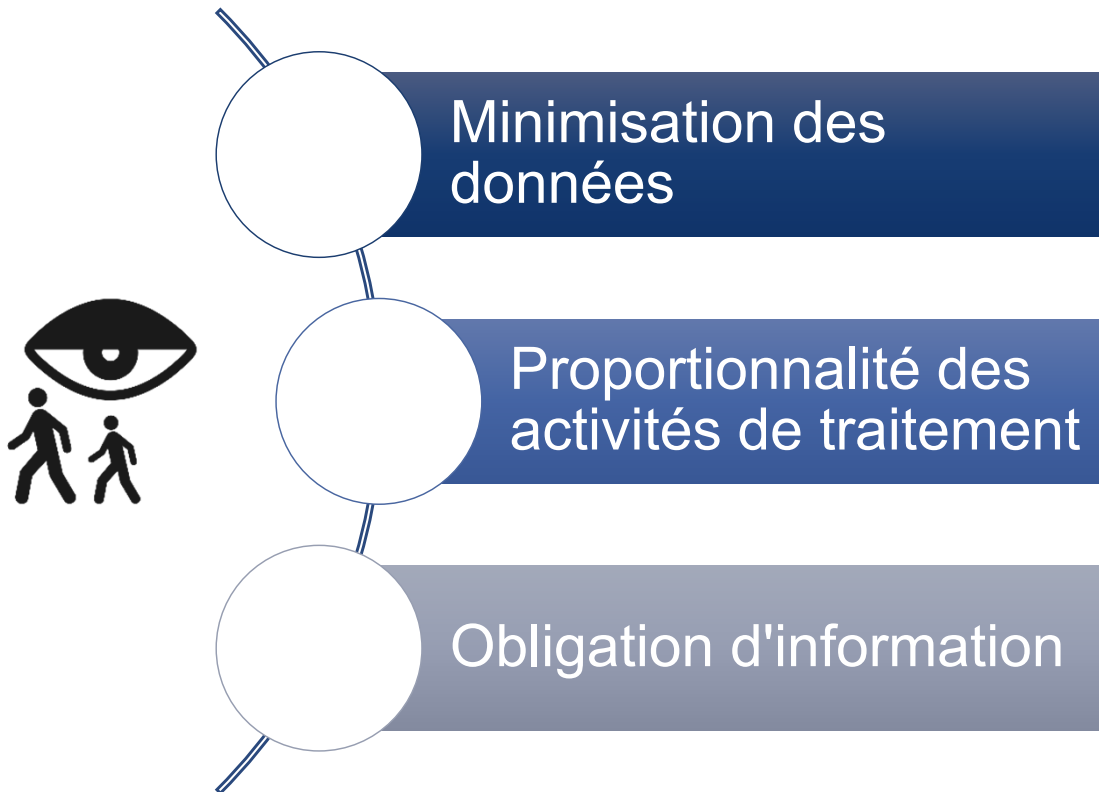
Des nouveautés concernant les sanctions...

- Amende effective, dissuasive et proportionnée (art. 83, §1 RGPD)
- Lignes directrices de l'EDPB 04/2022 du 12 mai 2022 → méthodologie harmonisée pour calculer le montant des sanctions :



II. Les décisions de la CNPD

1^{er} thème : Vidéosurveillance & géolocalisation



Principes clés rappelés
par la CNPD dans toutes
ses décisions concernant
ce sujet

Décisions en matière de surveillance et de géolocalisation : faits marquants

Nombre de décisions	33
Dates d'audit	• 12 audits ouverts de déc. 2018 à sept. 2019 – secteur public, industriel, tertiaire • 6 audits ont été réalisés en mars 2019 • Enquêtes sur place
Sanctions	• <u>Amendes</u>: 1K à 12.5K • <u>Mesures correctrices</u> : avertissements / injonctions de se conformer au RGPD
Violations principales	• Non-respect du principe de minimisation des données • Champ de vision des caméras disproportionné • Manque d'information des personnes concernées (qu'il s'agisse d'employés du responsable du traitement ou de tiers), l'utilisation du pictogramme n'étant pas suffisante pour satisfaire à l'article 13 du RGPD • Périodes de rétention excessives
Autres références	• Directives de la CNPD sur la vidéosurveillance • Les directives du WP "WP 260 rev01" sur la transparence (Groupe article 29) • Lignes directrices 3/2019 de l'EDPB sur le traitement des données personnelles par le biais de dispositifs vidéo

Principaux éléments à retenir de la décision la plus importante

- Décision 24FR/2021 - 29 juin 2021
- Secteur : Fabrication de pain et de pâtisseries fraîches

Amende administrative de 12.500€ + injonction de se conformer à l'art. 13 RGPD



Enregistrement des espaces publics

- Art. 5.1. c) du RGPD - Le RT doit se conformer au principe de **minimisation des données**.
- Ce n'est pas le cas lorsque les champs de vision des caméras permettent d'enregistrer les zones publiques entourant le magasin du RT.
- Le champ de vision doit être limité à la surface strictement nécessaire pour visualiser l'accès des personnes (compte tenu des objectifs poursuivis - c'est-à-dire la protection des biens du responsable du traitement, la sécurisation de l'accès aux locaux, la sécurité des utilisateurs et la prévention des accidents).



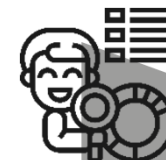
Enregistrement des employés

- Art. 5.1. c) du RGPD - Le RT doit mettre en place un **suivi proportionné**.
- La surveillance continue des employés sur le lieu de travail est disproportionnée au regard de la finalité du traitement.
- Constitue une atteinte excessive à la vie privée des employés à leur poste de travail



RT doit informer les personnes concernées

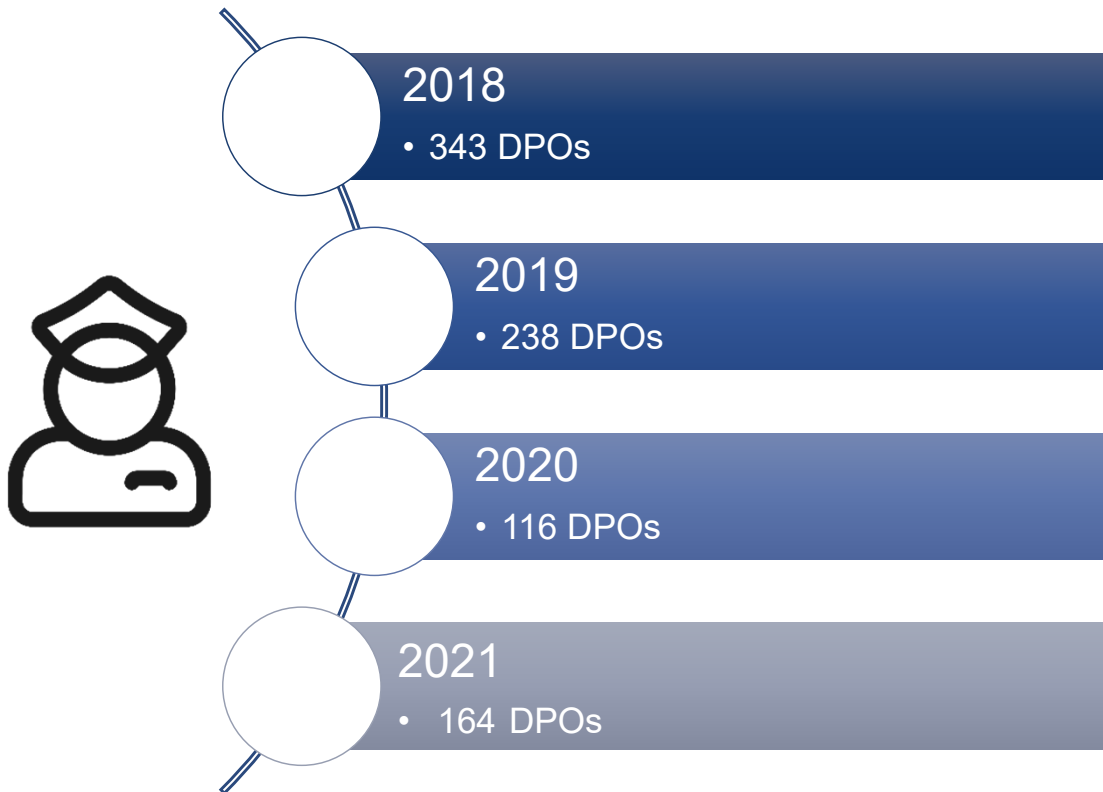
- Art 13 du RGPD
- Pour les tiers - l'apposition de pictogrammes mentionnant "pour votre sécurité, ce site est sous surveillance" n'est pas une information conforme au RGPD.
- Pour les employés - RT aurait dû informer ses employés avant les audits de la CNPD et l'information aurait dû contenir tous les détails requis par l'article 13 du RGPD.



Conclusion

- Minimisation et information
- Les champs de vision des systèmes de vidéosurveillance doivent être limités aux zones qui doivent être surveillées, ou bien ces systèmes doivent comporter des caractéristiques techniques permettant de masquer ou de brouiller les zones publiques.
- Les employés ont droit au respect de leur vie privée, même sur leur poste de travail, et la surveillance continue y porte atteinte.
- Les informations doivent être fournies de manière conforme au RGPD (par exemple, pictogrammes avec QR codes vers les politiques de confidentialité).

2ème thème : Délégué à la protection des données ("DPO")



1329
responsables de traitement
ont communiqué les
coordonnées de leur DPO à
la CNPD depuis le
25/05/2018

Décisions concernant les DPOs : faits marquants

Nombre de décisions	25
Dates d'audit	25 audits ouverts en 2018 dans le secteur privé et public / réalisés en 2021
Sanctions	<u>Amendes</u>: 13,2 K à 18,7 K <u>Mesures correctrices</u> : avertissements / injonctions pour se conformer au RGPD
Violations principales	- Communication tardive des informations du DPO - Qualifications professionnelles du DPO - Le temps et les ressources nécessaires mis à la disposition du DPO ne sont pas suffisamment documentés - Conflit d'intérêt Chief Compliance Officer / DPO - Violations en rapport avec les missions de contrôle / d'information et de conseil du DPO
Autres références	Lignes directrices de l'EDPB sur le délégué à la protection des données (WP 243)

DPO : les points clés de la décision la plus importante

- Décision 41/FR/2021 - 27 octobre 2021
- Secteur : banques / établissements de crédit

Amende administrative de 18 700€ + injonction de se conformer à l'art. 38.3 RGPD



Les personnes concernées doivent pouvoir **contacter** directement le DPO.

- Art. 37 §7 du RGPD
- Le site web du RT doit prévoir les coordonnées du DPO.



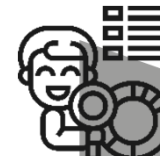
Le DPO doit être **impliqué** dans toutes les questions relatives à la protection des données.

- Art. 38 §1 du RGPD
- Ce n'est pas le cas lorsque le DPO ne participe que sur invitation ou sur une base ad hoc à des réunions ou comités internes portant sur des sujets liés à la protection des données.
- Le RT doit établir des règles formelles pour permettre au DPO de participer régulièrement à ces réunions.



Le DPO doit être **autonome** et indépendant

- Art. 38 §1 du RGPD
- Le DPO doit être rattaché au plus haut niveau de la hiérarchie afin de garantir une autonomie maximale (sans intermédiaire).

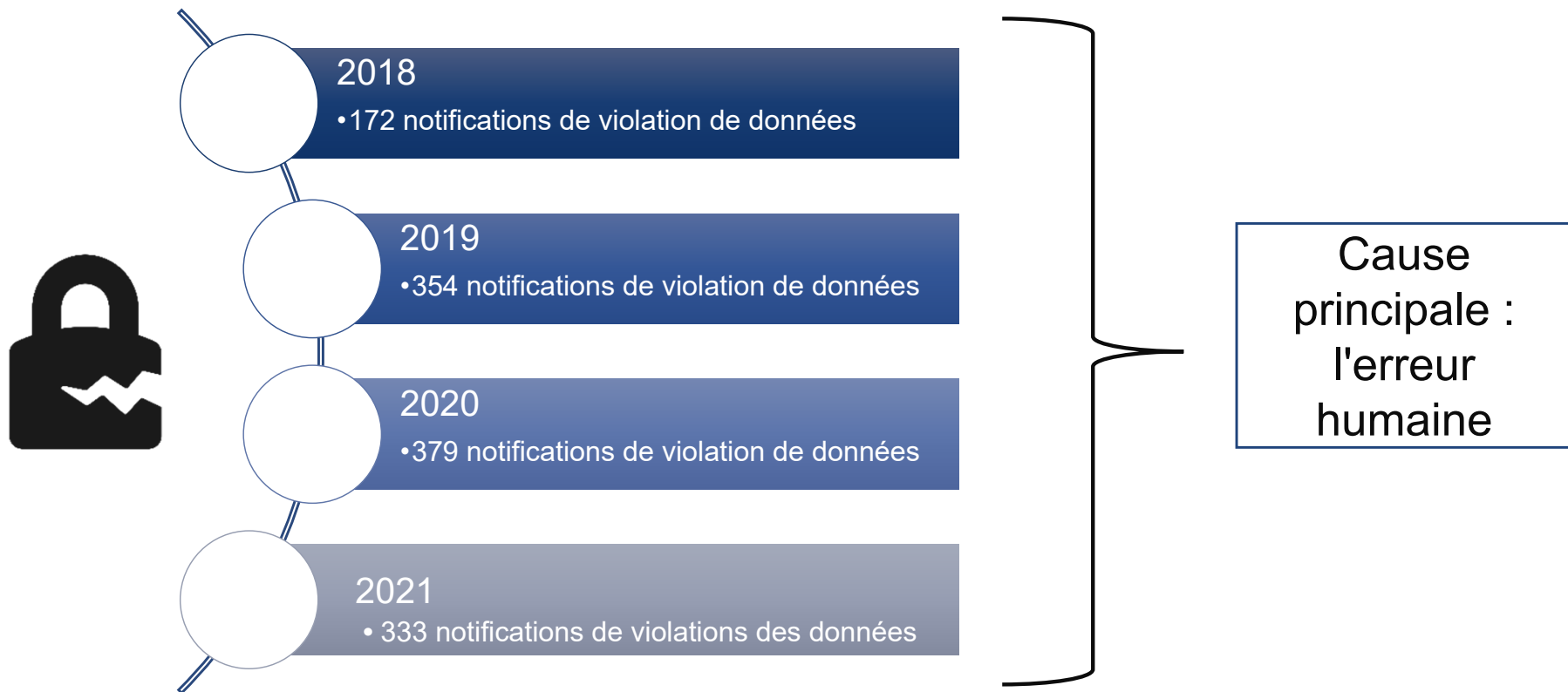


Mission de **contrôle** du DPO

- Art. 39 §1 du RGPD
- Un " plan de contrôle " formel de la protection des données doit être élaboré / mis en œuvre.
- En particulier, les registres internes doivent être rédigés / conservés et considérés comme un outil permettant au DPO d'exercer sa mission de contrôle.

3^{ème} thème : Violations des données

La violation des données doit être notifiée à la CNPD **sans retard excessif et, si possible, au plus tard 72 heures après en avoir pris connaissance**, à moins que la violation des données personnelles ne soit pas susceptible d'entraîner un risque pour les droits et libertés des personnes physiques (art. 33 du RGPD).

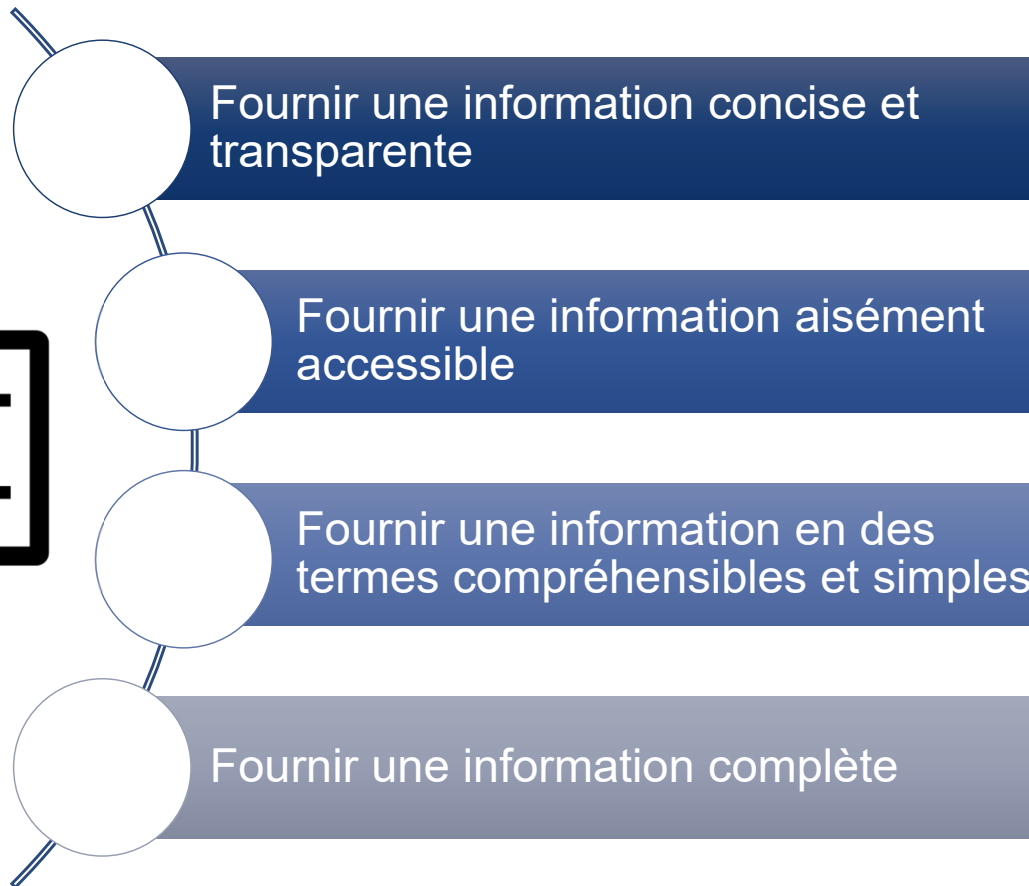


Basé sur les rapports annuels de la CNPD.

Décision sur la violation des données : faits marquants

Nombre de décisions	1 (Décision n° 31FR/2021 du 5 août 2021) Secteur : assurance et réassurance
Dates d'audit	• Plainte en mai 2019 • Ouverture d'une enquête en juin 2019 / inspection sur place en juillet 2019
Sanctions	• <u>Amende</u> : 135 K • <u>Mesures correctrices</u> : • injonction de se conformer au RGPD • protection des courriels contenant des données sensibles par des mesures appropriées
Violations principales	• Défaut de documentation de la violation des données personnelles • Défaut d'information de la CNPD • Défaut d'information des personnes concernées • Défaut d'assurer la sécurité du traitement des données
Autre référence	Lignes directrices de l'EDPB sur la notification des violations de données personnelles en vertu du règlement 2016/679 (WP 250).

4^{ème} thème : Principe de transparence



Principes clés rappelés
par la CNPD dans toutes
ses décisions concernant
ce sujet

Décision sur le principe de transparence: faits marquants

Nombre de décisions	6
Dates d'audit	• 6 audits ouverts en 2020
Sanctions	• <u>Amendes</u>: 700 à 3K • <u>Mesures correctrices</u> : injonction de se conformer au RGPD
Violations principales	• La politique de protection des données ne reflète pas la réalité des traitements • Les personnes concernées ne sont pas systématiquement informées de la mise à jour de la notice d'information et aucun résumé des principaux changements • La traduction de la notice d'information n'est disponible qu'en une seule langue alors que le portail est disponible en plusieurs langues • L'information relative aux durées de rétention n'est pas assez précise • Les bases légales ne sont pas rattachées aux traitements • Aucune information sur le transfert de données vers un pays tiers • Terminologie vague
Autres références	• Lignes directrices de l'EDPB sur le principe de transparence en vertu du règlement 2016/679 (WP 260) • Décision contraignante de l'EDPB du 1/2021 concernant le litige relatif au projet de décision de l'autorité de contrôle irlandaise concernant WhatsApp Ireland en application de l'article 65, paragraphe 1, point a), du RGPD

Principe de transparence : les points clés de la décision la plus importante

- Décision 20/FR/2022 - 13 décembre 2022
- Secteur : exploitation de portails internet et offre de services via ces portails

**Amende administrative de
3 000€**



La politique d'information doit mentionner tous les traitements réellement effectués

- Art. 12.1 du RGPD
- Sans anticipation de traitements qui pourraient éventuellement être mis en place par le contrôlé dans le futur.
- Chaque traitement répertorié dans le registre doit être mentionné dans la politique de protection des données.



Les personnes concernées doivent être informées de manière active lors de modifications substantielles de la politique d'information

- Art. 12.1 du RGPD
- Un résumé des principaux changements effectués doit être mis à la disposition des utilisateurs lorsque les modifications apportées à la politique de protection des données sont conséquentes.
- Un pop-up, une bannière d'information ou une communication électronique doit être mis en place.



Le RT doit fournir une information compréhensible

- Art. 12.1 du RGPD
- La politique d'information doit être disponible dans toutes les langues du portail.



Le RT doit fournir une information complète

- Art. 13 du RGPD
- L'ensemble des finalités des traitements opérés doivent être indiquées.
- Les bases légales doivent être indiquées.
- Les intérêts légitimes poursuivis doivent être indiqués.
- Les catégories de destinataires doivent être indiquées.
- L'information relative aux transferts de données vers des pays tiers doit être communiquée.
- Les durées de rétention doivent être communiquées.
- Tous les droits des personnes concernées doivent être indiqués.

Thématiques supplémentaires

**Défaut de base légale
pour justifier la licéité
du traitement**

N°18FR du 13 décembre 2022

**Non-respect du droit
d'accès/droit à
l'effacement de la
personne concernée -**

N°9FR du 10 mars 2022

N°34FR du septembre 2021

**Défaut de mise en
place de mesures de
sécurité appropriées**

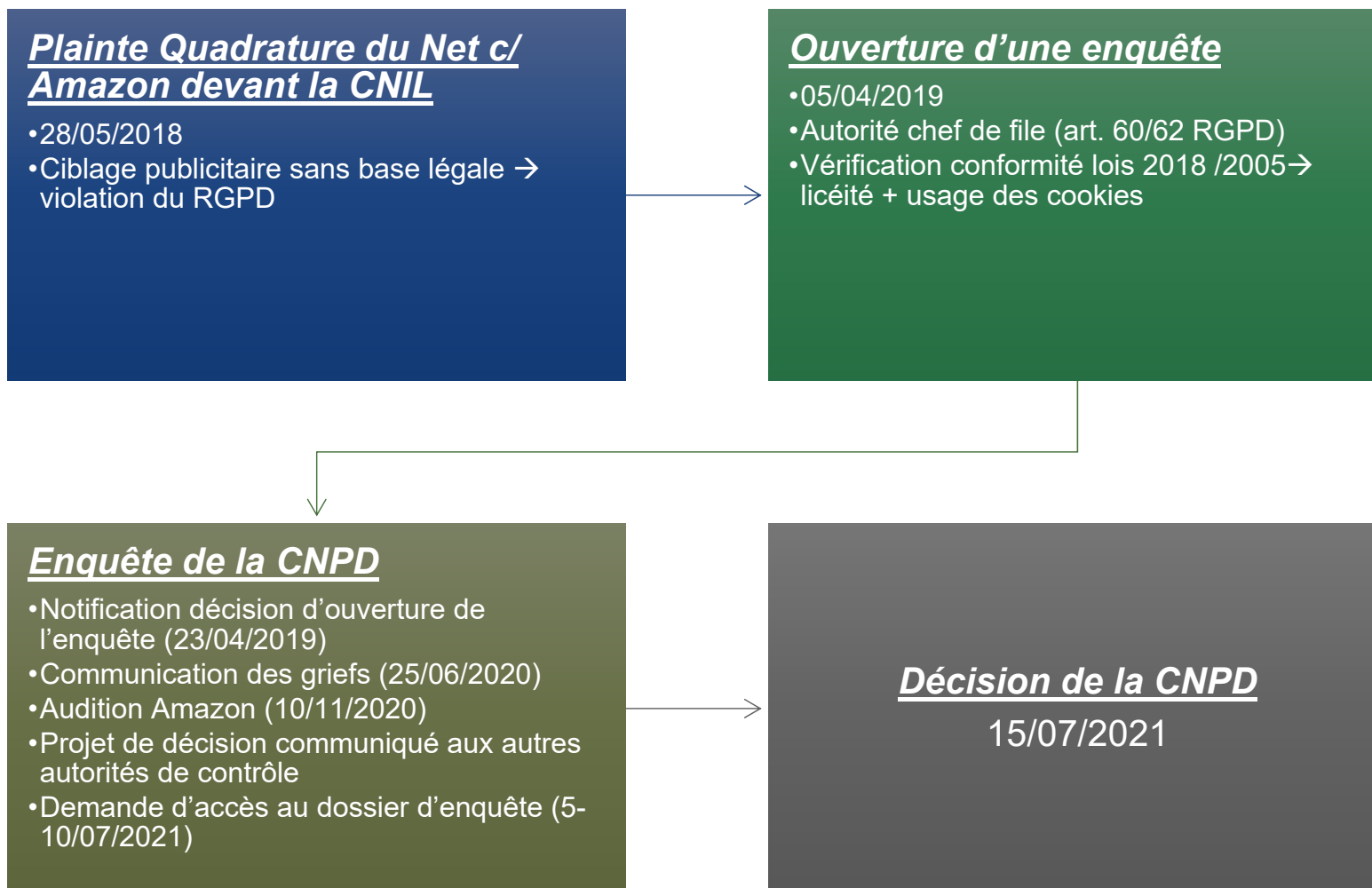
N°6FR du 4 mars 2022

**Utilisation illicite de la
banque des données
JU-CHA**

N°01 du 5 mars 2021

II. L'affaire Amazon

Affaire Amazon



Décision de la CNPD du 17 juillet 2021

■ Dispositif :

- Amende administrative de **746 millions d'euros** (violation art. 6.1, 12, 13, 14, 15, 16, 17 et 21 du RGPD)
- **Injonction de se mettre en conformité** avec ces articles dans un délai de **6 mois** suivant la notification de la décision (i.e. 01/2021):
 - Mise en conformité des traitements réalisés à des fins de publicité comportementale / art. 6.1 RGPD
 - Mise en conformité les mesures de transparence concernant ces traitements / art. 12, 13 et 14 RGPD
 - Mise en conformité des réponses données à toute future demande d'accès, modification et effacement / art. 15 à 17 du RGPD
 - Mise en conformité du mécanisme d'*opt-out* / art. 21 du RGPD
- Publication de la décision sur le site internet de la CNPD dès que les voies de recours sont épuisées



**Astreinte de 746.000 euros
par jour de retard**

*Justificatifs de la mise en conformité à
adresser à la CNPD au + tard avant
l'expiration du délai de 6 mois*

Suite à la décision de la CNPD...

- Amazon demande à la CNPD de confirmer que :
 - La décision devait être lue en ce sens que les mesures correctrices ne seront pas exécutées par la CNPD **avant que toutes les voies de recours soient épuisées**
- Réponse CNPD :
 - Seul le président du TA peut ordonner un sursis à l'exécution d'une décision administrative

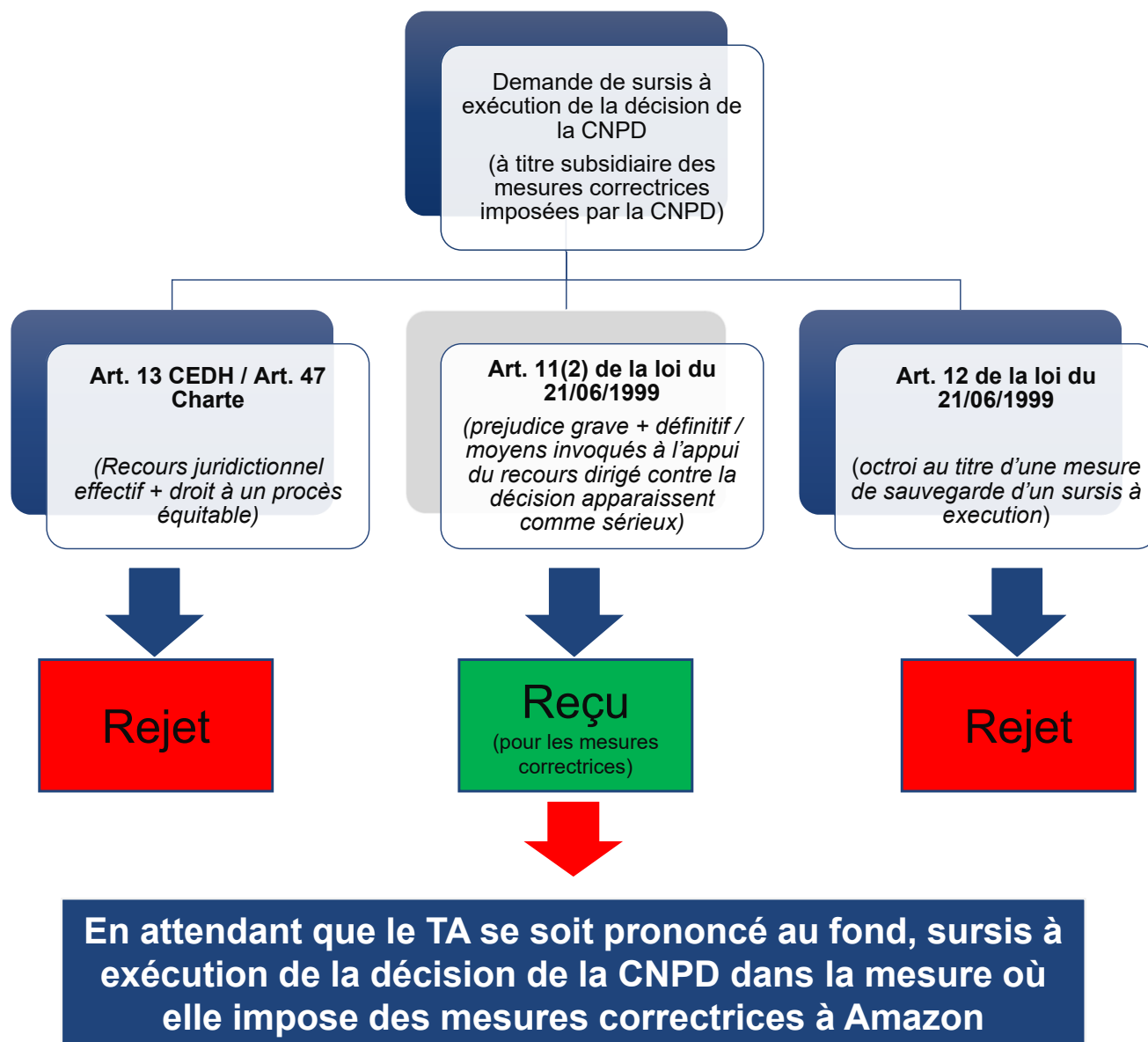


- Requête déposée par Amazon au TA le 15/10/2021 :
 - Recours en réformation sinon en annulation de la décision de la CNPD
 - Sollicite le bénéfice d'un effet suspensif du recours pendant le délai et l'instance d'appel

- Requête séparée du 29/10/2021 :
 - Instauration de mesures provisoires par rapport à la décision attaquée

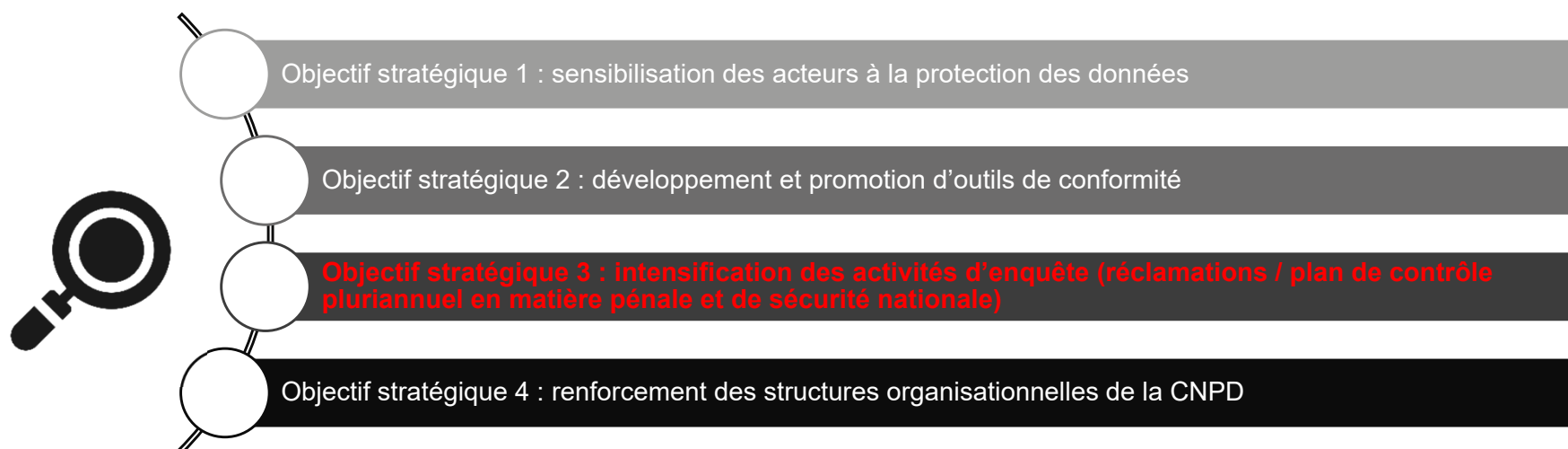


Ordonnance du TA de Luxembourg du 17 décembre 2021



Conclusion (1)

- Ces décisions montrent que la CNPD est active et que ses audits ne ciblent pas une industrie en particulier mais de nombreux secteurs différents
- La CNPD peut procéder à des audits de manière aléatoire, mais également suite à des plaintes de personnes concernées (employés, investisseurs, clients, etc.)
- **Programme de travail 2023/2024 de l'EDPB** → de nouvelles lignes directrices attendues
- **Programme de travail 2023/2025 de la CNPD**→



Conclusion (2)



- Rédiger et mettre en œuvre une procédure de *down-raid* interne
- Former votre personnel
- Impliquer un conseil juridique dès le début, en particulier lors des inspections sur place / réponse à la correspondance de la CNPD

Contact



Astrid Wagner

Associée

astrid.wagner@arendt.com

Tel.: +352 40 78 78 698



Faustine Cachera

Collaboratrice Senior

faustine.cachera@arendt.com

Tel.: +352 40 78 78 339



Sophie Calmes

Collaboratrice Senior

Sophie.Calmes@arendt.com

T +352 40 78 78 267



Julien Pétré

Collaborateur Senior

Julien.Petre@arendt.com

T +352 40 78 78 2139



Ines Nibakuze

Collaboratrice

Ines.Nibakuze@arendt.com

T +352 40 78 78 2078