

Protection des lanceurs d'alerte, mécanisme d'alerte interne et RGPD

Points d'attention pour les DPO

4 octobre 2022
Fanny COTON



I. Point sur la transposition en Belgique

II. Quelles alertes en matière de protection des données et de sécurité des réseaux ?

III. Le DPO peut-il être lanceur d'alerte ?

IV. Le mécanisme d'alerte interne : obligation ou faculté ?

V. Rôle du DPO dans le mécanisme d'alerte interne ?

VI. Protection des données du lanceur d'alerte et de la personne visée



Transposition



- Directive UE 2019/1937 sur les lanceurs d'alerte
- Délai de transposition : 17 décembre 2021

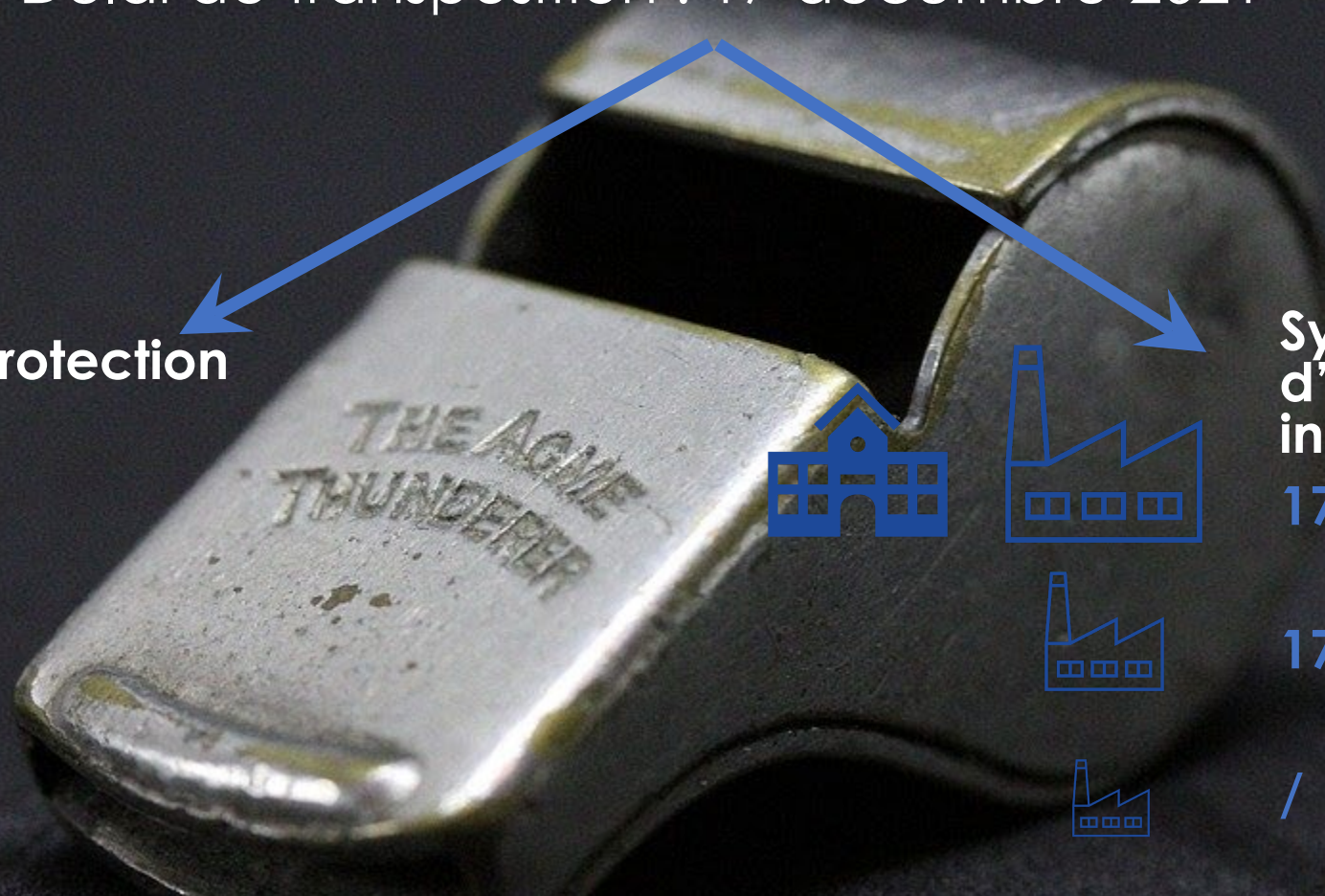


Protection

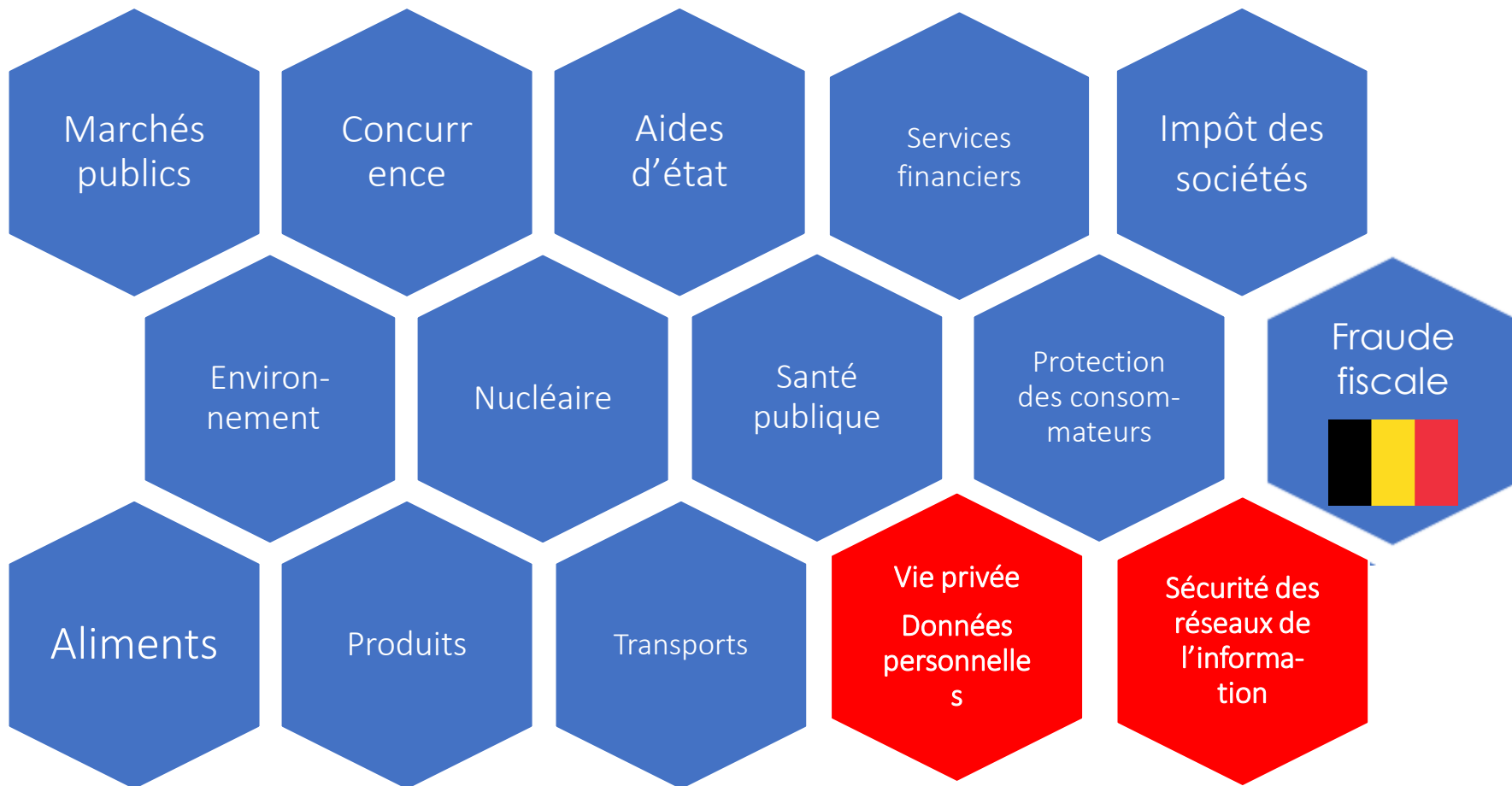
Système d'alerte interne

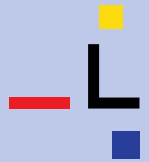
17/12/21

17/12/23



Champ d'application





- informations confidentielles
- dans certains domaines
- **à propos de pratiques qui constituent**
 - **une atteinte**
 - **ou une menace**



à l'intérêt général

- violations potentielles de ces réglementations, et aussi de leur esprit.

I. Point sur la transposition en Belgique

II. Quelles alertes en matière de protection des données et de sécurité des réseaux ?

III. Le DPO peut-il être lanceur d'alerte ?

IV. Le mécanisme d'alerte interne : obligation ou faculté ?

V. Rôle du DPO dans le mécanisme d'alerte interne ?

VI. Protection des données du lanceur d'alerte et de la personne visée

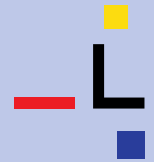


Quelles alertes potentielles en matière de protection des données et de sécurité des réseaux ?



(1) Violations de sécurité impliquant une obligation de notification

	Violation effective	Risque de violation
RGPD	v	x
E-privacy	v	v
NIS	v	x



(2) Niveaux de sécurité inadéquats

	obligations générales d'adoption de mesures de sécurité	Définition des mesures de sécurité ?
RGPD	v	/
E-privacy	v	/
NIS	v	Pas encore



(3) Faits sanctionnés pénalement

	Infraction	Dol spécial ?
RGPD	Absence de base de licéité	/
	traiter des données en violation de l'art 5	par négligence grave ou avec une intention malveillante
E-privacy	absence de mesure de sécurité adéquate	/
NIS	non-respect des mesures de sécurité imposées par arrêté royal ou par l'autorité sectorielle	/



(4) Non-respect des recommandations et lignes directrices

	Recommandations
RGPD	Débat sur force légale des recommandations ou de lignes directrices de l'APD ou du CEPD
	jurisprudence adoptée par la Chambre contentieuse dans une affaire à laquelle le responsable du traitement n'est pas partie ?
	Débats doctrinaux
E-privacy	Idem
NIS	/

I. Point sur la transposition en Belgique

II. Quelles alertes en matière de protection des données et de sécurité des réseaux ?

III. Le DPO peut-il être lanceur d'alerte ?

IV. Le mécanisme d'alerte interne : obligation ou faculté ?

V. Rôle du DPO dans le mécanisme d'alerte interne ?

VI. Protection des données du lanceur d'alerte et de la personne visée

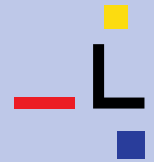


Obligation de désigner un DPO ?



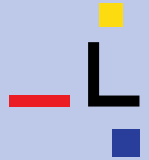
Norme	Obligation de notification	Obligation de désigner un DPO
RGPD	v	Pas systématique Dans 3 cas
E-privacy	v	fournisseurs au public de services de téléphonie, d'accès à l'Internet, de courrier électronique par Internet, les opérateurs fournissant des réseaux publics de communications
NIS	v	tout opérateur de services essentiels et tout fournisseur de service numérique visés à l'article

Rôle du DPO



Norme	Obligation de notification	Obligation de désigner un DPO	Protection du DPO
RGPD	v	Pas systématique	v
E-privacy	v	v	v
NIS	v	v	v

Obligation pour le DPO de sonner l'alerte ?



Devoir d'alerter plutôt qu'un droit de sonner l'alerte ?

Secret professionnel ?

I. Point sur la transposition en Belgique

II. Quelles alertes en matière de protection des données et de sécurité des réseaux ?

III. Le DPO peut-il être lanceur d'alerte ?

IV. Le mécanisme d'alerte interne : obligation ou faculté ?

V. Rôle du DPO dans le mécanisme d'alerte interne ?

VI. Protection des données du lanceur d'alerte et de la personne visée



Trois types de signalement



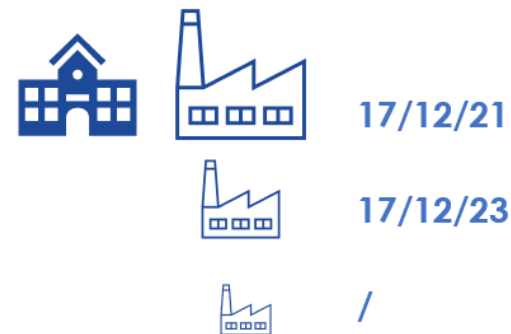
Interne



Externe



Divulgation
publique



Articulation des 3 types de signalements





Signalement par le DPO : par quelle voie ?



I. Point sur la transposition en Belgique

II. Quelles alertes en matière de protection des données et de sécurité des réseaux ?

III. Le DPO peut-il être lanceur d'alerte ?

IV. Le mécanisme d'alerte interne : obligation ou faculté ?

V. Rôle du DPO dans le mécanisme d'alerte interne ?

VI. Protection des données du lanceur d'alerte et de la personne visée



Rôle du DPO dans le mécanisme d'alerte interne

- **DPO = échelon du système d'alerte interne ?**
- **Pas d'incompatibilité**
- **Binôme souhaitable**





Quid si DPO n'agit pas et qu'il n'y a pas de mécanisme interne / ou que l'alerte interne n'a pas un suivi approprié ?

- Un manquement à la protection des données dont le DPD est déjà informé pourrait être signalé à l'autorité compétente (pas encore désignée mais probablement APD)



Autorité de protection des données



Divulgation publique

- Signalement au grand public si le signalement à l'APD n'apporte pas satisfaction au lanceur d'alerte ?

(la directive n'exige pas que le lanceur d'alerte soit désintéressé.

Il peut s'agir d'une alerte portant sur ses propres données)



I. Point sur la transposition en Belgique

II. Quelles alertes en matière de protection des données et de sécurité des réseaux ?

III. Le DPO peut-il être lanceur d'alerte ?

IV. Le mécanisme d'alerte interne : obligation ou faculté ?

V. Rôle du DPO dans le mécanisme d'alerte interne ?

VI. Protection des données du lanceur d'alerte et de la personne visée





- ✓ Réaliser AIPD
- ✓ Mettre à jour la politique de protection des données (travailleurs et tiers)
- ✓ Mettre à jour le registre de traitement
- ✓ Préparer un registre des signalements
- ✓ Contrat avec prestataire externe éventuel (sous-traitant)



- ✓ Respecter le principe de minimisation tout au long de l'enquête
- ✓ Simuler les cas de figures potentiels
- ✓ Quel suivi faire auprès du lanceur d'alerte ?



- ▶ **G29**, WP 117, Avis 1/2006 du 1^{er} février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements
- ▶ **EDPS**, Guidelines on processing personal information within a whistleblowing procedure, December 2019.
- ▶ **CPVP**, Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la LVP
- ▶ **CNIL**, Référentiel n° 2019-139 du 18 juillet 2019 - traitements de données destinés à la mise en œuvre d'un dispositif d'alertes professionnelles
- ▶ **EDPB** : /
- ▶ **APD** : /
- ▶ **Norme ISO/NP 37002** Whistleblowing management systems

**Merci
pour votre attention !
Des questions ?**

