NOTIFICATIONS DES VIOLATIONS DE DONNEES ET INCIDENTS DE SÉCURITÉ: PANORAMA LÉGISLATIF

LEGAL

AURÉLIE BANCK

28/03/2017

BNP PARIBAS
PERSONAL FINANCE

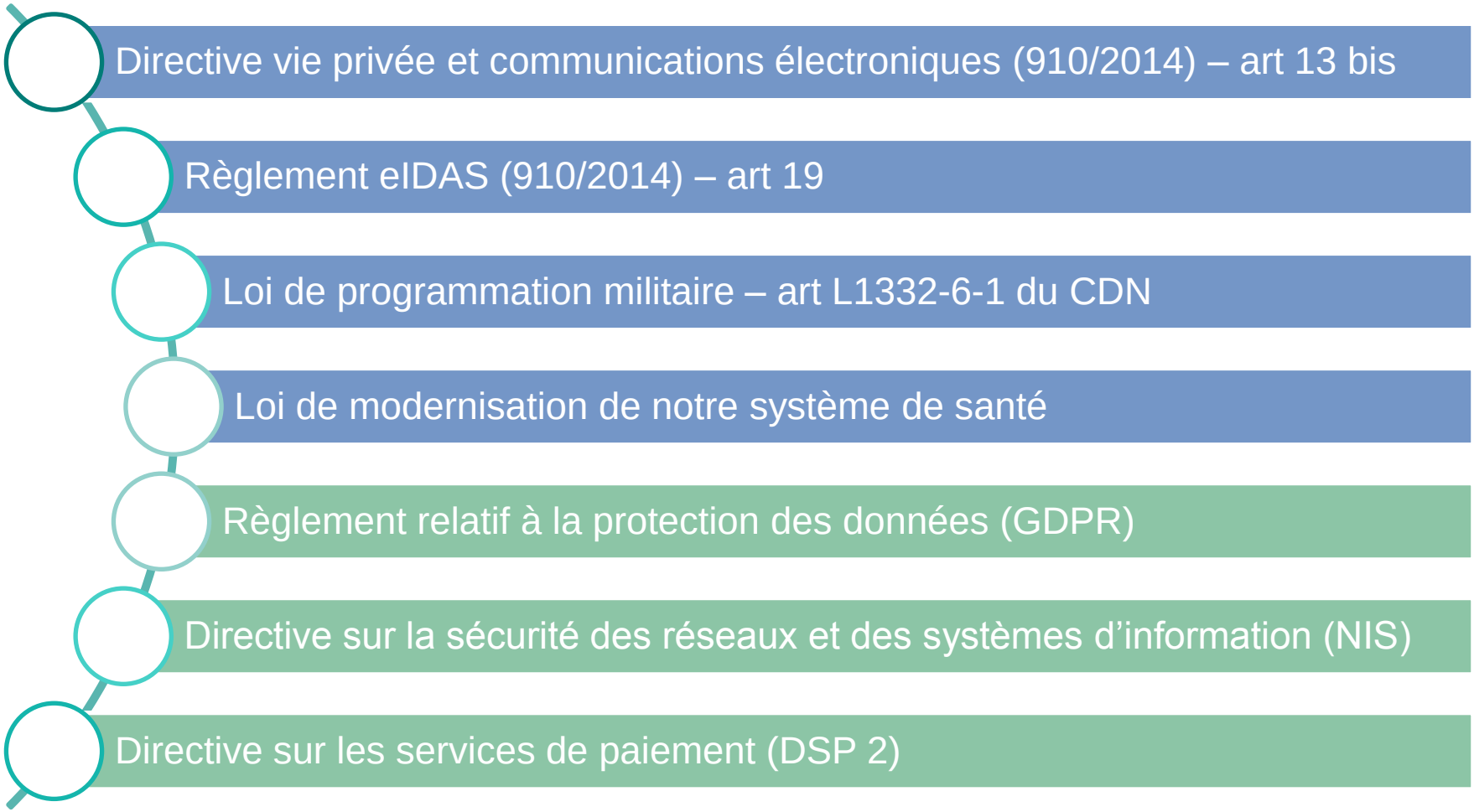
Plus responsables, ensemble

Enjeux et contexte

- Personnes de plus en plus sensibles à la protection de leurs données
- Failles de plus en plus nombreuses – *connues?*
- Risques :
  - Image/Perte de confiance
  - Sanctions financières

Multiplication des exigences de notification des violations de données

LEGAL



Le Règlement Protection des données (GDPR)

LEGAL

Références	• Articles 4, 33 et 84
Type d'événement	• Destruction, perte, altération, accès ou divulgation non autorisée de données personnelles
Entité devant procéder à la notification	• Responsable de traitement
Autorité compétente pour recevoir la notification	• Autorité de protection des données
Modalités	• Meilleurs délais, max 72 heures
Information des clients	• Oui si la violation est susceptible d'engendrer un risque élevé (*high risk*)
Sanctions	• Jusqu'à 2% du CA annuel mondial de l'exercice précédent

La Directive Network and Information System (NIS)

LEGAL

Références	• Articles 14 et 21
Type d'événement	• Les incidents ayant un impact *significatif* sur la continuité des services essentiels
Entité devant procéder à la notification	• Opérateurs de services essentiels/Services numériques
Autorité compétente pour recevoir la notification	• ANSSI *(sous réserve de transposition)*
Modalités	• Sans retard injustifié
Information des clients	• Néant
Sanctions	• Possibilité d'adopter des sanctions dans le cadre de la transposition

La Directive Services de Paiement 2 (DSP2)

LEGAL

Références	• Articles 96 et 103
Type d'événement	• Les incidents opérationnels ou de sécurité majeur
Entité devant procéder à la notification	• Les prestataires de services de paiement
Autorité compétente pour recevoir la notification	• ACPR?? *(sous réserve de transposition)*
Modalités	• Sans retard injustifié
Information des clients	• Oui, si incident susceptible d'avoir des répercutions sur les intérêts financiers des utilisateurs
Sanctions	• Possibilité d'adopter des sanctions dans le cadre de la transposition

La Directive Services de Paiement 2 (DSP2)

LEGAL

Références	• Articles 96 et 103
Type d'événement	• Les incidents opérationnels ou de sécurité majeur
Entité devant procéder à la notification	• Les prestataires de services de paiement
Autorité compétente pour recevoir la notification	• ACPR?? *(sous réserve de transposition)*
Modalités	• Sans retard injustifié
Information des clients	• Oui si incident susceptible d'avoir des répercutions sur les intérêts financiers des utilisateurs
Sanctions	• Possibilité d'adopter des sanctions dans le cadre de la transposition

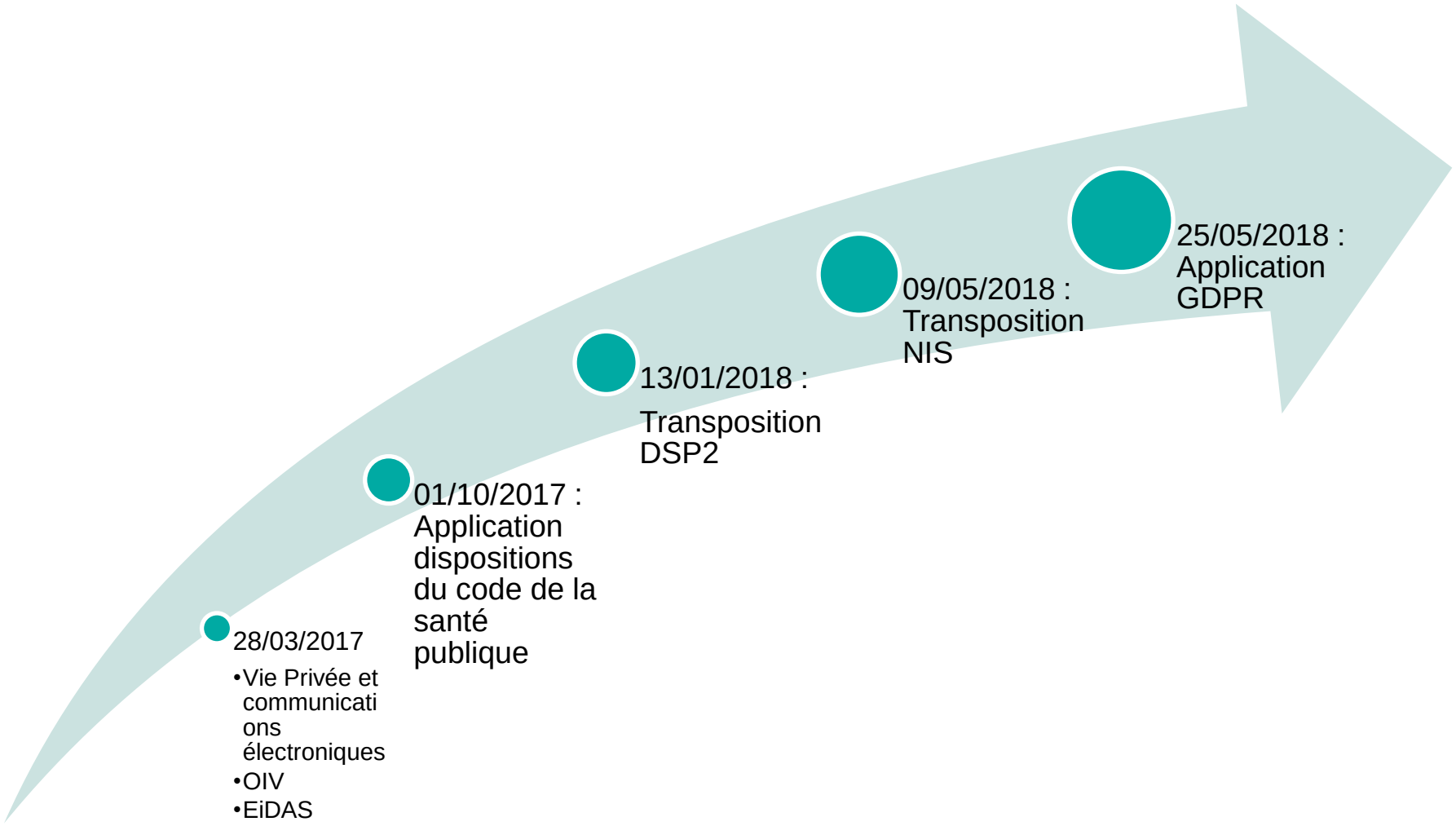
Les incidents grave de sécurité des SI en santé

LEGAL

Références	• Articles L1111-8-2 et D1111-16-2 du CSP
Type d'événement	• Les incidents ayant des conséquences potentielles/avérées sur la sécurité des soins • Les incidents ayant des conséquences sur la confidentialité/intégrité des données de santé • Les incidents portant atteinte au fonctionnement normal de la structure
Entité devant procéder à la notification	• Etablissements de santé, hôpitaux des armées, laboratoires de biologie, centres de radiothérapies
Autorité compétente pour recevoir la notification	• ARS
Modalités	• Sans délai
Information des clients	• Néant

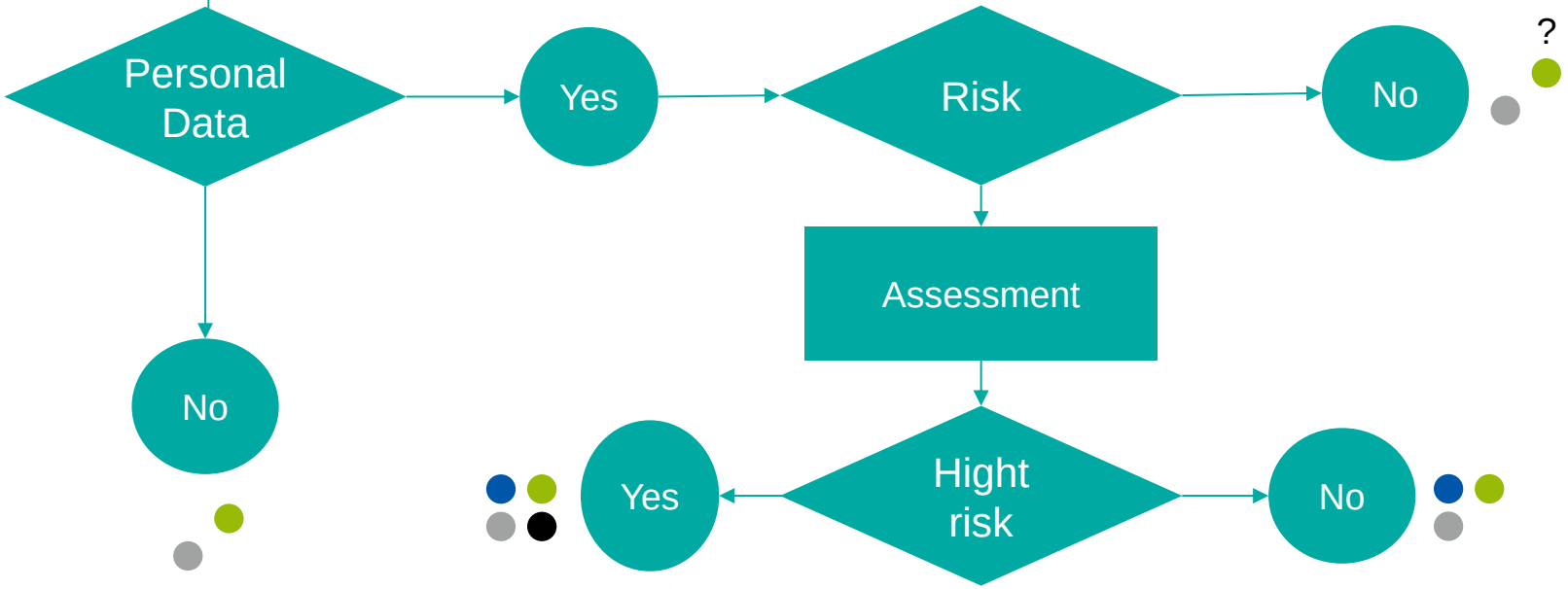
Calendrier

LEGAL



Articulation – Exemple d'un établissement de soins

LEGAL



Preparing for the inevitable

- Arbre de décision
- Approche par les risques
- Veille juridique, réglementaire et technologique
- Allocation des responsabilités avec mécanisme d'escalade
- Training de l'ensemble des équipes (incident response team, etc.)
- Simulations
- Assurance?

Conclusion

- Foisonnement législatif et réglementaire
- Environnement mouvant
- Niveau d'exposition important en fonction des activités
- Implication de l'ensemble des équipes (juridique, technique, business, etc.)

Questions???