Séminaire EIFR

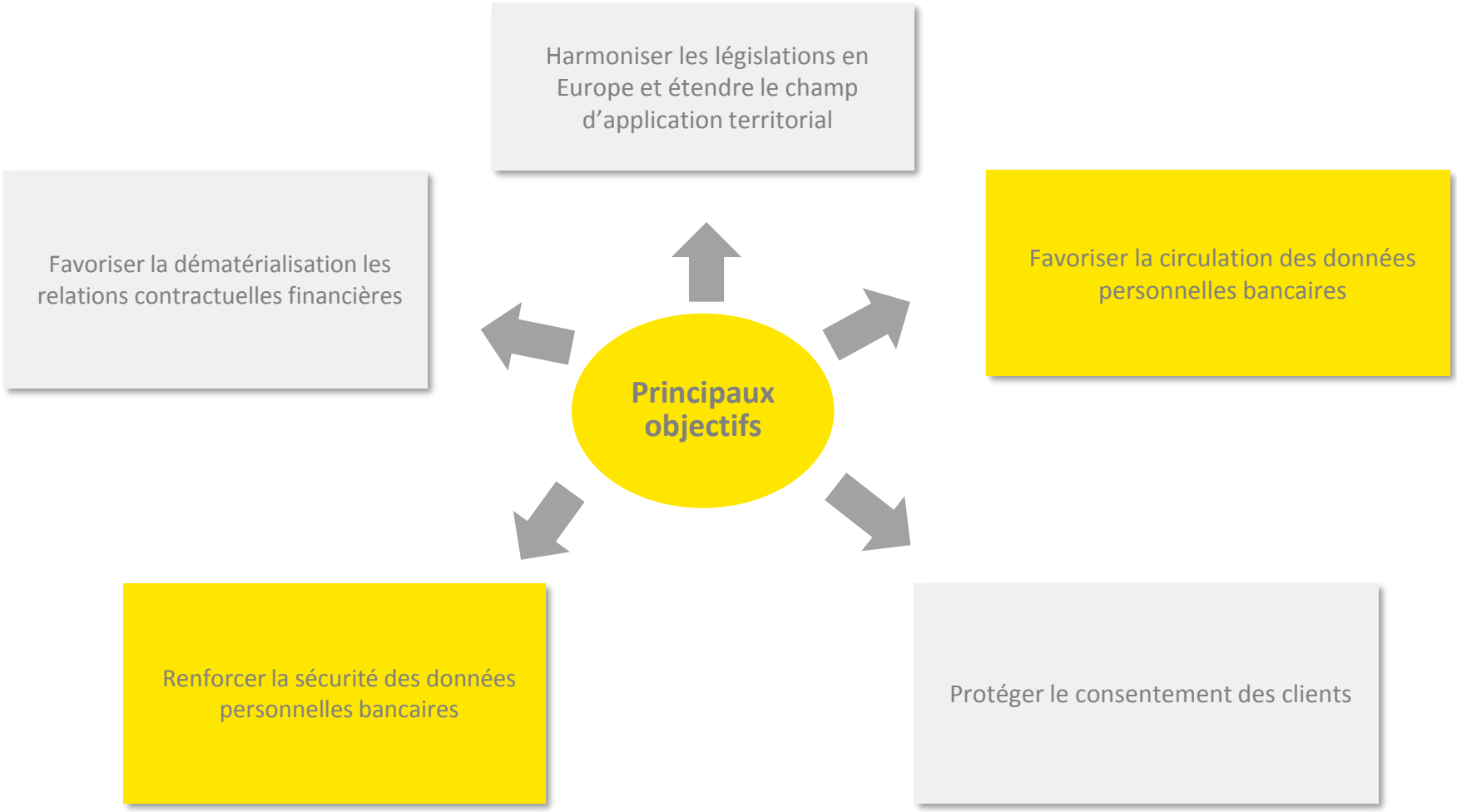
Sécurité des paiements et protection des données

3 avril 2018

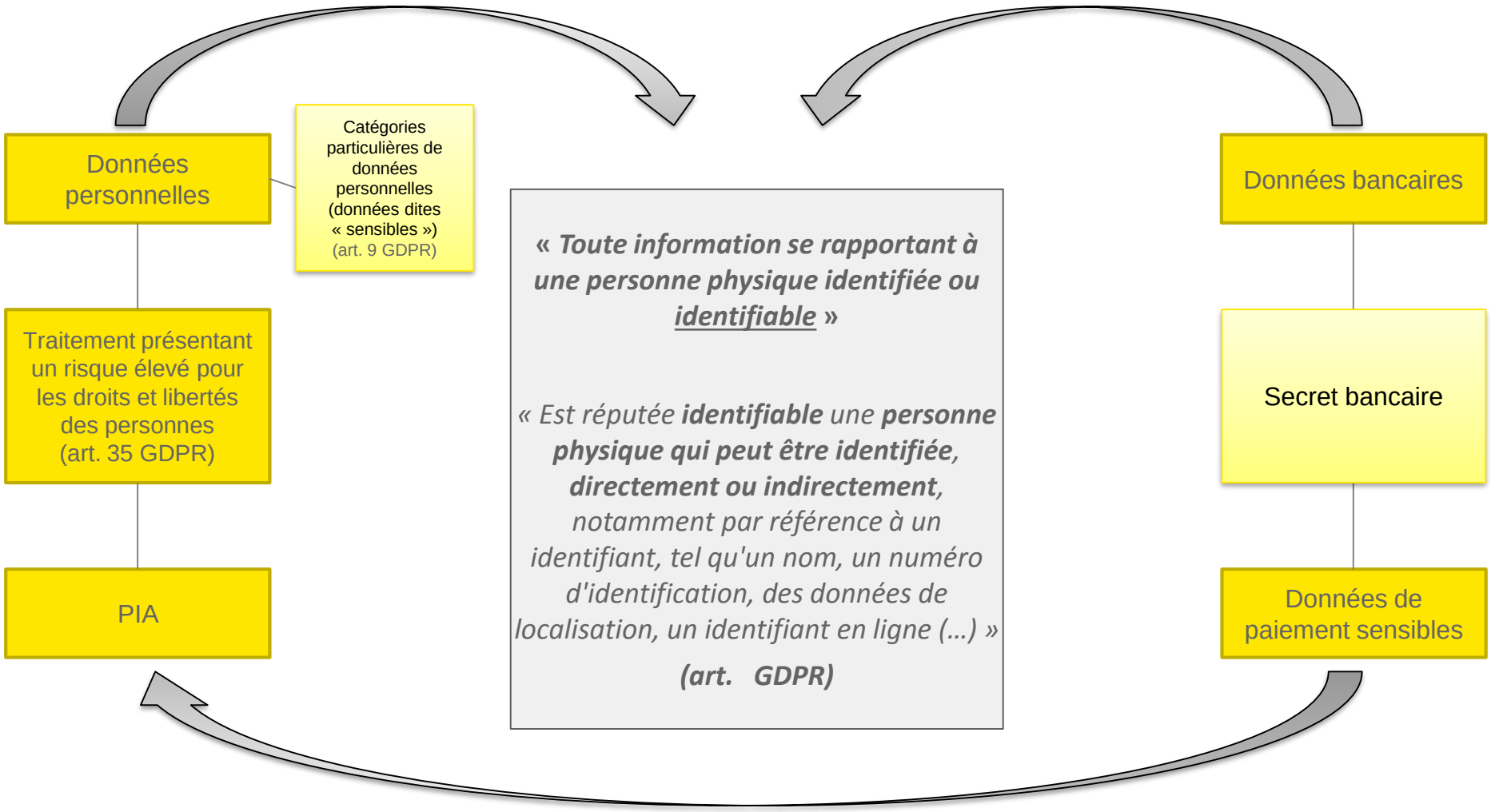
The better the question.
The better the answer.
The better the world works.

Building a better working world

1. DSP 2 et GDPR : des objectifs communs



2. Des interactions fortes



3. La nécessaire articulation des droits des personnes

Information

DSP 2	GDPR
• Informations sur les opérations de paiement isolées (art. L.314-9 et s. du CMF) • Informations sur les contrats cadres de services de paiements (L.314-12 et s. du CMF) • Informations après l'exécution de l'opération de paiement (art. L.314-14 CMF)	• Coordonnées du DPO • Base juridique du traitement et intérêt légitime poursuivi • Droits créés par le RGPD • Possibilité de retirer son consentement • Possibilité d'introduire une réclamation devant la CNIL • Le cas échant, l'existence d'une prise de décision automatisée (y compris un profilage) • Le cas échéant, éventuelles finalités ultérieures différentes • La possibilité d'organiser le sort des données après la mort

Gestion du consentement

DSP 2	GDPR
• Consentement exprès des payeurs pour l'accès, le traitement et la conservation des données personnelles nécessaires à l'exécution des paiements (L.521-5 CMF) • Compétence de la CNIL pour veiller au respect de l'article L.521-5 du CMF • Interdiction pour les PSP d'utiliser les données personnelles à des fins autres que la fourniture du service d'initiation de paiement ou d'information sur les comptes (L.133-40, 7° et L.133-41, 6° du CMF	• Le consentement consiste en une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement (art. 4 du GDPR) • Un consentement distinct est nécessaire pour chaque finalité spécifique (art. 6 GDPR)

Exercice des droits des personnes

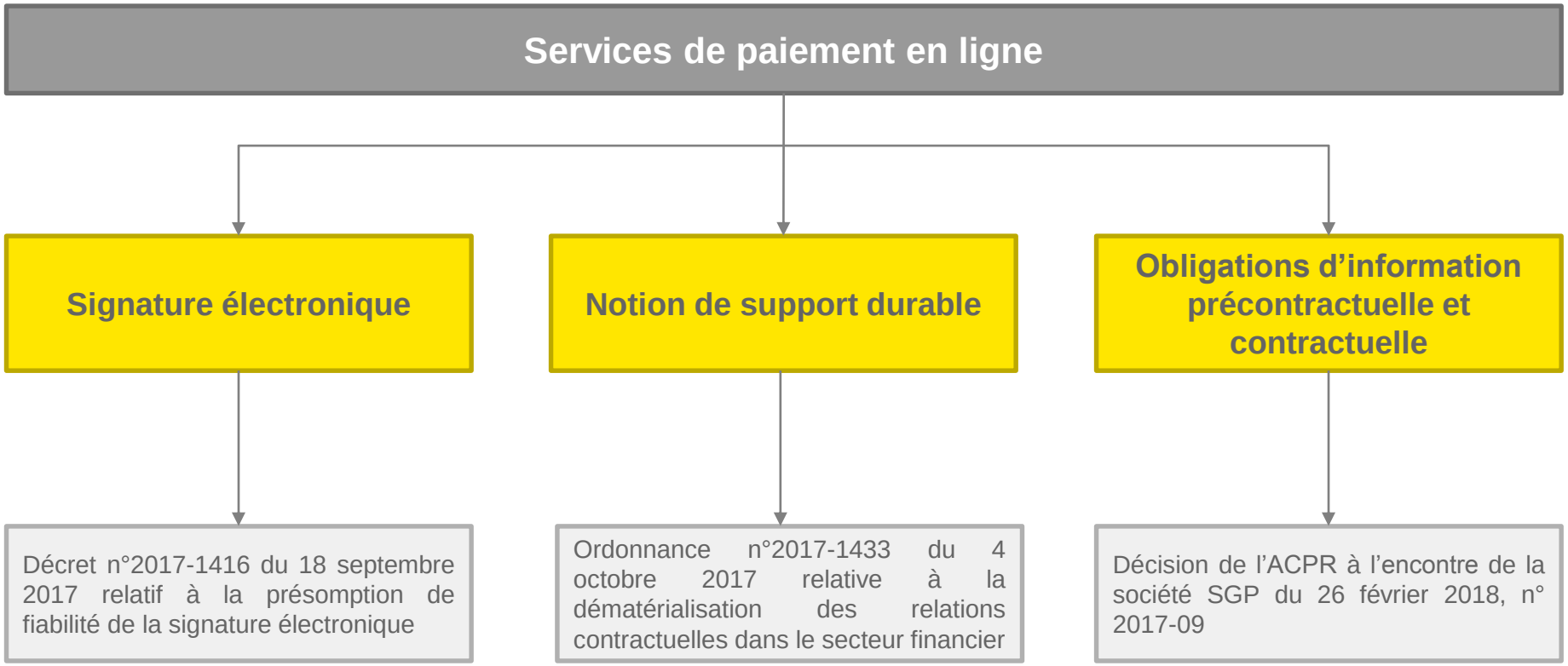
DSP 2	GDPR
	• Droit d'accès • Droit à la rectification • Droit à la portabilité • Droit à l'oubli

4. Les convergences en matière de sécurité

Les mesures de sécurité	
DSP 2	GDPR
- Prise en compte de la sécurité des données dès la procédure d'agrément - Authentification forte - Moyens de communication sécurisés entre PSP	- Privacy by design - PIA - Mesures de sécurité techniques et organisationnelles

La notification des failles de sécurité	
DSP 2	GDPR
- Notification à l'ACPR et à la Banque de France, sans retard injustifié, en cas d'incident opérationnel majeur ou de sécurité (L.521-10 CMF) - Notification à l'utilisateur des services de paiement, sans retard injustifié, lorsque l'incident a ou est susceptible d'avoir des répercussions sur ses intérêts financiers (L.521-10 CMF)	- Notification à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après avoir pris connaissance de la violation de données personnelles lorsqu'elle est susceptible d'engendrer un risque pour les droits et libertés des personnes (art. 32) - Notification à la personne concernée dans les meilleurs délais lorsque la violation est susceptible d'engendrer un risque élevé pour ses droits et libertés (art. 33)

5. Les autres réglementations participant de la sécurité des services de paiement électroniques



Merci pour votre attention