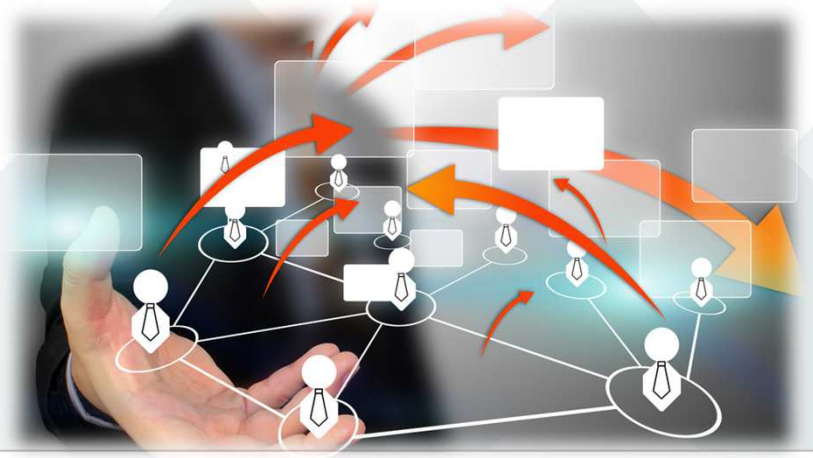
Club Urba-EA

Réunion d'information du 28 mars 2017

Laboratoire de la Flexibilité

Projet de Plateforme de conformité à la GDPR



René Mandel
Vice-Président du Club Urba-EA
Nicolas Chevalier
Consultant

Club Urba-EA
ENTERPRISE ARCHITECTURE

Agenda (1/2)

- L'initiative du Club Urba-EA
  - Orientation stratégique du Club
  - Le Laboratoire de la Flexibilité
  - L'enjeux de maîtrise des données personnelles
- La GDPR : évolution architecturale pour le SI
  - Les nouveautés de la GDPR
  - Les 3 types d'impact de la GDPR
  - Compte à rebours
- Cadre d'une « stratégie IT-GDPR » pour les Entreprises
  - Non-conformité déclinée selon les 3 impacts
  - Projet structurant de cible d'Architecture conforme

Agenda (2/2)

- Ciblage du projet
  - Cas du « Privacy by Design »
  - Bac à sable d'architecture
  - Schéma d'architecture de la plateforme
  - Liste de sujets proposés
- Modalités de travail
  - Statut de partenaire actif : financement, co-développement
  - Participant contributeur : adhésion au Club Urba-EA
  - Livrables
- Organisation Timing
  - L'Equipe du Club
  - Prochaines étapes

Rappels sur le Club Urba-EA

- Association de 1901 créée en 2000
  - Regroupe les Architectes d'Entreprise et Urbanistes SI
  - Centrée sur le retour d'expérience et le partage de pratiques
- Déontologie-positionnement :
  - Pas d'engagement dans une méthodologie
  - Indépendance par rapport aux fournisseurs
  - Partenaire du Cigref
- En 2017
  - 70 entreprises membres
  - 115 personnes adhérentes

Orientation stratégique : Etre plus proche du Business et de la Technologie

- Activités traditionnelles des Architectes d'Entreprise décalées de la réalité des évolutions business et technologiques :
  - risque de discrédit
  - Lourdeur méthodologique
- Besoin d'une vision transverse, prospective, ancrée dans la transformation en cours

Déplacer le Centre de Gravité de l'EA
Création du Laboratoire de la Flexibilité

Laboratoire du Club Urba-EA

- Nouveau mode de travail au sein du Club
  - Plus concret et ciblé
  - Avec une mise en pratique (bac à sable)
  - Sur des problématiques transverses aux métiers
  - Et des technologies du « monde connecté »

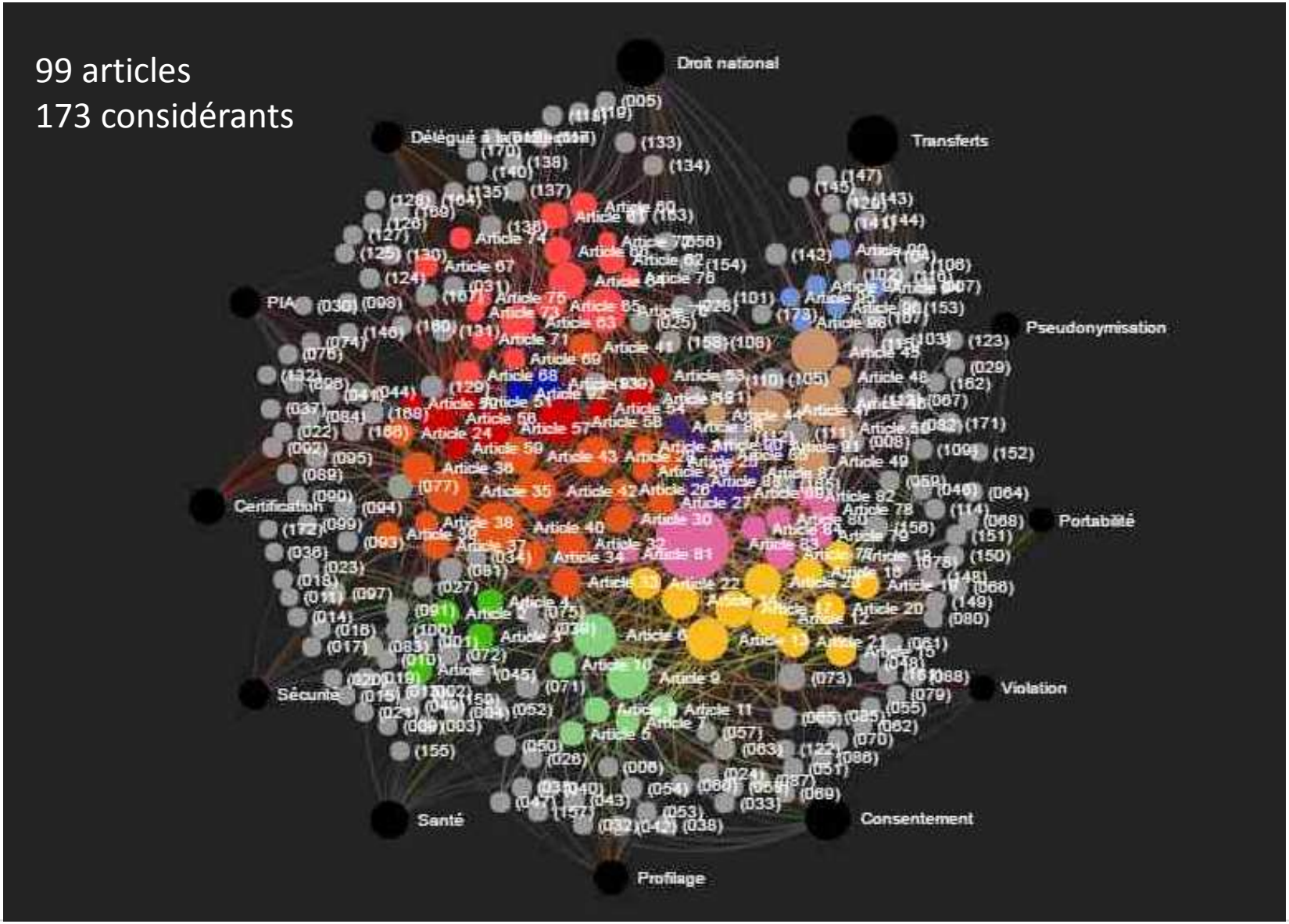
- Concours de circonstance
  - Emergence de la GDPR (General Data Privacy Regulation)
  - Premières mises en œuvre de l'Architecture Flexible

L’enjeux de maîtrise des données personnelles

- Un rapport de force déséquilibré
  - Les grandes structures se sont « approprié » les données
  - Les personnes veulent maîtriser les intrusions, leur vécu de l’utilité
  - Bascule vers une société connectée à l’utilité

- La GDPR : Etape importante pour engager un rééquilibrage
  - S’appui sur un existant et le prolonge, renforce le dispositif
  - Approche Européenne, donc globale
  - Risque de e-réputation si non conformité

99 articles
173 considérants



Club Urba-EA
Enterprise Architecture

Les nouveautés de la GDPR

- Transfert de responsabilité vers les Entreprises et Organisations
  - ✓ Désignation de Data Protection Officer
  - ✓ Obligation de déclaration des « violations de données personnelles »
  - ✓ Obligation d'étude d'impact (PIA : PRIVACY IMPACT. ASSESSMENT) pour les nouveaux traitements
  - ✓ Renforcement des pénalités et des procédures de contentieux
- Cadre de gestion des droits
  - ✓ droit à l'oubli,
  - ✓ droit d'accès et à la rectification,
  - ✓ portabilité,…

3 types d'impacts pour le SI

1 Des « domaines fonctionnels » spécifiques

Gestion des droits,

Mécanisme de portabilité

Transfert de données (hors UE)

Administration de la Protection des données privées

2 Des impératifs de sécurité renforcés

Anonymisation, cryptage

Architecture de sécurité

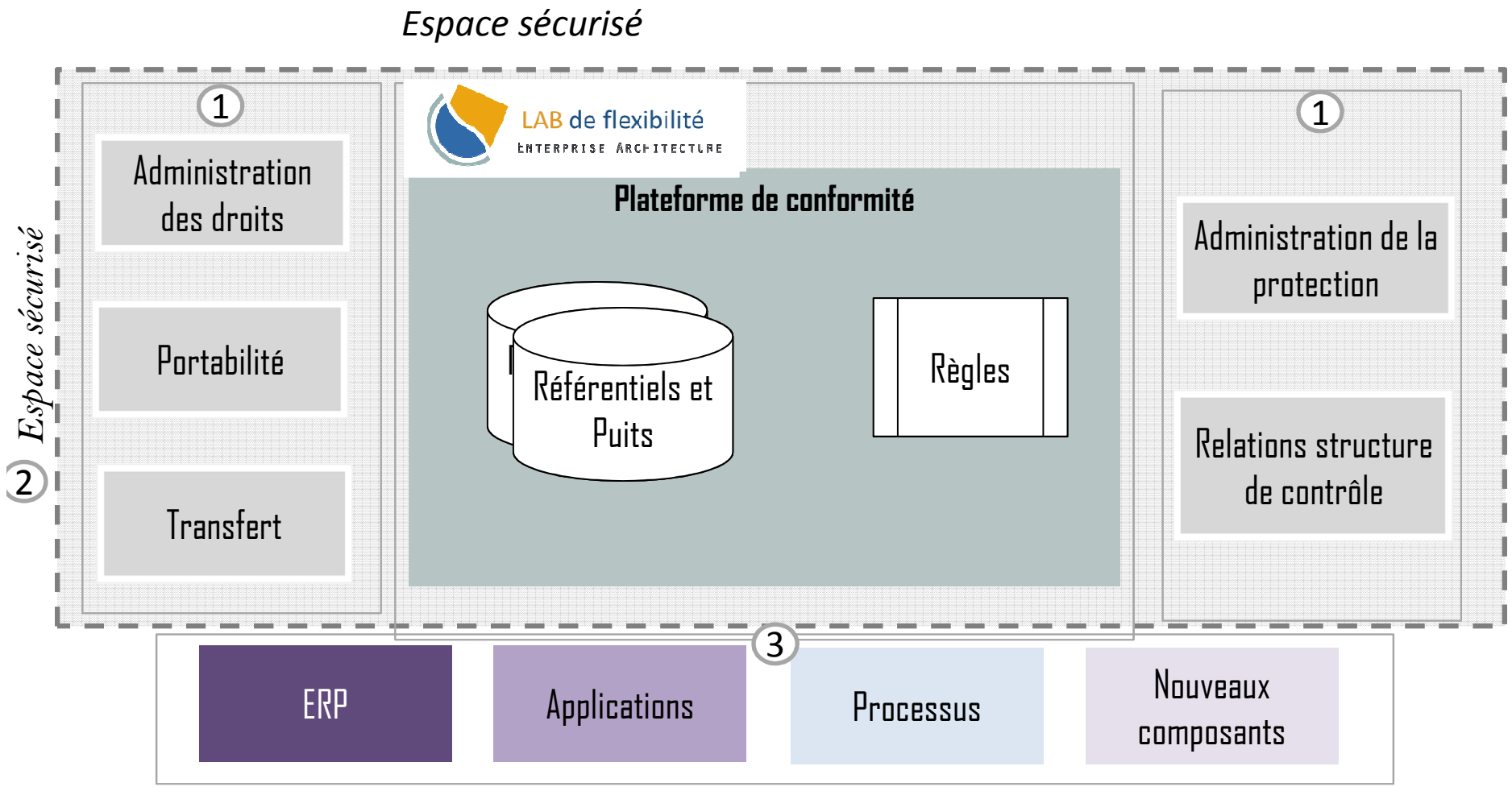
3 Un impact sur l'architecture du SI

y compris dans le patrimoine existant

Problématique typique d'urbanisation

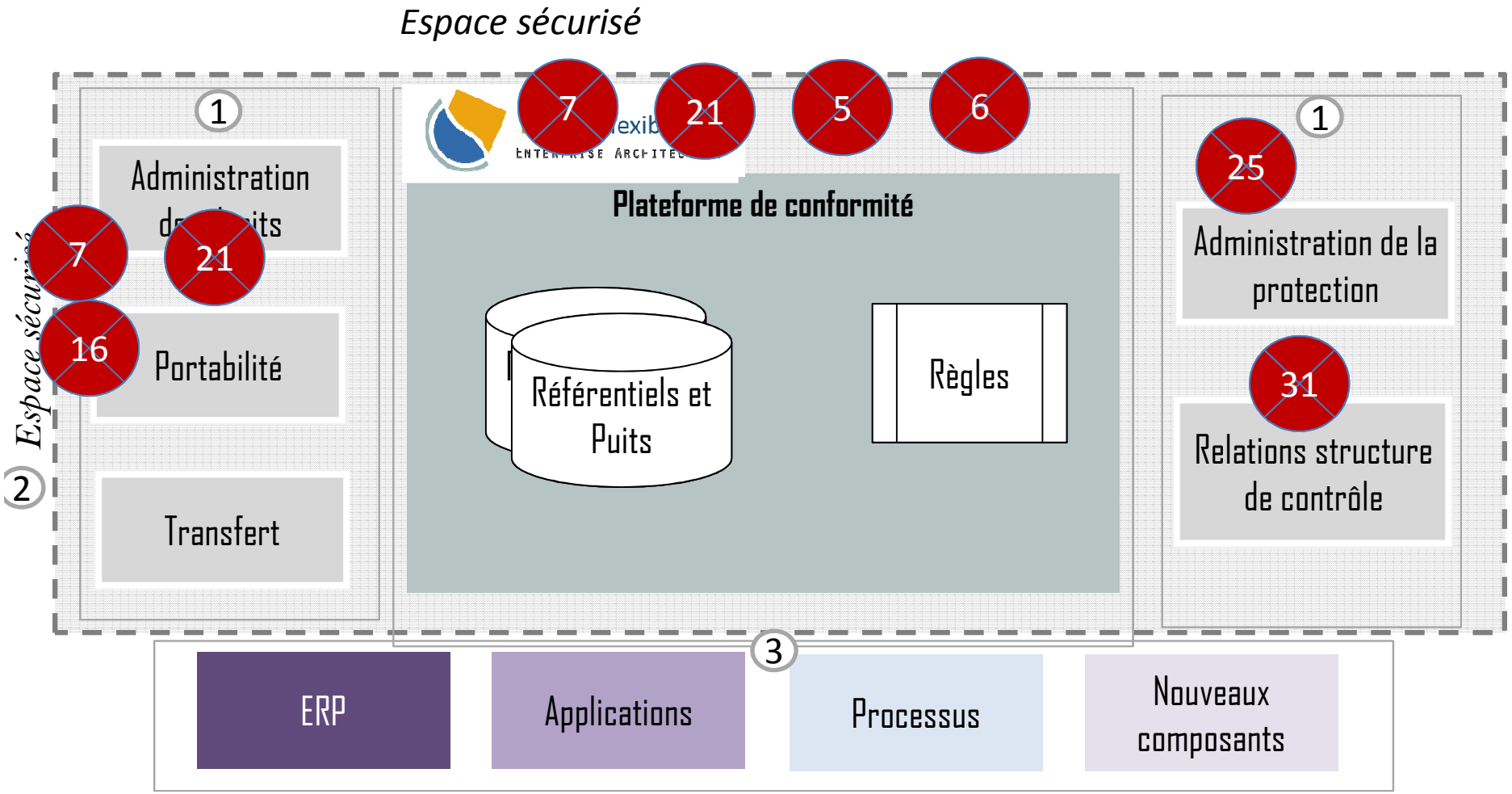
Zonage

1. Des « domaines fonctionnels » spécifiques
2. Des impératifs de sécurité renforcés
3. Un impact sur l'architecture du SI, y compris dans le patrimoine existant



Zonage

1. Des « domaines fonctionnels » spécifiques
2. Des impératifs de sécurité renforcés
3. Un impact sur l'architecture du SI, y compris dans le patrimoine existant



Impacts en terme d'Architecture du SI

détails troublant les silos SI

6

Article 6 1. Le traitement n'est licite que si, au moins une des conditions suivantes est remplie:
a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie …;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

6

Article 7 :
"le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant"..."La personne concernée a le droit de retirer son consentement à tout moment"

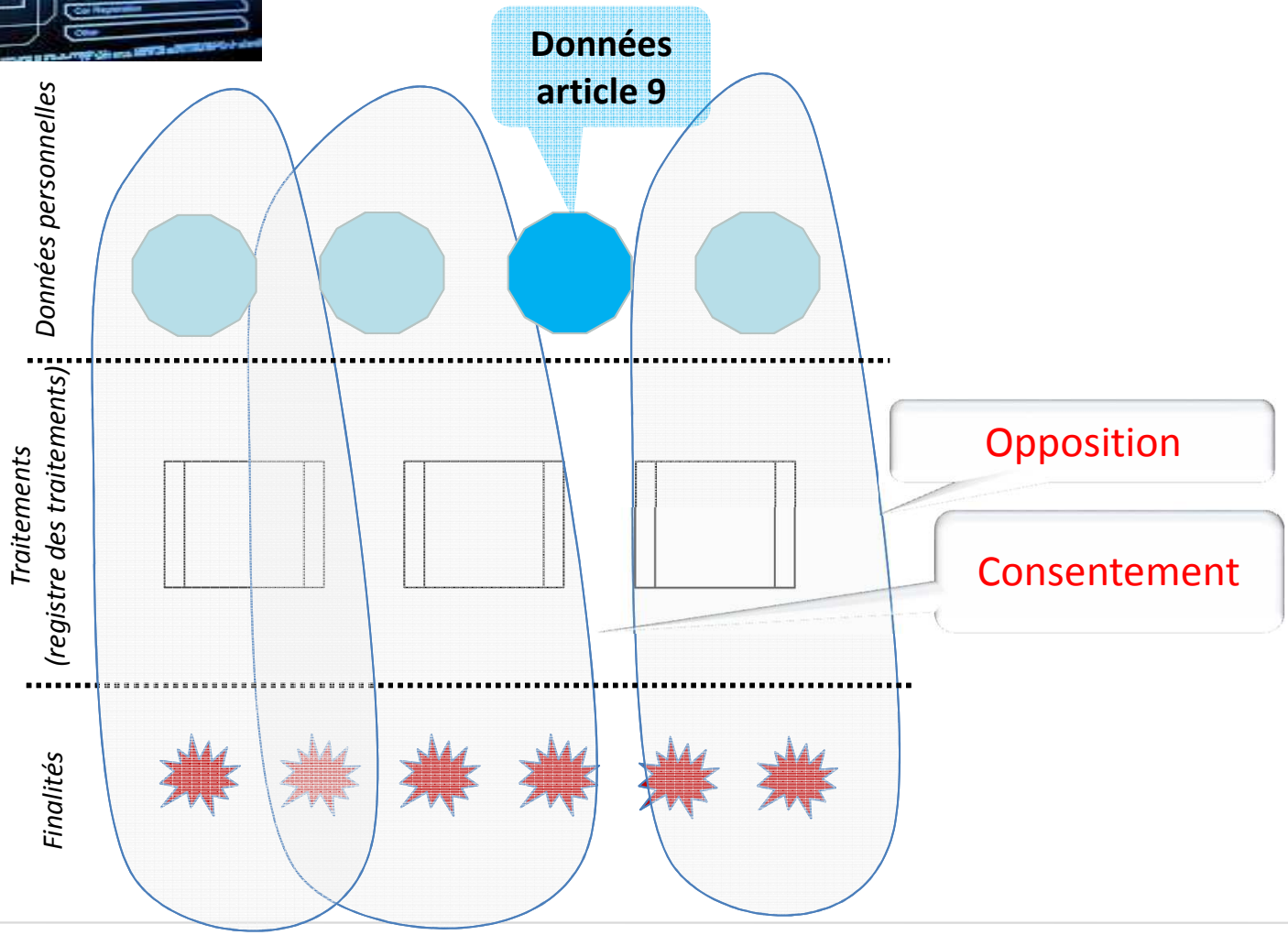
21

Article 21 :
« Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection »

GDPR : Logique des consentements et oppositions

Personne identifiée ou identifiable

Nécessité ou interdiction de droit

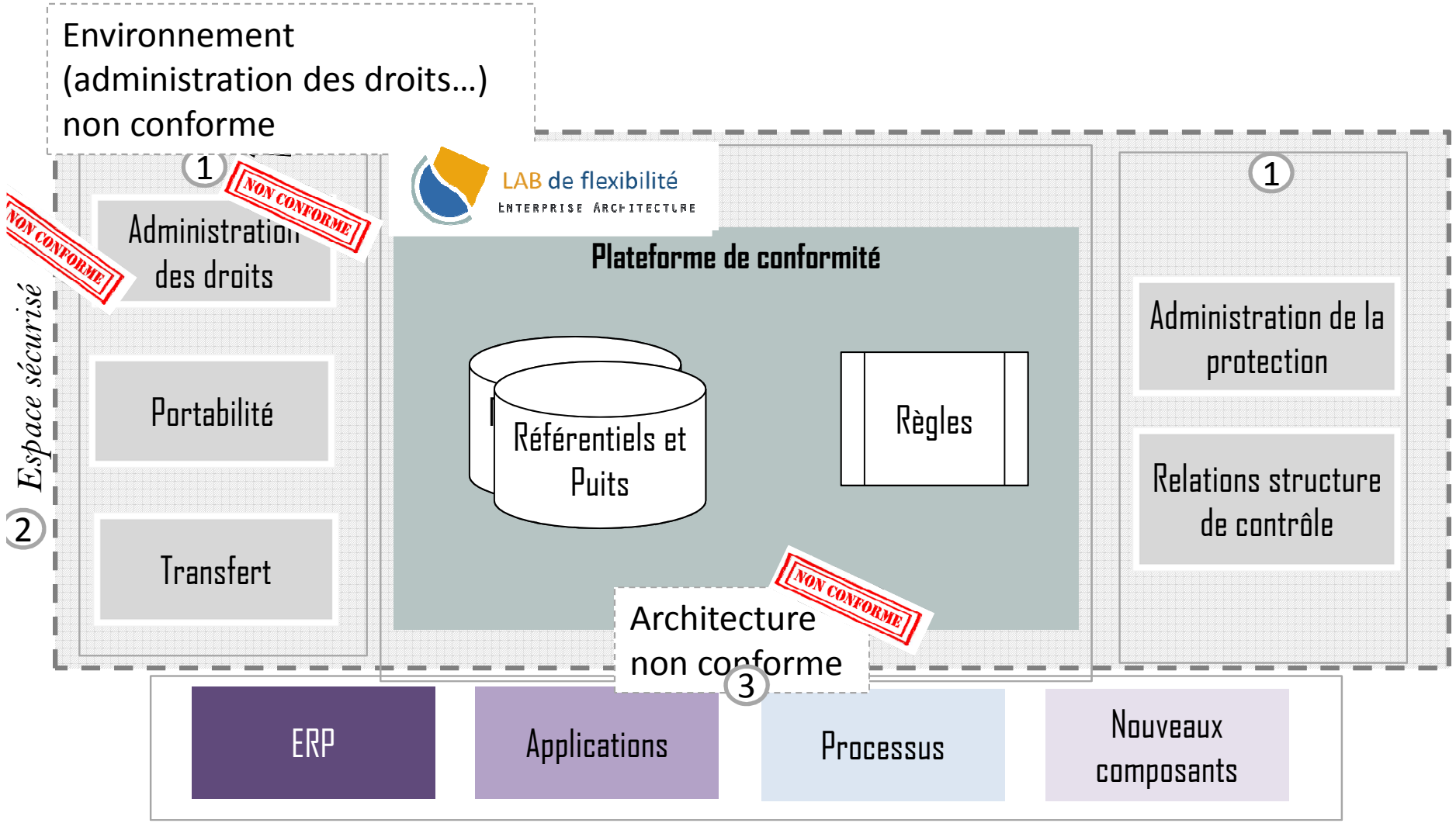


Le compte à rebours

- Cas des nouveaux traitements : Privacy by Design
  - Article 99 : » …Il est applicable à partir du 25 mai 2018. Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.
- Cas du patrimoine SI
  - Considérant 171 : « Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur »

Trois types de non-conformité IT

Cadre de « stratégie IT-GDPR »



Cas du patrimoine : modification « locale » pour mise en conformité

Cas du « Privacy by Design » : Nouveau traitement « nativement » non conforme : exemple : pas de gestion des consentements et oppositions

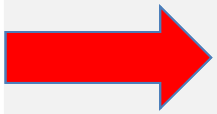
2 - Le projet : Ciblage

- **Pour une Entreprise** : l'Architecture Flexible s'adapte parfaitement au cas
  - Besoin de mutualiser des référentiels transverses :
    - Identification des personnes
    - Répertoire des traitements et finalités
    - Dictionnaire des informations
    - Tables de décision des règles
  - Besoin de mutualiser des « puits » transverses :
    - Puits des consentements
    - Puits des validations-invalidations de traitements
- **Pour la migration** : introduction progressive, non intrusive, d'une plateforme transversale

Zoom sur le « Privacy by Design »

Cas du « Privacy by Design »

- Incontournable à échéance mai 2018 pour les nouveaux traitements
- Avoir une cible d'Architecture en avance de phase (ne pas structurer des projets non conformes)
- La cible « idéale » en Etat de l'Art (ne pas structurer « ringard »)



Un projet central prioritaire

- **Ne peut être désimbriqué,** à placer au cœur du SI en espace **sécurisé**
- Doit fournir la **traçabilité** détaillée (piste d'audit)
- A **intégrer** dans son SI par chaque entreprise

Exemple de sujet à partager : Démonstrateur

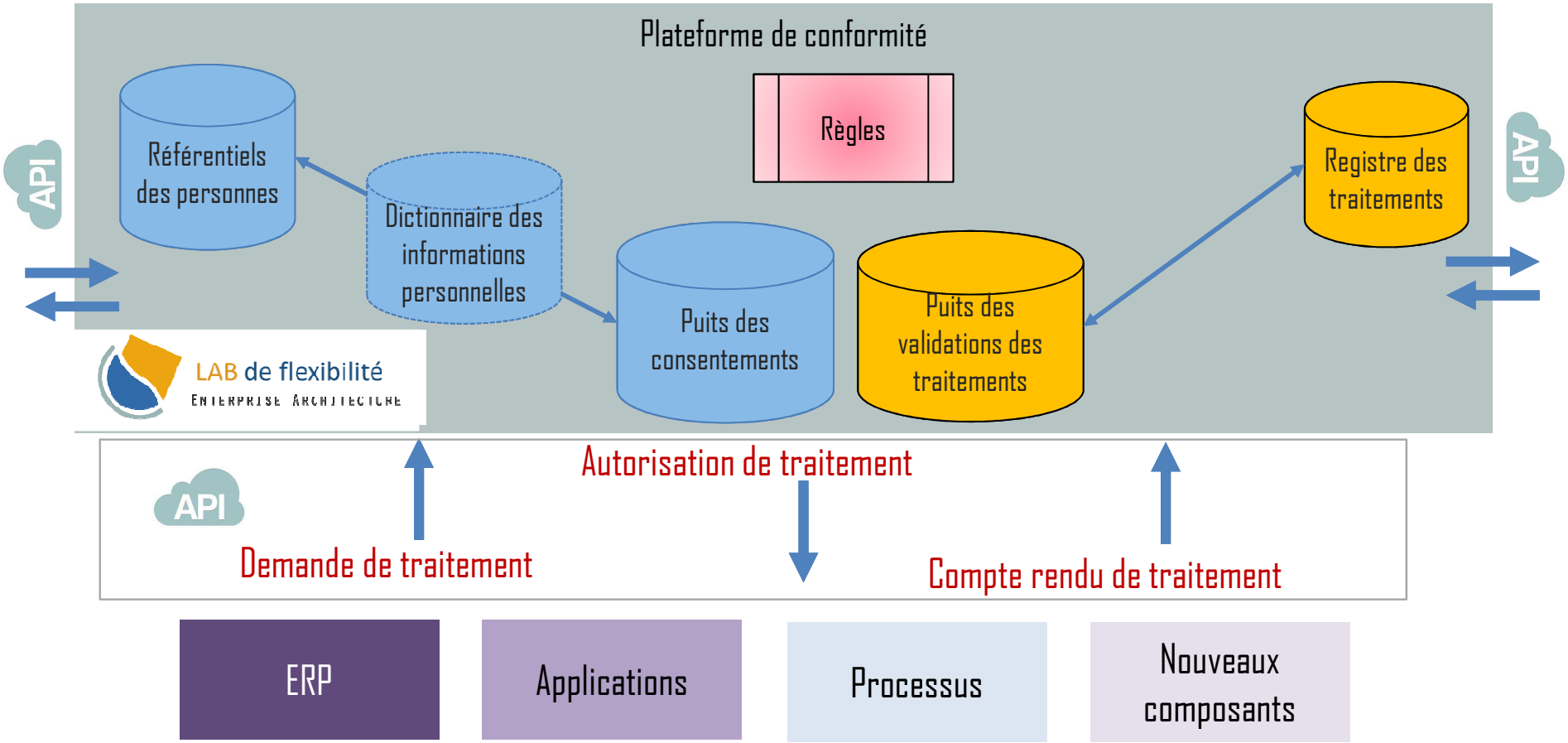
- Objectif : démontrer le fonctionnement simplifié
  - Architecture technique « bac à sable », non sécurisée, développement agile
  - Simplification fonctionnelles (règles principales du consentement)
  - Données fictives (personnes, informations, consentements, finalités)

- Un projet lisible et typique

> Rendre explicite le « modèle » d'une plateforme de conformité

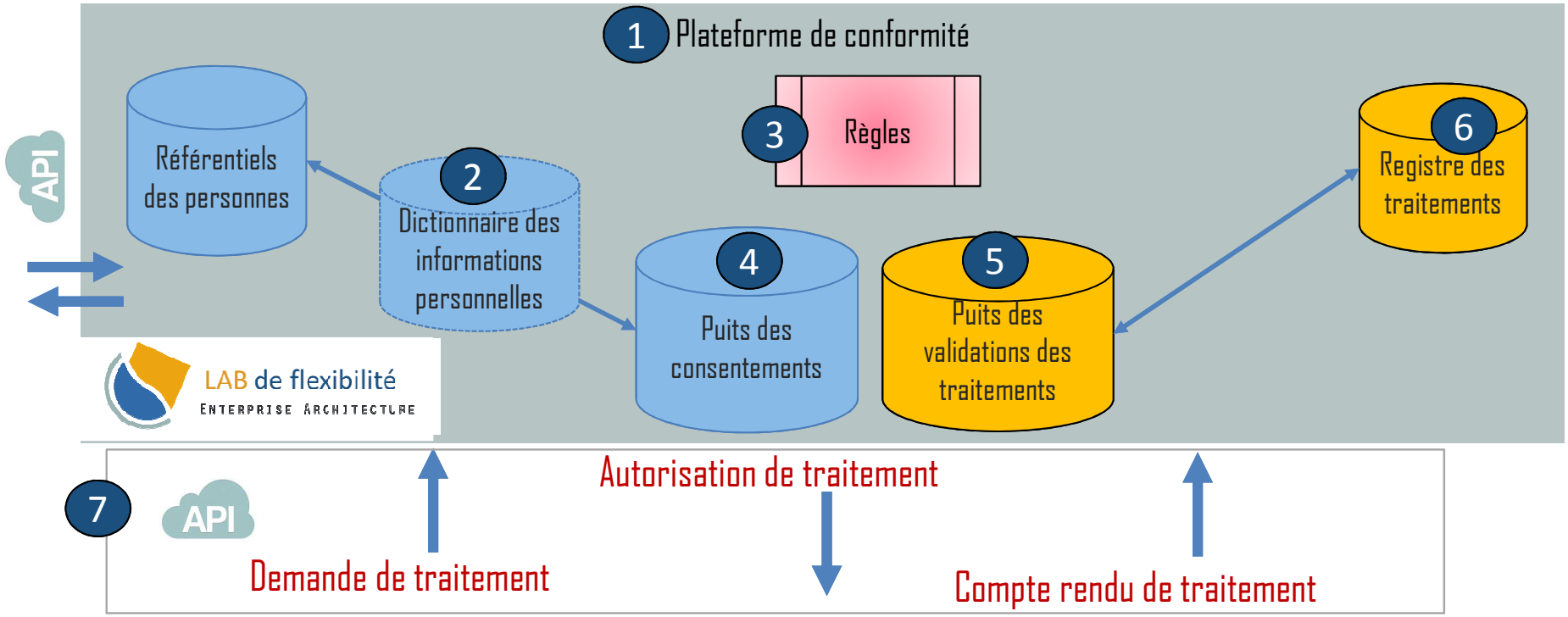
Schéma du modèle d'architecture

Composition de la plateforme

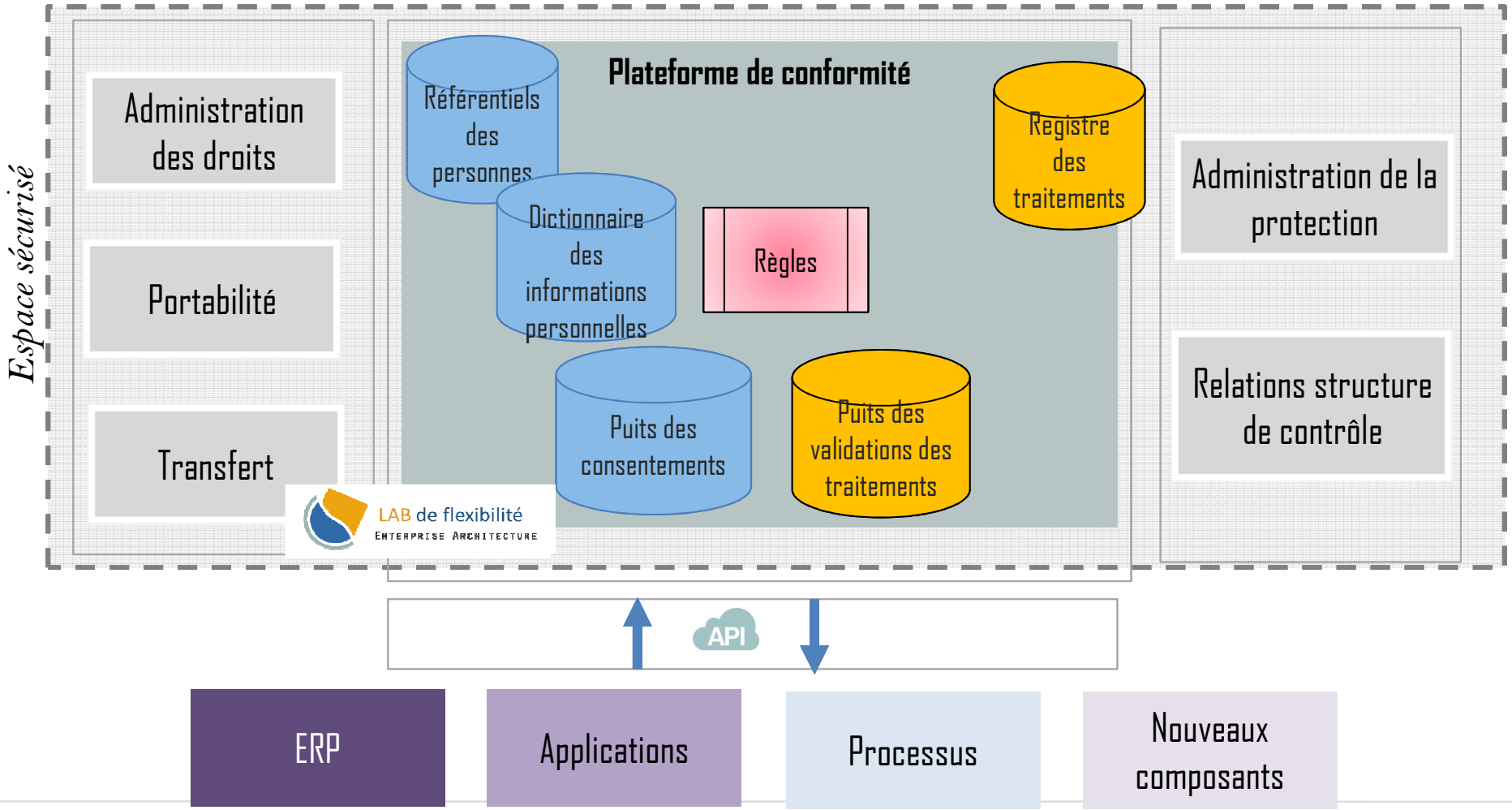


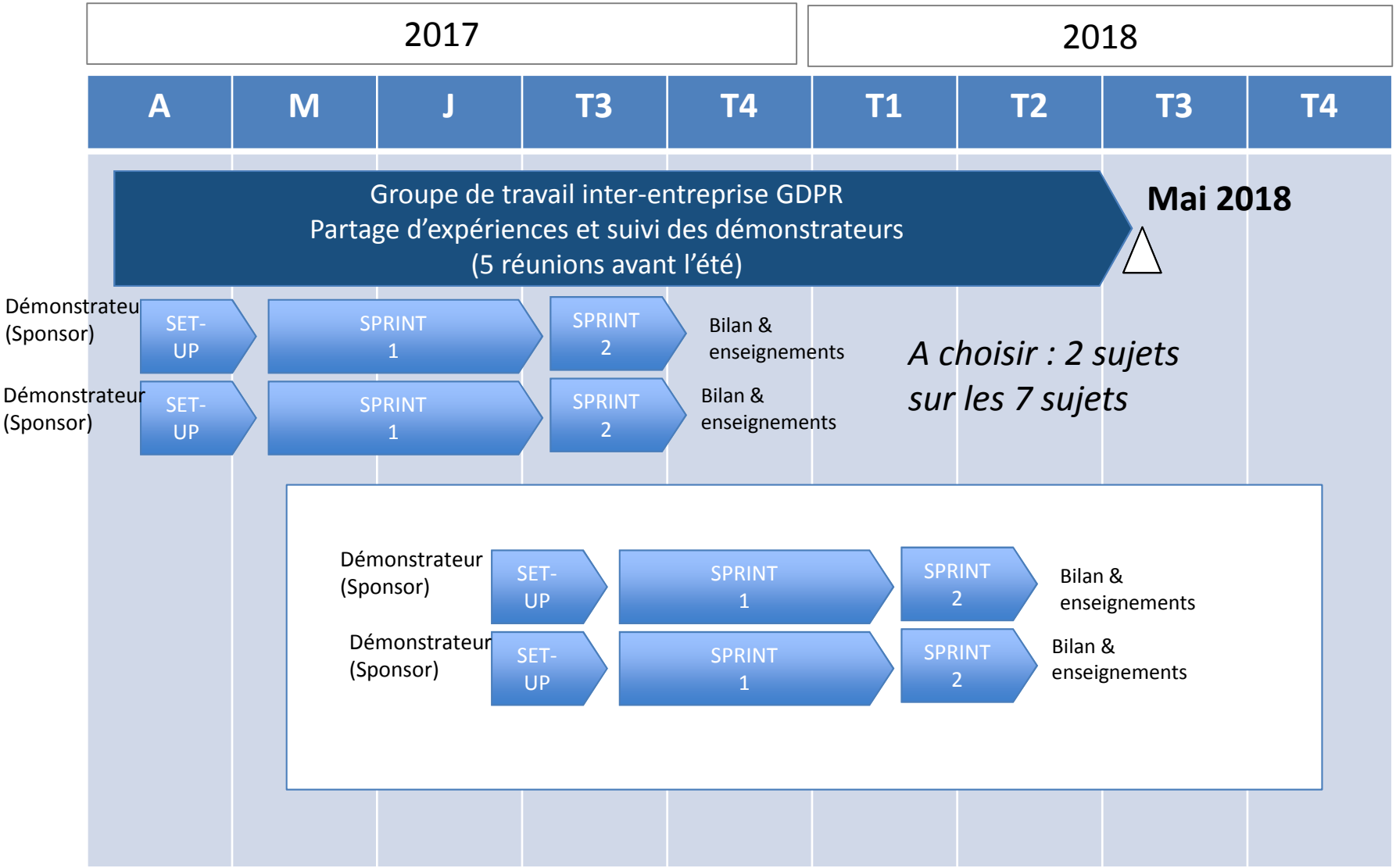
SUJETS

0	Validation du zonage	4	Puits des consentements
1	Plateforme de conformité	5	Puits de validation des traitements
2	Dictionnaire des infos personnelles	6	Registre des traitements
3	Moteur de règles de la réglementation	7	API de consultation (standards)



Club Urba-EA
ENTERPRISE ARCHITECTURE


Espace sécurisé
Administration des droits
Portabilité
Transfert
Plateforme de conformité
Référentiels des personnes
Dictionnaire des informations personnelles
Règles
Registre des traitements
Puits des consentements
Puits des validations des traitements
Administration de la protection
Relations structure de contrôle
LAB de flexibilité
Enterprise Architecture
API
ERP
Applications
Processus
Nouveaux composants


2017
2018
A
M
J
T3
T4
T1
T2
T3
T4
Groupe de travail inter-entreprise GDPR
Partage d'expériences et suivi des démonstrateurs
(5 réunions avant l'été)
Mai 2018
Démonstrateur (Sponsor)
SET-UP
SPRINT 1
SPRINT 2
Bilan & enseignements
Démonstrateur (Sponsor)
SET-UP
SPRINT 1
SPRINT 2
Bilan & enseignements
A choisir : 2 sujets sur les 7 sujets
Démonstrateur (Sponsor)
SET-UP
SPRINT 1
SPRINT 2
Bilan & enseignements
Démonstrateur (Sponsor)
SET-UP
SPRINT 1
SPRINT 2
Bilan & enseignements

Modalités de travail

Statuts

- Statut de partenaire actif : financement, co-développement
- Participant contributeur (hors prestataires) : adhésion au Club Urba-EA :
  - Urbaniste, architecte d'entreprise
  - Data Officer, CIL, DPO, …

Organisation Timing

- L'Equipe du Club :
  - René Mandel
  - Nicolas Chevalier
  - Bruno Rizzi
- Prochaine étape

Limites de l'exercice

- Des solutions partielles (selon le sujet)
- Pas d'offre sur le marché (hors objectif du Club)
- Solution technique non sécurisée
- Solution fonctionnelle du « cœur GDPR » volontairement sommaire
  - A étendre avec les fonctions spécifiques GDPR
  - Solution « générique » à transposer par les Entreprises

Liens utiles

- Voir aussi Architecture d'Entreprise et GDPR :
  - http://www.value-architecture.com/2017/03/la-reglementation-gdpr-defi.html

- Sur l'Architecture Flexible :
  - http://trame-business.fr/mon-installation/index.php/architecture-flexible/