APDL

Association pour la Protection des Données au Luxembourg

RGPD– IMPACTS TECHNOLOGIQUES

AGENDA

- Présentation générale
- Définitions
- Les articles phares
  - consentement
  - information simple et claire
  - oubli numérique et effacement
  - portabilité des données
  - limitation du profilage
  - privacy by design / by default
  - registre des activités de traitement
  - information en cas de piratage
  - codes de conduite et certifications
- Architectures existantes : quels enjeux ? comment les préparer ?
- Nouveau règlement ⇔ nouvelles architectures
- Vue 360°
- Emergence de nouveaux services
- Conclusion

PRÉSENTATION GÉNÉRALE

- à l'initiative du G29
- abroge la Directive 95/46/CE
- calendrier :
  - paru au Journal Officiel de l'UE le 4 mai 2016
  - entré en vigueur le 25 mai 2016
  - devra être transposé en loi locale avant le 6 mai 2018, pour une application effective à partir du **25 mai 2018**
- s'applique à toute entreprise située en UE ou proposant des biens ou services aux ressortissants de l'UE (article 3)
- principe d'***accountability*** : plus de déclaration préalable à la CNPD, mais une obligation de se conformer au nouveau règlement, et de pouvoir en faire la démonstration (article 22)
- nomination d'un délégué à la protection des données pour les structures à partir d'une certaine taille (restant à définir)

DONNÉE À CARACTÈRE PERSONNELLE ?

Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Article 4(1) du RGPD (définitions)

Exemples : nom, prénom, coordonnées bancaires, date/lieu de naissance, empreintes digitales, plaque d'immatriculation, adresse email, numéro de sécurité sociale…

TRAITEMENT ?

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Article 4(2) du RGPD (définitions)

LE NOUVEAU RÈGLEMENT (UE) 2016/679 … LES ARTICLES PHARES

- Articles 6, 7, 8 : **consentement explicite** requis pour une ou plusieurs **finalités spécifiques**. Il doit être aussi simple de retirer son consentement que de le donner
- Articles 12, 13, 14 : droit d'être **informé dans un langage simple et clair**
- Article 17 : droit à l'**oubli numérique** et à l'**effacement**
- Article 20 : **portabilité des données** dans un format structuré couramment utilisé permettant la réutilisation des données par la personne concernée ou un tiers de son choix
- Article 21 : limitations claires au recours au **profilage**
- Article 25 : *privacy by design / by default*
- Article 30 : instauration d'un registre des **activités de traitement**
- Articles 33, 34 : droit d'être **informé** en cas de **piratage** des données
- Article 40, 42 : mise en place de **codes de conduite** et de **certifications**

CONSENTEMENT

Toute 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. (article 4 du RGPD)

- Licéité du traitement (article 6) : le traitement n'est licite qu'à condition qu'il remplisse au moins un de ces (principaux) critères :
  - la personne concernée y a **consenti**
  - il est nécessaire à l'**exécution du service** proposé
  - il nécessaire au **respect d'une obligation légale**
  - il est nécessaire à l'exécution d'une **mission d'intérêt public**

  ➔ un traitement ne rentrant pas dans un de ces critères est interdit
- Article 7 : le responsable du traitement doit pouvoir apporter la preuve du consentement ➔ nécessité de conserver, pour chaque traitement, les informations sur la collecte du consentement (nature, date…)
- Article 7 : « Il est aussi simple de retirer son consentement que de le donner. »
- Article 8 : si la personne concernée par le traitement a moins de 16 ans, il est nécessaire que le consentement soit donné par le titulaire de la responsabilité parentale ➔ si la personne concernée a moins de 16 ans, proposer la validation d'un traitement la concernant au travers d'un lien envoyé dans un email à destination d'un des parents. Outre les détails concernant le traitements, l'email pourrait contenir un lien (sans limite de validité) permettant de retirer le consentement (article 7).

INFORMATION SIMPLE ET CLAIRE

- Article 12 : toute communication au sujet d'un traitement doit se faire « à la personne concernée d'une **façon concise, transparente, compréhensible et aisément accessible**, en des termes clairs et simples » ➔ fin programmée de la fameuse case à cocher « j'ai lu et j'accepte les conditions générales », plus gros mensonge d'Internet ☺.
- Article 13 : lorsque les données sont collectées **auprès de la personne concernée**, cette dernière doit être informée notamment :
  - des **détails concernant le responsable** des traitements
  - d'un éventuel **transfert** de ces données **à l'étranger**
  - de la **durée de conservation** des données.
- Article 14 : lorsque les données ne sont **pas collectées auprès de la personne** concernée :
  - mêmes obligations que celles apportées par l'article 13
  - s'y ajoute la nécessité d'**indiquer la provenance** des données

OUBLI NUMÉRIQUE ET EFFACEMENT

Suppression physique des données dans les meilleurs délais dans les cas suivants :

- les données ne **sont plus nécessaires** dans le cadre du traitement pour lequel elles étaient requises initialement
- la personne a **retiré le consentement** au traitement justifiant la collecte de ces données (voir article 7)
- la personne fait jouer son **droit d'opposition**, prévu dans l'article 21
- les données ont fait l'objet d'un **traitement illicite**
- **respect d'une obligation légale** définie par l'UE ou l'état membre auquel le responsable de traitement est soumis

Le cas échéants, les **sous-traitants du responsable** de traitement des données à effacer devront **répercuter l'opération.**

PORTABILITÉ DES DONNÉES

- Article 20(1) : « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un **format structuré, couramment utilisé et lisible par machine**, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle [...] »
- Considérant 68 : « Il y a lieu d'encourager les responsables du traitement à **mettre au point des formats interopérables** permettant la portabilité des données. » ➔ format du fichier (XML, JSON...), structure et nommage des champs : le législateur laisse les standards émergés d'eux-mêmes
- Article 20(2) : « Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible. » ➔ mise au point d'API permettant ces échanges

LIMITATION DU PROFILAGE

- Article 4(4) (définition) : « "profilage", toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données [...] pour **évaluer certains aspects personnels relatifs à une personne physique**, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique; »
- Article 21 : « La personne concernée a **le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière**, à un traitement des données à caractère personnel la concernant [...]. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne prouve qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. » ➔ mise en place d'un mécanisme d'opt-out pour chaque traitement

PRIVACY BY DESIGN

- Article 25(1) : « [...] le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des **mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données**, par exemple la minimisation des données » ➔ notion de *privacy by design*
- consiste à veiller de **manière proactive** au traitement des données personnelles **dès la conception** d'un système
- apparu dans les années 90 au Canada, sous l'impulsion d'Ann Cavoukian
- n'est pas (encore) formalisé sous la forme de norme ou standard ; pour le moment il s'agit simplement d'un framework
- **pseudonymisation** : consiste à **rendre impossible ou à défaut le plus compliqué** possible **l'attribution d'une donnée à une personne** ➔ *hash* des données, séparation claire (eg. utilisation de tables distinctes) entre les données permettant l'identification directe (nom, prénom...) et les autres données personnelles
- **minimisation** : collecter **le minimum de données nécessaires** au traitement auquel elles sont destinées ; et **limiter leur période de conservation** ➔ notion de *privacy by default*

REGISTRE DES ACTIVITÉS DE TRAITEMENT

- défini dans l'article 30 du RGPD : « chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un **registre des activités de traitement** mises en œuvre. »
- doit être **tenu à la disposition des autorités** de contrôle si besoin (principe d'*accountability*)
- les principales informations à y consigner :
  - le **nom et les coordonnées des différents acteurs** (responsable de traitement, co-responsable, représentant de l'organisme et le cas échéant, délégué à la protection des données personnelles)
  - les **finalités** du traitement
  - la **description des catégories de personnes concernées**, des catégories de données et des catégories de destinataires des données personnelles
  - les **transferts de données** personnelles avec identification des pays de destination et des garanties utilisées pour encadrer cette opération (BCR, clauses contractuelles types, etc.)
  - la **description des mesures** de sécurité adoptées
  - les **délais prévus pour l'effacement** des différentes catégories de donnée

INFORMATION EN CAS DE PIRATAGE

- définie dans l'article 33 du RGPD : « En cas de violation de données à caractère personnel, le responsable du traitement en **notifie la violation** en question à l'autorité de contrôle compétente [...] **dans les meilleurs délais** et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. »
- informations à communiquer :
  - la **nature de la violation** de données à caractère personnel y compris, [...] le **nombre approximatif de personnes concernées** par la violation et [...] le nombre approximatif d'enregistrements de données à caractère personnel concernés
  - le **nom et les coordonnées du délégué à la protection des données** ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues
  - les **conséquences probables** de la violation de données [...]
  - les **mesures prises ou que le responsable du traitement** propose de prendre pour remédier à la violation de données à caractère personnel [...]
- les **personnes concernées par la violation** de données se doivent d'être elles aussi **informées**, dans les meilleurs délais (article 34)

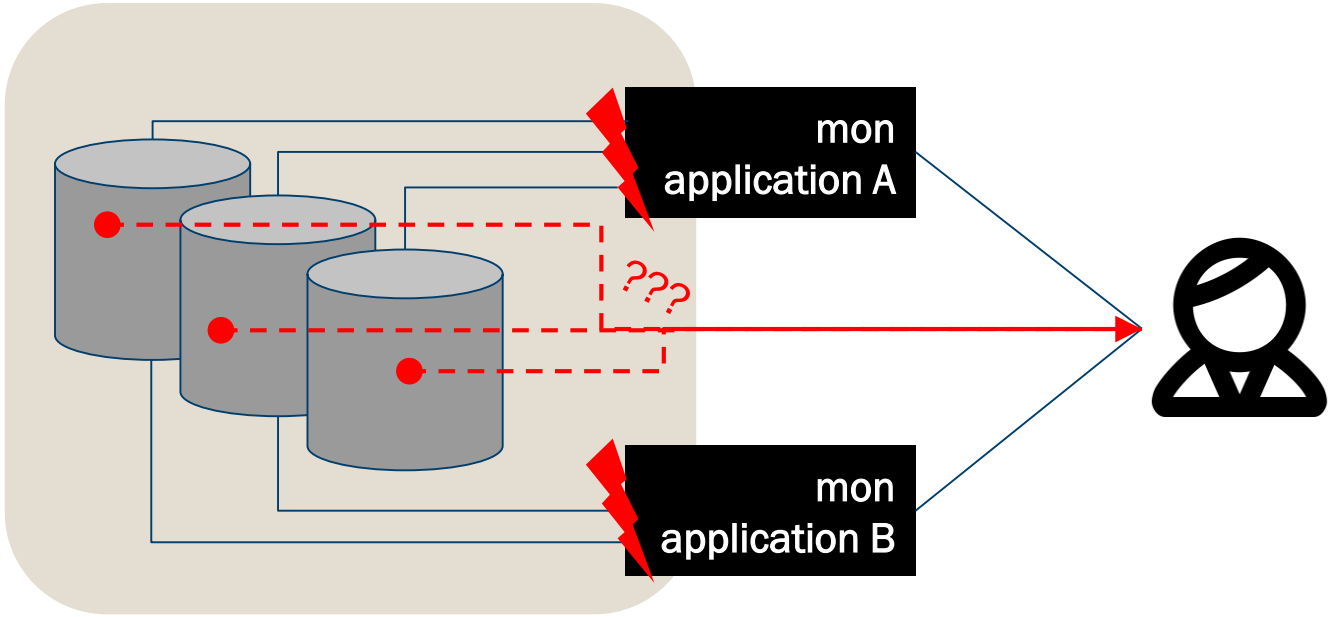
➔ mise en place et/ou renforcement de mesures veillant à renforcer la sécurité : chiffrement des bases de données *at rest,* chiffrement de tous les échanges HTTP...

CODES DE CONDUITE ET CERTIFICATIONS

- l'article 40 encourage **l'élaboration de codes de conduite** destinés à contribuer à la bonne application du règlement
- « les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement, telles que : »
  - le traitement loyal et transparent
  - les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques
  - la collecte des données à caractère personnel
  - la pseudonymisation des données à caractère personnel (➔ *privacy by design*, article 25)
  - les informations communiquées au public et aux personnes concernées
  - l'exercice des droits des personnes concernées
  - les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant (➔ article 8)
  - les mesures et les procédures en cas de piratage, la notification aux autorités de contrôle et aux personnes concernées (➔ articles 24 et 25)
- l'article 42 prévoit la mise en place de **certifications de conformité** avec le règlement

➔ la mise en œuvre du principe d'*accountability* se trouvera guidée par l'apparition de ces codes de conduite et la création de ces certifications

ARCHITECTURES EXISTANTES : QUELS ENJEUX ?

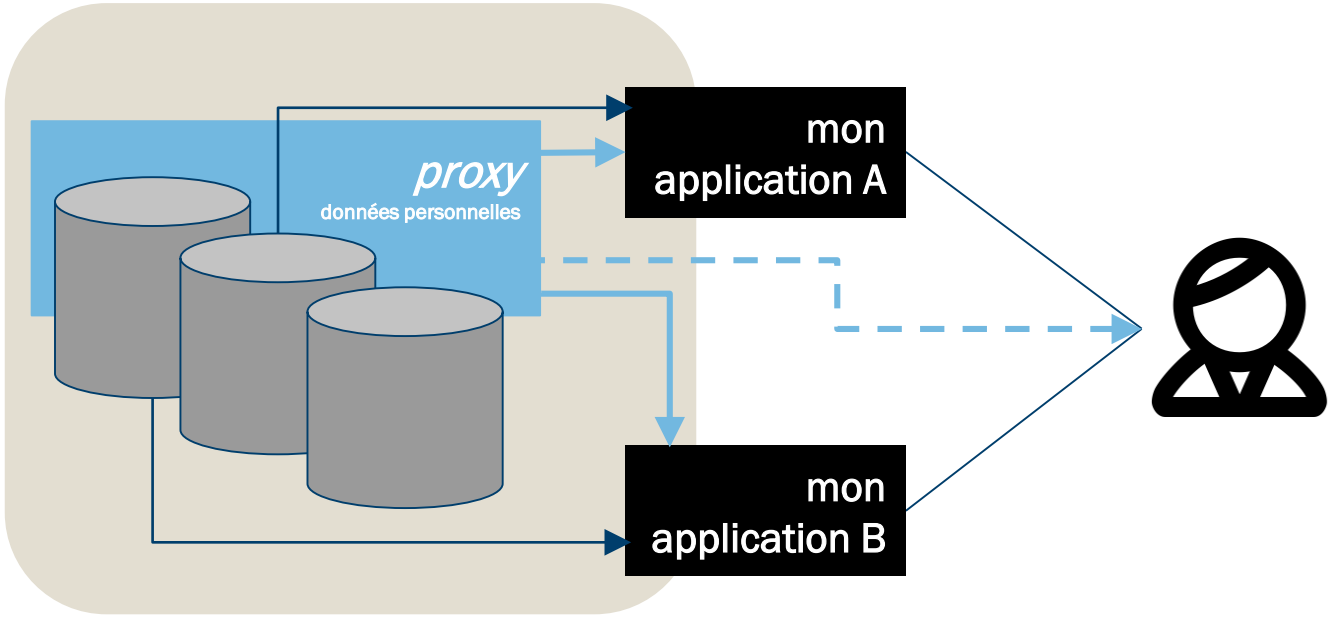


ARCHITECTURES EXISTANTES : COMMENT LES PRÉPARER ?

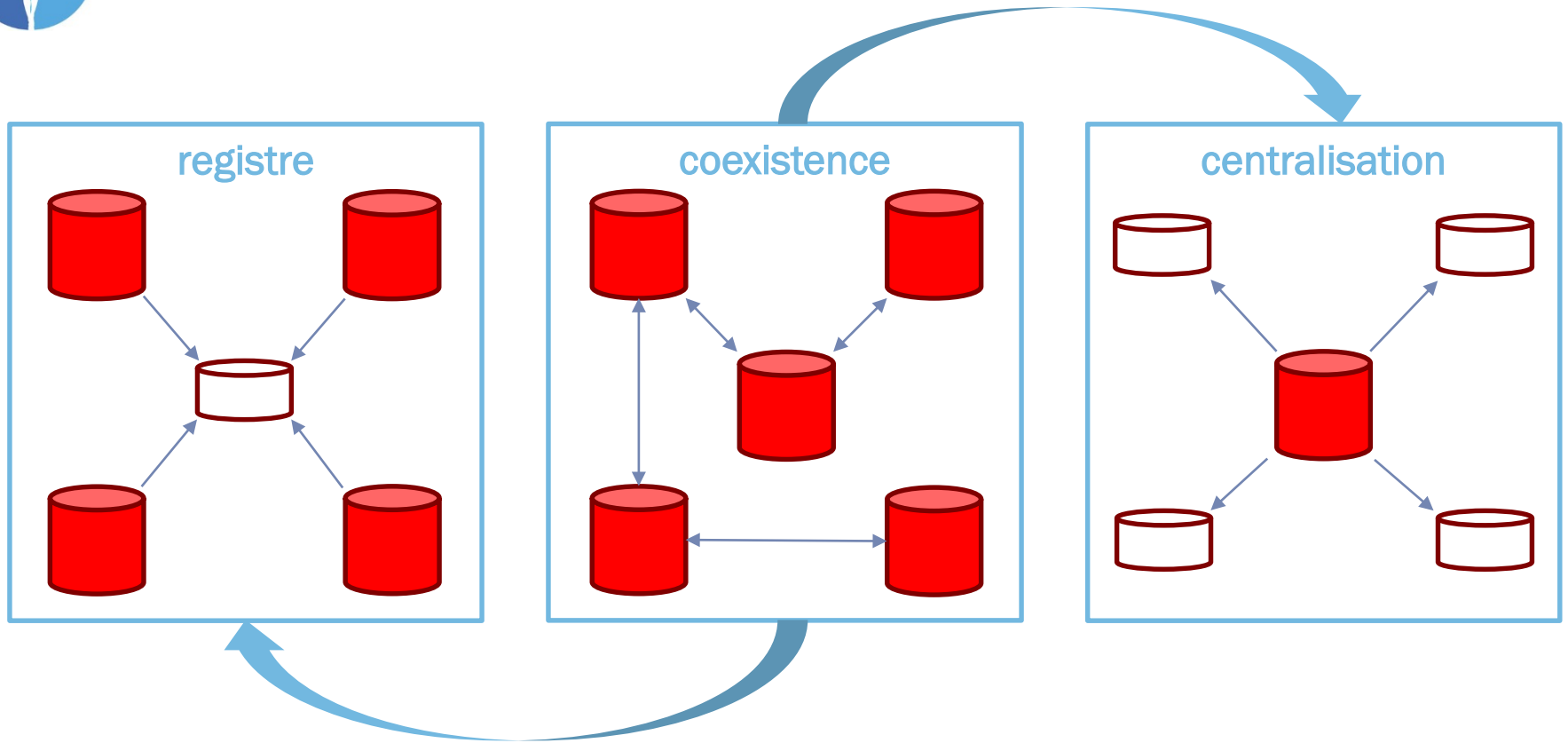
- **cartographier**, en couvrant l'ensemble du système d'information (y compris les services assurés par des sous-traitants), les **emplacements où se trouvent des données personnelles**
- pour chacune de ces données, lui adjoindre les métadonnées suivantes :
  - **date** à laquelle elle a été collectée ?
  - **raison** de la collecte ? traitement(s) appliqué(s) à la donnée ? (mise en place de codifications)
  - **origine** : la donnée provient-elle de l'utilisateur lui-même ou a-t-elle été obtenue auprès d'un tiers ?
  - **traitement(s)** appliqué(s)

➔ il n'est pas trop tôt pour démarrer ces travaux ! Ils devront quoi qu'il arrive être menés en vue de se préparer au RGPD

NOUVEAU RÈGLEMENT <=> NOUVELLES ARCHITECTURES… LA (UNE) SOLUTION



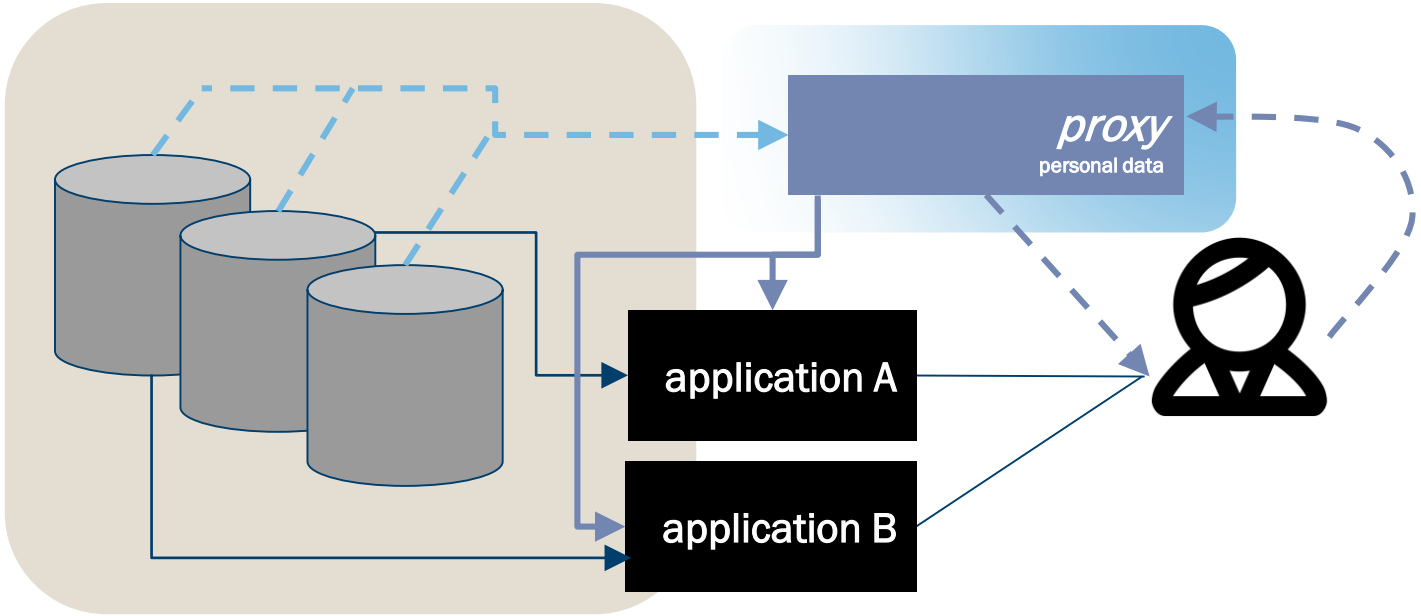
VUE 360°



VUE 360° – DEUX STRATÉGIES

- **Registre**
  - consiste à **collecter les données** à caractère personnel dans les différents systèmes puis les consolider
  - offre un **point d'entrée unique pour les recherc**hes dans l'ensemble du SI sur base de données personnelles
  - relativement **simple à mettre en œuvre** ; pas ou peu d'impacts sur le SI existant
  - les traitements (initialisation, mise à jour, suppression…) continuent d'être **faits dans les différents systèmes**
- **Centralisation**
  - consiste à créer un '**master record**' pour chaque client/utilisateur
  - utilisation de **plateforme de MDM** ; très souvent **coûteuses** et complexes à mettre en œuvre
  - les **traitements se trouvent simplifiés** : ils ne sont faits qu'une fois au niveau du master, avant d'être répercutés dans l'ensemble du SI
  - point bloquant : certains des systèmes peuvent ne **pas être conçus afin d'en permettre une mise à jour par un processus externe**

ÉMERGENCE DE NOUVEAUX SERVICES



CONCLUSION

- L'implémentation du RGPD concerne **quasiment toutes les entreprises**
- D'**importants challenges** sont à relever afin de se mettre en conformité
- Nécessitera **de l'inventivité** pour mettre en œuvre des concepts souvent peu formalisés
- Attention aux **exceptions** !
- Des **certifications et guides** à venir
- Opportunités d'**accroître la qualité des informations** détenues