APDL

Association pour la Protection des Données au Luxembourg

sopra steria

ORIENTATIONS SUR LA CONSERVATION ET LA DESTRUCTION DES DONNEES DANS LE CADRE DU RGPD

PAR LA COMMISSION TECHNIQUE APDL

MARDI 30MARS 2021

AGENDA


Mots de bienvenue


Cadre légal


Méthodologie et exemple pratique

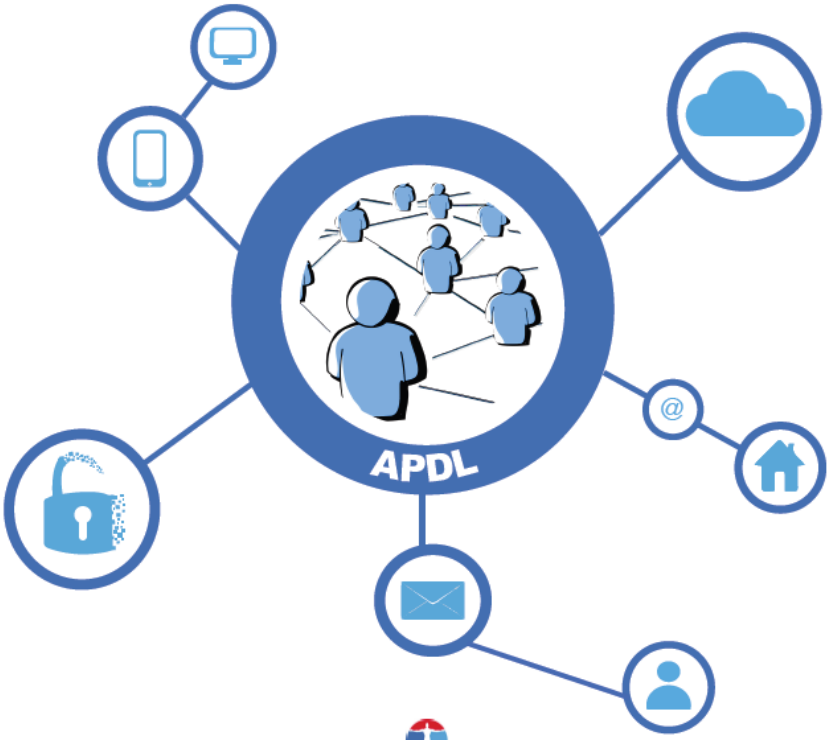

Aspects techniques


Outil de détection des données


Q&A

ACCUEIL

Association à but non lucratif créée par et pour les professionnels
de la protection des données au Luxembourg



Rejoignez-nous sur www.apdl.lu

APDL - bâtiment BDO Air, ZA de la Cloche d'Or, 1 rue Jean Piret, L-2350 Luxembourg R.C.S. Luxembourg : F9723

GROUPES DE TRAVAIL

Commission Data Protection Officer Arnaud CONSTANT
dpo@apdl.lu
Aider le DPO dans l'exercice de sa fonction

Commission Technique Romain SABEL
technique@apdl.lu
Mieux gérer les risques et étudier les outils liés à la protection des données

Commission Juridique Renaud LE SQUEREN
juridique@apdl.lu
Veiller et décrypter la législation afin d'en faciliter son application

Commission Communication et Sensibilisation Michaël TOME
sensibilisation@apdl.lu
Développer des solutions de sensibilisation et de communication

CADRE LEGAL

Bénédicte d'Allard, Arendt Regulatory & Consulting

GENESE DU DOCUMENT

- Décision des membres de la Commission Technique, en octobre 2018, de lancer un travail sur la gestion de la rétention et de l'effacement des données .
- Contributeurs membres de la Commission Technique:
  - Guy Isler (CCSS)
  - Philippe Simon (RBC Investor Services)
  - Miguel Martins (Talkwalker)
  - Pierre Van Wambeke (Seezam S.A.)
  - Marie-Emilie Mengal (Juriste spécialisée en TIC et protection des données)
  - Bénédicte d'Allard (Arendt Regulatory & Consulting)
  - Sylvie Dessolin (Sopra Steria PSF Luxembourg)
  - Romain Sabel (BDO Services Luxembourg)

CADRE LÉGAL (1/3)

Plusieurs articles du règlement RGPD posent les principes applicables en matière de conservation de données personnelles.

- **Limitation du traitement (Article 4.3))** : « marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur ».

- **Principe de légitimité du traitement des données à caractère personnel (Article 5, alinéa 1, b) :** « Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités .

CADRE LÉGAL (2/3)

- **Principe de minimisation des données (Article 5.c)** : les « données doivent être adéquates, pertinentes et limitées :

- **Principe de limitation de la conservation (Article 5.1e)** : les données doivent être «conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

- **Information à fournir à la personne concernée (Article 13.2a)** : « La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée doit être communiquée aux personnes concernées

CADRE LÉGAL (3/3)

- **Droit à la limitation du traitement (Article 18) :** la « personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement » dans certains cas spécifiques énumérés de a) à d).

- **Droit à l'oubli (Article 17) :** «La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs a) à f) s'applique ».

EN RESUME

Le responsable du traitement est autorisé à conserver les données personnelles tant que les finalités du traitement sont d'actualité.

Pas de traitement de données à caractère personnel sans finalités et, dès lors, pas de conservation de ces données sans subsistance de ces finalités déterminées, explicites et légitimes.

⇒ Difficile à respecter si non pris en compte lors de la conception du traitement et de la méthode de conservation des données.

⇒ Défi technique de l'effacement sélectif si les archives ne sont pas organisées correctement.

⇒ Le droit à l'oubli n'étant pas absolu, statuer sur les demandes au cas par cas.

CAS SPÉCIFIQUES

- Conservation des données à caractère personnel traitées par le responsable du traitement pour assurer l'exécution de ses missions (publiques pour les acteurs publics, commerciales, contractuelles mais aussi de leurs obligations légales pour les acteurs privés) dans le cadre de finalités déterminées, explicites et légitimes pour une durée limitée correspondant à la durée de subsistance de cette finalité.

- Conservation des données à caractère personnel traitées par le responsable du traitement, dans le cadre de ses missions de recherches (scientifique, historique ou statistique) ou dans le cadre de ses obligations légales découlant de la règlementation en matière d'archivage dans l'intérêt public, pour une durée limitée correspondant à la durée de subsistance de ces finalités particulières.

OBLIGATIONS EN CAS DE SOUS-TRAITANCE

« Selon le choix du responsable du traitement, **le sous-traitant supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement** au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'Etat membre n'exige la conservation des données à caractère personnel » (Article 28.g).

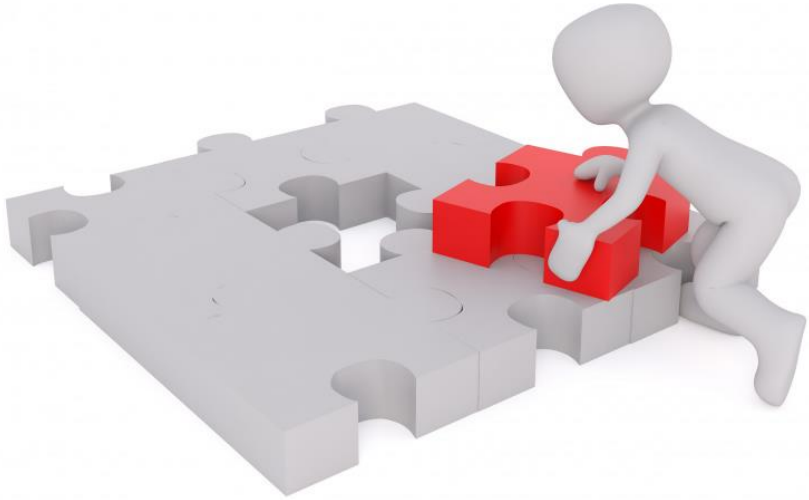
Le sous-traitant doit:

- Lui aussi organiser les données retenues pour le compte d'un responsable du traitement, de telle sorte qu'il soit capable de les extraire ou de les détruire.
- Respecter tous les principes de conservation.
- Aider le responsable du traitement à être conforme au RGPD, et donc aussi veiller aux méthodes de rétention choisies, afin de pouvoir assister le cas échéant le responsable du traitement à répondre aux différentes demandes de personnes concernées.

A régler par des clauses contractuelles détaillées, ainsi que des instructions documentées.

METHODOLOGIE ET EXEMPLE PRATIQUE

Sylvie Dessolin, Sopra Steria Consulting



« La mise en œuvre des mesures de sécurité et la prévention des fuites de données (RGPD article 32) »

MENACES

15/05/2018 - Leudelange

MESURES

En 2018 vous avez aimé la première publication de la Commission Technique de l'APDL (toujours disponible)

RETENTION ET DESTRUCTION… OU COMMENT FAIRE DE VOS DATA SUBJECT… DES SANS VISAGES

Par où commencer ? - Beginner's Guide

Par chance, les responsables de la protection des données vont recevoir l'aide des « ***Records Managers*** » et bénéficier de l'apport de cet autre domaine de la gestion de l'information (le « *Records Management* », qui consiste à gérer les données et documents dans une optique de valeur probante et d'efficience).

Le Records management : La gestion du cycle de vie

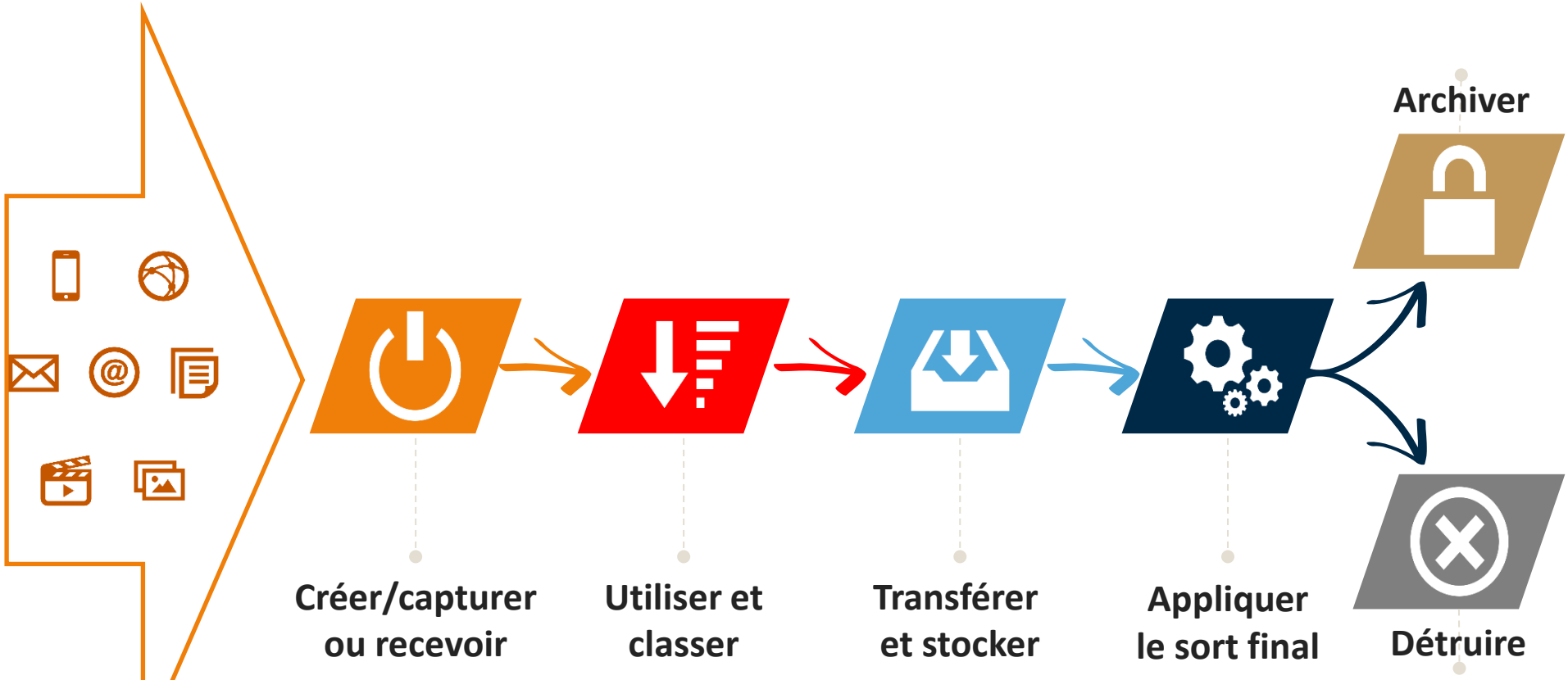
Documents / Informations d'activité (Records)

- **Informations créées, reçues et préservées comme preuve et actif par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité (ISO15489-1; 2016)**

Records Management :

- **Champ de l'organisation et de la gestion en charge d'un contrôle efficace et systématique de la création, de la réception, de la conservation, de l'utilisation et du sort final des documents d'activité y compris des processus de capture et de préservation de la preuve et de l'information liées aux activités et aux opérations sous la forme de documents d'activité (ISO15489-1; 2016)**

LE CYCLE DE VIE DES INFORMATIONS & DOCUMENTS



1 - L'approche processus

1. ANALYSER LES PROCESSUS (1/2)

Identifier

- les processus et les données qu'ils manipulent
- Les exigences légales, réglementaires, contractuelles, commerciales et opérationnelles applicables, ainsi que les besoins métiers de conservation
- Cette méthode va donc permettre de :

  - compléter le registre des traitements

  - mettre en œuvre les rétentions et destructions nécessaires

1. ANALYSER LES PROCESSUS (2/2)

Avantages:

- cette approche recoupe celles généralement utilisées notamment en matière de management de la qualité (ISO 9000) ou de sécurité de l'information (ISO 27000)
- permet au DPO et aux équipes qui accompagnent la conformité au RGPD de
- prendre rapidement connaissance des activités de l'organisme
- conduire de manière rapide l'identification des traitements
- construire le registre de traitements RGPD

2. IDENTIFIER LES OBLIGATIONS ET LES DURÉES DE RÉTENTION (1/4)

- Une fois que l'on a établi les traitements et les données en jeu et établi la licéité du traitement
- On recherche :
  - les textes légaux applicables
  - la durée de rétention qui peut être explicite dans le texte :

    + l'obligation de conserver une information pendant un certain nombre d'années
    + l'obligation de détruire après une certaine durée
    + le « trigger » *(l'« événement déclencheur » à partir duquel court la durée de rétention)*

2. IDENTIFIER LES OBLIGATIONS ET LES DURÉES DE RÉTENTION (2/4) : UNE ANALYSE PROPRE A CHAQUE ORGANISME, ET A MAINTENIR

- Il revient à chaque organisme de vérifier quelles données doivent être conservées, pendant quelle durée et dans quelles conditions
- L'organisation doit effectuer une « due diligence » et maintenir une veille sur les dispositions légales qui lui sont applicables

!!!!... ne pas utiliser (sans une relecture attentive et les vérifications qui s'imposent) les listes de rétention toutes faites !!!

EXEMPLE DE REFERENTIEL (EXTRAIT)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Archives nationales

Code série	Série	Liste des documents	DUA	Élément déclencheur de la DUA	Sort final	Remarques
R2-02	Recrutement et carrière - documents opérationnels ou doublons du dossier du CGPO	- Feuille de renseignement, copie des diplômes, questionnaire ou test précédant l'embauche et ses conclusions, lettre d'embauche, attestation de prise de connaissance du règlement intérieur, document attestant de la situation personnelle et familiale, certificat d'aptitude lors de l'embauche, extrait d'acte d'État-civil, relevé d'identité bancaire, lettre de démission et réponse, reconstitution de carrière et état des services, accusés de réception (clefs et badges d'accès au bâtiment), copie des arrêtés, attestation de prise de connaissance du document de l'organisation interne, de la politique de sécurité de l'information et de la charte de confidentialité, accord de confidentialité **- Extrait de casier judiciaire*** **- Affaires disciplinaires mineures** (avertissement, réprimande et amende ne dépassant pas le 5ème d'une mensualité brute du traitement de	75	Date de naissance de l'agent	D	**Justification de la DUA et du sort final :** Ces documents sont détruits car le dossier de carrière des agents est conservé auprès du CGPO *** Destruction au bout d'1 mois si candidature retenue** - Lettre circulaire du 17 mai 2019 relative aux délais de conservation des casiers judiciaires - Loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les États membres de l'Union européenne, art. 8-5 **** Destruction (mention rayée dans le dossier) après 3 ans** à compter de la décision sanctionnant l'agent si, dans les 3 ans qui suivent la décision disciplinaire, le fonctionnaire n'a encouru aucune nouvelle sanction disciplinaire - Loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'État, art. 54 §5

https://anlux.public.lu/dam-assets/pdf-statiques/STATEC-Convention-tableau-de-tri-V01-01.pdf

EXEMPLE DE REFERENTIEL (EXTRAIT)

Activités de traitement	Détails du traitement	Durées de conservation en base active	Durées de conservation en archives intermédiaires	Fondements juridiques Textes de références
Recherches impliquant la personne humaine (RIPH) et recherches nécessitant le recueil du consentement de la personne concernée : - Les recherches interventionnelles, y compris les recherches à risques et contraintes minimes ; - Les essais cliniques de médicaments à l'exception des essais cliniques par grappes ; - Les recherches nécessitant la réalisation d'un examen des caractéristiques génétiques;	**Recherche conforme à la MR[1]-001** *Données des personnes se prêtant à la recherche*	Conservation dans les systèmes d'information du RT, du centre investigateur ou du professionnel intervenant dans la recherche **jusqu'à la mise sur le marché du produit étudié** ou **jusqu'à 2 ans** à compter de la dernière publication des résultats de la recherche. En l'absence de publication : conservation **jusqu'à la signature du rapport final de la recherche**.	Archivage sur support papier ou informatique pour une **durée conforme à la réglementation en vigueur**	MR-001 Délibération n° 2018-153 du 3 mai 2018 Réglementation sectorielle applicable : code de la santé publique, arrêtés (ex : arrêté du 8 novembre 2006, bonnes pratiques cliniques, règlement n°536/2014)
	Recherche conforme à la MR-001 *Données des professionnels intervenant dans la recherche*	**15 ans** au maximum après la fin de la dernière recherche à laquelle les professionnels ont participé	Archivage sur support papier ou informatique pour une **durée conforme à la réglementation en vigueur**	MR-001 Délibération n° 2018-153 du 3 mai 2018 Réglementation sectorielle applicable : code de la santé publique, arrêtés (ex : arrêté du 8 novembre 2006, bonnes pratiques cliniques, règlement n°536/2014)

https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_recherches_dans_le_domaine_de_la_sante.pdf

2. IDENTIFIER LES OBLIGATIONS ET LES DURÉES DE RÉTENTION (3/4) : LES QUESTIONS À SE POSER

- Jusqu'à quand ai-je vraiment besoin des données pour atteindre l'objectif fixé ?
- Ai-je des obligations légales de conserver les données pendant un certain temps ?
- Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Lesquelles ?
- Jusqu'à quand puis-je faire valoir ce recours en justice ?
- Quelles informations doivent être archivées ? Pendant combien de temps ?
- Quelles sont les règles de suppression des données.
- Quelles sont les règles d'archivage des données ?

Source : CNIL https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees

2. IDENTIFIER LES OBLIGATIONS ET LES DURÉES DE RÉTENTION (4/4)

- il faut tenir compte de la durée d'un éventuel procès en cas de litige ou de contestation (litigation hold)
- si l'on n'a pas de texte applicable, on va considérer
  - la guidance des administrations, des associations professionnelles, les normes métiers, les référentiels de certification
  - les besoins du métier (mais uniquement la durée nécessaire au traitement

3. FORMALISER LES DURÉES DANS LE REGISTRE ET DANS LES PROCÉDURES (1/3)

- Les obligations et durées de rétention ainsi identifiées sont reportées, pour les besoins du RGPD, dans le registre, ou dans une procédure/un tableau annexe
- Il peut être utile d'indiquer le texte légal applicable, la durée de rétention ainsi que son point de départ (le « trigger »).
- Les organismes les plus avancés en matière de protection des données pourront en faire part aux personnes concernées, comme requis par le règlement, en même temps qu'ils informeront ceux-ci sur les traitements.

3. FORMALISER LES DURÉES DANS LE REGISTRE ET DANS LES PROCÉDURES (2/3)

Exemple Fiche REGISTRE AVEC DUREES et Textes (d'après modèle registre CNIL)

Finalité(s) du traitement effectué			
Finalité principale	Gestion de la paie		
Sous-finalité 1	Calcul des rémunérations		
Sous-finalité 2	Calcul du montant des versements adressés aux organismes sociaux		
Sous-finalité 3	Ordre de virement à la banque		
Catégories de données personnelles concernées	Description	Durée de conservation	Texte de réference
État civil, identité, données d'identification, images...	Noms, prénoms, adresses	5 ans à compter du versement de la paie	Article L3243-4
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter du versement de la paie	Modifié par LOI n°2009-526 du 12 mai 2009 - art. 26
Numéro de Sécurité Sociale (ou NIR)	Numéros de sécurité sociale des salariés	5 ans à compter du versement de la paie	L'employeur conserve un double des bulletins de paie des salariés ou les bulletins de paie remis aux salariés sous forme électronique pendant cinq ans.
Catégories de personnes concernées	Description	Précisions	
Catégorie de personnes 1	Salariés		

https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods

3. FORMALISER LES DURÉES DANS LE REGISTRE ET DANS LES PROCÉDURES (3/3)

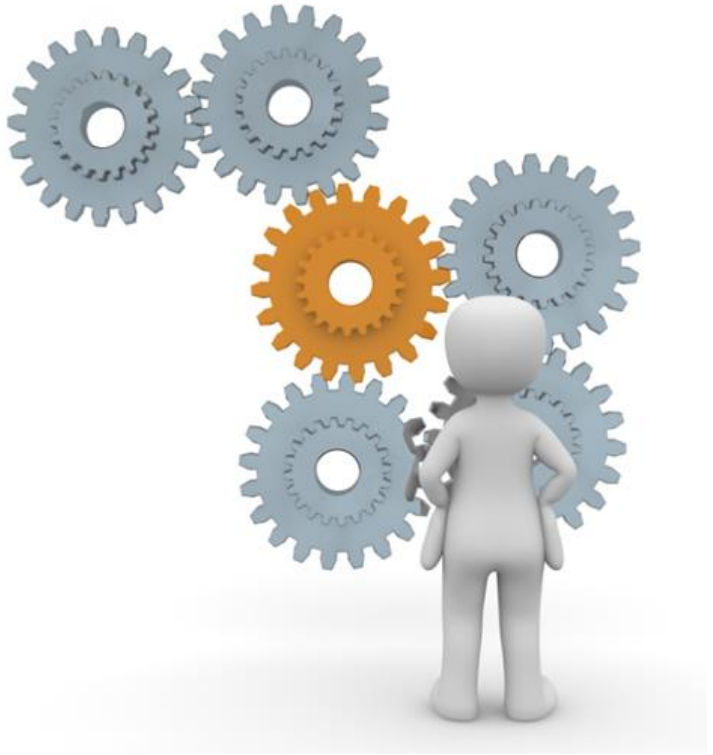
Une procédure de rétention spécifique, accompagnée d'un tableau en annexe ou d'une base de données peut aussi être mise en place

EXEMPLE PROCEDURE – EXTRAIT (ANNEXE : TABLEAU TEXTES, DUREES DE RÉTENTION ET TRIGGER PAR PROCESSUS ET SOUS PROCESSUS)

3 - PROCESSUS RESSOURCES HUMAINES					
	SOUMIS À LA RÉGLEMENTATION SUR LA PROTECTION DES DONNÉES A CARACTERE PERSONNEL :				
Données et documents visés	Personnes concernées	Types de données concernées	Texte légal	Durée de conservation	Début de la durée de conservation
PROCESSUS RECRUTEMENT					
Recrutement : extrait de casier judiciaire, certificat de bonnes vie et mœurs,...	-Candidats à l'embauche (recrutés ou non)	Données :	Art. 8-5 (2) de la Loi du 23/07/ 2016 relative à l'organisation du casier judiciaire	1 mois	A partir de la conclusion du contrat de travail
	-Salariés	-d'identification ;			
		condamnations			
PROCESSUS GESTION ET ADMINISTRATION des RH					
(...)					
SALAIRES					
Documents relatifs aux salaires dont les bulletins de paie, impôts, sécurité sociale, rémunération des heures supplémentaires, primes, avantages en nature, etc.	-Salariés	Données :	-Prescription des actions en paiement de salaires de toute nature est de 3 ans (article 2277 du CCivl et Art. L 221-2 du Code du travail)	10 ans	à compter de la clôture de l'exercice social de référence
		-d'identification ;	-Conservation des bulletins de paie (=pièces justificatives) pour une durée de 10 ans :Art. 14, 16 et 189 du CCom)		
		-financières			

ASPECTS TECHNIQUES

Romain Sabel, BDO



ASPECTS TECHNIQUES

Différents types de données exigent des traitements adaptés:

- Support:
  - Données nativement numériques
  - Données papier digitalisées
  - Données papier
- Format:
  - Données structurées
  - Données non structurées

DONNEES NUMERIQUES

Elles existent sous différentes formes:

- Données structurées:
  - Fichiers et Base de données
  - Indexées
- Données non structurées:
  - Messagerie, dossiers partagés, GED dans certains cas
  - Utilisation des métadonnées:
    - Date et heure de création
    - Identifiant utilisateur
    - Identification automatisée par OCR et recherche de mots clés

Index et métadonnées contiennent souvent des données à caractère personnel

DONNEES NUMERIQUES

Elles sont conservées sur différents type de support:

- Disques durs magnétiques et SSD
- Bandes ou cassettes magnétiques
- CD, DVD
- Clés USB
- Micro-fiches

DONNEES NUMERIQUES

Les données se trouvent souvent dans des environnements différents:

- Environnement de production
- Environnement de développement
- Environnement de tests et d'acceptation
- …

Attention aux données à conserver dans les différents environnements et aux droits d'accès attribués

DONNEES NUMERIQUES

Nous avons différents niveaux de conservation:

- Base active
  - Pendant la durée nécessaire à la réalisation de la finalité initiale
  - Accès large mais toujours basé sur le principe du « moindre privilège »
- Archivage intermédiaire
  - Obligation légale ou intérêt légitime (p. ex. en cas de litige en cours)
  - Accessible à un nombre restreint d'utilisateurs
  - Limité dans le temps
- Archivage définitif
  - Intérêt public (loi du 17 août 2018)
  - Jamais détruits
  - Gérés par les services d'archives publics compétents

DONNEES NUMERIQUES

Modalités techniques de l'archivage:

- Dans la base de production, mais en limitant les accès
- Dans une base spécifique réservée à l'archivage

- Mesures organisationnelles et techniques assurant la limitation de l'accès
- Attention d'imposer les mêmes règles au tiers si sous-traitance

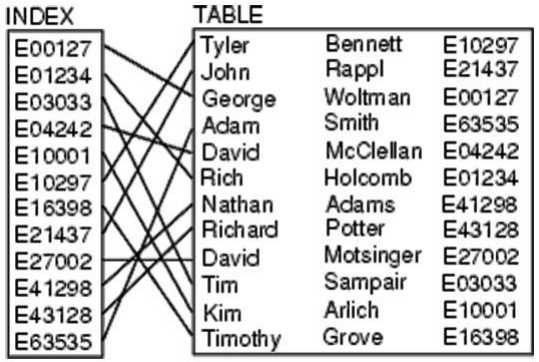
Point d'attention – limiter les accès

DONNEES NUMERIQUES

La destruction en fin de vie:

- Effacement courant
  - Déplacement dans la corbeille
  - Effacement dans l'index sans effacer les données elles-mêmes
  - Marquer un enregistrement dans une base de données
  - Systèmes de fichier historisés – crée une nouvelle copie sans écraser l'original
  - Sur les supports magnétiques persistance de l'information initiale liée aux caractéristiques du magnétisme

Effacement pas sûr ni définitif



DONNEES NUMERIQUES

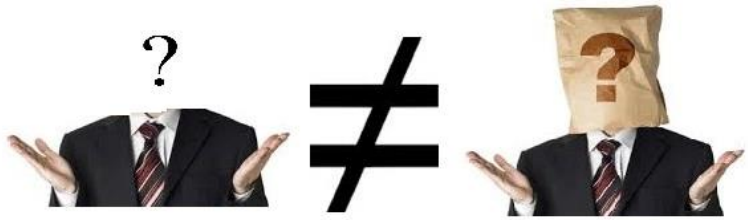
Destruction sécurisée:

- Programmes spéciaux
  - Réécriture en plusieurs phases de données aléatoires sur les supports magnétiques
  - Réinitialisation des cellules des SSD par algorithmes spéciaux (souvent fournis par le constructeur du SSD).
- Destruction physiques
  - Démagnétiser les bandes et cassettes
  - Broyeur (société spécialisée) – attention à la taille des résidus
  - Seul moyen pour les microfiches

DONNEES NUMERIQUES

Effacement logique:

- Pseudonymisation
  - Ce n'est pas une destruction car le lien avec la personne concernée peut être rétabli
- Anonymisation
  - **Correctement réalisée** les données ne sont plus des données personnelles
  - Agrégation des données
    - Bien choisir les agrégats – garder données pertinentes, mais anonymes
    - Rajouter des données aléatoires



DONNEES NUMERIQUES

Effacement logique:

- Anonymisation
  - Les risques
    - Les corrélations: retrouver la personne en utilisant les liens entre différents enregistrement
    - Les inférences: reconstruire un attribut à partir d'autres attributs
  - Les mesures possibles
    - Rajouter du bruit aléatoires
    - Permuter certains attributs

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

DONNEES NUMERIQUES

L'autre obligation – ne pas perdre les données:

- Politique de sauvegarde à plusieurs génération
- Séparation géographiques des différentes copies
- Au moment de l'effacement
  - Effacement ciblé sur toutes les sauvegardes presques impossibles
  - Attention en cas de restauration

DONNEES PAPIER

Leurs risques inhérents

- Protection physique
  - Clean Desk Policy pour les données en production
  - Limitation des accès aux locaux d'archivage
- Copies multiples pour faciliter le travail dans différents services
  - La digitalisation pourrait être une solution – mais attention à la réimpression
- Impossibilité d'une indexation multiple
  - Sans classement chronologique il est difficile de respecter les durées de rétention
  - Possibilité d'un fichier d'indexation – attention à effacement les enregistrement en même temps que les documents

DONNEES PAPIER

La destruction sécurisée

- Ne pas utiliser les poubelles « normales »
- Déchiqueteuse papier – attention à la taille des miettes résiduelles
- Containers fermés et traitement par une société spécialisée

Il reste le problème des archives historiques.

DONNEES PAPIER

L'obligation de conservation des données

- Presque impossible sans digitalisation de garantir la conservation
- Mesures de sécurité physique encore plus importantes

Et en cas de digitalisation

- Conservation ou non des documents papier?
- Valeur légale des documents digitalisés

Les principes de conservation s'appliquent aussi aux données papier, mais les techniques doivent être adaptées.

OUTIL DE DÉTECTION DES DONNÉES

Alejandro Del Rio / Michael Hofmann, EY

SUMMARY

1. Companies having complex technical infrastructure:

- Systems on premises/off site/cloud, hubs
- High number of data bases/applications, data warehouses, data lakes
- Little control data control over non structured data, mail and files servers
- With a high level system integration/interfacing
- Online and batch processing
- End user computing

2. Production systems have not been build with "privacy by design/default"

AGENDA

01 Use Cases

02 Data Discovery and Inventory

03 Data-Centric Audit and Protection

1

USE CASES

DATA SUBJECT REQUETS

GDPR reference: Articles 15, 16, 18, 20 & 21

Legal Context

As per GDPR article 12, "the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event **within one month** of receipt of the request"

Client Challenges

Context background:

Apart from providing transparency and possibility to data subjects to exercise their rights under GDPR, companies need to be able to respond back in one month as per the date of the request. Some issues to comply with this obligation are:

- Companies may have several IT systems and applications, and requester might be on several applications. Information needs to be correlated
- Data from a single individual might be found on different formats (e.g. second first names, second family names)
- The company relies on third parties such as Software as a Service (e.g. Office 365) or any other provider having personal data increases lack of visibility

Client Benefits

While performing data discovery exercises companies can understand where personal data resides within the different applications of a company.

A company can ensure to answer data subject requests within the obliged timeframe (one month) and correlate the data from a single data subject through several systems and applications.

Value added

- Increase of reputation towards customers
- Provide assurance to DPAs over GDPR compliance

Sector
Telecommunications, Media and Technology

Fine type
Insufficient legal basis for data processing

Area and country/region
Italy

Fine date
July 2020

Amount
16,700,000 €

- ***EDPS: Guidelines on the Rights of Individuals with regard to the Processing of Personal Data***
- ***ICO: Right of access***

DATA SUBJECT REQUETS

GDPR reference: : Articles 5 (e,f) & 17

Legal Context

As per GDPR article 17, “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her…”. Furthermore, as per article 19 “The controller shall communicate any rectification or erasure of personal data”.

Client Challenges

Context background:

Companies need to be able to delete the data, both upon request but also proactively. This is based on legal obligations and business requirements. Usually retention periods are recorded under “Data Retention Policy”, but main challenges are:

- In order to destroy the data, companies need to be able to identify where the personal data resides
- IT applications may have dependencies between each other, so deleting some pieces of data may corrupt some applications
- Legacy applications have not been built following privacy by design principles, and contain a lot of personal data that has been forgotten

Client Benefits

Complying with each companies’ data retention policy is a key requirement to achieve compliance with GDPR principles.

Data Protection Authorities are focusing more and more on this item, so a proper data deletion may demonstrate high-level of maturity with overall GDPR programs

Value added

- Proper data management
- Leveraging space on IT systems
- Increasing reputation with customers and former employees

Sector

Telecommunications, Media and Technology

Fine type

Insufficient legal basis for data processing

Area and country/region

Italy

Fine date

January 2020

Amount

27,800,000 €

- ***ICO: Principle Storage Limitation***
- ***IAPP: Data Retention Guidance***

FINES

Tough penalties

Fines up to

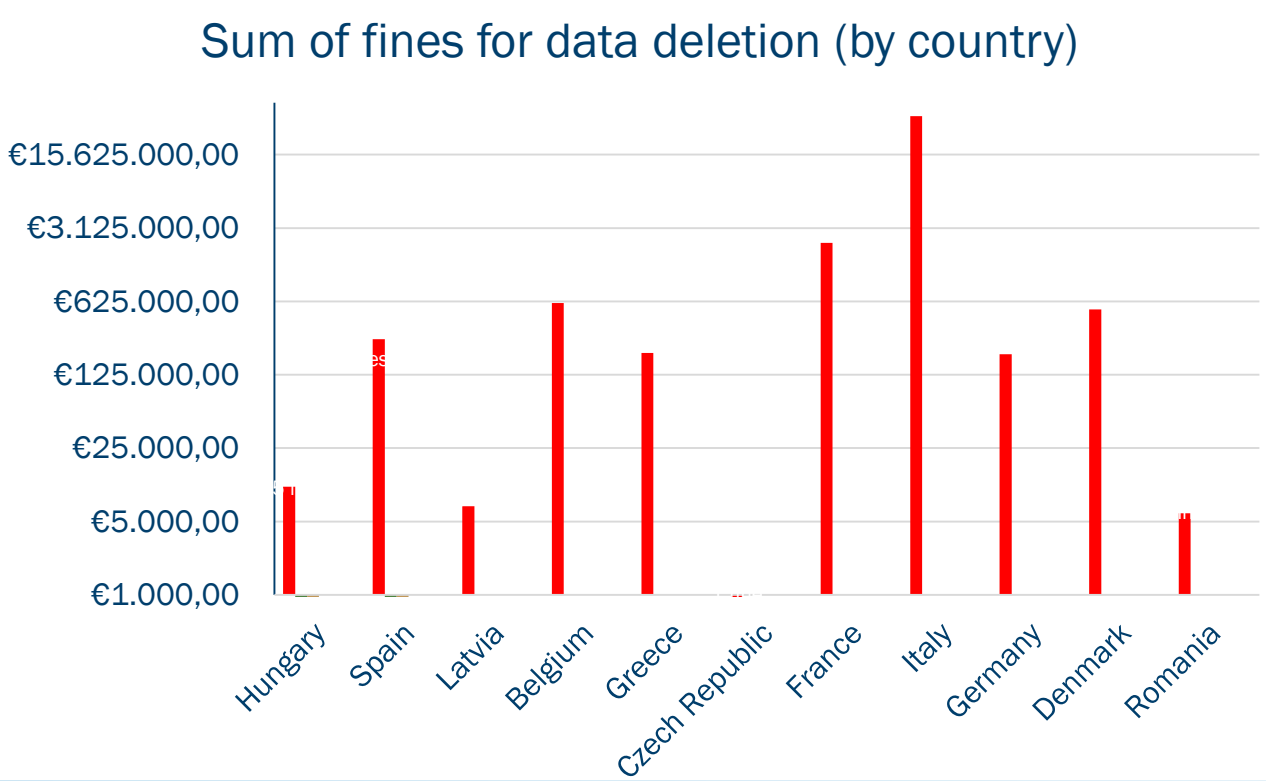
4% of annual global revenues

or

20 Million Euros

whichever is greater

- Total amount fined from July 2018 on for violation article 5 and 17 of the GDPR: **40.385.435 €**
- **32 fines** issued to-date
- Causes: non compliance with the storage limitation obligation or non compliance with the right to erasure



2

DATA DISCOVERY AND INVENTORY

WHERE PERSONAL DATA RESIDES

Discover

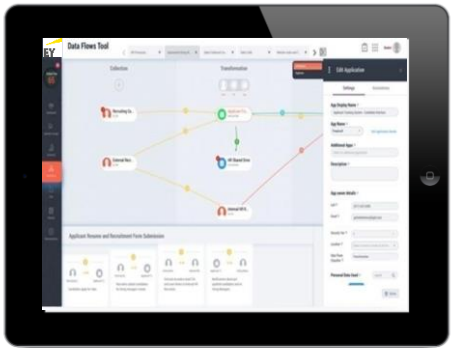
- Scale to hundreds of terabytes and across structured, non-structured, big data and cloud data sources
- Maintain dynamic and automated personal data discovery

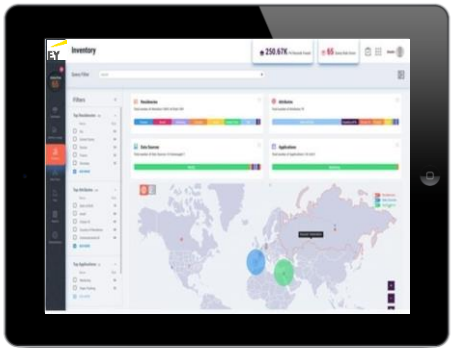
Correlate by data subject

- Associate personal information to data subject – not only personally identifiable information by location
- Identify dark data and new personal information by proximity, location and frequency

Visualize personal data

- Centralize visibility of personal data by person (data subject), residency, data type and attribute
- Create automated, data-driven mapping of processing flows by business process

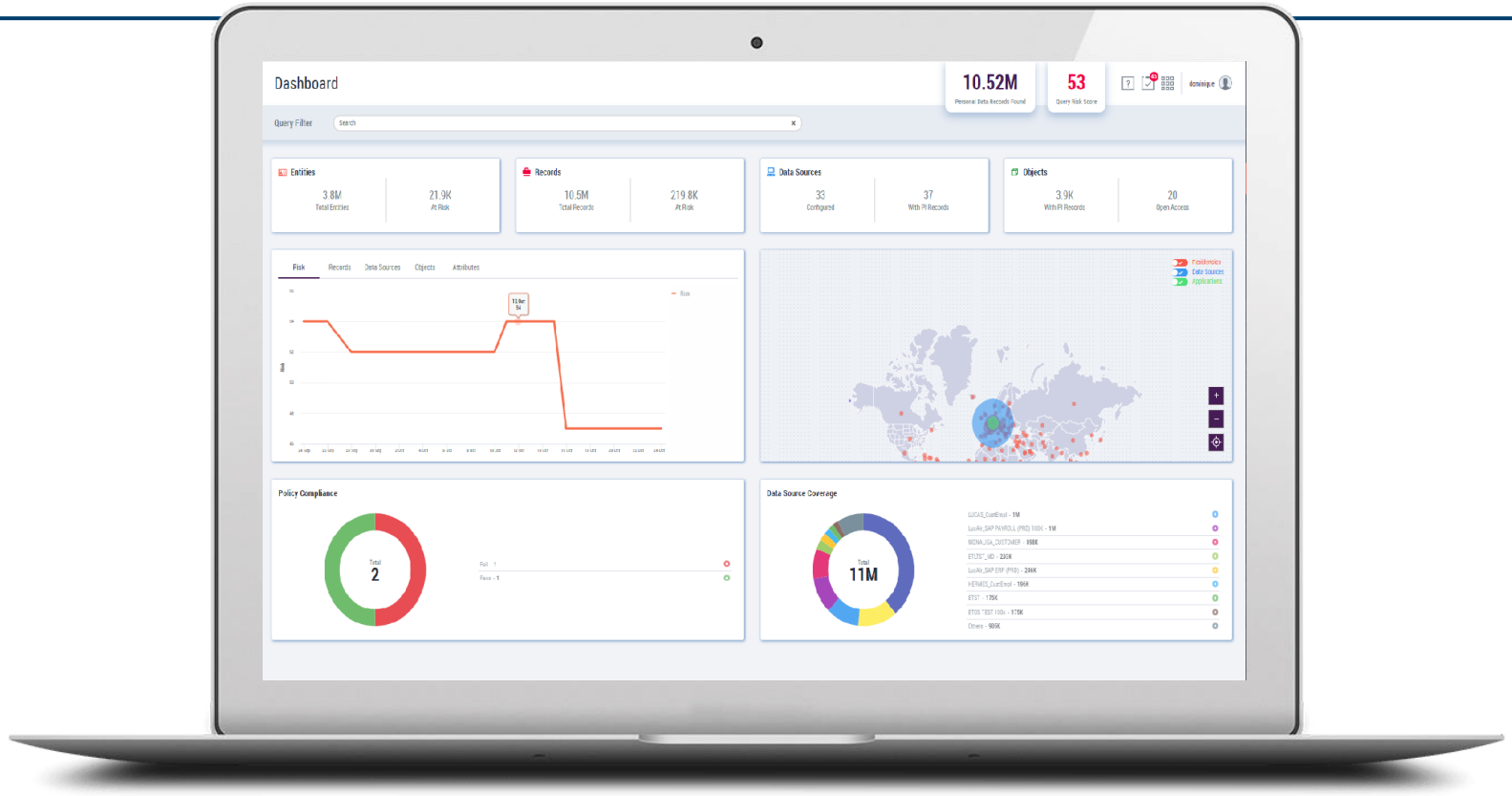




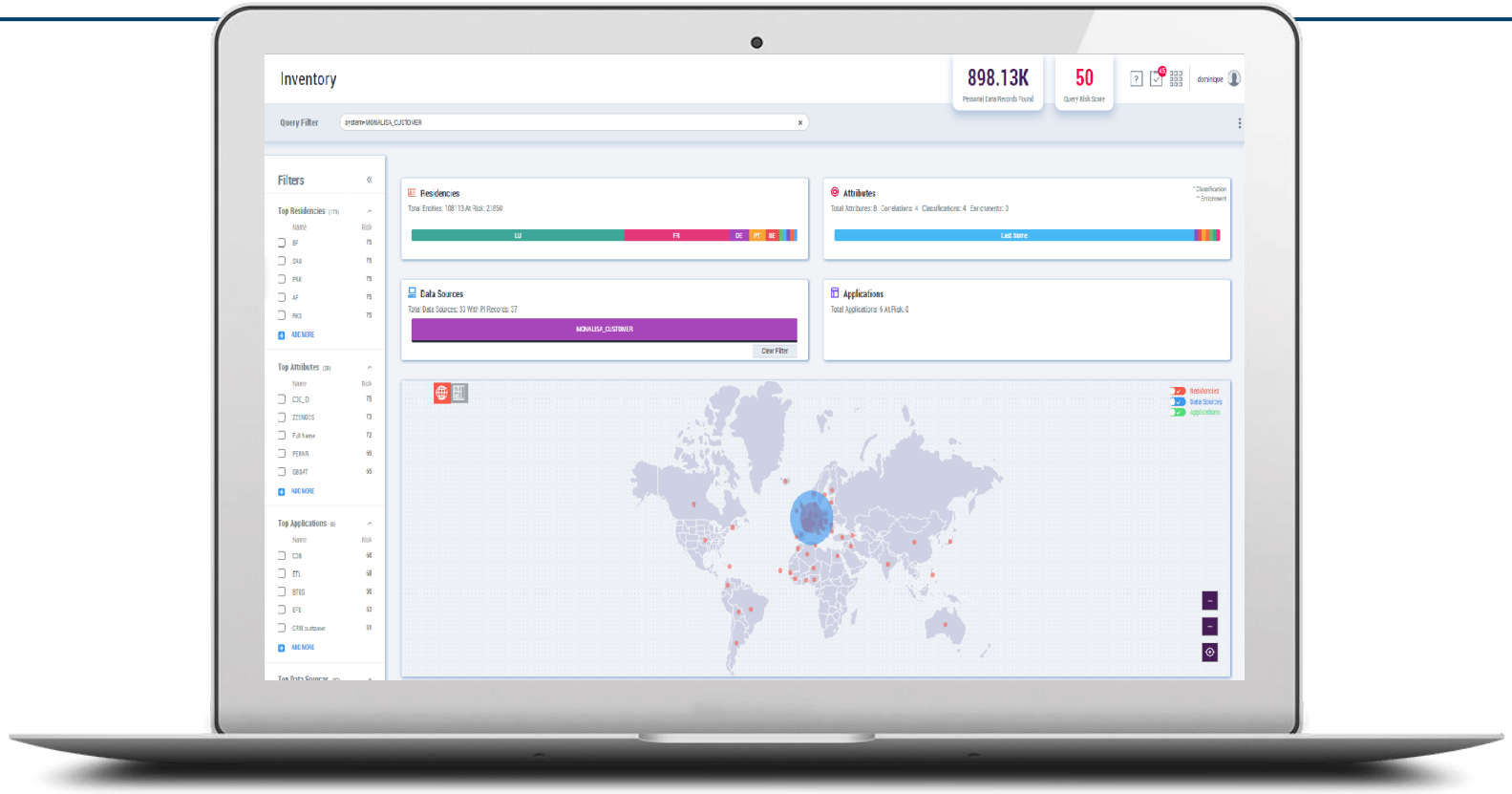
Automated Data Discovery and Inventory

- Automated Personal Data Discovery
  - Structured
  - Non-Structured
  - Semi-Structured
- Personal Data Correlation
- Data Context Awareness
- Record of Processing Activities
- Data Inventory
- Data Lineage and Mapping
- Data Subject Rights Orchestration
- Data Privacy Intelligence and Risk Determination
- Continuous Data Scanning and Compliance

WHERE PERSONAL DATA RESIDES



WHERE PERSONAL DATA RESIDES



DATA FLOW MAPPING

Data flow maps

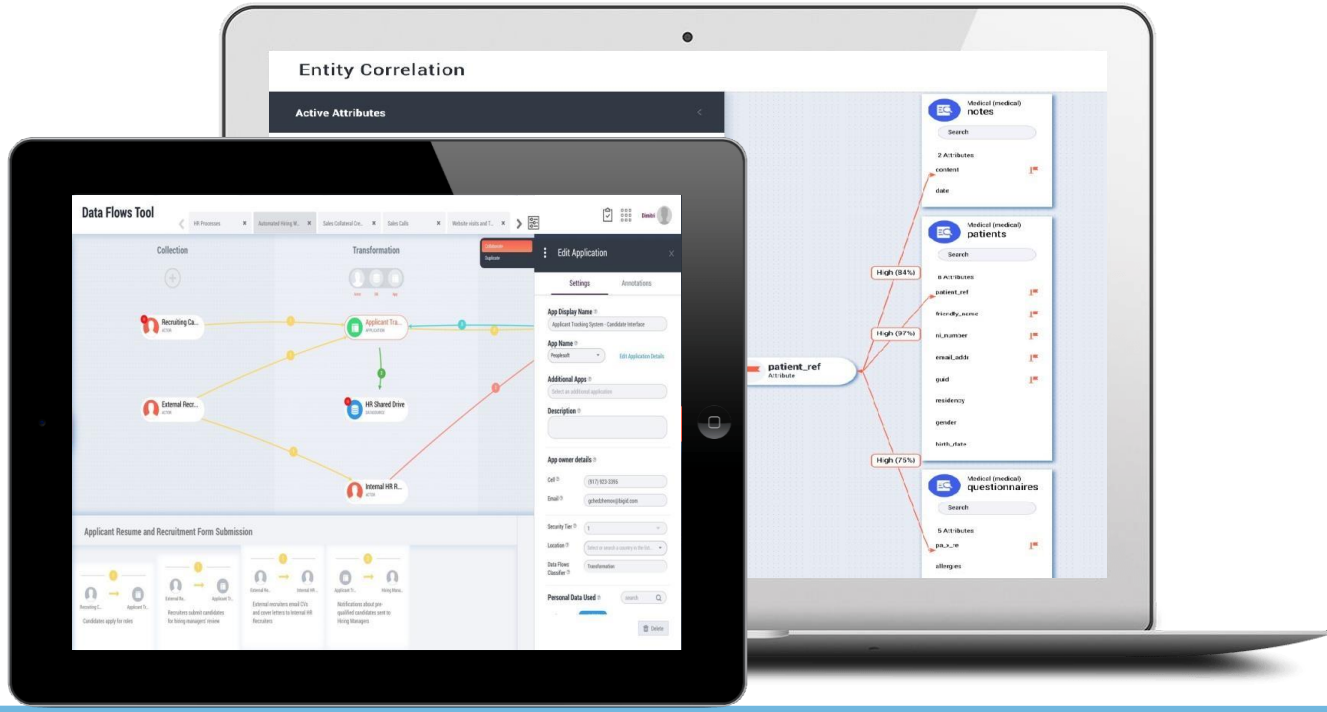
Data flow maps will be developed on key processing activities on the basis of interactions between processes and technologies in order to detect and reduce privacy risks. The data flow maps are automated and represented through a graphical interface as shown below:

EY's advanced correlation plus classification algorithms allow to map:

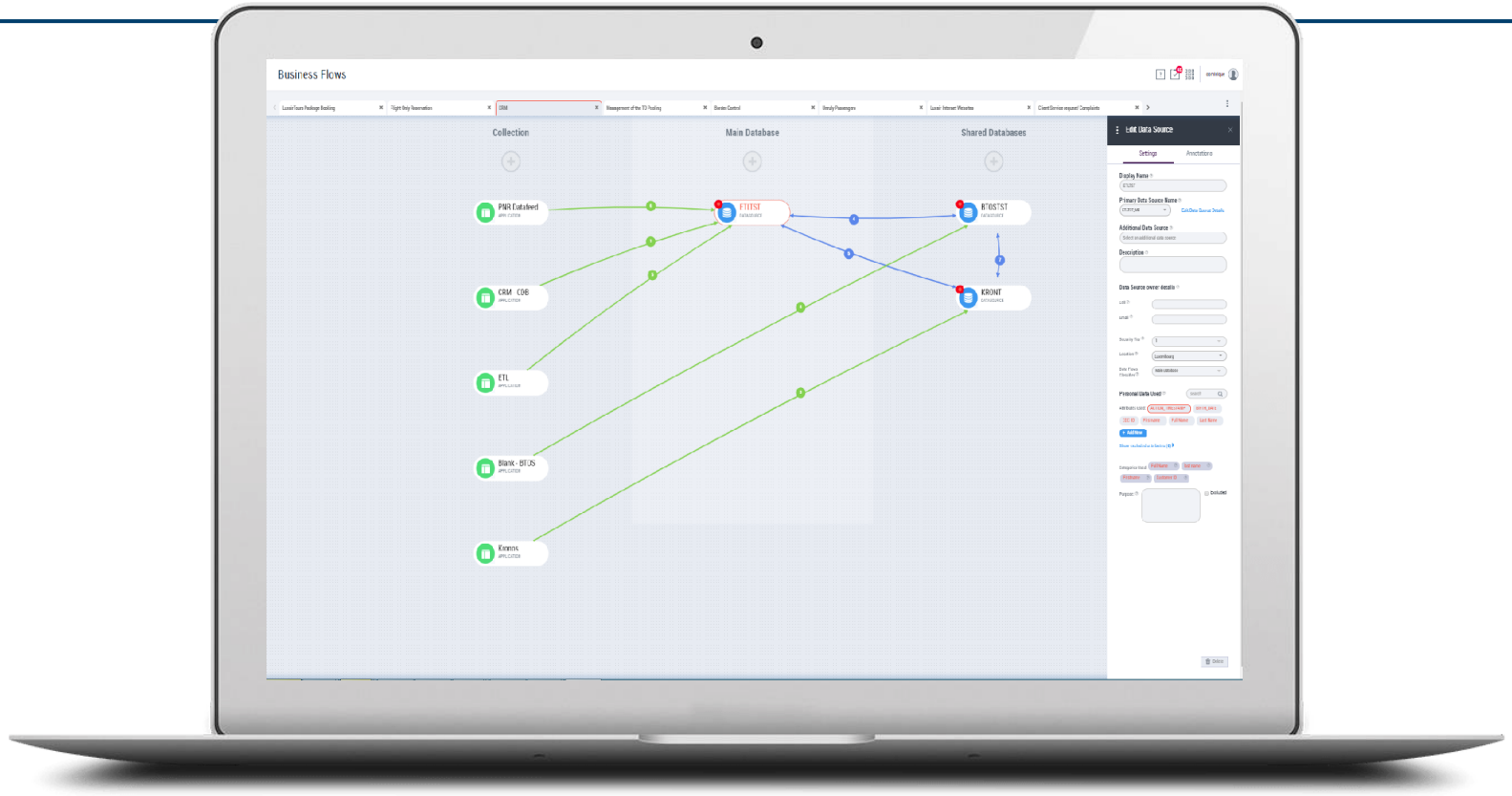
- Relationships across applications/systems
- Catalogue of personal data moving among the business applications preserving the integrity of data

This catalogue and Inventory can be further used to

- Auto-generate workflow maps
- Create new business data flows
- Map the flow of data between applications and data sources
- Automatically identify data attributes accessed by applications
- Generate reports



DATA FLOW MAPPING



3

DATA-CENTRIC AUDIT AND PROTECTION

A SIGNLE SOLUTION

Monitor & Audit

Automates data discovery and classification of personal and sensitive data by analyzing values across fields and metadata in targeted database sources

Real-time sensitive activity monitoring, classifying and auditing all sensitive user activity addressing DSAR requests.

Protect Sensitive Data at-rest and in-use

Sets level of sensitive data and transaction risks with multi-factor risk scoring including protection status, volume, user activity, location and classification

Apply Purpose-Based Access Control by Blocking, Alerting, Dynamic and Physical Masking, Filtering and Encrypting Sensitive user activities and APIs

Address Ever-Growing Regulations

Apply Consent, “Right of erasure”, DSAR and “Need-to-know” access controls

Delivers a rich array of dashboard drill-downs to provide enterprise visibility into data risk

Provides advanced subject data reporting, breach impact reporting, request history etc.

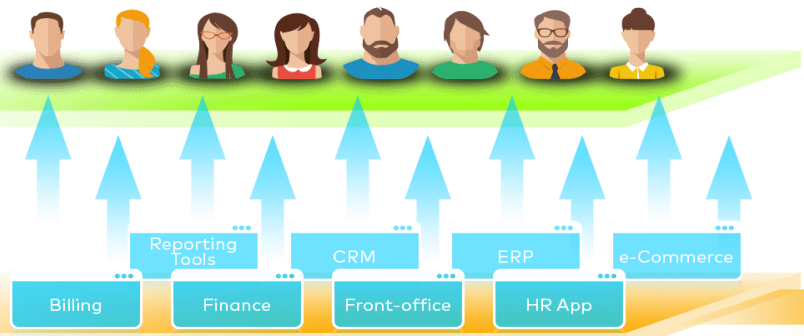
TRANSPARENT PLUG-INS

NO Code-changes | NO API Calls | NO network tapping | NO End-point Agents | NO Database Agents

End-users

Applications & Tools

Databases, DaaS,
no-SQL, Web-services



Central Policy Management Server

Capabilities:

- Discovery, data-flow mapping
- User Behavior Analytics (UBA)
- Monitoring & Auditing
- Dynamic Consent Controls
- Logical Deletion
- Physical Deletion

COMPREHENSIVE SOLUTION TOOLBOX

DATA OBFUSCATION / MASKING / DE-IDENTIFICATION

Use Cases:

- Protect Production & Non-Production Environment
- Reduce cost of compliance
- Enable offshoring & outsourcing initiatives
- Ensure data access on a need to know basis only across users communities
- Serve your entire IT ecosystem

DB ENCRYPTION & TOKENIZATION

Use Cases:

- Cloud data migration
- PII/PCI/PHI data compliance
- Data Privacy
- Protection against theft of data

DB ACTIVITY MONITORING

Use Cases:

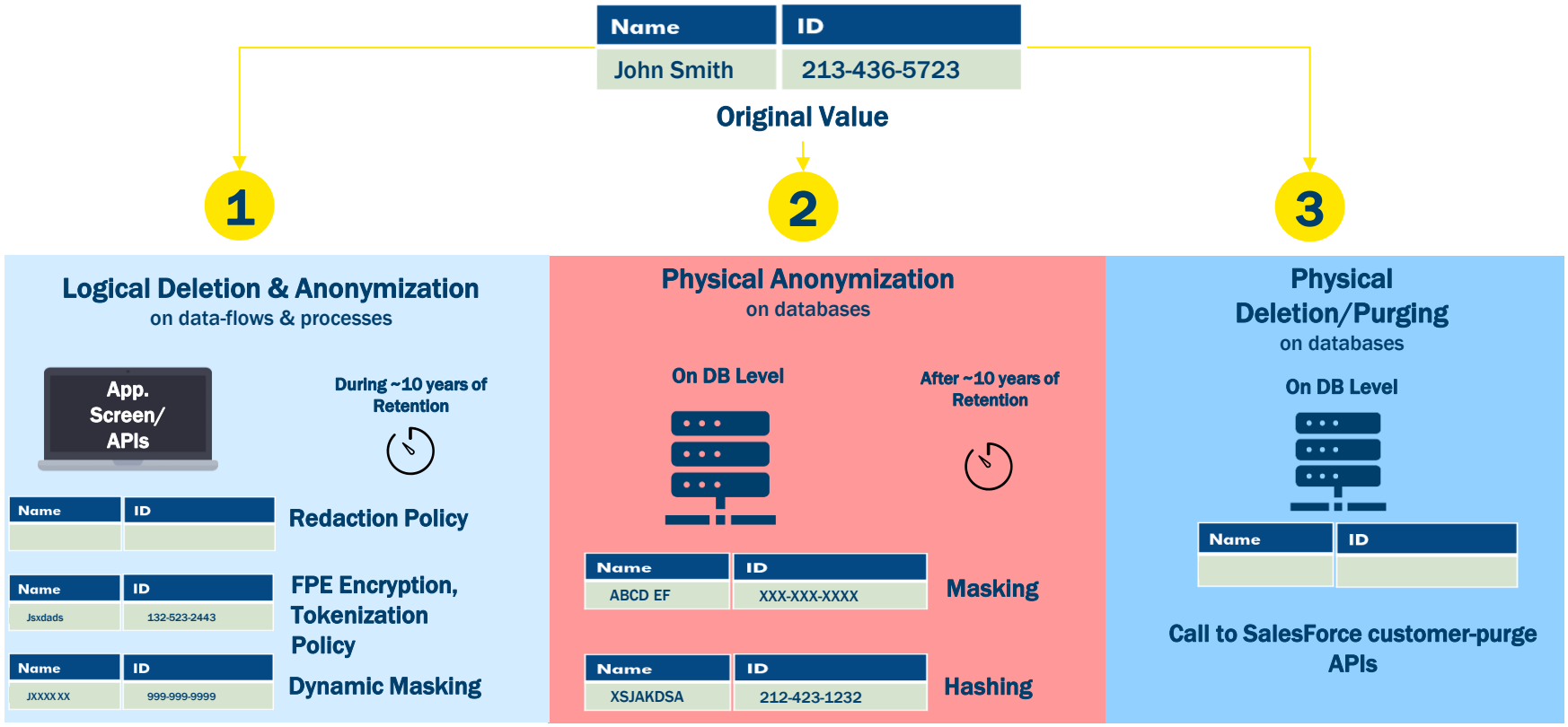
- Outsource of DBA & production support
- Control BD access from privileged users
- FINMA & other regulations
- Privacy & risks management
- Centralized Data access audit & Monitoring

DYNAMIC DATA MASKING

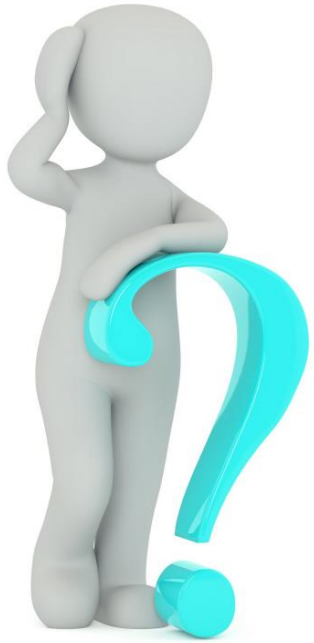
Use Cases:

- Fine grained access control
- Protecting the data from non-authorized users
- Enforce access control for multiple data consumption technologies

IMPLEMENTATION OF THE “RIGHT TO BE FORGOTTEN”



Q & A



MERCI POUR VOTRE ATTENTION