EPI-USE LABS
value through innovation

Invarture
Beyond your ERP

FACILITER LA MISE EN CONFORMITÉ AU RGPD
[DANS UNE OPTIQUE SAP]

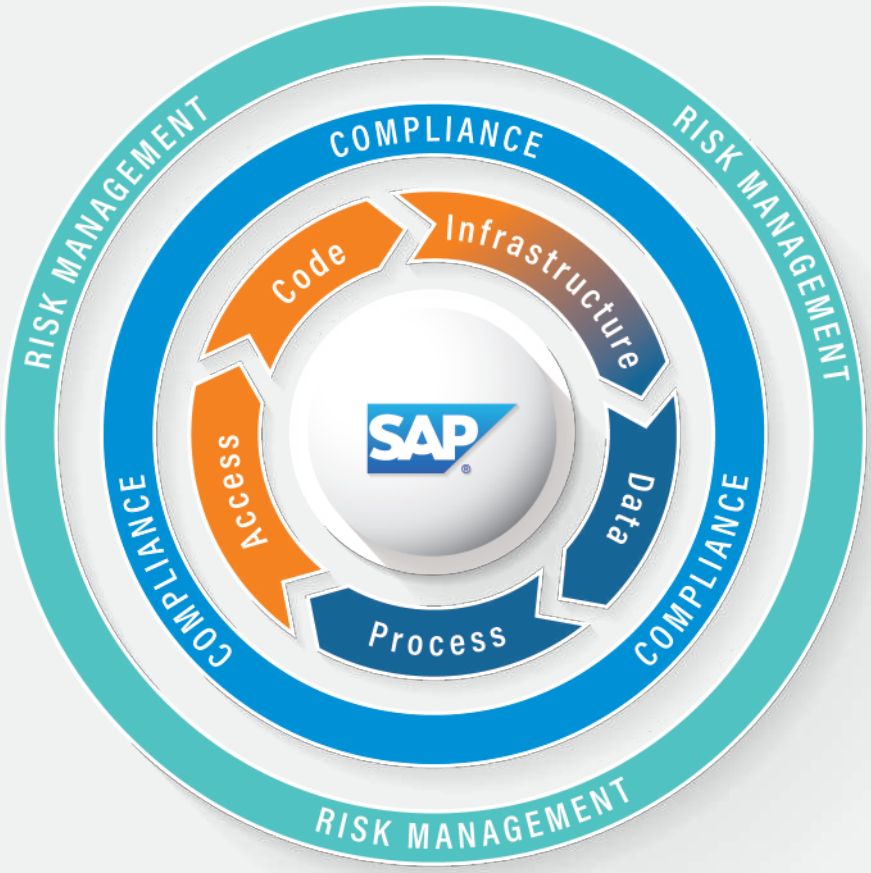
LIVRE BLANC : Warren Eiserman et Paul Hammersley

ÊTES-VOUS EN CONFORMITÉ AVEC LE RGPD ?

Avec la montée en puissance du règlement général sur la protection des données (RGPD), et cela bien au-delà de l'Union Européenne, la protection et la confidentialité des données sont devenues une priorité pour les entreprises du monde entier.

Avec les premières amendes aux montants élevés infligées maintenant, les organisations réalisent que la conformité au RGPD est plus importante aujourd'hui qu'elle ne l'était déjà en 2018.

Aucune solution unique ne peut traiter la totalité des aspects du RGPD et ses subtilités. La réalité pour la plupart des entreprises est que le RGPD ne constituera pas un exercice ponctuel, mais plutôt un parcours au cours duquel les compétences évolueront à mesure que les entreprises appréhenderont mieux ce qui fonctionne, et ce qui peut être acceptable ou non.



Toutes les entreprises devront revoir leurs processus et déterminer :

- quelles sont les données
- la finalité de collecte de ces données
- où les données sont stockées, comment elles sont transmises, et les enregistrements d'audit associés pour les données, (y compris les parties prenantes et les acteurs principaux)
- qui a accès aux données, et quels sont les tiers impliqués dans le traitement des données
- la durée obligatoire de conservation des données et les processus de suppression des données n'étant plus nécessaires (ex : plus de motifs légaux de conservation[i])
- la conformité aux dispositions du règlement de tous les documents juridiques (contrats de travail, politiques de confidentialité, formulaires de consentement, termes et conditions, enregistrements de communication électronique, accords de traitement des données, contrats de fournisseurs, etc.)

LA TECHNOLOGIE EST AU SERVICE DU RGPD

Le but de ce document n'est pas de fournir un contexte juridique au règlement, mais plutôt de montrer comment la technologie peut être un catalyseur de vos démarches de mise en conformité. La technologie peut vous aider dans les principaux domaines suivants :

DROIT D'ACCÈS DE LA PERSONNE CONCERNÉE (ARTICLE 15)

Les fonctionnalités de reporting fournies par SAP ont tendance à se focaliser sur les activités réalisées avec les données de base plutôt que sur les données de base elles-mêmes. Généralement, le nom, l'adresse, les informations bancaires, etc. des clients et des employés sont répartis dans plusieurs tables et souvent dupliqués dans des tables supplémentaires.

Le choix des informations à divulguer fait également l'objet de discussion au sein de chaque organisation, allant de la simple confirmation de l'existence de la personne concernée dans le système, jusqu'à la tentative de fournir chaque élément d'information stocké en relation avec cette personne. Le délai de réponse d'un mois défini dans l'article 12 implique que les organisations doivent être en mesure de traiter rapidement chaque demande. Du code personnalisé ou des rapports réalisés à l'aide de technologies existantes pourraient être utilisés pour collecter les informations, mais ces deux solutions exigent une connaissance approfondie du modèle de données SAP réparties dans plusieurs systèmes SAP.

Il existe des solutions tierces qui fournissent ces métadonnées et qui peuvent être étendues afin de pouvoir ajouter des tables personnalisées pour dupliquer ou stocker des données personnelles supplémentaires[ii] .

DROIT À L'EFFACEMENT («DROIT À L'OUBLI»)

La conception initiale du modèle de données SAP garantissait la cohérence et l'intégrité des données entre les différents secteurs de l'entreprise. Par exemple, lorsqu'une commande quittait l'entrepôt, le système financier était automatiquement mis à jour. Cette intégration rend très difficile la suppression des données d'un système SAP. L'archivage des données de base ne peut être effectué qu'une fois que les transactions associées sont supprimées du système. Cela peut être contraignant et chronophage. Certaines organisations ont utilisé l'expurgation (Redaction en anglais) comme un moyen plus simple d'assurer le droit à l'effacement, ou de supprimer des parties des données d'une personne concernée qu'ils n'ont plus de raisons légales de détenir. Cette approche a récemment été jugée comme suffisante par un tribunal autrichien[iii] .

Il n'existe pas de méthode standard de réaliser cette expurgation dans SAP, et il serait presque impossible de le faire via un code ABAP spécifique en raison des multiples emplacements où les données peuvent être dupliquées. Cependant, des solutions tierces sont disponibles[iv] .

DROIT À LA LIMITATION DU TRAITEMENT (ARTICLE 18)

Les données de base SAP clients et fournisseurs, et surtout Business Partner, permettent de bloquer divers types de traitement, mais en empêchant les transactions pour le client/fournisseur plutôt qu'en « traitant » le sujet tel que défini par le RGPD . À défaut d'archiver ou d'expurger l'enregistrement, il n'existe pas de mécanisme standard permettant d'empêcher temporairement l'accès à un enregistrement à des utilisateurs disposant par ailleurs d'une autorisation d'accéder aux données. SAP ILM comprend une fonctionnalité de "blocage" (voir la section "facilitateurs technologiques" ci-dessous).

OBLIGATION DE NOTIFICATION (ARTICLE 19)

Lorsque des données ont été traitées conformément aux articles 16, 17 ou 18, il existe une obligation de notifier la rectification, l'effacement ou la limitation du traitement effectué à toute autre partie avec laquelle les données ont été divulguées.

En fonction de la manière dont les données ont été partagées au départ, l'interface peut transmettre l'effacement ou la correction des données. Si ce n'est pas le cas, un mécanisme devra être mis en place à cet effet.

DROIT À LA PORTABILITÉ DES DONNÉES (ARTICLE 20)

Le reporting SAP standard comprend des informations simples sur les commandes à regrouper pour un client, les soldes courants ou les informations sur les limites de crédit, mais il ne comprend pas les données de base du client, telles que l'adresse, les informations bancaires, etc. qui seraient nécessaires pour la portabilité des données. Du code ABAP personnalisé pourrait être utilisé pour créer un tel résultat ou des outils Ad-Hoc ou des SAP Query. Des solutions tierces peuvent être utilisées pour permettre le téléchargement de données dans un format structuré, couramment utilisé et lisible par une machine[vi] .

REGISTRE DES ACTIVITÉS DE TRAITEMENT (ARTICLE 30)

Un large panel de technologies SAP assure les fonctions de création, de maintenance, d'archivage et de distribution de données sensibles dans l'entreprise. La maintenance des données de base et les flux de travail associés garantissent que les données personnelles sont saisies et conservées de manière appropriée. Les documents de modification (Change Documents) enregistrent qui a mis à jour les données, quand et comment. La journalisation des accès en lecture (Read Access Logging) peut être activée pour contrôler qui voit quoi.

Il est possible d'améliorer la surveillance des interfaces, des documents de modification et de l'accès aux données en extrayant des métadonnées non sensibles vers une plateforme telle que AppDynamics ou Splunk[vii viii].

SÉCURITÉ DU TRAITEMENT (ARTICLE 32)

SAP dispose d'un concept d'autorisation très mature fréquemment validé par des organisations du monde entier. Une mise en œuvre et une gestion correctes des rôles d'autorisation permettent à une organisation de contrôler qui peut voir, mettre à jour, télécharger et supprimer des données. D'autres contrôles de sécurité peuvent être mis en œuvre via le module GRC (Governance, Risk and Compliance) de SAP et il existe également des solutions tierces bien établies dans ce domaine[ix] .

La sécurité du réseau fait généralement partie de la sécurité globale du centre de données regroupant les serveurs de l'organisation. Les systèmes basés sur le Cloud sont sécurisés dans le cadre du service, mais il est essentiel de s'assurer que les « portes dérobées » courantes sont correctement verrouillées, comme les mots de passe par défaut et les logiciels obsolètes.
Lorsque les données à caractère personnel sont transmises, le cryptage doit être utilisé dans la mesure du possible. Les fichiers d'interface existants peuvent être cryptés en utilisant des solutions tierces internes ou externes aux systèmes SAP[x].

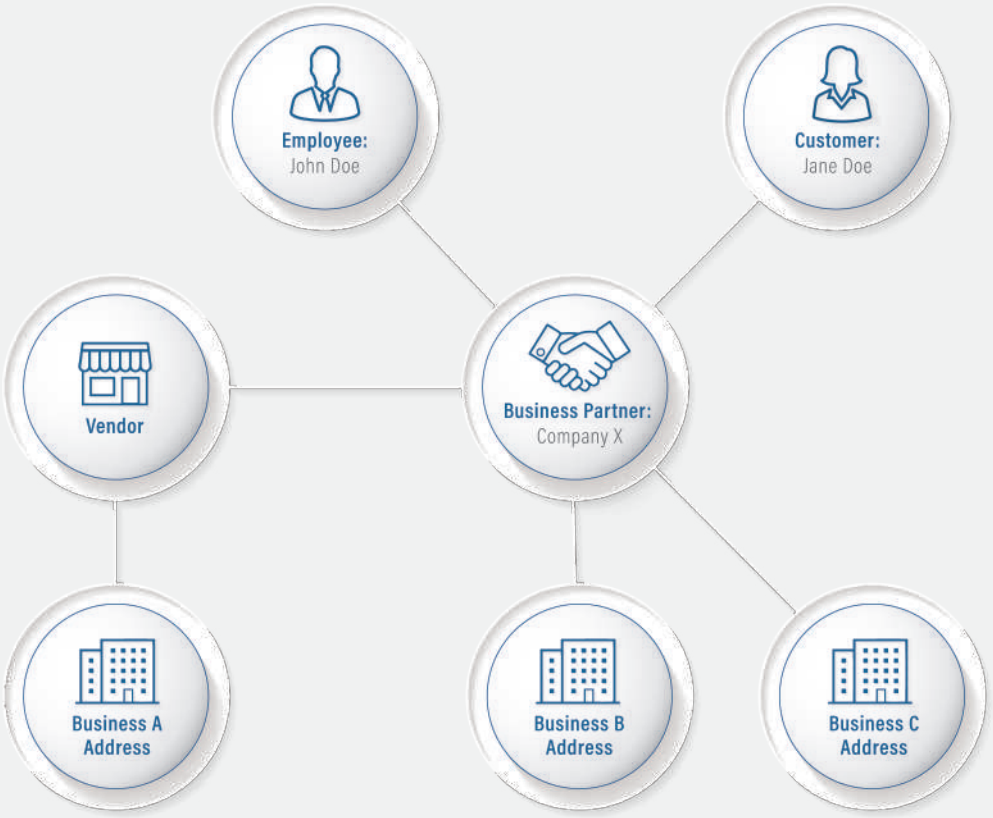
COMMUNICATION À LA PERSONNE CONCERNÉE D'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL (ARTICLE 34)

Bien qu'il n'existe pas d'outils SAP standard pour communiquer les informations aux personnes concernées, des technologies tierces vous permettent de télécharger un PDF crypté présentant l'empreinte de la personne concernée en incluant des détails spécifiques sur la violation potentielle, son l'impact et les prochaines étapes envisageables[xi].

Ces technologies peuvent également être utilisées pour communiquer des données rectifiées ou expurgées.

SAP ET LES DONNÉES PERSONNELLES

La nature intégrée de SAP implique que toutes les données de votre entreprise sont connectées et stockées dans des schémas de données complexes au sein du modèle de données SAP. SAP agit généralement comme un « système nerveux central » qui interagit avec de nombreux autres systèmes externes par le biais d'interfaces diverses.

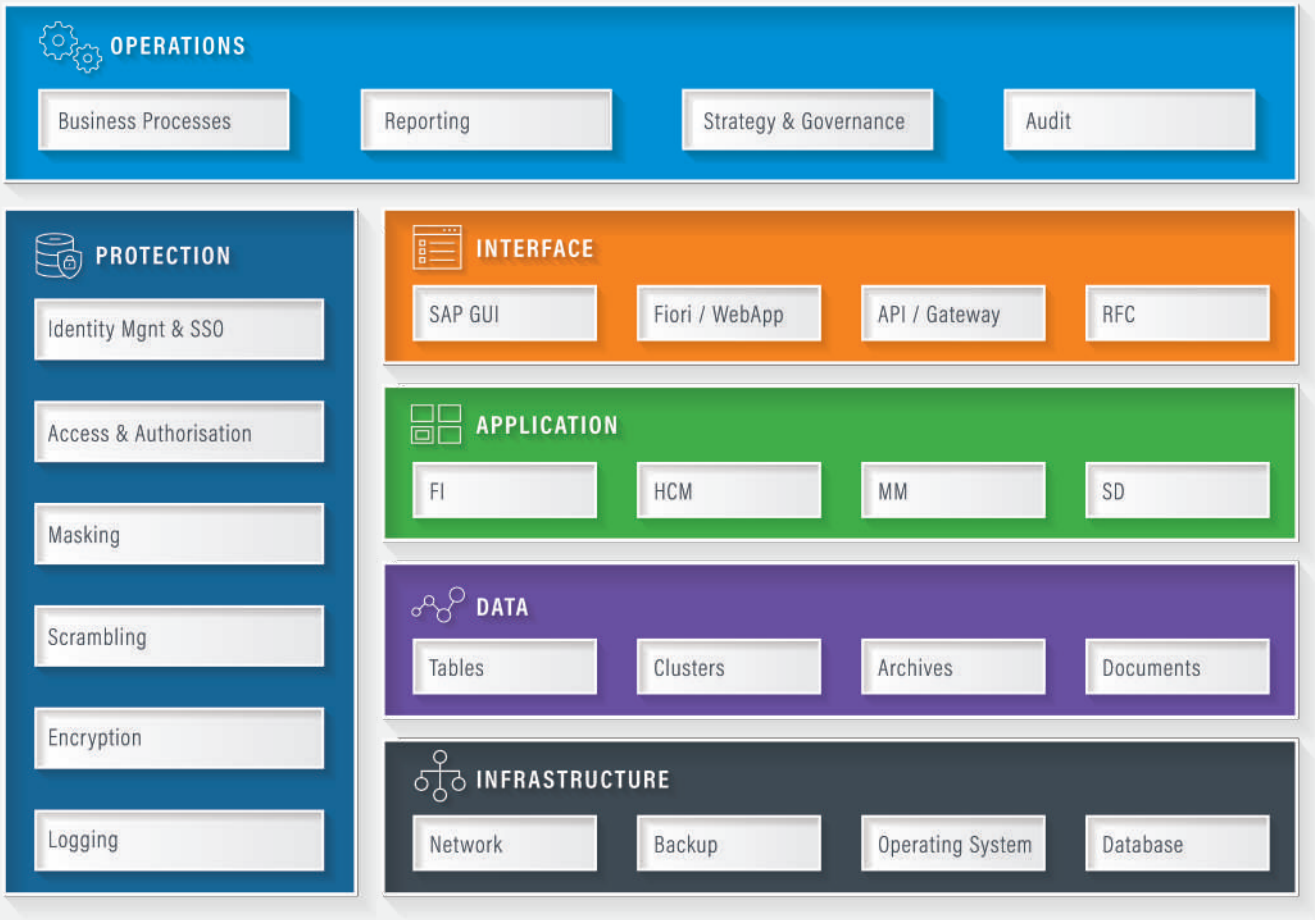


SAP introduit une certaine complexité dans la gestion des informations personnelles, mais présente également certains avantages :

AVANTAGES	ENJEUX
Modèle de données bien documenté pour les données personnelles des clients, des fournisseurs, des employés et des partenaires commerciaux.	
Constitue généralement la source de données primaire des données personnelles (le « Master ») qui alimente les systèmes en aval.	Le concept de « suppression » n'est pas vraiment compatible avec SAP ; les transactions initiales et les documents de suivi sont nécessaires pour assurer l'intégrité référentielle.
Une vaste base de clients ce qui permet de faire pression sur SAP pour fournir des solutions de conformité et de réglementation « prêtes à l'emploi ».	Les solutions Cloud SAP (SuccessFactors, Ariba, Concur, Cloud Integration ...) rendent les processus de protection de la vie privée inter systèmes plus complexes à gérer.
SAP et des entreprises tierces fournissent des solutions technologiques pour répondre au besoin de gérer les processus de risque et de conformité.	Les systèmes hors production ont besoin de données « réelles » pour les tests, nécessitant des copies sécurisées de la production ou la mise en œuvre d'une technologie de brouillage.
Les cabinets d'audit ont une connaissance approfondie de l'environnement SAP, et proposent des méthodologies éprouvées permettant de minimiser les risques.	SAP fait peser sur le client la responsabilité de ses données dans les systèmes hors production.

LES COUCHES DE L'ARCHITECTURE SÉCURITÉ DE SAP

Du point de vue de la confidentialité et de la sécurité, un système SAP se compose de nombreuses couches et applications, notamment les suivantes :



SAP ERP Logical Architecture Layers

Un autre aspect important à prendre en compte concernant l'architecture : les systèmes SAP sont généralement déployés dans un paysage à trois niveaux (DEV, QA et Production), ce qui ajoute de la complexité à la gestion des données de base et des transactions. Les systèmes de test et de développement ne devraient pas contenir de données sensibles, car ils ont généralement un accès plus « ouverts » pour les équipes de test, de développement et de configuration et sont souvent accessibles à un plus grand nombre de fournisseurs externes, dont certains peuvent même se trouver en dehors de l'Union Européenne. Cet accès à distance pourrait constituer un transfert de données nécessitant une approbation juridique.

LES PROJETS DE CONFORMITÉ IMPLIQUANT SAP SE COMPLIQUENT RAPIDEMENT

Une grande partie de votre démarche de mise en conformité consistera à mettre en place la stratégie, la feuille de route et la gouvernance de votre programme de protection de la vie privée. Cela dictera la manière dont vous traiterez les données sensibles dans votre environnement informatique. Votre projet de mise en conformité exige du temps et de l'engagement de la part d'un large éventail de départements de l'entreprise, notamment le service juridique et l'audit interne, les ventes et le marketing, les finances et l'informatique.

Gérer un projet complexe et sous haute pression est un défi, et comme tout défi, il suppose l'élaboration d'un plan.

LANCER UN PROJET DE MISE EN CONFORMITÉ AVEC LE RGPD

Généralement, les programmes de conformité commencent par une évaluation de l'impact des données à caractère personnel (Data Privacy Impact Assessment - DPIA) - c'est-à-dire un mécanisme permettant de déterminer les personnes, les processus et les systèmes concernés. En réalisant une DPIA, vous serez en mesure d'identifier les principaux risques concernant les droits des personnes concernées. Vous pourrez ensuite déterminer le risque encouru par votre entreprise dans le cas de traitement de données à caractère personnel incorrectes ou inexactes ainsi que dans le cas où il n'existe pas de motifs légaux au traitement tel qu'il se pratique actuellement.

Au cours de la DPIA, vous identifierez les processus qui interagissent avec vos systèmes SAP.

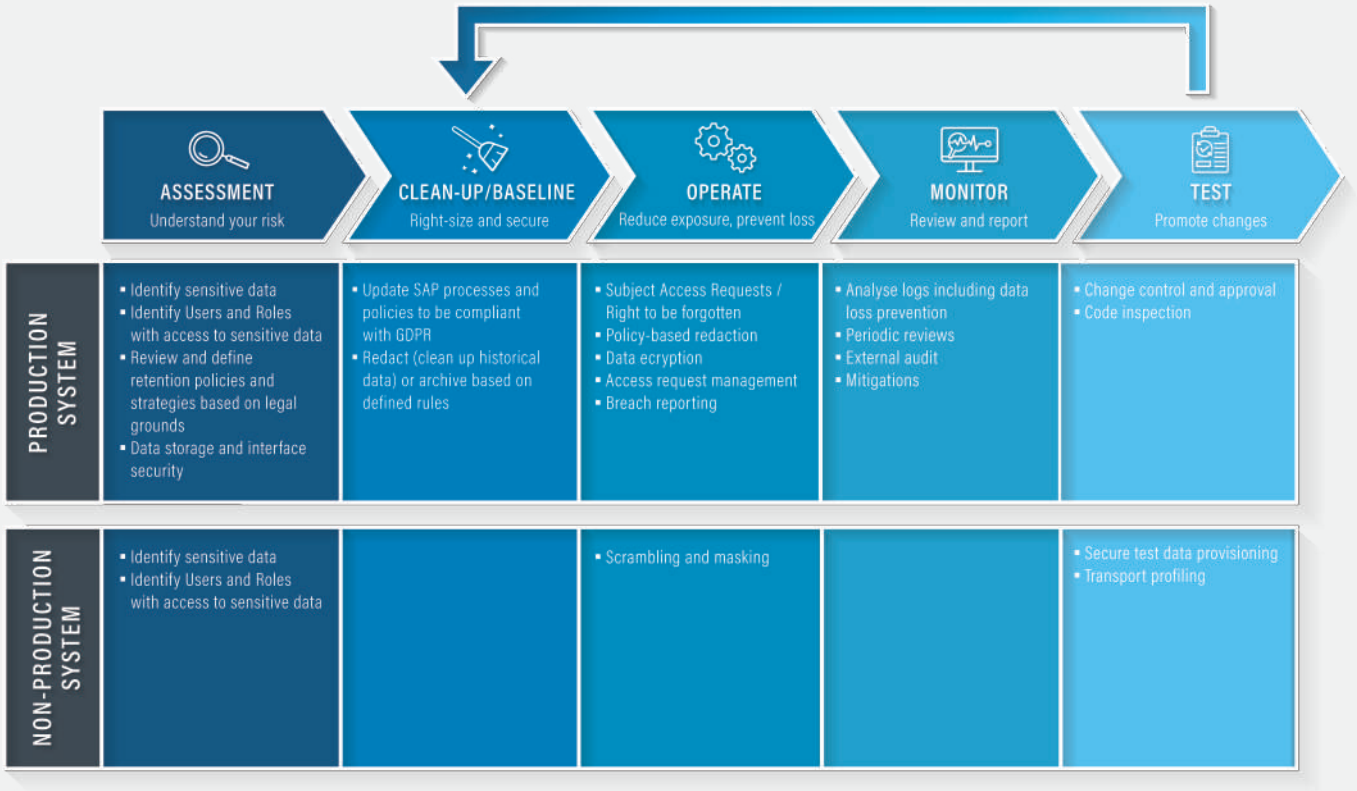
Les étapes du DPIA incluent :

- **Planification**
  - Identifier l'équipe et les parties prenantes
  - Définir le périmètre de l'évaluation
- **Évaluation**
  - Suivre les flux de données à travers les processus du périmètre
  - Examiner les politiques juridiques et de protection de la vie privée existantes
  - Déterminer les menaces pour le droit à la vie privée et les vulnérabilités des entreprises
  - Déterminer les contrôles et les contre-mesures
- **Mise en œuvre des contrôles**
  - Suivre les directives sur la protection des données
  - Déterminer les mesures de protection de la vie privée et la matrice des responsabilités
  - Concevoir ou sélectionner des éléments de sécurité
- **Finaliser le rapport**
  - Définir les procédures d'audit
  - Créer des activités de suivi

LES ÉTAPES D'UN PROGRAMME TYPIQUE DE MISE EN CONFORMITÉ DE SAP

Du point de vue SAP, d'après notre expérience de la mise en œuvre de solutions de protection de la vie privée, les programmes comportent généralement les éléments suivants :

1. Évaluation (composante de la DPIA)
2. Nettoyage / Base de référence
3. Exploitation
4. Surveillance / Contrôle
5. Test



Nous faisons la distinction entre les opérations SAP en production et hors production, car une quantité importante de données de test est généralement nécessaire pour tester efficacement les changements dans le paysage.

ÉVALUATION DE L'IMPACT SUR LA CONFIDENTIALITÉ DES DONNÉES : EXEMPLE DU RECRUTEMENT

Nous avons inclus quelques exemples d'évaluation de l'impact sur la confidentialité des données (DPIA) qui portent sur un scénario de recrutement typique.

EXEMPLE D'ÉVALUATION

Ci-dessous un exemple du type de questions qui pourraient être traitées dans le cadre d'une évaluation de la conformité d'un processus de recrutement :

1. **Processus RH principal**
    1. **Sous-processus Recrutement**
        i. **Consentement**
            a. Le consentement a-t-il été intégré dans les processus de candidature et d'entretien des candidats ?
            b. Le consentement explicite est-il enregistré ? Comment a-t-il été obtenu (web, physique, verbal) ?
            c. Les personnes peuvent-elles annuler leur consentement ? Quels sont le processus et la durée du consentement sur lesquels nous pouvons conserver les informations ?
            d. Est-il possible pour les personnes de limiter les motifs pour lesquels vous exploitez les informations ?
        ii. **Participation des personnes concernées**
            a. Existe-t-il des procédures pour traiter les demandes d'accès et de rectification des données ?
            b. Comment sont traitées les demandes de tiers pour les vérifications en matière d'éducation et de criminalité dans le processus d'évaluation ?
            c. Comment sont traitées les demandes de suppression de données dans le cadre des candidatures rejetées ?

iii. **Réduction des données**

a. Quels sont les procédures mises en place pour que les données soient réduites au minimum
   - Pendant la procédure de candidature ?
   - Après un recrutement réussi ?
   - Pour les candidatures rejetées ?

b. Comment les tests sont-ils gérés dans les systèmes de suivi des candidatures et dans l'onboarding RH ?

c. Quelle est la durée acceptable de conservation des données relatives aux candidats ?

d. Des procédures sont-elles en place pour anonymiser les données (si nécessaire) ?

iv. **Tierces parties**

a. Des accords de traitement des données sont-ils en place avec les partenaires commerciaux et les logiciels de RH fournisseurs (sites d'emploi, LinkedIn, etc.) ?

b. Un processus de notification des violations a-t-il été défini ?

v. **Traitement des données**

a. Les politiques de l'entreprise en matière de protection des données sont-elles incluses dans la procédure d'offre de poste et contrat ?

b. Un processus de notification des violations a-t-il été défini ?

c. Toutes les exigences réglementaires en matière de notification ont-elles été prises en compte dans le contexte de la confidentialité des données à caractère personnel ? (origine, religion, etc.)

vi. **Garanties de sécurité**

a. Quelles mesures de sécurité concernant l'intégrité et la confidentialité des informations sur les candidats ont-elles été mises en place ?

EXEMPLE DE MATRICE DE RISQUE ET DE CONTRÔLE

Ci-dessous un exemple de matrice de contrôle pouvant être utilisée.

PROCESSUS	SOUS-PROCESSUS	RISQUE	CONTRÔLE
Ressources humaines			
	Recrutement	Politiques et procédures non transparentes Données personnelles obsolètes	Examen régulier des politiques et audit externe Le consentement est géré de manière appropriée La conservation des données est gérée
		Effacement insuffisant des données à caractère personnel	Règles d'archivage et de conservation revues régulièrement
		Il y a violation de données	L'accès aux systèmes et aux données est géré Des tests de pénétration du système sont effectués régulièrement Le stockage des données est crypté selon les normes du secteur

EXEMPLE DE RÈGLES D'ARCHIVAGE

Ci-dessous, exemple de règles de rétention pouvant être définies pour accompagner le processus de recrutement.

SÉLECTION	RÈGLES	ACTION	RÉSULTAT
Candidat	Le statut du candidat est actif ; aucune action d'embauche en cours ; engagé dans aucun workflow.	Expurger les champs sensibles des candidats.	Analyse du rapport sur l'ancienneté des candidats. Examen du journal de traitement des expurgations.
	Retrait du consentement. Aucune autre exigence réglementaire n'existe concernant la conservation des données.	Supprimer tous les champs sensibles. Envoyer la demande d'expurgation à des tiers (si nécessaire).	Workflow des expurgations, email de confirmation.
Candidature	Candidatures non retenues datant de plus de 2 ans.	Supprimer les candidatures et les candidatures pertinentes associées non retenues.	Examen du rapport et du journal d'expurgation.

DIX RECOMMANDATIONS POUR VOTRE PARCOURS VERS LA MISE EN CONFORMITÉ DE VOS SYSTÈMES SAP AU RGPD

Sur la base de notre expérience dans la mise en œuvre de solutions de conformité pour les clients SAP, nous recommandons les éléments suivants :

1. Réaliser une analyse d'impact sur la confidentialité des données (DPIA)

- Impliquez vos auditeurs et votre conseil juridique dès le début ; ils vous conseilleront sur les principaux risques et vous fourniront un cadre de travail pour gérer la conformité de façon continue.
- Mettez en place une équipe de gestion du programme de protection de la vie privée. Désignez au minimum un responsable de la protection des données (DPO – Data Privacy Officer) et inscrivez-le auprès de l'autorité de régulation.
- Les analyses peuvent inclure les éléments suivants :
  - Inventaire des informations personnelles et cartographie des flux de données (par domaine d'activité) ;
  - Évaluation des insuffisances en matière de protection de la vie privée ;
  - Contrôles de due diligence par des tiers.

2. Sensibiliser au RGPD

- Entreprenez une évaluation de la culture de la protection de la vie privée afin de vérifier l'état de préparation et de compréhension des employés, et de s'assurer que ceux en contact avec la clientèle connaissent bien les droits correspondants.
- Informez vos employés et les parties prenantes sur le RGPD, sur ce qui est requis et sur les responsabilités associées (exploitez les solutions d'apprentissage en ligne disponibles sur le marché afin d'accélérer l'adoption).
- Adhérez à des organismes professionnels de protection de la vie privée, afin de tirer parti des meilleures pratiques (telles que l'Association internationale des professionnels de la protection de la vie privée, IAPP.org).

3. Effectuer un audit de l'endroit où les données sensibles sont stockées dans vos systèmes SAP

- Analysez votre environnement SAP pour déterminer les zones clés où sont stockées toutes les données personnelles et sensibles. Le traitement des demandes et la communication des informations personnelles seront difficiles sans une connaissance précise de l'endroit où sont stockées les données sensibles.
- Les équipes fonctionnelles SAP doivent savoir où sont stockées les données sensibles dans les systèmes SAP (y compris les composants intégrés comme le Workflow, SAP BW, les documents de modification, etc.) afin de pouvoir développer/concevoir des procédures permettant d'afficher et éventuellement de supprimer ces données.
- Passez en revue vos processus métiers et identifiez les étapes où des données sensibles (informations sur les clients, les employés, les fournisseurs, les partenaires commerciaux) sont accessibles.

4. Réduire le nombre de données sensibles sur vos systèmes SAP non productifs

- Réduisez votre profil de risque en protégeant intelligemment les données dans les systèmes non-productifs. En retirant vos systèmes de test de la problématique, vous pouvez réduire les risques et les frais généraux lors du traitement des demandes.
- Recherchez les clients/systèmes inutilisés contenant des données sensibles pouvant être supprimées ; ou des données sensibles qui ne sont pas requises sur certains mandants de test et qui pourraient être supprimées.

5. Sécuriser l'infrastructure

- Vérifiez régulièrement sur SAP One Launchpad la disponibilité de correctifs de sécurité spécifiques à vos versions de SAP, systèmes d'exploitation et types de base de données.
- Veillez à ce que la responsabilité de l'examen et de l'application des notes SAP soit clairement définie au sein de votre équipe.
- Assurez-vous que votre équipe dispose des compétences nécessaires pour protéger les systèmes et les parcs de clouds hybrides, y compris les règles relatives aux clouds et aux pare-feux.

6. Réviser ou mettre en œuvre des politiques de conservation des données visant à réduire les données historiques (au sein de SAP)

- Élaborez un cadre de politique d'archivage/d'expurgation et de conservation pour les données, qui précise clairement quand les données sensibles peuvent être soit archivées soit supprimées.
- Dans la mesure du possible, automatisez ces solutions d'expurgation et d'archivage afin que la conservation des données devienne partie intégrante de votre cycle d'activité habituel - et non plus un projet.
- Sur la base de vos politiques de conservation, lancez un projet de nettoyage et d'archivage afin de supprimer, d'archiver ou d'expurger les données que vous n'avez plus de raisons légales de conserver.

7. Gérer le risque d'accès au système SAP, pour limiter l'accès des employés aux données sensibles

- Déterminez où sont stockées vos données sensibles et personnelles (transactions, tables et objets métier associés).
- Identifiez les Rôles et les Users ayant accès à ces données et développez des ensembles de règles et des alertes afin que les demandes d'accès tiennent compte des risques.
- Mettez en place un processus permettant de vérifier régulièrement qui a accès aux données à caractère personnel.
- Documentez clairement les politiques d'accès et les étapes de validation.

8. Crypter les données sortant de votre système SAP

- Mettez en œuvre du cryptage afin de vous assurer que toutes les données stockées sur des serveurs de fichiers ou fournies par des interfaces soient cryptées avant leur transmission.
- Passez en revue votre politique de sécurité des points de sortie pour vous assurer que vous avez employé des solutions qui atténuent le risque des utilisateurs qui extraient des données sensibles par le biais de rapports, d'analyses et de partage de connaissances avec leurs collègues.

9. Vérifier la maturité du suivi et de la journalisation des audits dans SAP

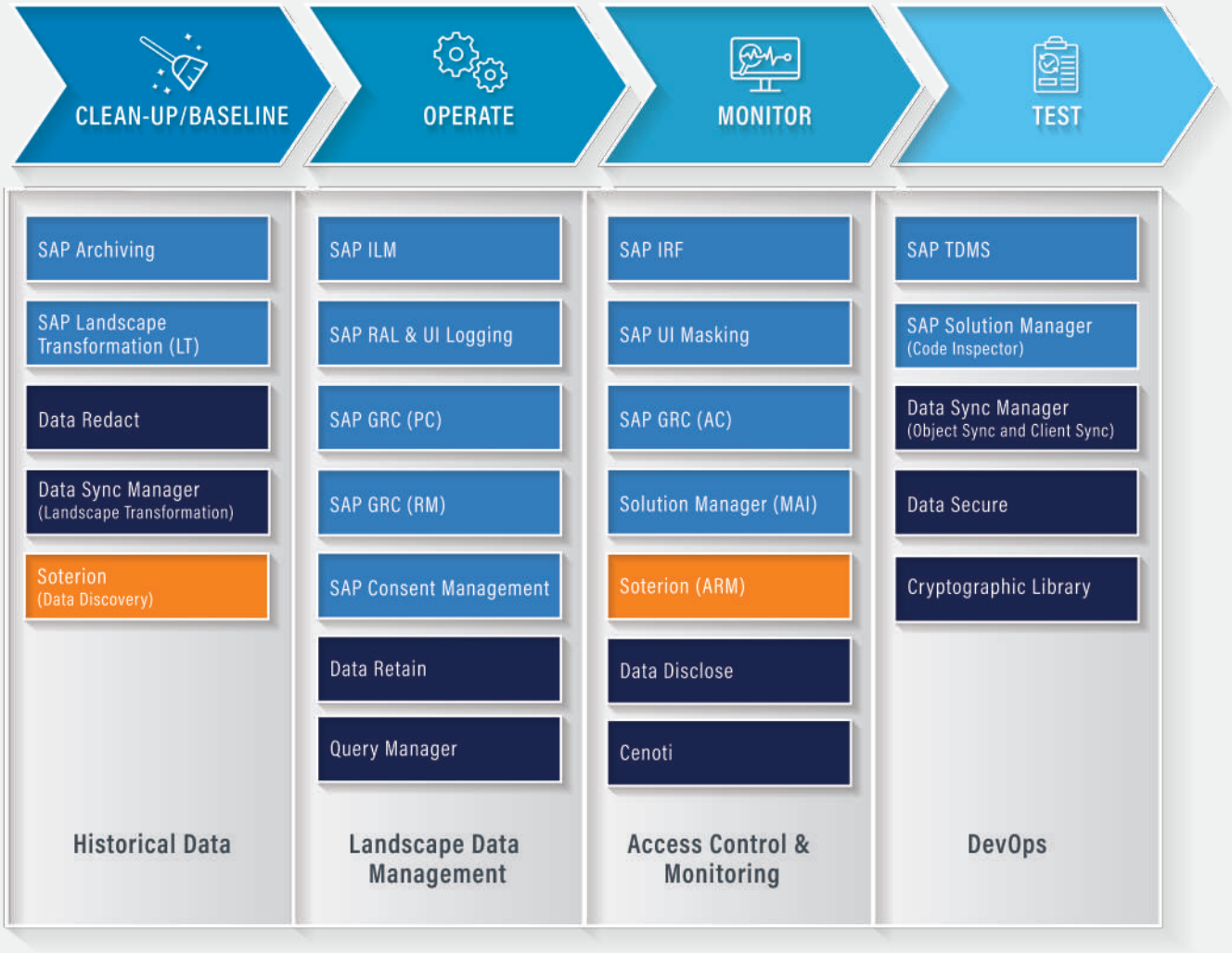
- Les utilisateurs SAP extraient des centaines d'enregistrements et de documents sensibles des systèmes et applications SAP à des fins de reporting, d'analyse et de partage des connaissances avec leurs collègues, partenaires et fournisseurs. La plupart des entreprises n'ont qu'une connaissance ou un contrôle très limité de la circulation de ces documents, des personnes qui y accèdent et de la manière dont ils sont utilisés. Les entreprises sont donc exposées à un risque élevé de perte de données due à des actes malveillants ou accidentels.
- Simulez une réponse à une violation de données et élaborez un plan d'action qui décrit les principales responsabilités de tous les acteurs concernés (basis, sécurité réseau, propriétaires d'applications, responsables des risques).

10. **Définir une feuille de route pour la mise en conformité des solutions**
    - Identifiez les solutions et processus SAP destinés à prendre en charge : le risque d'accès, la sécurité de l'infrastructure, l'évaluation des risques et les contrôles internes, l'archivage, la gestion des données non productives, la notification des violations et la gestion des demandes de communication.

LES DOMAINES CLÉS À PRIVILÉGIER AU SEIN D'UN PAYSAGE SAP

Voici les principaux domaines sur lesquels il est nécessaire de se focaliser :

1. Les données historiques de votre système de production
2. La gestion de l'exécution des processus
3. L'automatisation des activités de conformité en cours pour garantir que des contrôles internes adéquats sont mis en œuvre efficacement
4. La gestion des données sensibles dans vos processus DevOps, par exemple les données PII dans les systèmes non productifs
5. La gestion du consentement et des bases légales, y compris les demandes des clients



LES FACILITATEURS TECHNOLOGIQUES

Un certain nombre de solutions technologiques existent, qu'elles proviennent de SAP ou de fournisseurs tiers. Nous avons mis en évidence les principales offres de solutions ci-dessous, mais il ne s'agit pas là d'une liste exhaustive.

SOLUTIONS SAP

LES FONCTIONS INTÉGRÉES

Au sein des principaux systèmes de gestion SAP, tels que l'ERP, plusieurs approches sont possibles :

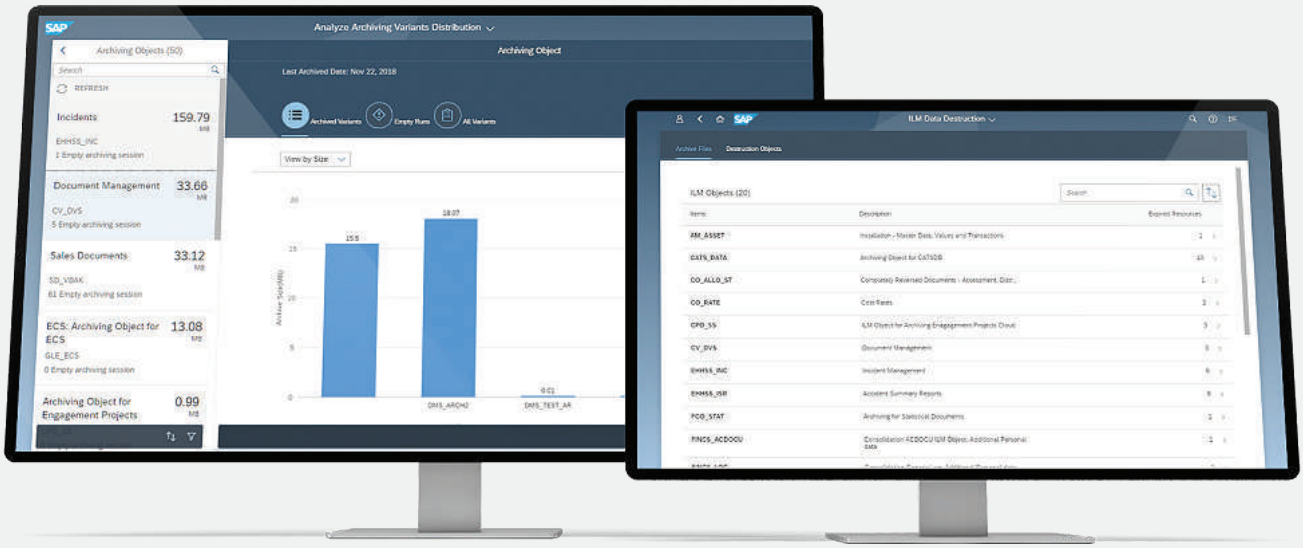
- Configuration pour ajuster les processus d'entreprise
- Rôles et autorisations
- Solutions SAP Business Workflow
- Solutions ABAP personnalisées, rapports et journalisation
- Archivage

SAP INFORMATION LIFECYCLE MANAGER (ILM)

Une solution pour gérer le cycle de vie de vos données basée sur un ensemble de règles, réparties en deux grandes catégories :

- **Les règles de résidence** définissent la période pendant laquelle vous souhaitez conserver les données liées à l'entreprise avant de les archiver, également appelée fin d'activité (End of Business - EoB).
- **Les règles de rétention** définissent la durée pendant laquelle vous devez « conserver » les données professionnelles dans leur ensemble, également appelée fin de la finalité (End of Purpose - EoP).

SAP ILM vient en supplément de la licence de votre système ERP et s'appuie sur les fonctionnalités classiques d'archivage des données dans SAP. La solution comprend un « mécanisme de blocage » pour la visualisation des données, et fournit un ensemble de fonctionnalités de configuration et de contrôle d'accès.
À partir de Netweaver 7.5, il est également possible de mettre en œuvre un système de règles de contrôle des données permettant de faciliter la définition de règles prenant en charge plusieurs exigences de conservation (telles que GDPR et POPIA). ILM fait également appel à l'Information Retrieval Framework (IRF), une fonction métier distincte permettant d'effectuer l'indexation des informations.



JOURNALISATION DES ACCÈS EN LECTURE ET MASQUAGE DE L'INTERFACE UTILISATEUR DE SAP

Le Read Access Logging (RAL) surveille l'activité des utilisateurs dans votre système SAP et fournit une piste d'audit de l'accès. Il vous permet de tracer :

- qui a eu accès aux données
- quelles données ont été consultées
- quand les données ont été consultées
- le mécanisme d'accès utilisé (transaction ou interface utilisateur)

L'approche de la configuration du RAL consiste à marquer les champs et les tables (y compris les tables personnalisées) contenant des données sensibles. Une fois activé, l'interrogation du journal est possible pour surveiller les activités. La fonction d'alerte est mise en œuvre à l'aide de l'infrastructure de surveillance et d'alerte (MAI - Monitoring and Alerting Infrastructure) de SAP Solution Manager et peut être configurée pour envoyer des alertes par courriel à votre équipe d'audit interne en fonction de critères spécifiques.

La solution permet de configurer le motif (Logging Purpose) et les domaines (Logging Domains) pour lesquels vous souhaitez activer les logs. Cela permet de consigner un contenu spécifique à des fins d'audit et de disposer de journaux détaillés si vous devez vérifier qui a accédé à des informations personnelles. Des configurations de journalisation par défaut sont disponibles par application SAP (voir la note SAP 2347271).

La fonctionnalité de masquage de l'interface utilisateur SAP[xii] garantit que les données personnelles sont masquées lors de l'affichage des données via SAP GUI, Web Dynpro ou Fiori. Les utilisateurs autorisés (disposant de droits d'affichage) peuvent afficher les données masquées ; toutefois, ils ne peuvent pas créer, modifier, copier ou effectuer des activités de suivi sur les données masquées. Les configurations de masquage sont basées sur les configurations existantes du Read Access Logging (RAL). Un produit additionnel appelé UI Logging est également disponible, qui peut être utilisé pour détecter et agir sur l'utilisation abusive de données légalement protégées ou critiques pour l'entreprise. Ce produit est généralement utilisé avec un produit de cyber sécurité SAP appelé SAP Enterprise Threat Detection (ETD).

FRAMEWORK DE RECHERCHE D'INFORMATION SAP (IRF[XIII] - INFORMATION RETRIEVAL FRAMEWORK)

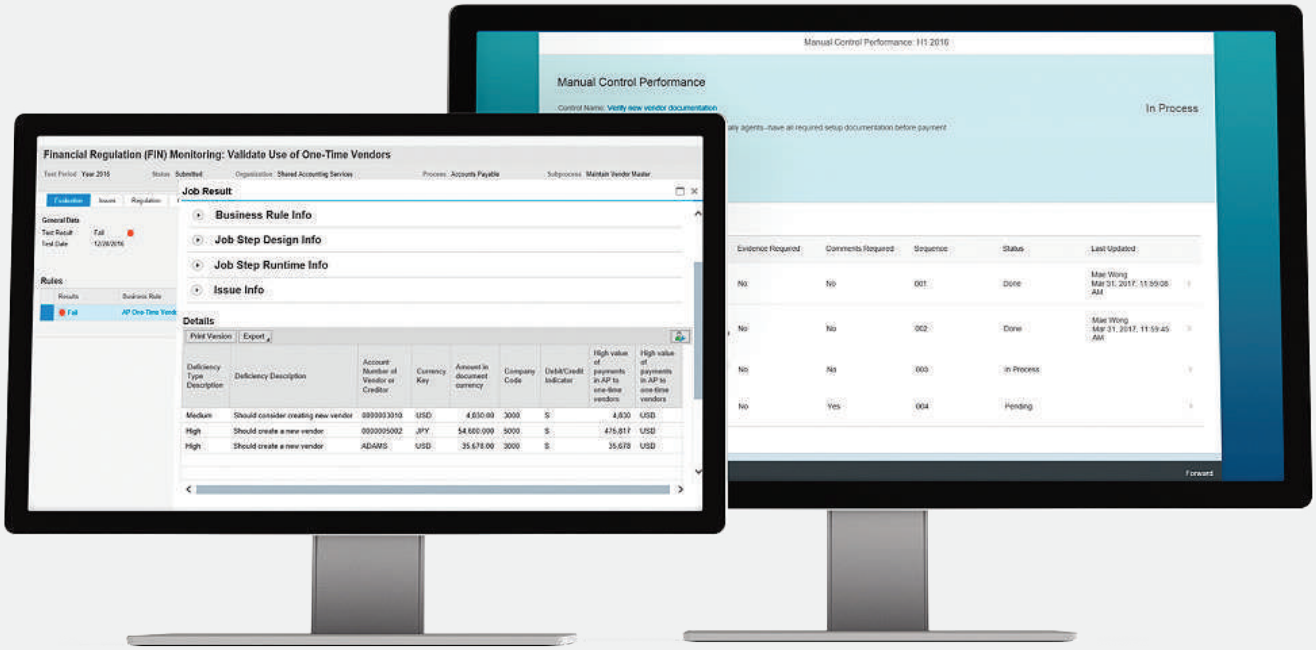
Cette fonction offre une solution de recherche et d'extraction des données à caractère personnel d'une personne spécifique. Cette fonction est exécutée dans tous les systèmes dans lesquels la fonction de gestion est active. Les résultats de la recherche renvoient une liste contenant les données à caractère personnel de la personne concernée, réparties en fonction de la finalité pour laquelle les données ont été collectées et traitées.

Pour pouvoir utiliser cette fonctionnalité d'extraction, vous devez créer votre propre modèle de données qui servira de base au processus d'extraction.

GOUVERNANCE, RISQUE ET CONFORMITÉ SAP (GRC – GOVERNANCE, RISK & COMPLIANCE)

La GRC peut exploiter les informations contenues dans vos applications métier existantes afin que vous puissiez évaluer les risques et appliquer des contrôles directement dans les processus métier. Ces sous-modules fonctionnent ensemble pour automatiser les activités GRC de bout en bout, notamment la gouvernance et la supervision de l'entreprise, la gestion des risques, les tests de contrôle et la gestion des cas de remédiation, l'accès des utilisateurs et les autorisations. Les solutions prennent en charge les fonctions critiques suivantes :

- Gestion centralisée des informations GRC dans un système d'enregistrement unique, y compris les politiques d'entreprise, les réglementations, les cadres de conformité et de contrôle, les flux de processus commerciaux et les bibliothèques de risques et de contrôles
- Identification, analyse et surveillance proactives afin de prévoir les menaces potentielles et d'y répondre
- Contrôles automatisés pour garantir un accès et une autorisation appropriés des utilisateurs
- Suivi des processus métier pour promouvoir les comportements souhaités et maximiser les résultats



La gestion du risque (RM - Risk Management)

GRC/RM fournit aux managers les moyens d'analyser correctement les arbitrages risque/récompense et d'apporter des réponses appropriées, étayées par des mesures quantitatives. La solution permet aux entreprises de mettre en œuvre des processus proactifs et collaboratifs afin de concilier opportunités et risques financiers, juridiques et opérationnels, à tous les niveaux de l'entreprise. Elle fournit un cadre de bonnes pratiques pour l'identification des risques de l'entreprise, l'analyse collaborative des risques, les réponses prédéfinies aux risques, ainsi que la surveillance et le reporting continus des risques, afin que vous puissiez anticiper et répondre efficacement à l'évolution de l'activité.

Les principaux indicateurs de risque vous permettent de surveiller l'ensemble du portefeuille de risques et d'alerter immédiatement la direction lorsque les risques à fort impact et à forte probabilité dépassent les seuils de risque spécifiques à l'entreprise.

Le contrôle des accès (AC - Access Control)

GRC/AC permet la mise en œuvre d'un système complet d'accès et d'autorisations basé sur les risques à travers votre organisation. L'outil d'analyse des risques d'accès permet d'identifier, d'analyser et de résoudre les risques d'accès. Un ensemble de règles extensible est utilisé pour détecter les conflits d'accès ou les personnes ayant accès à des informations personnelles. Des ensembles de règles sont développés pour contrôler quels utilisateurs ont accès aux informations personnelles.

Le contrôle des processus (PC - Process Control)

GRC/PC propose une approche basée sur les risques pour mettre en place votre environnement de contrôle et identifier les contrôles les plus efficaces et efficients nécessaires pour assurer la conformité à toute législation.
L'application s'intègre directement à la documentation de contrôle dans SAP GRC Repository, ce qui vous permet de centraliser la gestion des contrôles et d'éliminer la nécessité d'intégrer des outils distincts pour la documentation, les tests, la remédiation et le suivi des contrôles.

La solution permet de surveiller des centaines de processus critiques : procure-to-pay, order-to-cash, hire-to-retire et les contrôles IT. Un seul test de contrôle automatisé pour de multiples combinaisons de critères, tels que la dépersonnalisation des données, garantit la conformité.

Le test de contrôle manuel est envoyé à la personne appropriée pour une exécution rapide et guide le testeur à l'aide de procédures étape par étape et de modèles approuvés afin de minimiser les erreurs. Des fonctionnalités de sondages additionnelles (par exemple, les évaluations d'impact sur la confidentialité des données ou le consentement - POPIA SECTION 11 & 13) permettent l'auto-évaluation des contrôles au niveau de l'entité et l'approbation de la direction.

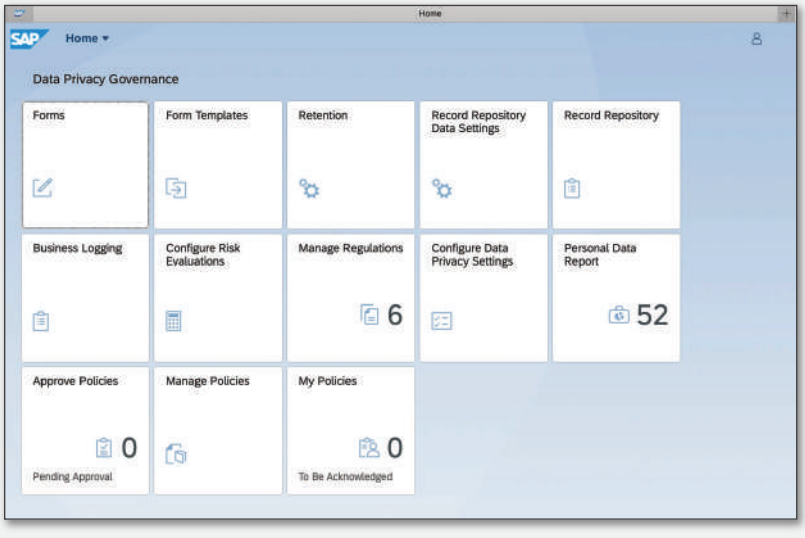
Fournit un soutien pour :

- La gouvernance et les politiques
- Les évaluations et enquêtes (y compris les évaluations de l'impact sur la confidentialité des données)
- La certification et le reporting.

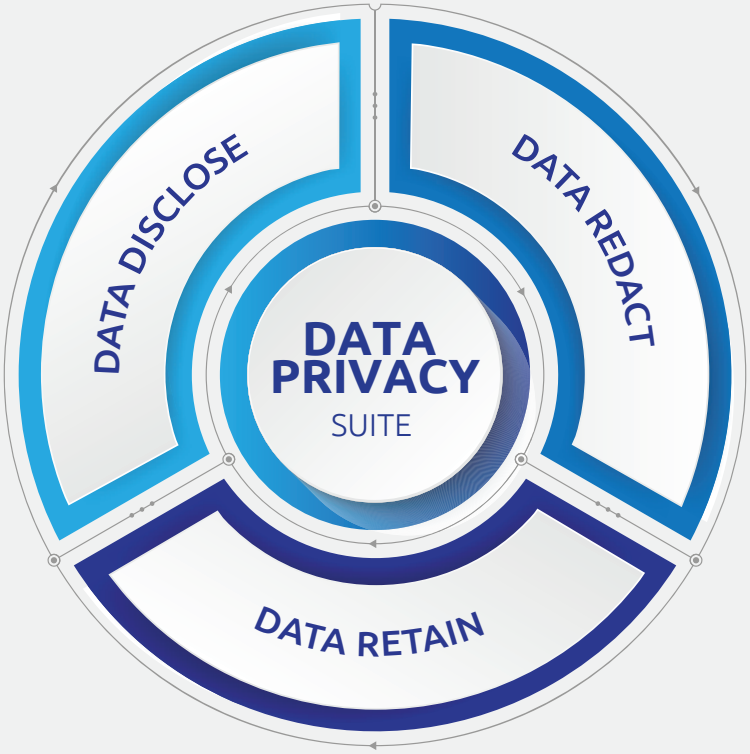
La GRC peut également être intégrée à la solution SAP ILM afin d'affecter des objets ILM aux zones d'audit (si nécessaire).

GOUVERNANCE DE LA CONFIDENTIALITÉ DES DONNÉES SAP

SAP étend son offre de confidentialité des données au-delà de la suite SAP GRC Privacy pour apporter de nouvelles fonctionnalités. SAP Privacy Governance est une application Software-as-a-Service fonctionnant sur la plateforme SAP Cloud, Cloud Foundry. Elle comprend des fonctionnalités prenant en charge la sécurité des données, ainsi que la gestion des préférences et du consentement des clients, permettant une gestion supplémentaire de la confidentialité des données, comme la gestion des enregistrements et des politiques.



SOLUTIONS TIERCES



LA DATA PRIVACY SUITE D'EPI-USE LABS

La solution de confidentialité et de conformité des données développée par EPI-USE Labs aide les entreprises à traiter efficacement la conformité au RGPD dans leurs systèmes SAP, grâce à des solutions préconstruites répondant aux principaux défis techniques et fonctionnels.

Cette solution est composée de trois éléments clés :

DATA DISCLOSE™ : LOCALISER LES DONNÉES

Data Disclose permet d'effectuer des recherches dans tous les systèmes SAP utilisés par une organisation afin de localiser les données personnelles. En général, l'enregistrement d'une personne concernée est stocké dans plusieurs systèmes de développement, de test et de production.

Les systèmes externes reliés à SAP et contenant une partie des données pourront être connectés à Data Disclose grâce aux API développées par EPI-USE Labs. La recherche, l'analyse et la présentation de l'ensemble de l'empreinte d'une personne concernée pourront alors se faire depuis un point unique.

DATA REDACT™ : EXPURGER LES DONNÉES

Un individu peut demander que les données personnelles qu'une entité détient à son sujet soient effacées (droit à l'oubli) pour en empêcher le traitement dans des circonstances spécifiques.

Data Redact vous permet de « supprimer » les données sensibles ou identifiantes sans supprimer l'ensemble du dossier. Les données sont soumises à l'expurgation, de sorte qu'elles ne puissent pas être identifiées par la suite.

DATA RETAIN™ : APPLIQUER LES RÈGLES D'EXPURGATION

Cette solution permet à une organisation d'élaborer des règles extrêmement configurables pouvant imposer des périodes de conservation à différents types de données. Lors de son exécution, les règles sont vérifiées afin d'identifier les jeux de données devant être expurgés. Cela vous permettra de continuer à appliquer des politiques de conservation et à expurger vous-même les données même après la fin de ce projet.

LA SUITE DATA SYNC MANAGER[xv] D'EPI-USE LABS

Data Sync Manager (DSM) permet de créer rapidement de nouveaux systèmes non-productifs, de réduire la taille des mandants existants lors de rafraîchissements ou de la création de nouveaux mandants, et de copier des données SAP sélectionnées à la demande, tout en garantissant la sécurité et la cohérence de ces données par un brouillage (scrambling) intégré.

DATA SECURE™ : ANONYMISATION DES DONNÉES

Data Secure est une solution de protection des données qui anonymise les données SAP pour les systèmes non-productif afin de protéger les informations sensibles, soit sur place soit « à la source ».

CLIENT SYNC™ : COPIE SÉLECTIVE DE MANDANTS

Client Sync permet de copier uniquement les sous-ensembles d'informations nécessaires à partir d'un système de production. Cette méthode présente des avantages considérables : elle réduit l'encombrement du nouveau mandant et économise un espace disque précieux - jusqu'à 90 % - ce qui signifie que les coûts et le temps de copie sont considérablement réduits, le tout sans perturber le paysage. Il est également possible d'exclure du nouveau mandant de test les codes d'entreprise sensibles ou les informations relatives aux employés.

QUERY MANAGER™

Query Manager permet aux utilisateurs fonctionnels de définir et de générer en toute sécurité des rapports sur des données sensibles de paie et HCM. Il offre la possibilité de crypter et de protéger par un mot de passe les rapports contenant des informations sensibles et personnelles[xvi].

DOCUMENT BUILDER™

Document Builder aide à la création de lettres, de documents, de rapports et de présentations au format élaboré, pour une distribution automatisée aux employés, aux responsables et aux partenaires commerciaux. La solution permet de crypter, de protéger par mot de passe ou d'inclure une fonction de signature numérique, afin de protéger les données des rapports[xvii] .

LA BIBLIOTHÈQUE CRYPTOGRAPHIQUE D'EPI-USE LABS

La bibliothèque cryptographique est une solution basée sur ABAP qui assiste les clients dans leurs démarches de protection des données. La bibliothèque peut protéger les données stockées au repos, ainsi que les communications sécurisées lors de la connexion à des systèmes externes en utilisant des algorithmes de cryptage standard[xviii] .

METTEZ EN PRATIQUE LE RGPD DÈS MAINTENANT

Les exigences du RGPD peuvent sembler décourageantes, mais si vous travaillez en étroite collaboration avec vos équipes d'audit et juridiques et que vous restez pragmatique, il existe un certain nombre de mesures efficaces que vous pouvez prendre en fonction de votre profil de risque. L'essentiel de vos activités portera sur l'examen de vos processus opérationnels et du cadre de conformité associé.

L'utilisation des outils technologiques vous permettra d'accélérer votre mise en conformité et de démontrer que vous avez pris des mesures pour soutenir le RGPD.

En tirant parti des outils technologiques, vous accélérerez votre mise en conformité et démontrerez à l'autorité de régulation des informations que vous avez pris des mesures pour vous conformer au RGPD.

NOTES ET RÉFÉRENCES

i. Clean your SAP data and reduce risk
ii. EPI-USE Labs' Data Disclose
iii. Austrian GDPR-Tracker: Data Protection Authority On Erasure By Way Of Anonymization
iv. EPI-USE Labs' Data Redact
v. *Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou à 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.*
vi. EPI-USE Labs' Object Extractor
vii. Evolutio
viii. Cenoti
ix. Soterion
x. EPI-USE Labs' Cryptographic Library
xi. EPI-USE Labs' Data Disclose
xii. SAP UI Masking & Logging solution
xiii. SAP Information Retrieval Framework (IRF)
xiv. EPI-USE Labs' Data Privacy Suite
    EPI-USE Labs' Data Disclose
    EPI-USE Labs' Data Redact
    EPI-USE Labs' Data Retain
xv. EPI-USE Labs' Data Sync Manager
    EPI-USE Labs' Data Secure
    EPI-USE Labs' Client Sync
xvi. EPI-USE Labs' Query Manager
xvii. EPI-USE Labs' Document Builder
xviii. EPI-USE Labs' Cryptographic Library