SAP BUSINESSOBJECTS
à l'ère RGPD
10 ÉTAPES POUR ASSURER ET MAINTENIR LA CONFORMITÉ

RÉSUMÉ GÉNÉRAL

Le Règlement Général sur la Protection des Données (RGPD) impose aux organisations la mise en oeuvre de moyens de protection des données personnelles des utilisateurs basés dans l'UE. Afin de se conformer au RGPD, les Responsables Décisionnels ou Business Intelligence doivent connaître la source, l'objet et la localisation des données personnelles en leur possession. Puisque SAP BusinessObjects représente la partie visible des données, son utilisation implique la mise en conformité RGPD. Wiiisdom, éditeur des solutions 360Suite dédiées à l'amélioration de SAP BusinessObjects, a mis au point un processus en 10 étapes pour aider les organisations à répondre aux défis de la conformité RGPD, en suggérant les actions les plus appropriées.

QU'EST CE QUE LE RGPD ?

Le terme RGPD est connu du plus grand nombre, de même que son objectif. En résumé, il s'agit d'une nouvelle réglementation européenne (effective depuis le 25 mai 2018) relative à la libre circulation des données personnelles. Celle-ci consacre notamment le droit fondamental de protection des données des personnes physiques. Le RGPD s'applique aux organisations établies au sein et hors de l'UE dès que celles-ci proposent des biens, des services ou lorsque celles-ci suivent le comportement de personnes (ou sujets) basés dans l'Union Européenne. Toute organisation ne respectant pas le RGPD s'expose potentiellement à une amende jusqu'à 20 millions d'Euros ou de 4% de son chiffre d'affaires mondial annuel.

QU'EST CE QU'UNE PERSONNE PHYSIQUE ?

Personne physique est un terme légal utilisé pour parler d'être humain individuel. Ce terme distingue les individus des organisations privées et publiques, lesquelles peuvent être qualifiées de personnes morales. Dans le cadre du RGPD, une personne physique est un sujet de données au sein des frontières de l'UE au moment du traitement de ses données personnelles. Il peut aussi s'agir de toute personne n'importe où dans le monde et dont les données personnelles sont traitées par un tiers établi au sein de l'UE.

COMMENT DÉFINIR LES DONNÉES PERSONNELLES ?

L'article 4(1) du RGPD définit les données personnelles comme «toute information relative à une personne physique identifiée ou identifiable». Les données permettant l'identification directe ou indirecte d'une personne comprennent les noms, numéros d'identification, informations de localisation, d'identification sur les réseaux (ex. : adresses IP, cookies, etc.), ainsi qu'un ou plusieurs traits physiques, psychologiques, génétiques, mentaux, économiques, culturels ou liés à l'identité sociale.

COMMENT TRAITER LES DONNÉES PERSONNELLES ?

L'article 4(2) définit le traitement comme «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». Dans le champ d'application du RGPD, toute donnée personnelle est sujette aux principes de légalité, d'équité, de transparence, de restriction d'utilisation, de minimisation des données, de précision, de limitation des durées de stockage, d'intégrité, de confidentialité, et de responsabilité. Les organisations sont rendues responsables de la collecte et de l'utilisation des données personnelles, exclusivement dans la poursuite d'objectifs spécifiés, explicites et légitimes. Elles sont également responsables du stockage et du traitement sécurisés des données personnelles ainsi que de leur suppression dans les délais les plus brefs possibles.

Certains types de données personnelles ne peuvent en aucun cas être traités. L'article 9(1) établit que le «Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits», sauf en cas d'application de l'une des dix exceptions mentionnées à l'article 9(2).

COMMENT QUALIFIER LE CONSENTEMENT ÉCLAIRÉ ?

Pour beaucoup d'organisations, le respect du principe de légalité implique généralement l'obtention du consentement des personnes concernées avant le traitement des données personnelles. L'article 4(11) définit le consentement comme «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». Pour qu'il puisse y avoir consentement, la personne concernée doit connaître l'identité du responsable du traitement et les raisons pour lesquelles celles-ci seront traitées. L'article 7(3) établit que «La personne concernée a le droit de retirer son consentement à tout moment» et que le retrait du consentement doit être aussi simple que l'octroi de ce dernier.

QUELS SONT LES DROITS DES PERSONNES CONCERNÉES ?

En plus du droit au retrait du consentement, le RGPD accorde les droits suivants aux personnes physiques :

- Le droit d'accès de la personne concernée (Articles 15) : Droit pour les personnes physiques de savoir si une entreprise possède leurs données personnelles, et si tel est le cas, les raisons et manière dont les données sont traitées, la durée de leur conservation, ainsi que les destinataires des données.
- Le droit de rectification (Article 16) : Droit de correction des données personnelles inexactes et/ou ajout de données manquantes.
- Le droit à l'effacement (droit à l'oubli) (Article 17) : Droit de demander la suppression des données personnelles en cas de retrait du consentement ou si une ou plusieurs autres conditions s'appliquent.
- Le droit à la limitation du traitement (Article 18) : Droit des personnes physiques de restreindre le traitement de leurs données personnelles si une ou plusieurs conditions s'appliquent.
- Droit à la portabilité des données (Article 20) : Droit des personnes physique de récupérer leurs données personnelles d'un responsable de traitement et de les transmettre à un autre.
- Droit d'opposition (Article 21) : Droit d'objection au traitement des données personnelles quel qu'en soit le motif, y compris le profilage et le démarchage direct.
- Droit d'introduire une réclamation auprès d'une autorité de contrôle (Article 13(2d))

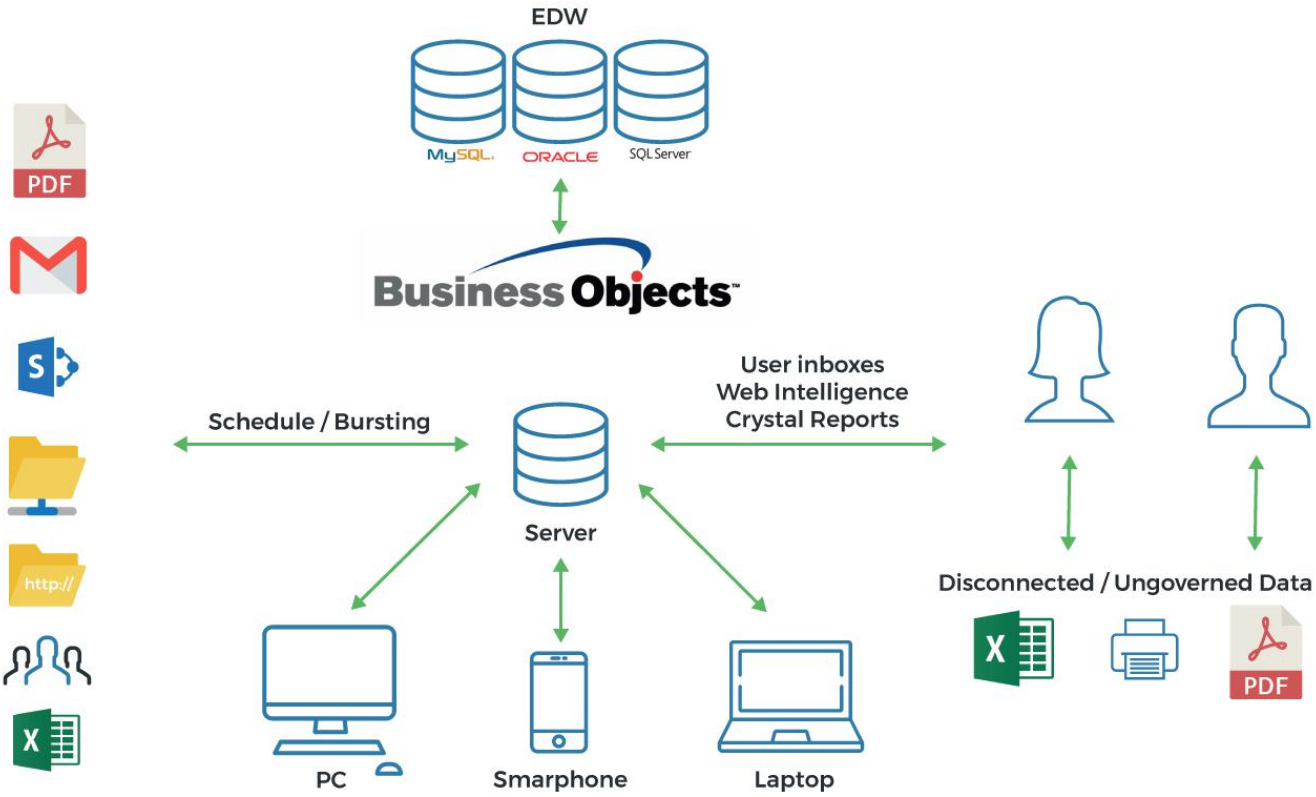
QUELLES SONT LES OBLIGATIONS DES REPRÉSENTANTS ET SOUS-TRAITANTS ?

Dans certaines situations, les représentants et sous-traitants sont assujettis aux mêmes obligations RGPD. Par exemple, les deux groupes ont l'obligation de maintenir l'historique des activités de traitement, d'implémenter les moyens techniques et organisationnels afin d'assurer un niveau de sécurité approprié au risque, ainsi que de nommer des délégués à la protection des données. Mais généralement, le RGPD considère les représentants comme les parties devant spécifiquement obtenir le consentement et ayant l'obligation d'appliquer les droits des personnes concernées. Les représentants doivent également notifier l'autorité de contrôle de toute fuite de données personnelles dans les 72 heures et ont l'obligation de signaler immédiatement ces fuites aux personnes concernées. Pour comprendre la différence entre représentants et sous-traitants, concentronsnous sur l'exemple d'UNION MANUFACTURING CO (UMC). UMC emploie 5000 personnes en France et externalise la paie, les ressources humaines et les services d'avantages sociaux à PAYME INC. UMC transmet les données à caractère personnel de ses employés à PAYME pour traitement. Dans ce cas précis, UMC est le représentant et PAYME est le sous-traitant. UMC est responsable de l'obtention des données personnelles et du consentement de ses employés afin de conserver les informations à jour et doit notifier à PAYME toute modification de ces données (objectif : appliquer les droits des personnes concernées).

QUEL EST L'IMPACT DU RGPD SUR SAP BUSINESSOBJECTS ?

On peut affirmer, sans trop de risques, que les outils informatiques tels que les plateformes CRM, systèmes ERP et applications BI (ex. : SAP BusinessObjects, Tableau, Power BI) comprennent des informations personnelles issues de bases de données. Pour se conformer au RGPD, les responsables Business Intelligence (BI), y compris les centres d'excellence BI (BI CoE) et les centres de compétence BI (BICC), doivent être en mesure de répondre en détail aux questions relatives à leurs plateformes :

1. Quelles sont les données à caractère personnel sur la plateforme ?
2. Où sont stockées les données à caractère personnel ?
3. Quel est le cycle de vie des données à caractère personnel ?
4. Qui a accès aux données à caractère personnel ? Qui utilise cet accès ?
5. Comment sont traitées les données à caractère personnel ?
6. Quelles sont les mesures mises en place pour sécuriser les données à caractère personnel ?
7. A quel moment les données à caractère personnel doivent-elles être chiffrées ou pseudonymisées ?
8. Quelle est la durée de conservation des données à caractère personnel? Quels sont les moyens de suppression de ces données ?
9. Où sont situés les utilisateurs (ex. : dans quels pays) ?
10. Que conserve-t-on des informations relatives aux activités de traitement des données à caractère personnel ?



QU'EST-CE QUE 360SUITE ?

360Suite est une suite de **solutions agiles de gouvernance** dédiée pour SAP BusinessObjects, développée par Wiiisdom.

Chez Wiiisdom, nous vous accompagnons pour faire de votre **patrimoine Analytics**, un lieu fiable qui permette de maximiser l'utilisation de vos données et de prendre de **meilleures décisions** au quotidien.

360Suite est un ensemble de solutions permettant d'assurer la qualité, la fiabilité, la performance et l'efficacité de SAP BusinessObjects au travers de méthodologies de **tests**, d'audit, de monitoring, de catalogage et de planifications de tâches. 360Suite s'adresse aux grandes organisations souhaitant se prémunir des **risques** liées aux données, d'**automatiser** leurs opérations, et représente une solution de choix pour tout type de projet de migration.

Un processus en 10 étapes a été élaboré pour assister les organisations dans la mise en oeuvre des mesures techniques et structurelles requises par le RGPD dans le cadre de l'utilisation de SAP BusinessObjects.

SAP BusinessObjects entre dans l'ère RGPD

10 étapes pour garantir et maintenir la conformité

1 Sauvegardez vos données

2 Ciblez les données personnelles

3 Marquez les données personnelles

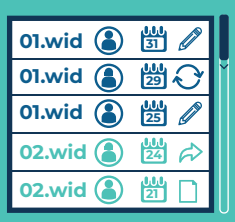
4 Analysez vos données personnelles

5 Assurez la cohérence des données personnelles

6 Assurez la traçabilité des données personnelles

7 Sécurisez vos données personnelles

8 Corrigez ou supprimez les données personnelles de façon définitive



9 Surveillez l'utilisation des données personnelles

10 Démontrez votre conformité RGPD

SAP® Certified
Integration with SAP BusinessObjects

360 Suite

SAP Partner

ÉTAPE 1 : SAUVEGARDE DES DONNÉES

Que les données soient stockées sur place ou dans le cloud (ou les deux pour les architectures hybrides), le RGPD exige la mise en place d'un plan de sauvegarde et restauration. L'article 32(1)(c) établit l'obligation pour les responsables du traitement et les sous-traitants de maintenir «des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique». La seule sauvegarde du contenu SAP BusinessObjects ou l'utilisation de machines virtuelles ou de services de sauvegarde dans le cloud ne suffisent pas dans le cadre de la conformité RGPD. Pourquoi ? Car les données personnelles modifiées ou supprimées après la dernière sauvegarde en date seraient restaurées à un état antérieur lors d'une éventuelle récupération de SAP BusinessObjects. De même, en cas de corruption des environnements, les sauvegardes peuvent également être affectées, que celles-ci soient sur serveur, machine virtuelle ou dans le cloud.

SAP BusinessObjects utilise des fichiers Business Intelligence Archive Resource (BIAR) volumineux et peu flexibles contenant de grandes quantités d'objets. Les stratégies conventionnelles de récupération SAP BusinessObjects impliquent en général la sauvegarde complète du serveur afin de restaurer le système dans son intégralité en cas de défaillance. Cependant, de telles pratiques ne permettent pas les restaurations sélectives, la récupération d'univers ou d'objets supprimés individuellement. La restauration intégrale d'environnements SAP BusinessObjects prend beaucoup de temps, parfois plusieurs jours.

360Plus crée un fichier BIAR par objet et lance des sauvegardes delta incrémentales dynamiques. Ceci permet la restauration de versions précédentes de n'importe quel objet à n'importe quel moment. En donnant aux organisations la possibilité de restaurer en quelques secondes des éléments spécifiques ou des environnements entiers en quelques minutes ou heures, 360Suite assure la continuité des opérations et satisfait aux exigences RGPD en matière de restauration rapide des données à caractère personnel. [Limitation des risques liés à la sauvegarde et à la récupération après désastre sous SAP BusinessObjects.]

[Limitation des risques liés à la sauvegarde et à la récupération après désastre sous SAP BusinessObjects.]

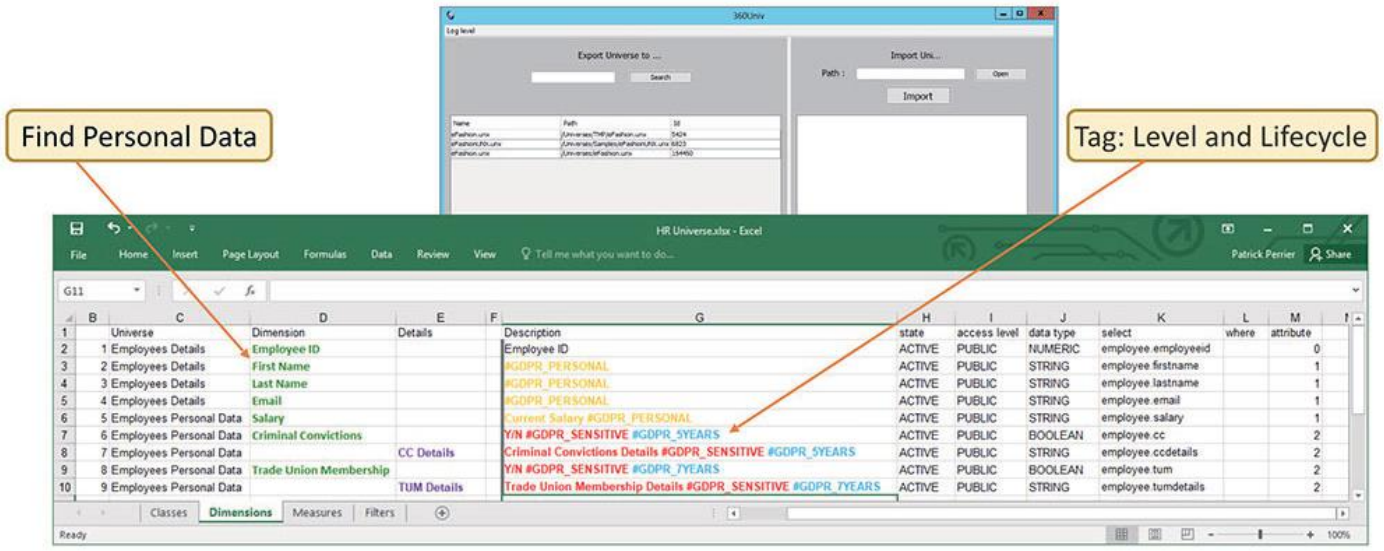
ÉTAPE 2 : INVENTAIRE DES DONNÉES PERSONNELLES

Dans un premier temps, l'établissement d'un inventaire est nécessaire afin d'obtenir une vue détaillée des données à caractère personnel stockées dans chaque environnement. Mais repérer les données personnelles présentes dans les univers Business Objects n'est pas une tâche aisée. L'outil SAP BusinessObjects Information Design Tool (IDT) permet l'extraction des données, mais cet utilitaire est réservé aux services techniques, et n'est donc pas disponible aux utilisateurs finaux. 360Univ donne aux utilisateurs finaux la possibilité d'inventorier les données à caractère personnel grâce à l'export des objets d'univers vers des fichiers au format Excel (plus simples à manipuler pour la recherche et le repérage de données personnelles).

ÉTAPE 3 : MARQUAGE DES DONNÉES PERSONNELLES

Suite à l'inventaire, les données personnelles doivent être marquées pour signalement. L'article 30 établit l'obligation pour les responsables du traitement de tenir «un registre des activités de traitement effectuées sous leur responsabilité». L'article 7 établit que les responsables du traitement doivent être «en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant». Et l'article 14(2)(f) établit que si «les données à caractère personnel n'ont pas été collectées auprès de la personne concernée" le responsable du traitement a l'obligation de fournir la source d'où proviennent ces données.

Pour créer et maintenir les historiques de traitement, les listes de preuves de consentement et les sources de données, les responsables BI doivent être en mesure de relier les données personnelles aux éléments signalés. 360Univ permet le marquage des données à caractère personnel en y adjoignant les informations requises telles que l'objectif du traitement, la source desdites données, la catégorie de la personne concernée (et sa sensibilité), la catégorie du destinataire, les transferts vers des pays ou organisations tiers, les mesures techniques et organisationnelles, et le délai avant suppression. Les marqueurs (tags) peuvent différer d'une unité organisationnelle à l'autre. Par exemple, le principe de restriction de stockage impose de ne pas conserver les données à caractère personnel plus longtemps que nécessaire. Cette durée peut être de 6 mois pour un département de service client, 2 ans pour un service support, et 7 ans pour un service comptabilité. Les marqueurs doivent donc être suffisamment détaillés pour rendre compte du cycle de vie complet des données. Les informations hautement confidentielles (ex. : informations médicales) doivent être marquées comme devant bénéficier de mesures complémentaires incluant le chiffrement ou la pseudonymisation.



ÉTAPE 4 : ANALYSE DES DONNÉES À CARACTÈRE PERSONNEL

L'étape faisant suite au marquage des données à caractère personnel est l'analyse de ces dernières selon les règles de confidentialité imposées par le RGPD. Les données personnelles sont-elles exploitées ou non ? Comment sont-elles exploitées ? Par quel biais les données ont-elles été obtenues ? Directement des personnes concernées ou d'un tiers ? De quelle manière les données seront-elles traitées ? Le traitement est-il légal (principe de légalité, d'équité et de transparence) ? Les personnes concernées ont-elles donné leur consentement au traitement des données ? Les données incluent-elles des informations prohibées par l'article 9 (ex.: race, ethnie, religion, etc.) ? Les données ont-elles été recueillies pour un but spécifié, explicite et légitime (principe de limitation de l'objectif) ? Les données sont-elles pertinentes et limitées au strict nécessaire au regard du but poursuivi et pour lequel celles-ci sont traitées (principe de réduction des données) ? Les données sont-elles exactes et maintenues à jour (principe d'exactitude) ? Les données sont-elles conservées sous une forme permettant l'identification des personnes concernées? La conservation des données n'excède-t-elle pas la durée effectivement nécessaire (principe de limitation du stockage) ? Les données sontelles traitées avec toutes les garanties de sécurité (principe d'intégrité et de confidentialité) ? Les données à caractère personnel ne satisfaisant pas à ces principes n'ont pas leur place dans un entrepôt de données d'entreprise (Enterprise Data Warehouse ou EDW), et doivent donc être définitivement supprimées. 360Eyes fournit toutes les indications relatives à l'utilisation (ou non) des données, tandis que 360View permet la suppression en masse automatique des données non-exploitées.

Universe: /HR/HR Universe

Class Name	Dimension	Details	Description	Select
Employees Details	Employee ID		Employee ID	employee.employeeid
	First Name		#GDPR_PERSONAL	employee.firstname
	Last Name		#GDPR_PERSONAL	employee.lastname
	Email		#GDPR_PERSONAL	employee.email

Class Name	Dimension	Details	Description	Select
Employees Personal Data	Salary		Current Salary #GDPR_PERSONAL	employee.salary
	Criminal Convictions		Y/N #GDPR_SENSITIVE	employee.cc
		CC Details	Criminal Convictions Details #GDPR_SENSITIVE	employee.ccdetails
	Trade Union Membership		Y/N #GDPR_SENSITIVE	employee.tum
		TUM Details	Trade Union Membership Details #GDPR_SENSITIVE	employee.tumdetails

ÉTAPE 5 : GARANTIE DE LA COHÉRENCE DES DONNÉES À CARACTÈRE PERSONNEL

La cohérence ne s'applique pas aux seules données, mais également à la manière dont celles-ci sont intégrées dans les rapports et à qui ces rapports sont communiqués. Les outils de la solution 360Suite garantissent cette cohérence. 360Bind automatise les tests de non-régression et contrôle que les modifications au niveau ETL, base de données, et univers n'altèrent pas le contenu des rapports. Les extractions générées par 360Eyes peuvent être utilisées dans le suivi des modifications apportées à la sécurité, aux univers et aux objets au fil du temps. Ceci facilite les analyses d'impact sur les rapports en cas de changements liés aux données personnelles. 360Vers assure le suivi des modifications de rapports et d'univers à tout moment et par n'importe quel utilisateur. L'outil fournit également un système avancé de gestion des versions avec possibilité d'affichage et d'audit des modifications, de déverrouillage sécurisé, et de mise en place de processus d'approbation pour une meilleure traçabilité. Assurer le suivi des versions des rapports contenant des données personnelles est une bonne pratique. Ceci permet, au besoin, le retour simple et rapide aux versions antérieures tout en garantissant la conformité RGPD au Délégué à la Protection des Données. Enfin, la fonction de suppression de 360View autorise les administrateurs à supprimer tout rapport accidentellement expédié vers les boîtes de réception des utilisateurs.

ÉTAPE 6 : GARANTIE DE LA TRAÇABILITÉ DES DONNÉES À CARACTÈRE PERSONNEL

Garantissez la traçabilité des données à caractère personnel, tout particulièrement lors de leur transmission à une organisation tierce ou hors de SAP BusinessObjects. Le RGPD (101) établit que, "lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale." En d'autres termes, les responsables du traitement restent responsables de la protection des données personnelles, obtenues directement ou indirectement, même après le transfert de données personnelles.

Lors du transfert de données personnelles depuis le format SAP BusinessObjects natif (Webi) vers un format non-natif (ex. : PDF, XLS), les organisations doivent impérativement prendre des mesures de sécurité, telles que la protection par mot de passe des données en question grâce à 360Cast par exemple. Pour chaque transfert de données à caractère personnel à un tiers, les organisations doivent s'assurer que ces données comportent les informations de conformité requises (ex. cycle de vie), telles que celles créées à l'aide de 360Univ (voir étape 3). Quel que soit le type de transfert, les organisations ont l'obligation de marquer chaque instance des données à caractère personnel, ce qui est possible avec 360Cast.

ÉTAPE 7 : SÉCURISATION DES DONNÉES À CARACTÈRE PERSONNEL

Suite à l'inventaire, le marquage et l'analyse des données à caractère personnel, la sécurisation des accès s'avère essentielle. Le RGPD établit que «Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement.». L'article 25 spécifie que «par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité». Les responsables du traitement ont la charge de la sécurisation des accès aux données à caractère personnel obtenues directement ou indirectement, ainsi que des données transmises à des tiers. Les organisations doivent également prévenir toute activité malicieuse et développer des plans d'actions.

Il est possible de sécuriser les données personnelles de différentes manières. Les responsables de Business Intelligence peuvent contrôler et re-certifier les utilisateurs ayant accès aux données. 360Eyes monitore et documente l'état de la sécurité au fil du temps. 360View renforce la sécurité grâce à une vue détaillée complète des droits hérités et à double héritage. Cet aspect est particulièrement important lors du traitement des données personnelles en raison des éventuels effets en cascade à chaque modification de la sécurité. 360View simplifie également le processus d'audit et de modification de la sécurité tout en assurant la séparation des privilèges (Segregation of Duties).

En parallèle de la re-certification des comptes utilisateur/accès, les gestionnaires Business Intelligence peuvent sécuriser les données à caractère personnel par recertification des comptes en ne conservant que les données véritablement essentielles. Les données sont considérées non-essentielles, notamment si celles-ci ne sont jamais utilisées ou arrivent à expiration. 360Eyes simplifie le processus de re-certification en fournissant le détail de l'exploitation ou de l'absence d'exploitation des données à caractère personnel. 360View permet la suppression en masse des données, ainsi que la purge forcée des boîtes de réception, des Webis et le nettoyage automatique des déploiements.

Les gestionnaires BI peuvent aussi compter sur une autre stratégie de sécurisation des données : la mise en place de mesures techniques rendant les données inintelligibles (ex. : pseudonymisation) ou sélectivement inintelligibles à toute personne ne disposant pas des accès requis (ex. : données chiffrées).

ÉTAPE 8 : MODIFICATION OU SUPPRESSION DÉFINITIVE DES DONNÉES À CARACTÈRE PERSONNEL

Assurez-vous de la permanence des modifications apportées aux données personnelles, même en cas d'incident technique ou physique. L'un des piliers fondamentaux du RGPD est le droit des personnes physiques à rectifier ou supprimer leurs données. L'article 16 établit que «la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes». L'article 17 établit que «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». Une restauration de la copie de sauvegarde la plus récente annulera donc tous les changements apportés aux données. Prenons par exemple le cas d'une organisation ayant effectué sa dernière sauvegarde SAP BusinessObjects le 1er Mars. Celle-ci modifie des données personnelles le 2 Mars et subit un incident le 3 Mars. La restauration de la copie du 1er Mars entraînera par conséquent la perte des modifications effectuées le 2 Mars. Les sauvegardes delta dynamiques (360Plus) combinées aux extractions (360Eyes) permettent la détection de toutes les modifications depuis la sauvegarde précédente, et donc la restauration sélective de versions précédentes de n'importe quel objet.

ÉTAPE 9 : SUIVI DE L'EXPLOITATION DES DONNÉES À CARACTÈRE PERSONNEL

Le suivi de l'exploitation des données à caractère personnel constitue une stratégie de sécurité complémentaire. L'audit des actions sur les données dans SAP BusinessObjects est rendu possible par 360Eyes : suivi des données personnelles dans les rapports, de l'utilisation des rapports eux-mêmes (y compris les actions sur ces derniers), détection des doublons et des modifications d'univers. 360Eyes est aussi capable d'identifier les utilisateurs ayant accédé à ces données, retrace l'historique des actions effectuées et conserve les adresses IP à l'origine de ces actions. Enfin, 360Eyes génère des extractions des déploiements SAP BusinessObjects couvrant de longues périodes. Ces extractions peuvent être exportées et comparées dans le cadre des procédures d'audit. 360Suite n'utilise aucun système d'interception des données et collecte les informations hors des heures d'utilisation pour éviter toute dégradation des performances en production.

ÉTAPE 10 : PREUVE DE CONFORMITÉ RGPD

Apportez la preuve de conformité pour répondre rapidement aux demandes des Délégués à la Protection des Données et aux autorités de certifications. Au regard de l'article 24 du RGPD, les organisations doivent pouvoir établir la preuve de leur conformité. (Le représentant doit «être en mesure de démontrer que le traitement est effectué conformément au présent règlement»). Les solutions 360Suite, incluant 360Plus, 360Univ, 360View, 360Cast, 360Eyes, 360Bind et 360Vers permettent aux organisations d'assurer le respect des principes d'excellence. La conformité RGPD ne fait pas exception. 360Suite ne se limite pas au traitement des données à caractère personnel dans le respect du RGPD, mais apporte également aux organisations les moyens d'assurer la conformité des documents. Ainsi, 360Suite se comporte à la fois comme une solution métier et un outil technique conduisant les parties en présence vers leur but commun : le succès organisationnel.

GLOSSAIRE DES TERMES UTILISES

Business Intelligence
Processus technique d'analyse des données assistant les utilisateurs finaux dans la prise de décisions métier.

Consentement
Tout accord sans ambiguïté, informé, spécifique et librement délivré autorisant le traitement des données à caractère personnel.

Données personnelles / Données à caractère personnel
Toute information liée à une personne physique identifiée ou identifiable

Personne Physique
Être humain individuel distinct d'une organisation privée ou publique (voir Personne morale)

Règlement Général sur la Protection des Données (RGPD)
Règlement de l'Union Européenne visant à standardiser et renforcer les politiques de protection des données des résidents des nations membres de l'UE

Représentant
Personne physique ou morale, autorité publique, agence ou tout autre entité individuelle ou en collectivité définissant les buts et moyens de traitement des données à caractère personnel.

Sous-traitant
Personne physique ou morale, autorité publique, agence ou toute autre entité traitant les données à caractère personnel au nom d'un représentant

Traitement
Toute opération réalisée sur les données à caractère personnel par des moyens automatisés ou non

Union Européenne (UE)
Union politique comprenant actuellement 28 nations membres

Auteur: Bruno Masek
Kristen Champagne Gray

SE METTRE EN CONFORMITÉ **RGPD** AVEC **360SUITE?**

360 Suite

Visiter www.wiiisdom.com/fr/360suite