Aider à devenir et rester conforme au GDPR

Avec les produits et les services Cloud de Microsoft

Cette page est laissée intentionnellement blanche.

Table des matières

Avertissement

Ce livre blanc est un commentaire sur le Règlement Général sur la Protection des Données (RGPD, plus communément désigné par son acronyme anglais GDPR) tel qu'il est perçu par Microsoft à la date de publication du présent document. Malgré une réflexion très longue sur les objectifs et la signification du GDPR, sa mise en œuvre ne peut se fonder que sur des actions concrètes. Nombre des aspects et interprétations du GDPR qui ne sont pas encore bien établis nécessiteront des éclaircissements et de nouvelles réflexions.

Par conséquent, le présent document est fourni exclusivement à titre informatif et ne saurait être considéré comme constituant un quelconque avis juridique ou permettant de déterminer comment le GDPR pourrait s'appliquer à vous et à votre organisation. Nous vous encourageons à collaborer avec un professionnel dûment qualifié afin d'aborder le GDPR, à vérifier la manière dont ce Règlement s'appliquera spécifiquement à votre organisation et à déterminer la meilleure façon d'en assurer la conformité.

MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE, IMPLICITE OU LÉGALE, RELATIVE AUX INFORMATIONS CONTENUES DANS CE LIVRE BLANC. Le livre blanc est fourni « EN L'ÉTAT » sans garantie d'aucune sorte et ne saurait être interprété comme un engagement de la part de Microsoft.

Microsoft ne peut pas garantir la véracité des informations présentées. Les informations de ce livre blanc, comprenant notamment et sans que la liste ne soit exhaustive, les références de site web Internet et URL, sont susceptibles de changer à tout moment, sans préavis. De plus, les avis exprimés dans ce livre blanc représentent la vision actuelle de Microsoft France sur les points cités à la date de publication du présent livre blanc et sont susceptibles de changer à tout moment sans préavis.

Publication : Octobre 2017
Version 1.0

Résumé

À l'ère de la transformation numérique, la protection de la vie privée et l'amélioration de la sécurité sont devenues des sujets de société incontournables. Le prochain Règlement Général sur la Protection des Données (RGPD, plus communément désigné par son acronyme anglais « GDPR ») définit une nouvelle étape importante pour les droits à la vie privée, la sécurité et la conformité.

Le GDPR impose de nombreuses exigences et obligations pour les organisations à travers le monde. Le respect de cette réglementation nécessitera des investissements importants dans la gestion des données et leur protection pour un très grand nombre d'organisations et d'entreprises.

Les clients de Microsoft qui sont soumis au GDPR, qu'ils effectuent des traitements en interne, dans le cloud ou en mode hybride, devront s'assurer que les données personnelles au sein de leurs systèmes qui participent aux traitements de ces données sont correctement traitées et protégées selon les principes du GDPR. Cela signifie que de nombreux clients devront réviser ou modifier leurs procédures de traitement de données, l'implémentation de leurs traitements, en particulier en ce qui concerne la sécurité desdits traitements des données comme stipulé dans le GDPR.

Microsoft a une expérience significative dans la gestion des principes de protection des données et de conformité à des réglementations complexes. Cette expérience se traduit au travers des produits et des services Cloud proposés par Microsoft qui peuvent aider les clients de Microsoft à respecter les objectifs et les exigences de protection de la vie privée du GDPR pour leurs traitements de données. Dans ce contexte, ce document met en exergue les apports de ces solutions dans le cheminement vers la conformité avec le GDPR.

Introduction

Après plus de quatre années de négociations qui ont débuté lorsque la Commission a présenté ses propositions en janvier 2012, le Conseil de l'Europe a adopté le 14 avril 2016 le Règlement Général sur la Protection des Données[1] (RGPD), plus communément désigné par son acronyme anglais GDPR (et ainsi dénommé dans la suite de ce document) : General Data Protection Regulation.

Le Règlement est entré en vigueur le 24 mai de cette même année et sera applicable directement dans tous les États membres après un délai de 2 ans, soit le 25 mai 2018, dans moins d'un an à la date de publication de ce livre blanc.

Le GDPR s'intéresse fondamentalement à la question de protéger la vie privée des personnes et d'affirmer des droits en la matière. Le GDPR établit pour cela un ensemble d'exigences globales des plus strictes qui s'imposent aux organisations et aux entreprises en termes de protection de la vie privée. Ces exigences régissent la façon dont vous devez gérer et protéger les données personnelles des citoyens ou des entreprises européens tout en respectant leurs choix individuels, peu importe où ces données sont traitées, stockées, ou envoyées.

Ainsi, Microsoft et ses clients sont désormais engagés dans un voyage pour atteindre les objectifs de protection de la vie privée fixés par le GDPR. Chez Microsoft, nous croyons que la vie privée constitue un droit fondamental, et nous pensons que ce règlement constitue une avancée importante en termes de protection de la vie privée et des droits associés. Nous reconnaissons aussi, dans le même temps, que le GDPR imposera des changements significatifs aux organisations et aux entreprises du monde entier.

Dans ce contexte, et comme le souligne Brad Smith, Président et Directeur juridique de Microsoft Corporation, « *le nouveau Règlement élève la barre de façon significative quant aux droits en matière de protection de la vie privée, à la sécurité et à la conformité* ».

Un premier livre blanc GDPR - S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR[2] suggère une trame de programme et une trajectoire pour la mise en conformité avec le GDPR. Il aborde des questions importantes, comme la relation avec les sous-traitants, la sécurité des données personnelles, la notification auprès de l'autorité de contrôle pour ne reprendre ici que quelques-uns des points clés.

Fort de cette trame en matière de fondation programmatique, il nous parait important à présent de partager comment, grâce à nos solutions en local et à nos services de cloud, Microsoft (peut) vous aide(r) à localiser et cataloguer les données personnelles de vos traitements dans vos systèmes, à construire un environnement (hybride) plus sécurisé et à simplifier la gestion et le suivi des données personnelles.

Les services Cloud de Microsoft, tels que Microsoft Azure[3], Microsoft Dynamics 365[4] et Microsoft Office 365[5], vous permettent par exemple de faciliter les processus que vous devez mettre en œuvre pour assurer la conformité avec le GDPR grâce à l'Intelligence Artificielle (IA), l'innovation et la collaboration.

---

[1] REGLEMENT (UE) 2016/679 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIF A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES, ET ABROGEANT LA DIRECTIVE 95/46/CE (REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES) : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

[2] GDPR - S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR : https://aka.ms/GDPRprocess

[3] Microsoft Azure : https://azure.microsoft.com/fr-fr/

[4] Microsoft Dynamics 365 : http://www.microsoft.com/fr-fr/dynamics365/

[5] Microsoft Office 365 : https://products.office.com/fr-fr/

Remarque Microsoft Azure est une collection croissante de services de cloud intégrés de type IaaS et PaaS - calcul, stockage, réseau, base de données, analytique avancée, mobile, Web, API, etc. - qui permettent à nos clients d'aller plus vite, de réaliser plus et de faire des économies pour la mise en œuvre de leurs (activités de) traitements. Azure sert à la fois d'environnement de développement (dans le cas de pratique DevOps notamment), de service d'hébergement et d'environnement d'exécution et de gestion de services pour héberger, mettre à l'échelle et gérer des applications et traitements sur Internet.

Remarque Microsoft Dynamics 365 est la prochaine génération d'applications d'entreprise intelligentes qui permet aux organisations de toute taille de se développer, d'évoluer et de se transformer pour répondre aux besoins de leurs clients quels qu'ils soient et de saisir de nouvelles opportunités. Il combine nos services de cloud actuels en matière de progiciel de gestion de la relation client (Customer Relationship Management en anglais ou CRM) et de planification des ressources d'entreprise (Enterprise Resources Planning en anglais ou ERP) en un seul service et comprend de nouvelles applications spécifiques pour aider à gérer les fonctions spécifiques d'une organisation (marketing, connaissances des clients, ventes, finances, services à la clientèle, opérations, automation des services projet, etc.).

Remarque Microsoft Office 365 est conçu pour répondre aux besoins des organisations en termes de productivité utilisateur, de fiabilité, et de sécurité élevée. Office 365 intègre la suite bureautique familière Microsoft Office avec les versions basées sur le Cloud des services de collaboration et de communication de nouvelle génération de Microsoft - exploitant l'Internet pour aider les utilisateurs à être plus productifs de pratiquement n'importe où depuis n'importe quel appareil.

En avançant avec un fournisseur de services de cloud « hyper-scale » comme Microsoft et en utilisant des services de cloud comme Azure, Dynamics 365 et Office 365, vous pouvez bénéficier de « l'économie de la conformité ». Les services Cloud de Microsoft vous permettent de réduire les efforts de programmation et les fardeaux administratifs requis pour devenir conforme avec le GDPR.

Remarque Pour de plus amples informations, nous vous invitons à lire le billet ACCELERATE YOUR GDPR COMPLIANCE WITH THE MICROSOFT CLOUD[6] de Julia White, notre Vice-Présidente Entreprise, Plateforme Cloud.

Objectifs du livre blanc

Ce livre blanc vise à illustrer les apports des produits et services Cloud de Microsoft dans le cheminement vers la conformité avec le GDPR, et par exemple la mise en œuvre des contrôles de sécurité appropriés en termes de mesures techniques (les mesures organisationnelles ne seront que très peu ou pas abordées par ce livre blanc compte tenu de son objet.)

L'approche retenue est résolument pragmatique et facilement activable pour les organisations au travers de l'étude de quelques activités de traitement de données fictives. L'objectif est d'illustrer un ensemble de situations types dans la collecte, le traitement et le stockage de données personnelles.

Ces situations permettent d'aborder, pour le traitement global, les trois états possibles des données : au repos, en traitement et en transit.

Ainsi, les axes de mise en conformité avec le GDPR développés pour ce traitement de données personnelles sont l'occasion de mettre en perspective dans une approche de bout-en-bout et concrète les technologies, produits et services Cloud de Microsoft.

[6] ACCELERATE YOUR GDPR COMPLIANCE WITH THE MICROSOFT CLOUD : https://blogs.microsoft.com/blog/2017/05/24/accelerate-gdpr-compliance-microsoft-cloud/

Organisation du livre blanc

De façon à répondre aux objectifs présentés ci-avant, et au-delà d'un rappel des engagements publics de Microsoft envers le GDPR, ce document est organisé selon les sections suivantes :

- VOUS AVEZ DIT « TRAITEMENT DE DONNEES PERSONNELLES » ?
- PRENDRE DES DISPOSITIONS POUR LA MISE EN CONFORMITE.
- EN GUISE DE CONCLUSION.

Nous espérons que l'organisation ainsi proposée apporte progressivité et clarté dans les différents domaines abordés.

Audience de ce livre blanc

Ce document est destiné aux Responsables de la Sécurité du Système d'Informations (RSSI), Directeurs de la gestion des risques, Directeurs de la gestion de la vie privée, Directeurs de la conformité, Directeurs des Données, Directeurs de l'information numérique, Délégué à la Protection des Données[7] professionnels de l'informatique, spécialistes de la sécurité et aux architectes des systèmes qui s'intéressent à la compréhension des piliers du GDPR et à la manière de s'assurer que les standards et les pratiques de l'organisation en termes de sécurité et de protection de la vie privée permettent de se conformer avec le GDPR.

[7] Plus d'informations sur ce nouveau rôle créé par le GDPR en https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees.

Rappels des engagements de Microsoft envers le GDPR

Nous avons souligné notre engagement envers le GDPR et la façon dont nous soutenons nos clients dans le billet GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD[8] publié par notre responsable de la protection de la vie privée Brendon Lynch[9] et le billet EARNING YOUR TRUST WITH CONTRACTUAL COMMITMENTS TO THE GENERAL DATA PROTECTION REGULATION[10] de Rich Sauer[11], Vice-Président et Directeur juridique adjoint de Microsoft Corp.

Cet engagement figure depuis le 1er septembre dans les termes des services en ligne[12] (Online Services Terms en anglais ou OST).

Bien que votre cheminement vers la conformité avec le GDPR puisse vous sembler difficile, nous sommes là pour vous y aider.

> **Remarque** Pour des informations spécifiques sur le GDPR, nos engagements et le début de votre voyage, visitez la section GDPR[13] dédiée du Centre de confiance[14] (Trust Center) Microsoft.

[8] GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD : https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/#4J5lDmd47PkIv6xL.99

[9] Blog de Brendon Lynch : https://blogs.microsoft.com/on-the-issues/author/brendonlynch/

[10] EARNING YOUR TRUST WITH CONTRACTUAL COMMITMENTS TO THE GENERAL DATA PROTECTION REGULATION : https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/#6QbqoGWXCLavGM63.99

[11] Blog de Rich Sauer : https://blogs.microsoft.com/on-the-issues/author/rsauer/

[12] LICENSING TERMS AND DOCUMENTATION : http://go.microsoft.com/?linkid=9840733

[13] Section GDPR du Centre de confiance Microsoft : http://www.microsoft.com/GDPR

[14] Centre de confiance Microsoft : https://www.microsoft.com/fr-fr/trustcenter

Vous avez dit « traitement de données personnelles » ?

Scénario « représentatif » de traitement

De façon à pouvoir illustrer comment les produits et les services Cloud de Microsoft peuvent aider à devenir et à rester conforme, nous avons souhaité nous appuyer sur un scénario « représentatif » de traitement de données.

Ce scénario permet de mettre en perspective des apports concrets dans le cheminement vers la conformité au GDPR. Cela permet dans le même temps d'illustrer certaines des activités de l'approche programmatique décrite dans le livre blanc S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR.

Ce scénario, que nous utiliserons comme fil directeur pour la suite de ce livre blanc, nous est proposé par la société « Litware 369 SARL » en France.

Litware 369 SARL, une société fictive connectée

Litware 369 SARL est une entreprise spécialisée dans le marché des alarmes d'habitation. Elle propose une offre large d'alarmes connectées pour répondre aux différents types d'habitat avec un bouquet de services à même de répondre aux exigences les plus diverses en matière de télésurveillance et d'intervention sur site.

Cette entreprise s'appuie sur un réseau d'entreprises partenaires pour l'installation des systèmes d'alarmes, la mise en place des services et options souscrites, le suivi du service, etc.

Pour un véritable relai local et une présence de proximité, Litware 369 a su développer un partenariat étroit avec des entreprises partenaires localisées dans chaque département (voire dans chaque grande localité du département).

Suite à la mise sur le marché d'une nouvelle génération d'alarmes connectées innovantes, l'entreprise connait une activité accrue. Elle a ainsi dû augmenter (la qualité de) sa présence sur Internet avec, à la clé, de nouvelles interfaces Web. Cela se traduit par :

- Un nouveau site web institutionnel pour la promotion de ses offres et la prise de commandes en ligne ;
- Un nouveau portail Clients pour le suivi des contrats des services en place ;
- Un nouveau portail Partenaires pour l'acceptation de prise en charge des commandes et le suivi et la mise à jour des dossiers d'installation client.

Ces interfaces Web de type B2C (Business-To-Consumer) et B2B (Business-To-Business) s'accompagnent d'un flux de traitement semi-automatisé couvrant le processus complet de la prise de commande à la mise en place effective du service souscrit.

La mise en ligne de ces nouvelles interfaces et le flux de traitement permettent ainsi de collecter des commandes d'abonnement et les traiter en vue de la mise en place du service ; ce qui en constitue la finalité principale.

Compte tenu de la nature des données collectées, utilisées et stockées, ce traitement de données rentre dans la catégorie des traitements de données personnelles tels que couverts par le GDPR.

Ce nouveau traitement impose à la société Litware 369 dans ce cas précis – d'autres traitements en place au sein de Litware 369 peuvent nécessiter le même regard – de se conformer au GDPR en répondant à ses nombreux objectifs et exigences.

Traitement envisagé

Comme rapidement brossé ci-avant, la finalité du traitement est de collecter des commandes d'abonnement et de les traiter en vue de la mise en place du service.

Afin d'être « représentatif » des traitements mis en œuvre dans la vie réelle, ou du moins sur certaines de ses facettes, nous avons souhaité un traitement implémenté sous une forme hybride, c'est-à-dire avec des composantes du traitement en interne au sein du système d'information local de Litware 369, mais également avec des services en cloud. Une telle mise en œuvre représente à la fois la capacité à tirer parti de ressources internes existantes – un annuaire Active Directory, une base de données SQL Server et un serveur de fichiers Windows Server - tout en bénéficiant des augmentations de fonctionnalité pertinentes proposées par le cloud public afin d'accompagner la transformation numérique de Litware 369. Une telle approche apporte à Litware 369 un meilleur temps de mise à disposition (« time to market ») de l'environnement de prise et de traitement des commandes, une meilleure réponse technique à certaines exigences propres au traitement, ainsi qu'une meilleure agilité.

Ce scénario « représentatif » nous autorise par ailleurs à articuler ici un traitement réparti entre un responsable de traitement et un sous-traitant au sens du GDPR, en l'occurrence Microsoft pour les services de cloud Azure, Dynamics 365 et Office 365.

> **Remarque** L'article 4[15] du Règlement introduit les différents rôles et concepts de protection des données à caractères personnel et, en particulier, ceux du responsable de traitement et sous-traitant. Dans la pratique, c'est au responsable du traitement qu'incombe l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer qu'un traitement des données personnelles est conforme aux objectifs et exigences du GDPR. Il doit, de plus, être en mesure de le démontrer à tout moment.
>
> Lorsqu'il fait appel à des sous-traitants, comme ici à Microsoft pour les services de cloud considérés, il doit s'assurer que ceux-ci offrent les garanties suffisantes pour lui permettre d'être conforme avec le GDPR et qu'ils traitent les données personnelles selon ses instructions, plus particulièrement concernant les transferts en dehors de l'Union Européenne.

Ce scénario « représentatif » permet enfin d'envisager dans le cadre du traitement, non seulement la collaboration B2B (Business-to-Business) avec les entreprises partenaires, mais également des accès B2C (Business-to-Consumer) pour les clients ; autant d'éléments également au cœur de la transformation numérique quand il s'agit de trouver de nouveaux usages et de définir de nouveaux modèles d'affaires.

Nouveau traitement oblige, ce traitement est par définition à priori dûment cartographié – à tout le moins pour ce qui est de sa conception et de sa construction - en termes de services, applications et dépôts mis en œuvre pour le matérialiser, de flux de données et de cycle de vie associés.

Abordons à présent les grandes étapes de notre scénario de traitement.

[15] ARTICLE 4 – DEFINITIONS : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4

Etapes du scénario de traitement

Le scénario envisagé couvre quatre étapes :

1. Enregistrement d'une commande ;
2. Prise en charge déléguée de la commande ;
3. Installation et mise en place du service ;
4. Activation du service.

Les sections suivantes décrivent le déroulement de ces étapes dans le cadre du traitement envisagé. Elles précisent également dans ce contexte certains éléments de mise en œuvre nécessaires à la compréhension des évolutions, actions et contrôles proposés dans la suite de ce document. Ces éléments concernent en particulier les « protagonistes » techniques du traitement en termes de produits, services de cloud, applications et dépôts de données.

Enregistrement d'une commande

Comme indiqué précédemment, un site web institutionnel de l'entreprise Litware 369 permet de souscrire à une offre d'alarmes connectées et de préciser les éventuelles options selon l'offre.

Ce site web est mis en œuvre avec le service de type PaaS (Platform-as-a-Service) Azure App Service[16] destiné à l'hébergement d'applications cloud performantes pour les clients web et mobiles. Ce site web est accessible en accès anonyme, c.à.d. sans authentification.

Des pages dédiées permettent de parcourir les différentes offres proposées par la nouvelle gamme d'alarmes connectées et de souscrire à l'une d'elles si l'on est convaincu de sa pertinence. Des brochures d'informations techniques sont téléchargeables à la demande pour informer sur les solutions ainsi proposées sous forme de service.

> **Remarque** La force de vente de Litware 369, avec ses commerciaux, dispose d'une application mobile pour la prise de commandes dans le démarchage de prospects ou lors de salons Grand Public. Nous y reviendrons dans la suite de ce document (Cf. section § PROTEGER LES DONNEES DANS LES APPAREILS MOBILES ET DES APPLICATIONS MOBILES).

[16] Azure App Service : https://azure.microsoft.com/fr-fr/services/app-service/

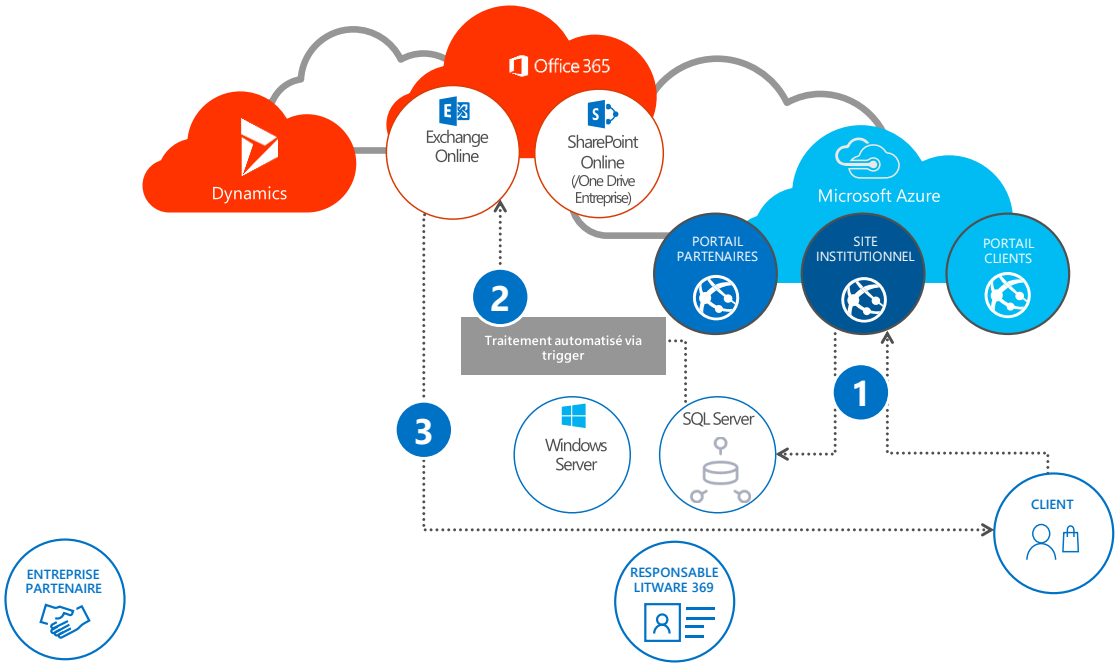

Figure 1 Vue d'ensemble de l'enregistrement d'une commande

Lors de la prise de commande, le contact (et futur client) est amené à préciser les informations et types de données nécessaires à la prise de commande, à savoir :

- Un contact : Nom, prénom, adresse complète, numéro de téléphone ;
- Et d'autres informations nécessaires à l'exécution de la commande : offre d'alarme connectée sélectionnée et options souhaitées, type d'habitation, etc.

Lors de la commande, une mention quant à l'usage de ces informations est d'ores et déjà présente dans la page, ainsi qu'une demande de consentement explicite afin d'utiliser ces informations pour le traitement de la commande.

Il est notamment précisé que ces informations seront partagées avec les entreprises partenaires de Litware 369 du département dans lequel est situé le lieu d'habitation du contact. Un lien permet d'accéder à la liste complète de ces entreprises avec leurs coordonnées complètes, le numéro de SIRET de l'établissement géographiquement localisé de l'entreprise pour le département concerné, le cas échéant un renvoi sur le site de l'entreprise, etc.

Des liens additionnels permettent d'accéder aux pratiques de Litware 369 en matière de protection de la vie privée.

Lors de la confirmation de la commande :

1. Un numéro de commande est généré automatiquement pour cette commande et la date de commande mémorisée ;
2. Un courriel de confirmation est envoyé au contact avec le numéro de commande, la date de la commande, un récapitulatif de la commande, un ensemble d'informations sur les prochaines étapes du traitement de celle-ci, un lien pour suivre la commande en cours, un lien pour se rétracter et résilier la commande sous un délai de 14 jours, etc.

Une base de données SQL Server en interne permet l'enregistrement des commandes depuis le site web institutionnel. Cette base de données SQL Server est accessible depuis le site web par le biais des capacités de connexions hybrides d'Azure App Service[17].

Ceci clôt cette première étape du traitement.

Prise en charge déléguée de la commande

Cette seconde étape du traitement commence par une extraction journalière des nouvelles commandes. Cette extraction est effectuée par département sous forme de fichiers .CSV (un par commande) reprenant l'ensemble des éléments de la commande.

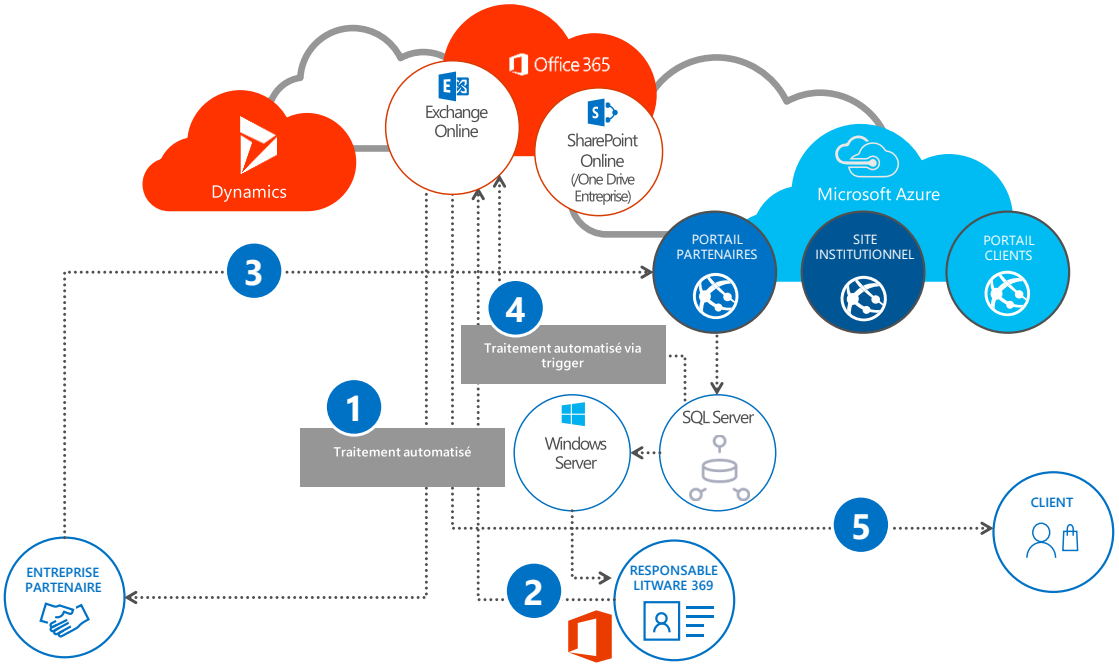

Figure 2 Vue d'ensemble de la prise en charge déléguée d'une commande

Les fichiers .CSV ainsi générés sont stockés sur un serveur de fichiers interne Windows Server, avec un dossier par département.

Le responsable en charge de chaque département au sein du service Partenaires de Litware 369 transmet par courriel au(x) partenaire(s) qualifié(s) du département les commandes en vue d'une prise en charge et du traitement.

Pour des raisons de simplicité, et comme cela n'apporte rien de particulier vis-à-vis de l'objet de ce document, nous supposons pour la suite de ce document qu'une seule entreprise partenaire par département a la charge du traitement effectif des commandes en cours.

> **Remarque** Une autre variante possible consisterait à s'appuyer pour Litware 369 sur un ensemble d'entreprises partenaires avec, à la clé, une gestion par exemple du type « premier à accepter/premier servi ».

Un composant logiciel enfichable (add-in) Outlook personnalisé permet le traitement automatisé des fichiers .CSV pour la génération des courriels. Le courriel est envoyé à une adresse préalablement dûment établie avec chaque entreprise partenaire.

---

[17] CONNEXIONS HYBRIDES D'AZURE APP SERVICE : https://docs.microsoft.com/fr-fr/azure/app-service/app-service-hybrid-connections

Remarque importante Pour la suite de notre propos, nous introduisons une déviation envers ce processus établi : tous les responsables au sein du service Partenaires ne suivent pas ce processus compte tenu de leur proximité avec l'entreprise partenaire qualifiée et retenue du département. Ce type de déviation, classique dans bon nombre d'entreprises, cherche à illustrer une pratique communément connue sous l'appellation « Shadow IT ».

Ainsi, certains responsables copient « simplement » le ou les fichiers .CSV du jour dans divers dépôts cloud partagés (Box, Dropbox, etc.). D'autres envoient des courriels à des adresses sociales non convenues.

L'entreprise partenaire remonte dans le portail Partenaires de Litware 369 son acceptation de chaque commande reçue. Pour cela, elle procède à la mise à jour de la commande en cours et de son statut. Une date du rendez-vous client et la plage horaire prévisionnelle pour ce rendez-vous sont notamment enregistrées pour la commande (numéro de commande).

Cette mise à jour provoque la génération et l'envoi d'un courriel de rendez-vous au contact. Ce courriel contient le numéro de commande, les informations sur le rendez-vous proposé, les informations sur le partenaire qui procèdera à l'installation et à la mise en service de l'offre, un lien pour modifier le rendez-vous, un lien pour suivre la commande en cours, etc.

D'un point de vue technique, le portail Partenaires s'appuie sans surprise également sur Azure App Service. Il impose en revanche un accès B2B authentifié pour les entreprises partenaires. Chaque entreprise partenaire dispose pour cela d'un compte générique qui lui a été communiqué par les services informatiques de Litware 369.

La même base de données SQL Server interne est utilisée dans cette étape avec les mêmes modalités de connexion depuis le portail Partenaires, à savoir via les connexions hybrides d'Azure App Service.

Pour ce qui est de l'accès authentifié, une table de comptes partenaires est présente dans cette base de données SQL Server interne, avec un compte générique par partenaire. Le mot de passe n'est pas stocké directement. Un petit traitement permet son salage et le calcul d'un condensat de condensat en faisant appel à l'algorithme SHA-256. C'est ce résultat qui est stocké.

Ces quelques détails d'implémentation étant précisés, ceci nous amène à la troisième étape de notre traitement.

Installation et mise en place du service

Cette étape du traitement correspond, comme son libellé le précise, à la matérialisation effective de la commande. Le rendez-vous client permet à l'entreprise partenaire de procéder à l'installation de l'alarme connectée correspondant à l'offre souscrite et à la mise en place du service conformément aux options sélectionnées pour cette offre.

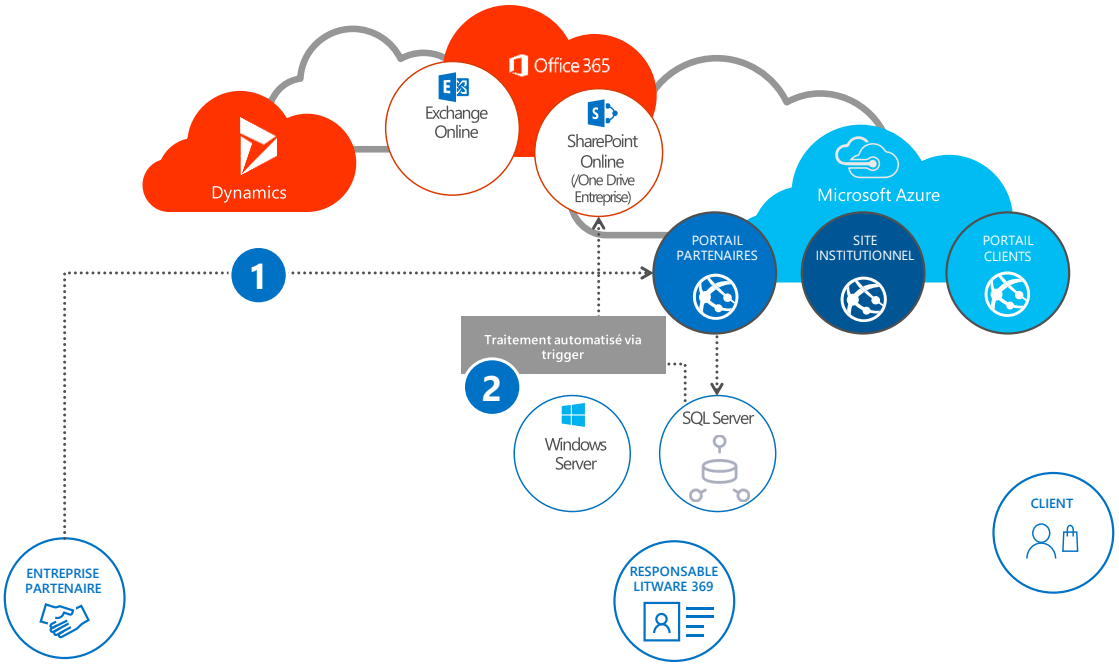

Figure 3 Vue d'ensemble de l'installation et de la mise en place du service

Une fois le rendez-vous effectué, l'entreprise partenaire met à jour - toujours depuis le portail Partenaires précédent - le dossier de commande avec cette fois les caractéristiques techniques de l'installation réalisée en vue de l'activation complète du service et des options souscrites au niveau de l'infrastructure technique spécifiquement mise en œuvre par Litware 369 pour cette nouvelle gamme d'alarmes connectées.

> **Remarque** Cette infrastructure technique repose sur Microsoft Azure IoT Suite[18] qui regroupe plusieurs services de l'environnement Azure avec des extensions personnalisées en tant que solutions préconfigurées pour faciliter la mise en route de projets IoT. Ces solutions préconfigurées[19] - à l'image des solutions de surveillance à distance/pilotage à distance et de la maintenance prédictive - constituent des implémentations de base des modèles de solution IoT courants qui ont séduit Litware 369 notamment, au-delà des fonctionnalités et capacités proposées, vis-à-vis de la réduction du temps de mise à disposition d'une solution IoT, fondation de la nouvelle gamme d'alarmes connectées de l'entreprise.

> **Remarque importante** Ce livre blanc ne s'intéresse pas aux traitements de données associés aux alarmes connectées mis en place.

Un identifiant client est généré dans la base Clients pour l'accès sur le portail Clients de Litware 369. Cette base est hébergée par le même serveur SQL Server interne. Le portail Clients consiste également en une autre application déployée dans l'environnement Azure à l'aide du service Azure App Service. La base de données est accessible comme précédemment au travers des connexions hybrides d'Azure App Service.

Ce portail Clients accessible depuis le site web institutionnel de Litware 369 nécessite une authentification des clients. Pour cela, le numéro de téléphone sert par défaut pour l'identification ; un mot de passe est généré lors du premier accès (Cf. étape suivante). Cette génération s'appuie sur une

[18] Azure IoT Suite : https://www.microsoft.com/fr-fr/internet-of-things/azure-iot-suite

[19] QUE SONT LES SOLUTIONS PRECONFIGUREES AZURE IOT SUITE ? : https://docs.microsoft.com/fr-fr/azure/iot-suite/iot-suite-what-are-preconfigured-solutions

vérification de la personne au travers de la saisie d'un code d'activation du compte : la première partie du code est envoyée par SMS au numéro de téléphone, la seconde par courriel à l'adresse de messagerie précisée lors de la commande.

Enfin, cette étape du traitement comprend une extraction journalière des commandes terminées. Cette extraction génère automatiquement sous forme de formulaires Word les commandes terminées et les insère dans une bibliothèque SharePoint Online de Litware 369.

Ceci nous amène à la quatrième étape du traitement.

Activation du service

Lors de quatrième étape et dernière étape du traitement, les formulaires Word sont ensuite traités par le service Abonnements de Litware 369.

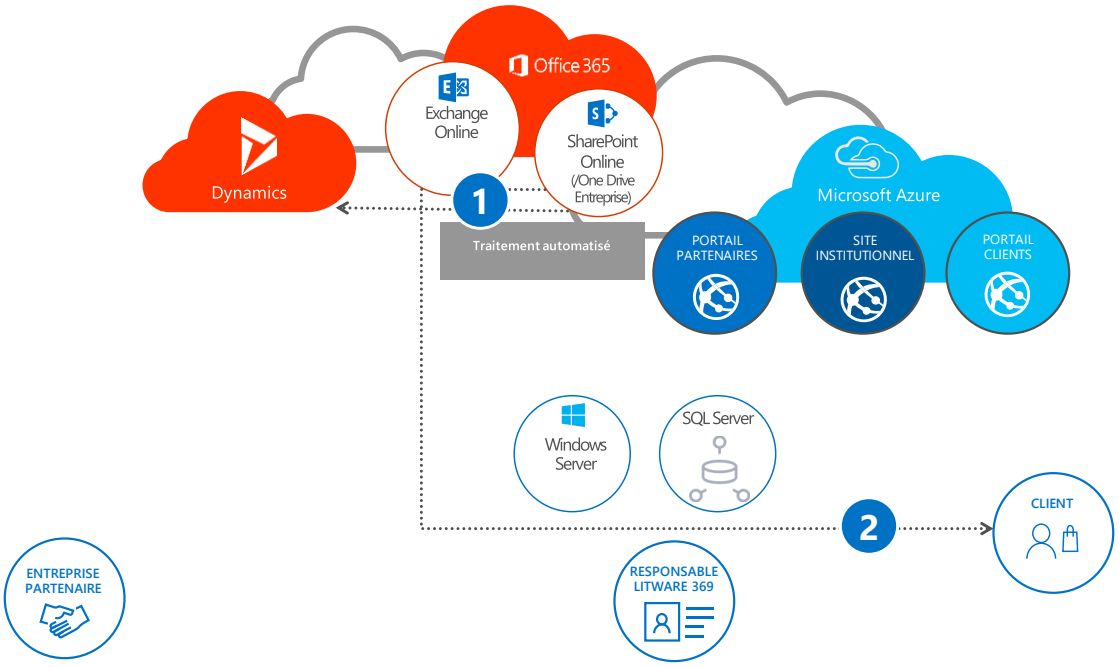

Figure 4 Vue d'ensemble de l'activation du service

Un nouveau compte client et un nouveau contrat sont créés dans Dynamics 365 pour la facturation de l'offre d'alarme connectée souscrite, le suivi de contrat, etc.

Un courriel de confirmation est envoyé au client avec toutes les informations de connexion pour gérer son abonnement et les demandes associées. Comme souligné à l'étape précédente, le numéro de téléphone sert par défaut d'identifiant. Le courriel comprend une demande de RIB pour la facturation.

Ceci conclut la description du traitement de données qui doit se conformer aux objectifs et exigences du GDPR.

Prendre des dispositions pour la mise en conformité

Activités pour la mise en conformité du traitement

La mise en œuvre d'un programme GDPR dans le cheminement vers la conformité avec le GDPR fait ressortir typiquement 4 étapes principales dans le cadre des processus et Framework qui en découlent :

1. **DECOUVRIR**. Identifier les données personnelles dont vous disposez et où celles-ci résident ;
2. **GERER**. Gouverner l'accès et l'utilisation des données personnelles ;
3. **PROTEGER**. Prévenir, détecter et répondre aux vulnérabilités et aux violations de données personnelles ;
4. **RAPPORTER**. Maintenir la documentation requise, et gérer les demandes relatives aux données personnelles et les notifications de violation.

Comme la portée et l'ampleur d'un programme GDPR diffèrent d'une organisation à une autre, Litware 369 a effectué préalablement au travers de l'outil **«** GDPR Assessment »[20] une autoévaluation sur son niveau global de maturité au regard de son contexte et des principales exigences du GDPR.

Cet outil sous forme de questionnaire est gratuit, disponible en ligne et fournit un Benchmark selon les 4 étapes principales précédentes. Il précise, le cas échéant, les solutions Microsoft susceptibles d'aider à répondre à ces exigences. Nous allons y revenir dans la suite de ce livre blanc.

Par ailleurs, et au-delà de la dimension technologique des choses (qui représente généralement moins de 20 % de l'ensemble), les activités élémentaires associées à ces étapes principales sont à intégrer selon l'approche qui convient le mieux à l'entreprise (et ses pratiques de type Agile ou non dans la conduite de ses programmes et projets).

Nous suggérons et détaillons une approche programmatique dans le livre blanc GDPR – S'organiser et mettre en place les bons processus pour la mise en conformité au GDPR[21]. Le programme ainsi proposé repose sur une approche multicycle sur la base d'un modèle PDCA (PLAN-DO-CHECK-ADJUST) qui nous parait apporter une pertinence certaine dans ce contexte.

[20] GDPR Assessment : https://www.gdprbenchmark.com/

[21] GDPR – S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR : https://aka.ms/GDPRprocess

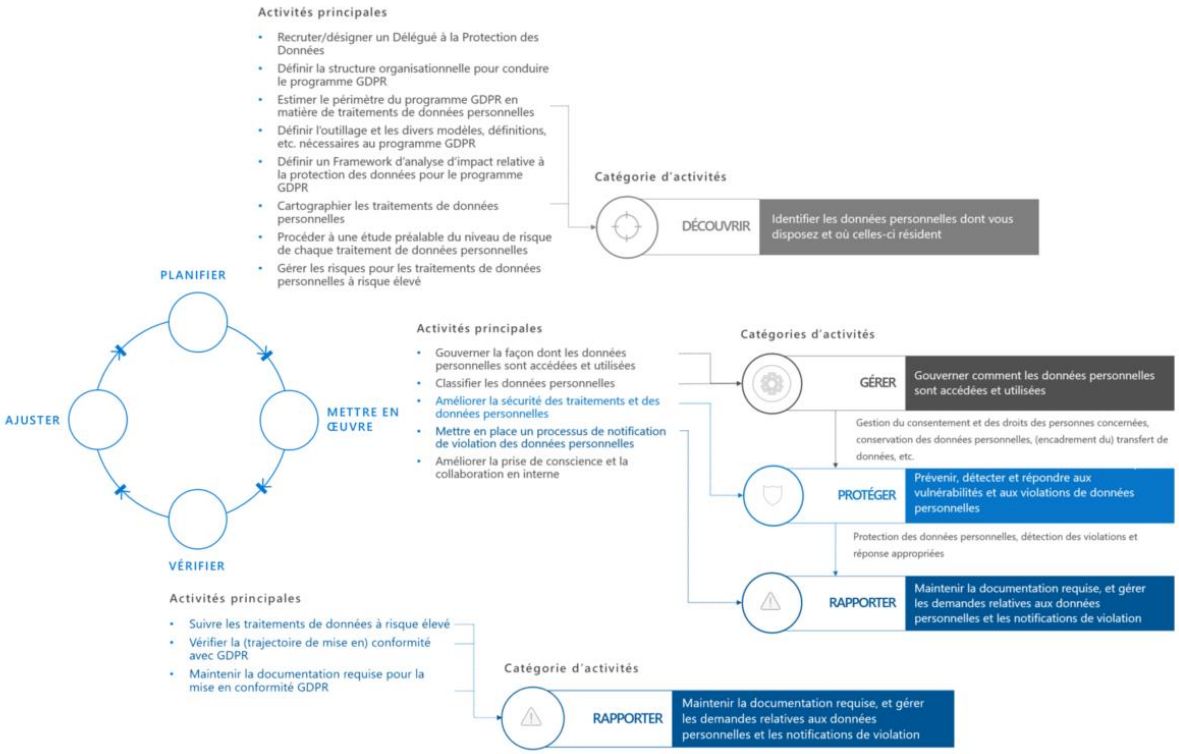

Figure 5 Vue consolidées des activités principales à conduire lors d'un cycle PDCA et regroupement par grandes catégories

Les étapes principales précédentes (et leur activité(s) élémentaire(s)) s'intègrent naturellement dans les phases de ce modèle PDCA : **PLANIFIER**, **METTRE EN ŒUVRE**, **VERIFIER** et **AJUSTER**.

La suite du livre blanc reprend donc cette articulation de façon à mettre en perspective des exemples de produits, de (fonctionnalités offertes par des) services de cloud et de ressources de Microsoft qui peuvent être utilisés et le déroulé d'un programme GDPR et des activités qui sont typiquement conduites dans ce contexte.

Ces exemples sont utilisés pour répondre aux objectifs et exigences de chacune de ces étapes principales dans le cheminement vers la conformité avec le GDPR vis-à-vis de notre scénario « représentatif » de traitement de données personnelles précédent. Chaque étape principale est abordée dans une section spécifique. Commençons donc par la première étape, à savoir la découverte des données personnelles.

Découvrir - Identifier les données personnelles dont vous disposez et où celles-ci résident

Cette première étape principale de découverte des données personnelles se traduit en tant qu'un ensemble d'activité(s) de la phase **PLANIFIER** (du modèle PDCA) du programme GDPR suggéré par le livre blanc GDPR – S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR.

A ce stade, nous supposons que plusieurs activités de cette phase **PLANIFIER** ont déjà été menées pour s'assurer de :

- La nomination et l'entrée en fonction, le cas échéant, d'un délégué à la protection des données au sein de Litware 369 ;
- De la mise en place de la structure organisationnelle du programme GDPR conformément aux objectifs et processus nécessaires à la réalisation des résultats attendus, dûment établis ;
- La définition de l'outillage et des différents modèles nécessaires à la conduite du programme GDPR ;
- La détermination et la priorisation du portefeuille des traitements de données personnelles (incluant les services, applications et dépôts associés).

Dans le scénario qui nous intéresse, le périmètre se trouve volontairement réduit à un traitement dont la finalité, les principes et les différentes composantes ont déjà été décrits. Cette première cartographie inclut le traitement, les lieux de stockage des données personnelles et la gestion de leur cycle de vie. On dispose également d'une vision sur les contrôles mis en place pour leur protection ; ce qui permettra dans les étapes suivantes de s'assurer que ceux-ci sont suffisants et correctement utilisés pour garantir la conformité avec le GDPR.

Cependant, il reste nécessaire de valider le caractère exact et complet de la connaissance au regard de l'implémentation réalisée ainsi que son utilisation réelle au sein de la société Litware 369. En effet, l'une des exigences du GDPR est de s'assurer que la description des activités dans le Registre des traitements est à jour, et que les mesures de sécurité techniques et organisationnelles mises en place sont effectives et correctement décrites.

Intéressons-nous dans un premier temps à la pertinence et à la complétude de la cartographie disponible pour le scénario « représentatif » de traitement.

Compléter la cartographie réalisée

L'identification des données personnelles collectées, stockées et traitées par une organisation comme Litware 369, et par voie de conséquence la connaissance fine des activités de traitement associées, constitue un préalable afin de se conformer aux objectifs et exigences du GDPR.

Il s'agit donc d'inventorier les données personnelles et cartographier les activités de traitement de façon précise et exhaustive en fonction des déclarations des métiers, branches, divisions, départements, entités, etc. de l'organisation voire au-delà.

Découvrir les applications cloud dans votre environnement et bénéficier d'une visibilité approfondie sur l'activité des utilisateurs

Cette section se concentre sur le scenario d'utilisation de dépôts Box, Dropbox, etc. pour transmettre les commandes aux entreprises partenaires. Il s'agit, comme évoqué précédemment, d'une déviation par rapport au déroulé du traitement envisagé.

Souscrire un abonnement et utiliser une application dans le cloud est plus facile que jamais et diverses entités dans les entreprises comme Litware 369 évitent leurs services informatiques lorsque ceux-ci ne sont pas assez à l'écoute et/ou réactifs. De ce fait, ces entités couvrent leur(s) besoin(s) métier avec des applications dans le cloud qui ne sont pas alors gérées de manière centralisée. Cette « informatique fantôme » ou « Shadow IT » soulève inévitablement un certain nombre de défis en matière de sécurité, de protection de la vie privée et les paradigmes de sécurité classique en matière de sécurité périmétrique se trouvent ébranlés... (L'article HOW SAAS ADOPTION IS CHANGING CLOUD SECURITY[22] constitue à cet égard un angle de regard intéressant.)

L'objectif est d'identifier cette dimension « Shadow IT », les applications et risques afférents, pour maîtriser ces actifs « non-identifiés » concernés par le GDPR.

Pour protéger des données personnelles, il faut d'abord les identifier de façon exhaustive. Dans la pratique, il n'existe aucun moyen de disposer de la visibilité pour mettre en œuvre les contrôles nécessaires des applications (et donc les traitements et les données personnelles afférentes) pour lesquelles une organisation comme Litware 369 ne dispose d'aucune capacité de contrôle. Comme le souligne le billet WHY YOU NEED A CASB FOR GDPR COMPLIANCE[23], il s'avère donc nécessaire de « faire sortir de l'ombre » ces applications concernées.

Cela implique de pouvoir identifier les données personnelles en transit et au repos pour une large palette d'applications dans le cloud, d'évaluer les risques en fonction des sous-traitants identifiés et, finalement, de contrôler les flux de données personnelles et les transferts de données.

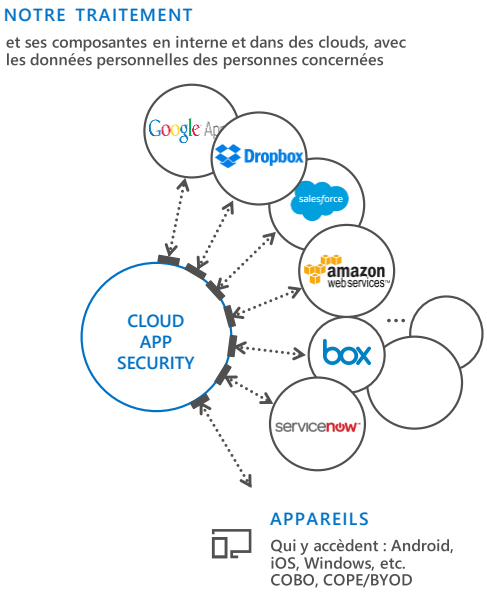

Figure 6 Découvrir les applications cloud avec Cloud App Security

Dans ce contexte, Cloud App Security[24] permet de découvrir, sans qu'aucun agent ne soit nécessaire, toutes les applications dans le cloud de l'environnement de Litware 369, grâce à la fourniture, par l'équipe d'analystes Microsoft d'un catalogue en constante évolution de plus de 15 000 applications du

[22] HOW SAAS ADOPTION IS CHANGING CLOUD SECURITY : http://www.darkreading.com/perimeter/how-saas-adoption-is-changing-cloud-security-/a/d-id/1316015

[23] WHY YOU NEED A CASB FOR GDPR COMPLIANCE: https://blog.cloudsecurityalliance.org/2017/04/04/need-casb-gdpr-compliance/

[24] SECURITE DE QUALITE PROFESSIONNELLE POUR VOS APPLICATIONS CLOUD : https://www.microsoft.com/fr-fr/cloud-platform/cloud-app-security

cloud. Il est également possible d'identifier les utilisateurs de ces applications ainsi que l'utilisation qui est faite. Un score de risque est obtenu pour chaque application permettant leur évaluation au regard des certifications et accréditations réglementaires, des normes du secteur et autres bonnes pratiques. Cette évaluation des risques permet d'autoriser ou non l'accès des utilisateurs à ces applications. Autrement dit, il est possible d'utiliser Cloud App Security comme Litware 369 pour identifier l'utilisation d'applications dans votre organisation grâce à ce catalogue, d'analyse les risques encourus sur la base de plus de 60 critères objectifs renseignés et ensuite de refuser le cas échéant l'usage de ces applications via la définition de scripts à destination des équipements réseaux de l'organisation.

Remarque Pour plus d'informations, vous pouvez consulter l'article QU'EST-CE QUE CLOUD APP SECURITY ?[25] et visionner les webinaires INTRODUCING MICROSOFT CLOUD APP SECURITY[26] et GET VISIBILITY, DATA CONTROL AND THREAT PROTECTION WITH MICROSOFT CLOUD APP SECURITY[27].

Identifier facilement des données

Pour poursuivre avec l'identification des données, cette section étudie scénario de l'usage de SharePoint Online si celui-ci n'est pas été répertorié précédemment établie.

Maîtriser les actifs comme SharePoint Online avec Cloud App Security

Dans la continuité de ce qui a été ci-avant, Cloud App Security propose un ensemble de connecteurs d'application pour intégrer la solution à des applications dans le cloud à l'image d'Office 365 dans le cas qui nous intéresse ici. Les connecteurs d'application utilisent les API des fournisseurs d'application cloud et étendent le contrôle et la protection. Ils donnent aussi accès aux informations directement à partir de ces applications dans le cloud, pour une analyse par Cloud App Security.

Dès lors, Cloud App Security offre la visibilité, le contrôle et la protection contre les menaces pour les données stockées dans ces applications. Il est possible de configurer la sécurité dans le cloud en définissant des stratégies et en les mettant en œuvre dans les applications et solutions de cloud de tiers et de Microsoft. Pour finir, lorsque Cloud App Security détecte une anomalie, vous recevez une alerte.

Identifier rapidement les données personnelles dans Office 365 avec la découverte électronique (eDiscovery) (avancée)

Au-delà de cette intégration avec Office 365, nous souhaitons souligner que l'environnement Office 365 en la matière « n'est pas en reste ». Ainsi, par exemple, la fonctionnalité de recherche de la découverte électronique (eDiscovery) d'Office 365[28] peut être utilisée pour rechercher du texte et des métadonnées dans les ressources Office 365 (SharePoint Online, OneDrive Entreprise, Skype Entreprise Online et Exchange Online) de Litware 369.

En outre, grâce aux technologies d'apprentissage automatique (Machine Learning, une des branches de l'IA), la découverte électronique (eDiscovery) avancée permet d'identifier rapidement les documents pertinents pour un sujet spécifique (par exemple, une commande en cours) avec une meilleure précision

[25] QU'EST-CE QUE CLOUD APP SECURITY ? : https://docs.microsoft.com/fr-fr/cloud-app-security/what-is-cloud-app-security

[26] INTRODUCING MICROSOFT CLOUD APP SECURITY : https://youtu.be/DyUmFWfJQvU

[27] GET VISIBILITY, DATA CONTROL AND THREAT PROTECTION WITH MICROSOFT CLOUD APP SECURITY : https://youtu.be/zPS1_WuGSW8

[28] Solutions de conformité Office 365 : https://products.office.com/fr-fr/business/compliance-tools-ediscovery

qu'à l'aide de la recherche de mots clés traditionnelle ou d'un examen manuel d'un grand nombre de documents.

Remarque Pour plus d'informations, vous pouvez consulter le billet REDUCE EDISCOVERY COSTS AND CHALLENGES WITH OFFICE 365 ADVANCED EDISCOVERY[29] et visionner le webinaire OFFICE 365 ADVANCED EDISCOVERY[30].

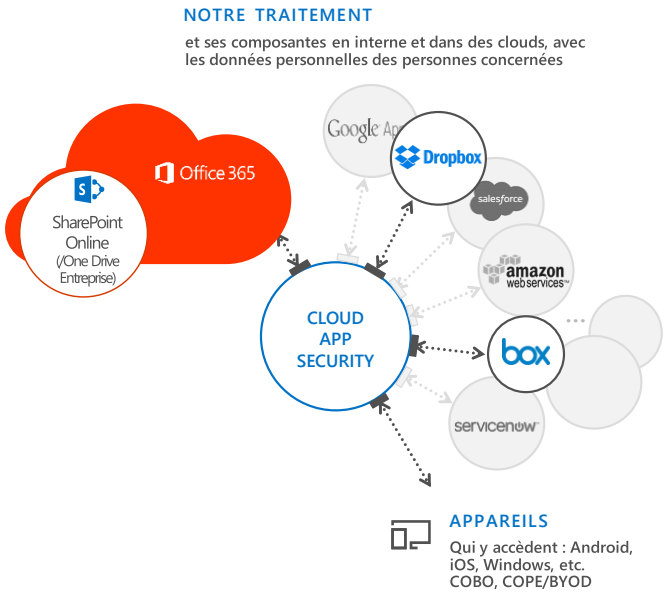

Figure 7 Identifier les données de SharePoint Online avec Cloud App Security et la Gouvernance évoluée des données d'Office 365

Mettre à jour le Registre des traitements

Les étapes précédentes ont permis à Litware 369 de s'assurer de la réalité du traitement en termes d'implémentation et donc de pouvoir mettre à jour les données d'inventaire.

Cet inventaire est consigné dans une fiche de traitement et contient, en accord avec l'article 30, les éléments d'information suivants :

- **Pour le responsable de traitement et les sous-traitants**, c'est-à-dire, Microsoft pour les services de cloud Azure, Dynamics 365 et Office 365 ainsi que le réseau d'entreprises partenaires en France (pour l'installation de ses systèmes d'alarmes, la mise en place des services et options souscrites, le suivi du service, etc.) :
    - Le nom et les coordonnées du responsable de traitement / sous-traitant, ainsi que les représentants, notamment le délégué à la protection des données s'il y en a ;
    - Le cas échéant, les éventuels transferts de données personnelles vers des pays tiers avec le nom du pays et la documentation des moyens mis en œuvre pour protéger les données si le transfert est fondé sur des motifs légitimes. Ceci concerne dans notre illustration les services Cloud de Microsoft. (Cf. section suivante) ;

[29] REDUCE EDISCOVERY COSTS AND CHALLENGES WITH OFFICE 365 ADVANCED EDISCOVERY : https://blogs.office.com/2015/12/10/reduce-ediscovery-costs-and-challenges-with-office-365-advanced-ediscovery/

[30] OFFICE 365 ADVANCED EDISCOVERY : https://youtu.be/yPEGF3Auw_M

- Une description générale des mesures de sécurité sur les plans techniques et organisationnels (si applicable). Sont précisées dans ce contexte les différentes mesures illustrées dans la section § ETAPES DU SCENARIO DE TRAITEMENT vis-à-vis des 4 grandes étapes envisagées du traitement.

- **Pour le responsable de traitement** :
  - L'objectif du traitement, ici, la collecte des commandes d'abonnement et leur traitement en vue de la mise en place du service pour l'alarme connectée sélectionnée et ses options ;
  - Les catégories de personnes concernées, ici les contacts et (futurs) clients pour l'offre ainsi souscrite ;
  - Les catégories de données personnelles, ici lors de la prise de commande, notamment les nom, prénom, adresse complète, et numéro de téléphone ;
  - Les destinataires d'un traitement de données, ici le futur client et l'entreprise partenaire qui réalise la qualification, l'installation et la mise en service de l'offre souscrite ;
  - Les périodes de rétention (là où c'est applicable).
- **Pour chaque sous-traitant** :
  - Les noms et détails contractuels de chaque sous-traitant dans la chaine de sous-traitance ainsi que le type de traitement qui est effectué par chaque sous-traitant (Cf. section suivante).

La notion de fiche de traitement est abordée dans le livre blanc GDPR – S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR déjà mentionné.

Dans le cadre du programme GDPR mis en place par Litware 369, le Registre des traitements se matérialise sous la forme d'une bibliothèque SharePoint Online. Cette bibliothèque fait partie d'un environnement de gestion de programme constitué sur la base de la souche logicielle « GDPR Activity Hub[31] » mise à disposition en open source par Microsoft sur la forge communautaire GitHub pour aider les organisations à démarrer et à avancer dans leur cheminement vers la conformité avec le GDPR.

Cette souche vise ainsi à donner aux organisations une base leur permettant de conserver une trace de l'ensemble des activités principales, des tâches associées, des événements essentiels, des demandes reçues, etc. pour le respect des exigences GDPR.

Mettre à jour le Registre (des risques) des sous-traitants

Comme souligné ci-avant, les étapes précédentes ont également permis à Litware 369 de préciser les informations relatives aux sous-traitants et tiers intervenant dans le traitement servant d'illustration.

Litware 369 s'appuie sur la souche logicielle précédente « GDPR Activity Hub » pour également matérialiser la notion de Registre (des risques) des sous-traitants.

La fiche de traitement renseignée à la section précédente permet à Litware 369 d'identifier et de passer en revue l'ensemble des contrats des sous-traitants et d'imposer que ceux-ci prennent en considération le GDPR avec les obligations et responsabilités qui incombent désormais aux sous-traitants. On parle de coresponsabilité ou de responsabilité partagée.

[31] GDPR Activity Hub : https://github.com/SharePoint/sp-dev-gdpr-activity-hub

Cela suppose donc pour Litware 369 de s'assurer de la présence de clauses contractuelles en matière de sécurité et de protection des données personnelles. Ainsi, pour cela et ce qui est de Microsoft comme sous-traitant identifié, Litware 369 peut de façon non-exhaustive pour les services Cloud Azure, Dynamics 365 et Office 365 utilisés dans le cadre du traitement :

- S'appuyer sur les ressources de la section GDPR[32] du Centre de confiance (Trust Center) Microsoft vis-à-vis des services de cloud considérés ;
- Revoir les termes des services en ligne[33] (Online Services Terms en Anglais ou OST) associés ;
- Statuer sur l'emplacement de données pour ces services, comme par exemple pour Office 365[34] dans le cadre de l'utilisation faite par le service Abonnement de Litware 369 et les éventuels transferts de données personnelles vers des pays tiers, Cf. page EMPLACEMENT DE VOS DONNEES[35] sur le Centre de confiance (Trust Center) Microsoft ;

  Dans la pratique, les clients qui souhaitent ou doivent maintenir leurs données dans un emplacement géographique spécifique, comme au sein de l'Union Européenne pour Litware 369, peuvent compter sur l'infrastructure globale de centres de données Microsoft à travers le monde. Microsoft se conforme aux lois internationales de protection des données en ce qui concerne les transferts de données des clients à travers les frontières ;

Remarque Microsoft et ses filiales aux États-Unis se conforment au cadre juridique du « EU-U.S. Privacy Shield » concernant la collecte, l'utilisation et la rétention des informations transférées de l'Union Européenne vers les États-Unis, Cf. communiqué MICROSOFT AND THE UE-U.S. PRIVACY SHIELD.

En effet, suite à l'invalidation du « Safe Harbor » en octobre 2015 dernier, le Groupe de l'Article 29 a défini avec le Département du Commerce des Etats-Unis un nouveau cadre réglementaire, le « EU-U.S. Privacy Shield », qui encadre les flux de données entre l'Europe et les Etats-Unis sur des bases juridiques solides.

Ce nouveau cadre, adopté par la Commission Européenne le 12 juillet 2016, offre plus de transparence, un meilleur contrôle et des possibilités de recours accrues vis-à-vis de son prédécesseur. Ainsi, ce cadre garantit aux européens le droit au redressement judiciaire, renforce le rôle des autorités de protection des données, présente un organe de contrôle indépendant, et il clarifie les pratiques de collecte de données par les agences de sécurité américaines. En outre, il présente de nouvelles règles pour la conservation et le transfert ultérieur des données. Autre point important, les principales dispositions de ce cadre s'étendent aux autres mécanismes de transfert, tels que les Clauses contractuelles types de l'Union européenne (UE).

- Passer en revue les rapports relatifs aux vérifications effectuées au moins chaque année vis-à-vis de plusieurs normes globales de protection de données, comprenant plusieurs normes ISO/IEC, le Registre STAR de la CSA (Cloud Security Alliance), HIPAA et HITECH. Ces rapports sont accessibles à l'adresse https://servicetrust.microsoft.com/Documents/ComplianceReports.

Litware 369 doit, par ailleurs, contractualiser avec l'ensemble de son réseau d'entreprises partenaires qui constitue de fait autant de sous-traitants. Il s'agit là aussi de s'assurer que tous ces partenaires offrent les nécessaires garanties en la matière quant aux exigences de GDPR.

Tous ces éléments sont consignés par sous-traitant dans le Registre (des risques) des sous-traitants.

---

[32] THE GENERAL DATA PROTECTION REGULATION (GDPR) : https://www.microsoft.com/GDPR

[33] Licensing Terms and Documentation : http://go.microsoft.com/?linkid=9840733

[34] WHERE IS MY DATA? : http://o365datacentermap.azurewebsites.net/

[35] EMPLACEMENT DE VOS DONNEES : https://www.microsoft.com/fr-fr/trustcenter/privacy/where-your-data-is-located

Mettre en place un catalogue des données

La cartographie des traitements constitue, par ailleurs, l'opportunité pour Litware 369 de décloisonner ses différents « silos applicatifs » et dépôts de données en établissant, au sein de l'entreprise, les bases d'un véritable catalogue des données. Pour se faire, Litware 369 a décidé de s'appuyer sur le service Cloud Azure Data Catalog[36].

Azure Data Catalog est un service de cloud qui permet à une organisation comme Litware 369 de mieux exploiter les investissements existants, à l'image de son environnement local SQL Server. Ce service inclut pour cela un modèle de crowdsourcing de métadonnées et des annotations pour le référencement de sources données. Il centralise l'ensemble des éléments qui permettent aux utilisateurs d'une organisation de partager leurs connaissances et de créer une communauté et une culture des données. Ainsi, n'importe quel utilisateur (analyste, scientifique de la donnée ou développeur) peut détecter, comprendre et utiliser des sources de données.

> **Remarque** Pour plus d'informations, vous pouvez consulter l'article QU'EST-CE QU'AZURE DATA CATALOG ?[37].

Exemples de solutions

La mise à jour de la cartographie du scénario « représentatif » de traitement montre comment Cloud App Security ainsi que la découverte électronique (eDiscovery) (avancée) dans Office 365 contribuent à renforcer la connaissance du traitement et la pertinence de sa cartographie.

La découverte des données personnelles d'une façon générale et non pas uniquement vis-à-vis du cadre restreint de notre illustration peut tirer parti d'autres produits et solutions de cloud de Microsoft.

> **Remarque** Le livre blanc LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES[38] propose des exemples d'actions à entreprendre avec Microsoft dès aujourd'hui pour entamer votre cheminement vers la conformité avec le GDPR. Vous pouvez consulter ce livre blanc pour une illustration des mesures à prendre dans ce contexte pour l'étape principale de découverte des données personnelles et la façon les produits et services de cloud de Microsoft peuvent contribuer à la mise en œuvre (ou à la traduction effective) de celles-ci.

Ceci clôt notre « exploration » de la première étape principale. Passons donc à la seconde.

[36] Azure Data Catalog : https://azure.microsoft.com/fr-fr/services/data-catalog/

[37] QU'EST QU'AZURE DATA CATALOG : https://docs.microsoft.com/fr-fr/azure/data-catalog/data-catalog-what-is-data-catalog

[38] LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES : https://aka.ms/gdprwhitepaper

Gérer - Gouverner comment les données personnelles sont accédées et utilisées

Cette étape de gestion des données personnelles se traduit en tant qu'un ensemble d'activité(s) de la phase **METTRE EN OEUVRE** (du modèle PDCA) du programme GDPR suggéré par le livre blanc GDPR – S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR.

A ce stade, nous supposons que plusieurs activités des phases **PLANIFIER** et **METTRE EN OEUVRE** ont été menées pour s'assurer que :

- La cartographie à jour du (scénario « représentatif » de) traitement a été effectuée avec les flux de données personnelles et la description des contrôles mis en place ;
- La fiche descriptive du traitement a été construite et insérée dans le Registre des traitements ;
- Une étude préalable a été conduite et la décision a été prise de ne **pas** procéder à une analyse d'impact relative à la protection des données (Data Protection Impact Analysis en anglais ou DPIA) comme aucun des critères nécessitant une telle analyse n'ont été associés au traitement (traitement à grande échelle, catégories de données particulièrement sensibles, profilage, etc.).

L'étude préalable a par ailleurs permis de définir un ensemble d'actions et de mesures qu'il convenait de conduire et de prendre afin d'inscrire le traitement qui nous intéresse dans une trajectoire de cheminement vers la conformité avec le GDPR.

Il s'agit en particulier d'assoir un plan complet de gouvernance des données personnelles avec la définition des politiques, des rôles et des responsabilités pour la gestion et l'utilisation des données personnelles selon leurs type(s) et sensibilité(s). La gouvernance des données personnelles s'intéresse à la façon dont les données sont accédées et utilisées.

Cela implique donc une connaissance des données et suppose donc de s'intéresser à la classification et à la labélisation des données. Nous supposons ici que Litware 369 dispose déjà d'une taxonomie de classification adaptée sur laquelle la société peut reposer.

Classifier et labeliser les données personnelles

Une fois le traitement de données dûment cartographié et les données personnelles identifiées, l'objectif poursuivi consiste à les organiser et labéliser de façon à i) permettre l'identification des données personnelles dans les dépôts de données, et ii) appliquer les mesures de sécurité qui s'imposent, le tout en fonction des type(s) et sensibilité(s).

Cette section examinera le scénario de traitement des données semi-structurées ou non structurées, à savoir :

- Le serveur de fichiers Windows Server avec les fichiers CSV ;
- Les courriels générés depuis le composant logiciel enfichable (add-in) Outlook.

Labéliser les données personnelles avec Azure Information Protection dans un monde hybride

Azure Information Protection[39] contribue à garantir que les données personnelles de Litware 369 sont identifiables de façon à pouvoir les sécuriser en conséquence, selon leurs type(s) et sensibilité(s) - ce

[39] Azure Information Protection : https://www.microsoft.com/fr-fr/cloud-platform/azure-information-protection

qui est une exigence clé du GDPR – et ce, peu importe leur emplacement de stockage ou la façon dont elles sont partagées.

Azure Information Protection permet de classifier, labéliser conformément à la classification établie au sein de l'organisation et le cas échant, selon la stratégie appliquée, de protéger les données nouvelles ou existantes (Cf. section § FAIRE RESPECTER DES POLITIQUES DE PROTECTION DES DONNEES).

> **Remarque** Pour plus d'informations, vous pouvez visionner les webinaires AN INTRODUCTION TO MICROSOFT AZURE INFORMATION PROTECTION[40] et LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION[41].

Les opérations précédentes peuvent être réalisées lors de la création de ces données avec Office ou bien, vis-à-vis de données existantes, par exemple directement au niveau du serveur de fichiers Windows Server pour les fichiers CSV des nouvelles commandes passées.

Dans ce second cas, un ensemble de cmdlets PowerShell[42] permet de réaliser très facilement en ligne de commande les opérations au niveau d'un dossier pour appliquer un même label pour ces commandes.

Une fonction de type « scanner » sera disponible très prochainement afin de permettre une scrutation des diverses ressources du réseau interne (ainsi que les sites SharePoint Server en local) de l'organisation pour appliquer les labels de classification qui s'imposent selon les données personnelles considérées.

Utiliser le Data Classification Toolkit pour le serveur de fichiers

Le kit d'outillage de classification des données[43] (Data Classification Toolkit en anglais) peut être utilisé de façon alternative. En effet, ce kit est conçu afin de permettre à une société comme Litware 369 d'identifier, de classifier et de protéger les données personnelles sur ses serveurs de fichiers Windows Server. Des exemples de classification et de règles en matière de recherche d'expressions (régulières) aident les organisations à générer et à déployer leurs politiques visant à protéger ces informations sur leurs serveurs de fichiers Windows Server.

> **Remarque** Pour plus d'informations, vous pouvez consulter les articles DATA CLASSIFICATION TOOLKIT[44] et IMPORTANT INFORMATION ABOUT THE DATA CLASSIFICATION TOOLKIT[45].

Faire respecter des politiques pour les données personnelles

Quelle que soit l'approche retenue, les labels sont ensuite pris en compte pour l'application des stratégies en matière de gestion et/ou de protection.

Ainsi, dans notre illustration, et pour poursuivre avec le serveur de fichiers, le contrôle d'accès dynamique[46] (Dynamic Access Control en anglais ou DAC), fondé sur le domaine, permet d'appliquer des autorisations de contrôle d'accès et des restrictions basées sur des règles qui peuvent inclure les labels

---

[40] AN INTRODUCTION TO MICROSOFT AZURE INFORMATION PROTECTION : https://youtu.be/N9Ip0m6d3G0

[41] LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION : https://youtu.be/ccBus_Yx69g

[42] PowerShell : https://msdn.microsoft.com/en-us/powershell/mt173057.aspx

[43] Data Classification Toolkit for Windows Server 2012 R2 : http://go.microsoft.com/fwlink/p/?LinkId=226045

[44] DATA CLASSIFICATION TOOLKIT : https://msdn.microsoft.com/en-us/library/hh204743.aspx

[45] IMPORTANT INFORMATION ABOUT THE DATA CLASSIFICATION TOOLKIT : https://msdn.microsoft.com/en-us/library/hh367453.aspx

[46] DYNAMIC ACCESS CONTROL OVERVIEW : https://docs.microsoft.com/en-us/windows/access-protection/access-control/dynamic-access-control

précédents. Par ailleurs, à l'aide de l'Explorateur de fichiers Windows ou de PowerShell, il est possible de restreindre le traitement des données personnelles en révoquant l'accès aux fichiers contenant les données personnelles cibles.

S'intégrer avec d'autres solutions

Il s'agit de pouvoir s'intégrer avec des fonctionnalités ou solutions de protection contre la perte de données (Data Loss Prevention en anglais ou DLP), de type CASB (Cloud Access Security Broker en anglais), etc.

Ainsi, dans notre illustration, les stratégies de protection contre la perte de données[47] dans Office 365 permettent aux entreprises comme Litware 369 de configurer, sur la base des labels précédents, des mesures à prendre afin de protéger les informations sensibles et d'empêcher leur divulgation accidentelle.

> **Remarque** Les stratégies de protection contre la perte de données dans Office 365 permettent également d'identifier plus de 80 types de données sensibles courants,[48] y compris les informations d'identification personnelle.

De même, Cloud App Security abordé précédemment avec la détection d'applications dans le cloud dans un contexte de « Shadow IT » contribue, en ce qui concerne le contrôle des données personnelles, à modeler l'environnement cloud de Litware 369 avec l'utilisation de stratégies personnalisées ou prêtes à l'emploi pour le partage de données, ainsi que pour la protection contre la perte de données. Ces stratégies peuvent bien évidemment reposer sur l'exploitation des labels précédents pour les données concernées.

Ainsi, la classification définie par l'entreprise à travers Azure Information Protection peut être utilisée par Cloud App Security, par le biais de l'intégration entre ces deux services. Cloud App Security s'appuie alors sur les labels de classification pour détecter, dans les applications cloud qu'il contrôle, les fichiers sensibles contenant par exemple des données personnelles entrant dans le périmètre du GDPR. Cloud App Security offre par là-même une vision centralisée des fichiers labelisés sensibles ainsi que leur emplacement. A travers l'utilisation de filtres, il est possible de rechercher les fichiers qui ne respecteraient pas les politiques de l'entreprise. Par exemple, il est possible de créer un filtre permettant d'obtenir la liste des fichiers avec un label « Données personnelles » qui seraient stockés sur OneDrive, Box ou Dropbox, en contradiction avec les politiques de sécurité[49].

De plus, l'intégration avec le service de protection d'Azure Information Protection, en l'occurrence Azure Rights Management, permet d'appliquer une protection sur les fichiers détectés comme sensibles – ici au sens de GDPR et non pas de l'organisation - selon leur label que ce soit manuellement depuis le portail de Cloud App Security ou de manière automatique par l'utilisation de règles[50].

---

[47] VUE D'ENSEMBLE DES STRATEGIES DE PROTECTION CONTRE LA PERTE DE DONNEES : https://support.office.com/fr-fr/article/Vue-d-ensemble-des-stratégies-de-protection-contre-la-perte-de-données-1966b2a7-d1e2-4d92-ab61-42efbb137f5e

[48] TYPES D'INFORMATIONS SENSIBLES DANS EXCHANGE 2016 : https://technet.microsoft.com/fr-fr/library/jj150541(v=exchg.160).aspx

[49] INTEGRATION D'AZURE INFORMATION PROTECTION : https://docs.microsoft.com/fr-fr/cloud-app-security/azip-integration

[50] En cours d'intégration à la date de rédaction. Disponible pour SharePoint Online et OneDrive pour Entreprise.

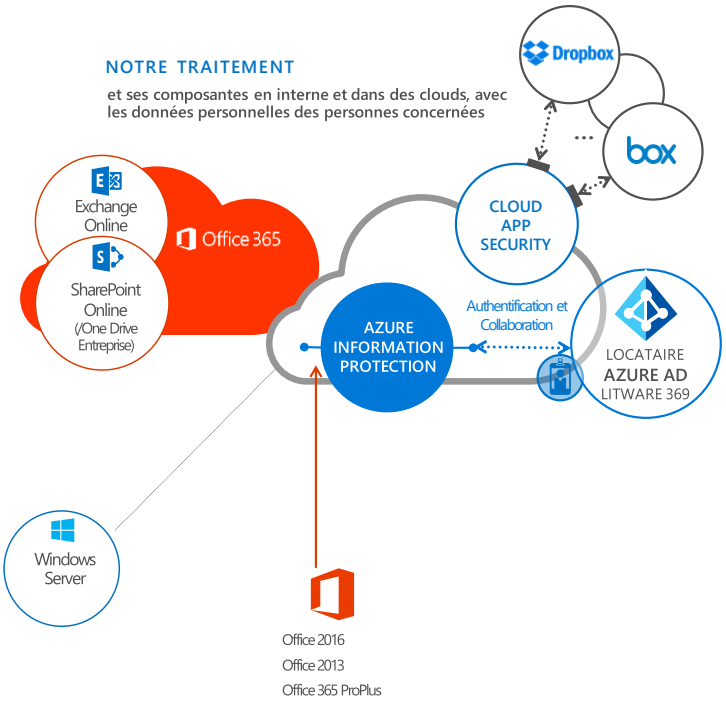

Figure 8 Labéliser les données personnelles et s'intégrer avec de multiples solutions

La section § FAIRE RESPECTER DES POLITIQUES DE PROTECTION DES DONNEES dans la suite de ce livre blanc s'intéresse spécifiquement comme son titre l'indique à l'expression de politiques pour la protection des données et à leur application en termes de contrôles des données personnelles.

> **Remarque** Pour plus d'informations, vous pouvez également consulter le livre blanc PROTECT AND CONTROL YOUR KEY INFORMATION ASSETS THROUGH INFORMATION CLASSIFICATION[51].

Pour l'instant, poursuivons « notre exploration » sur la dimension Gestion des données.

Se prémunir automatiquement contre le risque de suppression accidentelle

Dans cette section, le scénario de traitement étudié concerne la bibliothèque de formulaires Word présente dans SharePoint. Celle-ci contient les dossiers de commandes avec les caractéristiques techniques de l'installation.

La protection contre le risque de suppression accidentelle peut pleinement reposer, dans Office 365, sur l'exploitation des mécanismes de gouvernance évoluée des données. En effet, la gouvernance évoluée des données d'Office 365 tire parti des informations assistées par ordinateur pour aider Litware 369 à trouver, classifier, définir des stratégies et prendre des mesures pour gérer le cycle de vie des données essentielles pour l'entreprise.

[51] PROTECT AND CONTROL YOUR KEY INFORMATION ASSETS THROUGH INFORMATION CLASSIFICATION - CLASSIFY, LABEL, PROTECT, AND AUDIT (CLPA) YOUR KEY INFORMATION ASSETS: https://aka.ms/classify

Remarque Pour plus d'informations, vous pouvez consulter le billet ADVANCED DATA GOVERNANCE IN OFFICE 365[52] et visionner le webinaire OFFICE 365 ADVANCED DATA GOVERNANCE OVERVIEW[53].

Au-delà d'une classification automatique des données, il s'agit donc i) de pouvoir bénéficier de recommandations de stratégies intelligentes, de conservation et de disposition fondées sur du Machine Learning et ii) d'appliquer des actions pour préserver les données personnelles et nettoyer ce qui est redondant ou obsolète, avec à la clé :

- Des analyses pour détecter ce qui est important, supprimer ce qui ne l'est pas, et partager en respectant des stratégies ;
- Une journalisation des actions.

La fonctionnalité de conservation des données dans Office 365 peut ainsi aider à gérer le cycle de vie des courriels et les documents en gardant le contenu dont ici la société Litware 369 a besoin et de supprimer ce contenu lorsqu'il n'est plus nécessaire. L'un des principes énoncés par le GDPR précise qu'il est de votre responsabilité de limiter le stockage de données personnelles à la durée nécessaire à la finalité visée.

Remarque Pour plus d'informations, vous pouvez consulter l'article CONSERVATION DANS LE CENTRE DE CONFORMITE ET DE SECURITE OFFICE 365[54].

Il convient de souligner enfin la possibilité d'importer des disques, des sauvegardes, etc. de façon à bénéficier et à assurer une gouvernance (plus) globale.

Gérer les rôles et les responsabilités

Il est temps de s'intéresser à présent à la façon de définir les politiques, les rôles et les responsabilités pour la gestion et l'utilisation des données personnelles :

1. Qu'elles soient : au repos vs. en traitement vs. en transit ;
2. Et dans le cycle de vie : stockage vs. recouvrement vs. conservation (« retention ») vs. archivage vs. disposition (« disposal »).

La protection des données personnelles commence par la sécurisation des identités et le contrôle des accès en « commençant à la porte d'entrée ».

Litware 369 assure la gestion des identités et des accès (IAM) pour ses collaborateurs avec Azure Active Directory[55] (Azure AD).

Azure AD contribue à garantir que seuls les utilisateurs autorisés aient accès aux environnements informatiques, aux données et aux applications, et il fournit des outils tels que l'authentification multi-facteurs[56] pour une ouverture de session hautement sécurisée.

---

[52] ADVANCED DATA GOVERNANCE IN OFFICE 365 : https://blogs.office.com/2016/09/26/office-365-news-in-september-at-ignite-intelligence-security-collaboration-and-more/

[53] OFFICE 365 ADVANCED EDISCOVERY: https://youtu.be/dL5DF7LN07s

[54] CONSERVATION DANS LE CENTRE DE CONFORMITE ET DE SECURITE D'OFFICE 365 : https://support.office.com/fr-fr/article/R%c3%a9tention-dans-le-centre-de-conformit%c3%a9-s%c3%a9curit%c3%a9-Office-365-2a0fc432-f18c-45aa-a539-30ab035c608c

[55] Azure Active Directory: https://azure.microsoft.com/fr-fr/services/active-directory/

[56] Azure Multi-factor Authentication: https://azure.microsoft.com/fr-fr/services/multi-factor-authentication/

Remarque Pour plus d'informations, vous pouvez consulter l'article QU'EST-CE QU'AZURE ACTIVE DIRECTORY ?[57].

Dans le cadre de notre illustration, Azure AD est utilisé par les services Cloud Azure, Dynamics 365 et Office 365. Ainsi, dans Azure, au-delà du contrôle de l'accès au portail de gestion, il convient de noter qu'Azure AD permet à Litware 369 la ségrégation des rôles dans la création et la configuration des ressources des différentes charges de travail mises en œuvre avec un contrôle d'accès fondé sur les rôles (Role-Based Access Control en anglais ou RBAC)[58]. La gestion des identités privilégiées est utilisée dans ce contexte comme nous le développons par la suite.

Un déploiement existant d'Active Directory (AD) en interne constitue par ailleurs le socle local de la sécurité pour les charges de travail en local, les serveurs et les postes de travail.

Remarque Pour son déploiement d'AD, Litware 369 a mis en place très tôt, en interne, un certain nombre de mesures techniques pour sécuriser ses accès privilégiés. En matière de cyberattaques, les attaquants ciblent ces comptes et d'autres éléments de l'accès privilégié pour accéder rapidement à des données ciblées et des systèmes via le vol d'informations d'identification comme Pass-the-Hash et Pass-the-Ticket[59].

Ainsi, pour atténuer les risques, tous les employés de Litware 369 dotés de privilèges administratifs disposent d'un compte dédié pour les tâches d'administration. Ils utilisent également dans ce contexte des stations de travail à accès privilégié (Privileged Access Workstations en anglais ou PAW) qui, comme décrit dans l'article éponyme PRIVILEGED ACCESS WORKSTATIONS[60], fournissent un environnement dédié afin que les tâches sensibles soient protégées contre les attaques Internet et autres vecteurs de menace.

En outre, tous les postes de travail et les serveurs Windows de Litware 369 disposent de mots de passe aléatoires et uniques qui ont été configurés grâce à l'outil LAPS[61] (Local Administrator Password Solution) et enregistrés dans l'AD interne. Ces mots de passe sont protégés par des listes de contrôles d'accès (ACL) garantissant que seuls les utilisateurs légitimes puissent les lire ou les réinitialiser.

Toutes ces mesures permettent d'offrir un premier niveau en termes de séparation et de protection de l'administration. Pour plus d'informations, vous pouvez consulter l'article SECURISATION DE L'ACCES PRIVILEGIE[62].

Azure AD Connect[63] permet de constituer virtuellement un seul et même annuaire avec une synchronisation maitrisée des informations entre Azure AD et AD et donc de fournir une identité commune aux collaborateurs de Litware 369 pour les applications Dynamics 365 et Office 365, et autres applications (SaaS) intégrées à Azure AD. Les utilisateurs de Litware 369 ont ainsi accès à leurs ressources en interne ou dans le cloud en toute transparence et ce depuis l'intérieur ou l'extérieur de l'entreprise. Tous les accès n'en sont pas moins rigoureusement authentifiés et contrôlés.

---

[57] QU'EST-CE QU'AZURE ACTIVE DIRECTORY ? : https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-whatis

[5858] UTILISER LE CONTROLE D'ACCES EN FONCTION DU ROLE POUR GERER L'ACCES AUX RESSOURCES D'UN ABONNEMENT AZURE : https://docs.microsoft.com/fr-fr/azure/active-directory/role-based-access-control-configure

[59] Pass-the-Hash (PtH) : https://technet.microsoft.com/en-us/security/dn785092

[60] PRIVILEGED ACCESS WORKSTATIONS: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

[61] Local Administrator Password Solution (LAPS): https://www.microsoft.com/en-us/download/details.aspx?id=46899

[62] SECURISATION DE L'ACCES PRIVILEGIE : https://docs.microsoft.com/fr-fr/windows-server/identity/securing-privileged-access/securing-privileged-access

[63] INTEGRER DES REPERTOIRES LOCAUX A AZURE ACTIVE DIRECTORY : https://docs.microsoft.com/fr-fr/azure/active-directory/connect/active-directory-aadconnect

Remarque Azure AD Connect Health[64] permet de surveiller et d'analyser l'infrastructure d'identité locale et les services de synchronisation de Litware 369. Il permet ainsi de maintenir une connexion fiable à Azure AD en fournissant des fonctionnalités de surveillance des composants d'identité clés en local tels que les serveurs Azure AD Connect (moteur de synchronisation), les contrôleurs de domaine AD, etc. En outre, Azure AD Connect Health permet d'obtenir des données d'utilisation et d'autres informations importantes pour prendre des décisions avisées sur cette infrastructure.

Gérer de façon sécurisée l'accès B2B aux données, applications et autres ressources

Cette section étudie le scénario de traitement du portail Partenaires de Litware 369 et dans ce contexte, vis-à-vis des accès nécessairement authentifiés à celui-ci, une base de comptes Partenaires au niveau du serveur de données SQL server interne.

Les collaborateurs d'une entreprise ont un besoin naturel de collaborer avec des partenaires pour partager facilement dans leur quotidien des données (personnelles) avec les bonnes personnes des sociétés considérées dans ce contexte. Ce scénario de traitement n'y fait pas exception.

Dans le même temps, ces mêmes entreprises partenaires recherchent la simplicité pour les échanges : si possible sans que cela passe par de nouveaux comptes, sans aucune fédération à configurer, sans aucun serveur à installer ou de configuration à faire évoluer. Pour Litware 369, il s'agissait donc de définir une identité « générique » par partenaire.

Si cette approche a l'avantage d'être simple et de constituer une réponse rapide au besoin de disposer de ce traitement, elle ne satisfait pas le RSSI de Litware 369 qui souhaite, pour les accès des partenaires, une capacité de contrôle, de surveillance et d'audit beaucoup plus granulaire.

La sécurisation des identités, au-delà de celles des collaborateurs de Litware 369 avec le nécessaire élargissement de son réseau de partenaires pour accompagner sa volonté de croissance, est un élément essentiel à la protection des données (personnelles) de l'entreprise.

Les fonctionnalités d'Azure AD B2B collaboration permettent à toute organisation utilisant Azure AD de travailler en toute sécurité avec des utilisateurs de n'importe quelle autre organisation, petite ou grande, avec ou sans annuaire Azure AD ; et même, avec ou sans service informatique.

Azure AD B2B collaboration permet à Litware 369 de bénéficier de toutes les fonctions de gestion des identités et des accès (Identity and Access Management en anglais ou IAM) pour les partenaires. Les organisations utilisant Azure AD comme Litware 369 peuvent donner accès aux documents, ressources et applications à leurs partenaires, tout en conservant un contrôle complet sur les données d'entreprise. Autrement dit, les entreprises partenaires gèrent, quelle que soient leurs tailles et leurs environnements techniques, leurs propres informations d'identification et Litware 369 gère la politique de contrôle d'accès pour ces comptes « invité ». Dans ce contexte, Litware 369 est à même d'afficher les termes d'utilisation relatif à telle ou telle application ainsi exposée et d'en demander notamment l'acceptation préalable pour conférer un accès selon les termes convenus.

[64] SURVEILLEZ VOTRE INFRASTRUCTURE D'IDENTITE LOCALE ET VOS SERVICES DE SYNCHRONISATION DANS LE CLOUD : https://docs.microsoft.com/fr-fr/azure/active-directory/connect-health/active-directory-aadconnect-health

Remarque Pour plus d'informations, vous pouvez consulter l'article Qu'est-ce qu'Azure AD B2B Collaboration ?[65] et visionner le webinaire Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services[66].

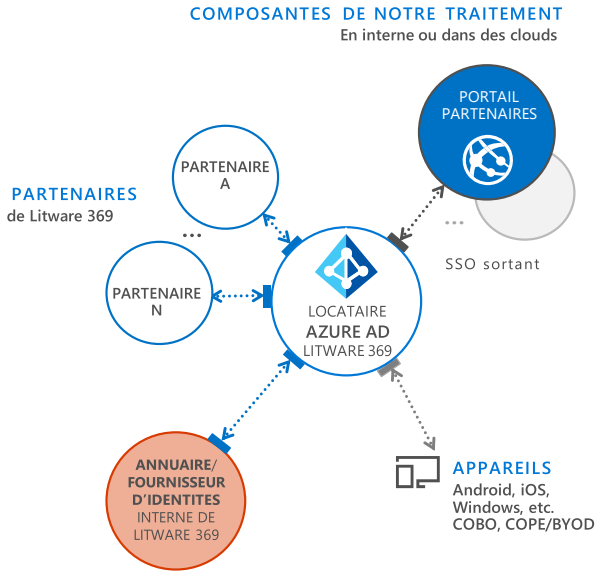

Figure 9 Disposer avec Azure AD B2B collaboration de toutes les fonctions IAM pour les partenaires

Gérer de façon sécurisée l'accès B2C aux données, applications et autres ressources

Le scénario de traitement concerne pour cette section le portail Clients de Litware 369 et dans ce contexte vis-à-vis des accès nécessairement authentifiés à celui-ci une base de comptes Clients au niveau du serveur de données SQL server interne.

Azure Active Directory B2C[67] (Azure AD B2C) est un service de gestion des identités dans le cloud permettant de mettre à disposition des applications web et mobiles auprès de clients en leur offrant une expérience entièrement personnalisable.

Remarque Pour plus d'informations, vous pouvez consulter l'article Azure AD B2C : concentrez-vous sur votre application, nous nous chargeons de l'inscription et de la connexion[68] et visionner le webinaire Azure AD B2C: How to enable consumer logins and access management for your B2C apps[69].

Basé sur Azure AD, cette solution offre une évolutivité, une fiabilité et une disponibilité optimales pour les applications destinées aux clients de Litware 369.

---

[65] Qu'est-ce qu'Azure AD B2B Collaboration ? : https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-b2b-what-is-azure-ad-b2b

[66] Azure Active Directory B2B Collaboration: simple, secure external sharing of your Apps and Services : https://youtu.be/AhwrweCBdsc

[67] Azure Active Directory B2C: https://azure.microsoft.com/fr-fr/services/active-directory-b2c/

[68] Azure AD B2C : concentrez-vous sur votre application, nous nous chargeons de l'inscription et de la connexion : https://docs.microsoft.com/fr-fr/azure/active-directory-b2c/active-directory-b2c-overview

[69] Azure AD B2C: How to enable consumer logins and access management for your B2C apps: https://azure.microsoft.com/en-us/resources/videos/azure-ad-b2c-how-to-enable-consumer-logins-and-access-management-for-your-b2c-apps/?v=17.23h

Azure AD B2C permet à Litware 369 de bénéficier de toutes les fonctions de gestion des identités et des accès orientées clients (Customer Identity and Access Management en anglais ou CIAM), et ce, en particulier vis-à-vis pour le portail Clients pour gérer une audience de clients attendus.

Cela se traduit en particulier par la capacité :

- De gérer l'identité à l'échelle (et de s'affranchir de la gestion des comptes dans la base de données SQL Server interne) ;
- D'offrir de meilleurs parcours et expériences utilisateurs (enregistrement, connexion, gestion du profil, réinitialisation du mot de passe, etc.), c.à.d. plus attractifs tout en renforçant la sécurité ;
- De bénéficier pour cela de parcours prédéfinis ou de construire en fonction des parcours personnalisés et de pouvoir recueillir dans ce contexte si besoin un consentement ;
- De permettre la réutilisation d'identités sociales pour (l'amorce de) l'authentification : Amazon, Google, LinkedIn, Microsoft, Twitter, etc. ;
- De pouvoir disposer d'un profil utilisateur personnalisé puisque la plupart des applications grand public doivent aujourd'hui stocker certains types d'information.

  Ceci passe par le biais de la définition d'attributs personnalisés ; ces attributs peuvent ensuite être traités de la même façon que toute autre propriété d'un compte utilisateur.

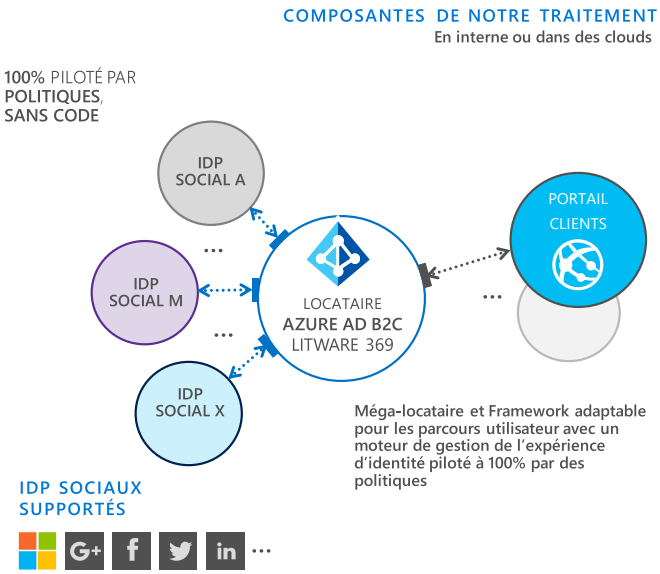

Figure 10 Disposer avec Azure AD B2C de toutes les fonctions CIAM pour les clients

Permettre l'exercice des nouveaux droits pour les personnes concernées

L'identité constituant le nouveau périmètre, notamment en termes de mesures de sécurité, les efforts de rationalisation consentis par Litware 369 dans la gestion des identités et des accès ((C)IAM) pour le B2E, B2B et le B2C contribue, dans ce cadre, à faciliter l'exercice des nouveaux droits pour les personnes concernées, qu'ils s'agissent des collaborateurs de Litware 369 (B2E), des partenaires de Litware 369 (B2B), ou des contacts et clients de Litware 369 (B2C). Pour mémoire, le GDPR impose d'offrir des droits étendus quant à l'accès, à la rectification ou à la suppression des données erronées, à l'effacement des données (également appelé droit à l'oubli), etc.

Litware 369 peut pleinement bénéficier des capacités des offres Azure AD utilisées pour cela. Voyons ce qu'il en est dans les sections suivantes en fonction de la nature des identités considérées : B2E vs. B2B vs. B2C.

Permettre l'exercice des nouveaux droits pour les collaborateurs de Litware 369

En termes de gestion des identités de ses collaborateurs, Litware 369 tire parti de précédents investissements dans Microsoft Identity Management (MIM)[70] et l'(inter)connexion de ces identités avec la solution RH utilisée, l'annuaire technique AD, d'autres solutions/silos applicatifs dans l'environnement local.

MIM permet en effet de simplifier la gestion du cycle de vie de ces identités avec des workflows automatisés ainsi que des règles d'entreprise et offre dans ce contexte une intégration facile à des plateformes hétérogènes dans l'environnement local ou le cloud. Des rapports détaillés montrent et permettent suivre les changements et l'historique de ces identités ainsi que les notifications, e-mails personnalisés et approbations afférentes.

Un portail utilisateur ad 'hoc permet, en interne, aux collaborateurs d'avoir accès à leur information d'identité, et de pouvoir procéder à la rectification ou à la suppression des données erronées.

Au-delà de l'usage de requêtes LDAP envers l'annuaire AD, l'implémentation du portail pour l'exercice de ces droits repose également sur l'usage des APIs Microsoft Graph[71] qui permettent de cibler ces mêmes utilisateurs dans Azure et Office 365 et d'obtenir des propriétés détaillées d'un utilisateur ainsi que des informations de contexte enrichies comme les appareils enregistrés, le nom du manager, s'il est à son bureau ou non, etc. Ces mêmes APIs permettent de mettre à jour des propriétés d'un utilisateur, de le désactiver ou de le supprimer (seuls les services RH ont accès à la désactivation ou à la suppression).

> **Remarque** Les APIs Azure AD Graph[72] peuvent être utilisées de façon alternative pour accéder aux seules ressources Azure AD. Il convient cependant de souligner que nos efforts de développement sont maintenant axés sur Microsoft Graph et qu'aucune autre amélioration n'est prévue pour l'API Azure AD Graph. Dans la pratique, il existe un nombre très limité de scénarii pour lesquels l'API Azure AD Graph peut être appropriée. Pour plus d'informations, vous pouvez consultez le billet MICROSOFT GRAPH OU AZURE AD GRAPH[73].

Ce portail renvoie par ailleurs sur les fonctions en libre-service de MIM afin de permettre aux utilisateurs de résoudre eux-mêmes les problèmes liés à leur identité, notamment pour ce qui est des fonctions d'adhésion aux groupes, de réinitialisation de mot de passe, etc.

Une interface facile d'utilisation augmente finalement la productivité et la satisfaction tout en offrant le respect des exigences du GDPR en la matière.

Permettre l'exercice des nouveaux droits pour les partenaires de Litware 369

Comme abordé à la section précédente § GERER DE FAÇON SECURISEE L'ACCES B2B AUX DONNEES, APPLICATIONS ET AUTRES RESSOURCES, Litware 369 s'appuie sur Azure AD B2B collaboration pour un accès authentifié au

[70] Microsoft Identity Manager 2016: https://www.microsoft.com/fr-fr/cloud-platform/microsoft-identity-manager

[71] Microsoft Graph: https://developer.microsoft.com/fr-fr/graph

[72] API AZURE ACTIVE DIRECTORY GRAPH: https://docs.microsoft.com/fr-fr/azure/active-directory/develop/active-directory-graph-api

[73] MICROSOFT GRAPH OR THE AZURE AD GRAPH: https://dev.office.com/blogs/microsoft-graph-or-azure-ad-graph

portail Partenaires. Chaque collaborateur dûment habilité des entreprises partenaires de Litware 369 dispose ainsi d'un compte Azure AD « invité » propre.

Une section dédiée de ce portail permet d'offrir à ces utilisateurs externes des droits étendus, au-delà de l'accès à leurs informations d'identité, quant à la rectification ou à la suppression des données erronées les concernant. Ils peuvent par ailleurs demander l'effacement de ces mêmes données. Cette dernière action a pour effet de supprimer leur compte et par voie de conséquence leur accès au portail Partenaires de Litware 369 ainsi qu'à toute autre ressource intégrée à Azure AD que Litware 369 mettrait à disposition de ces utilisateurs externes sur la base du contrôle d'accès en place.

La mise en œuvre de cette section du portail Partenaires repose dans la pratique sur les APIs Azure AD Graph, Cf. section précédente. Litware 369 s'est par ailleurs appuyé sur le code de l'exemple de portail d'inscription en libre-service[74] mis à disposition en open source par Microsoft sur la forge communautaire GitHub.

Permettre l'exercice des nouveaux droits pour les contacts et clients de Litware 369

Le traitement envisagé comprend vis-à-vis (du stockage) des données personnelles collectées deux grands temps :

1. Avant la mise en œuvre du service ;
2. Une fois le service activé.

Voyons ce qu'il en est de l'exercice des nouveaux droits.

Avant la mise en œuvre du service

Lors de la confirmation de la commande effectuée par un contact, ce dernier dispose dans le courriel de confirmation qui lui est envoyé d'un lien pour se rétracter et résilier la commande sous un délai de 14 jours.

L'utilisation de ce lien personnalisé renvoie vers une page Web. Cette page décrit les modalités de l'opération de résiliation et précise qu'aucune information personnelle n'est conservée à l'issue de la transaction.

Après une demande de confirmation, tous les enregistrements relatifs à cette commande sont supprimés au niveau de la base SQL Server. Seuls sont conservés le numéro de commande, la date de commande initiale, les date et heure de résiliation pour des besoins de traçabilité des opérations exécutées. La commande étant marquée comme résiliée, elle apparait comme telle, le cas échéant, dans le portail Partenaires sans autres informations que celles conservées ci-avant. La transaction se clôture par l'envoi d'un courriel de confirmation de suppression de la commande et des informations personnelles associées.

> **Remarque** A la vue des grandes étapes de notre traitement « représentatif » et des traitements déclenchés, la résiliation effective imposerait des contrôles de cohérence supplémentaires et, le cas échéant, des opérations additionnelles en fonction du l'état courant dudit traitement. Le but poursuivi ici consiste simplement à en illustrer le principe pour expliciter le propos.

[74] SELF-SERVICE PORTAL FOR AZURE AD B2B COLLABORATION SIGN-UP: https://aka.ms/b2bselfservice

Une fois le service activé

Comme indiqué précédemment, lorsque l'entreprise partenaire a procédé à l'installation en vue de l'activation complète du service et des options souscrites, le service Abonnements de Litware 369 procède à la création du nouveau compte client :

- Un nouveau compte client et un nouveau contrat sont créés dans Dynamics 365 pour la facturation de l'offre d'alarme connectée souscrite, le suivi de contrat, etc. ;
- Une nouvelle identité est créée dans le répertoire Azure AD B2C de Litware 369 via les APIs Azure AD Graph pour l'accès au portail Clients, Cf. section précédente § GERER DE FAÇON SECURISEE L'ACCES B2C AUX DONNEES, APPLICATIONS ET AUTRES RESSOURCES.

  L'identifiant est l'adresse mèl précédemment communiquée et utilisée jusqu'alors dans les échanges ; un mot de passe temporaire est généré. Par ailleurs, le numéro de téléphone est stocké dans les attributs de ce compte B2C ; il servira à l'authentification multifacteur dans les différents parcours et expériences utilisateurs proposés par le portail : finalisation de l'enregistrement lors de la première connexion avec un consentement explicite, connexion, gestion du profil, réinitialisation du mot de passe, etc.

Un courriel de confirmation est alors envoyé au client avec toutes les informations de connexion (identifiant et mot de passe) pour gérer son abonnement et les demandes associées depuis le portail Client.

Pour l'accès au portail Clients et à son compte client, le client doit s'identifier avec son adresse mèl. Lors de la première connexion, la possibilité lui est cependant donnée d'utiliser une identité sociale pour (l'amorce de) l'authentification au lieu et place de cette adresse mèl.

Une fois connecté, le client peut accéder à son compte client pour le service d'alarme souscrit ainsi qu'à son profil. Les informations relatives à son contrat tout comme ses différentes informations personnelles sont consultables et modifiables si besoin. Les services Web Microsoft Dynamics 365[75] et les APIs Azure AD Graph sont utilisées pour cela.

Ces mêmes services Web et APIs permettent de mettre en œuvre le droit à l'effacement des données (également appelé droit à l'oubli), avec à clé la possibilité de supprimer toutes les informations non sujettes à un impératif de conservation (« retention »).

Ceci conclut les exemples que nous souhaitions donner en termes de capacités de mise en œuvre d'une gouvernance des données personnelles sur le périmètre de notre illustration.

Exemples de solutions

La classification et la labélisation des données personnelles, ainsi que la gestion des identités et des rôles pour le scénario « représentatif » de traitement montrent comment Azure Information Protection, Azure AD, Azure AD B2B collaboration, et Azure AD B2C contribuent à renforcer la gouvernance des données personnelles.

Cette gouvernance des données personnelles, d'une façon générale et non pas uniquement vis-à-vis du cadre restreint de notre illustration, et le plan qui en découle, peuvent tirer parti d'autres produits et solutions de cloud de Microsoft au-delà des exemples pris ici.

[75] UTILISER LES SERVICES WEB MICROSOFT DYNAMICS 365 : https://msdn.microsoft.com/fr-fr/library/mt608128.aspx

Remarque Le livre blanc LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES[76] propose des exemples d'actions à entreprendre avec Microsoft dès aujourd'hui pour entamer votre cheminement vers la conformité avec le GDPR. Vous pouvez consulter ce livre blanc pour une illustration des mesures à prendre dans ce contexte pour la gestion des données personnelles et la façon dont les produits et services Cloud de Microsoft contribuent à la mise en œuvre (ou à la traduction effective) de celles-ci.

[76] LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES : https://aka.ms/gdprwhitepaper

Protéger - Prévenir, détecter et répondre aux vulnérabilités et aux violations de données personnelles

A l'instar de l'étape de gestion précédente (Cf. section § GERER - GOUVERNER COMMENT LES DONNEES PERSONNELLES SONT ACCEDEES ET UTILISEES), cette étape de protection des données personnelles se traduit dans un ensemble d'activité(s) de la phase **METTRE EN OEUVRE** (du modèle PDCA) du programme GDPR suggéré par le livre blanc GDPR – S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR. Ces activités et actions associées consistent à améliorer la sécurité des traitements et des données personnelles.

Compte tenu des résultats de l'étude préalable, il a été décidé, pour limiter les risques de fuite d'information ou d'accès non-autorisé aux données personnelles, d'en renforcer la protection en s'appuyant sur les fonctionnalités de chiffrement des systèmes sur lesquelles elles sont stockées.

Voyons comment ces actions peuvent se traduire à l'aide d'exemples de produits et de services Cloud Microsoft.

Protéger les données au repos

La protection des données au repos passe notamment par leur chiffrement.

Chiffrer les données au repos

Le chiffrement des données est l'une des mesures techniques explicitement citées par le GDPR. Voyons ce qu'il en est dans notre scénario « représentatif » de traitement.

Chiffrer les commandes sur le serveur de fichiers Windows Server

Dans le processus de traitement des nouvelles commandes, une extraction de la base de données SQL située en interne est effectuée sur une base journalière sous forme de fichiers CSV stockés sur un serveur de fichiers Windows Server. Même si ce serveur est situé dans les locaux de l'entreprise Litware 369, celle-ci souhaite s'assurer que les données personnelles contenues dans les fichiers CSV et qui résident sur des disques de ce serveur sont chiffrées au repos.

Dans ce but, Litware 369 a décidé de mettre en œuvre la technologie BitLocker. La technologie de chiffrement des disques BitLocker, présente nativement dans Windows (Server), fournit une fonctionnalité de chiffrement de qualité professionnelle pour protéger les données personnelles en cas de perte ou de vol d'un disque. BitLocker chiffre entièrement les disques d'un ordinateur pour empêcher les utilisateurs non autorisés d'accéder à vos données.

BitLocker permet de couvrir les risques d'accès au disque du système d'exploitation et aux disques de données lorsqu'un ordinateur est perdu ou volé, ou lorsqu'un disque est mis hors service ou recyclé.

Remarque BitLocker offre une protection maximale lorsqu'il s'appuie sur un composant matériel de confiance appelé TPM (Trusted Platform Module) présent sur la plupart des configurations récentes. Pour encore plus de sécurité, il est possible d'imposer l'entrée d'un code PIN au démarrage du serveur si celui n'est pas connecté au réseau de l'entreprise en activant la fonction de déblocage réseau.

Pour plus d'informations, vous pouvez consulter les articles VUE D'ENSEMBLE DU CHIFFREMENT DE LECTEUR BITLOCKER[77] et BITLOCKER: HOW TO ENABLE NETWORK UNLOCK[78], ainsi que le livre blanc PROTECTING YOUR DATA WITH WINDOWS 10 BITLOCKER[79].

Remarque Pour plus d'informations sur la sécurité de la plateforme Windows, vous pouvez consultez la présentation de Sécurité de Windows Server 2016[80] et de Sécurité de Windows 10[81].

Chiffrer les commandes dans la base de données SQL Server interne

Dans la phase initiale de prise de commande par les clients depuis le site web institutionnel de la société Litware 369, les informations associées à la commande, dont les données personnelles du client, sont stockées dans la base de données interne SQL Server. La protection de ces données au repos est assurée nativement par le chiffrement transparent des données (Transparent Data Encryption en anglais ou TDE) de la base de données SQL Server.

Le chiffrement transparent des données protège les données au repos en chiffrant la base de données, les sauvegardes associées et les fichiers du journal des transactions au niveau de la couche de stockage physique. Ce mode de chiffrement est transparent pour site institutionnel et utilise l'accélération matérielle pour améliorer les performances.

Remarque Pour plus d'informations, vous pouvez consulter l'article CHIFFREMENT TRANSPARENT DES DONNEES (TDE)[82].

Pour une protection renforcée, Litware 369 souhaite reposer sur ses propres clés de chiffrement dans la mise en œuvre du chiffrement transparent des données et bénéficier dans ce contexte du coffre-fort de clés Azure Key Vault pour stocker et protéger ses clés, Cf. section § CHIFFRER LES FORMULAIRES CLIENT DE LA BIBLIOTHEQUE SHAREPOINT ONLINE

DANS LA fin du processus de traitement, une extraction journalière des commandes terminées est effectuée et génère automatiquement des formulaires Word qui sont stockés dans une bibliothèque SharePoint Online de Litware 369. Les formulaires Word contiennent des données personnelles des clients (le dossier de commande avec les caractéristiques techniques de l'installation). Il est donc important qu'elles soient protégées au niveau de la bibliothèque SharePoint Online utilisée ici.

Aucune action particulière n'est nécessaire puisque le service de cloud SharePoint Online (ou le service de stockage OneDrive Entreprise) offre par **défaut un chiffrement au repos au niveau** fichier.

---

[77] VUE D'ENSEMBLE DU CHIFFREMENT DE LECTEUR BITLOCKER : https://technet.microsoft.com/fr-fr/library/cc732774(v=ws.11).aspx

[78] BITLOCKER: HOW TO ENABLE NETWORK UNLOCK: https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-how-to-enable-network-unlock

[79] PROTECTING YOUR DATA WITH WINDOWS 10 BITLOCKER: https://www.microsoft.com/en-us/download/details.aspx?id=53006

[80] AMELIOREZ LA SECURITE AVEC WINDOWS SERVER 2016 : https://www.microsoft.com/fr-fr/cloud-platform/windows-server-security

[81] UNE PROTECTION CONTRE LES NOUVELLES MENACES DE SECURITE : https://www.microsoft.com/fr-fr/WindowsForBusiness/Windows-security

[82] CHIFFREMENT TRANSPARENT DES DONNEES (TDE) : https://docs.microsoft.com/fr-fr/sql/relational-databases/security/encryption/transparent-data-encryption-tde

Remarque Chaque fichier est divisé en un ou plusieurs morceaux, selon la taille du fichier et chaque partie est chiffrée en utilisant sa propre clé unique. Les clés sont ensuite stockées chiffrées dans une base de données de contenu en ligne SharePoint avec la carte de répartition des morceaux de fichiers, informations qui seront utilisées pour reconstruire le fichier lors d'une demande d'accès.

Pour plus d'informations, vous pouvez consulter le livre blanc CONTENT ENCRYPTION IN MICROSOFT OFFICE 365.

Litware 369 tire ici partie également de l'intégration récente avec Azure Key Vault.

Remarque Pour plus d'informations, vous pouvez consulter le billet NEW MICROSOFT 365 FEATURES TO ACCELERATE GDPR COMPLIANCE.

Stocker et protéger les clés de chiffrement dans Azure Key Vault ci-après. Pour cela, le connecteur SQL pour Azure Key Vault assure l'intégration entre la base de données interne SQL Server et le service Azure Key Vault.

Remarque Le connecteur SQL Server est un fournisseur de gestion des clés extensible (Extensible Key Management en anglais ou EKM) qui permet à SQL Server d'utiliser Azure Key Vault comme un espace de protection et de gestion des clés de chiffrement SQL. Cela signifie que vous pouvez utiliser vos propres clés de chiffrement pour le chiffrement SQL Server et les protéger dans Azure Key Vault. Au-delà du chiffrement transparent des données (TDE) qui nous intéresse ici, le connecteur SQL Server permet également de configurer le chiffrement au niveau colonne (CLE) ainsi que le chiffrement des sauvegardes.

Pour plus d'informations, vous pouvez consulter le billet SQL SERVER CONNECTOR FOR AZURE KEY VAULT IS GENERALLY AVAILABLE[83].

Chiffrer les boîtes aux lettres dans Exchange Online

Dans le processus de traitement, une fois les nouvelles commandes stockées sous forme de fichiers CSV sur le serveur de fichiers interne, un courriel est envoyé automatiquement à chaque partenaire par l'intermédiaire d'un composant logiciel enfichable (add-in) Outlook. Chaque courriel contient des données qui sont indirectement liées au client (numéro de commande) et des liens qu'il pourra utiliser pour suivre sa commande, se rétracter, etc. Plus tard dans le traitement, lorsque le partenaire a procédé à l'installation des alarmes connectées chez le client, d'autres courriers électroniques sont envoyés contenant des informations de connexion propres à chaque client. Il est donc important que les boites aux lettres contenant ces courriels soient protégées dans leur lieu de stockage c'est-à-dire dans la messagerie Exchange Online d'Office 365.

Exchange Online offre nativement la fonctionnalité de **chiffrement au niveau de la boite aux lettres** de chaque utilisateur, permettant ainsi de protéger chaque contenu de boîte aux lettres par une clé différente. Ce chiffrement de niveau service offre comme avantage de rendre impossible l'accès aux contenus client par un administrateur système ou un opérateur indélicat du service de cloud et fournit, de fait, une protection supplémentaire par rapport au chiffrement de volume BitLocker appliqué au niveau des volumes disque pour le service de cloud Exchange Online.

Dans la lignée des dispositions prises dans le chiffrement des données de la base SQL Server interne, Litware 369 souhaite également reposer ici sur ses propres clés de chiffrement dans la mise en œuvre du chiffrement des boîtes aux lettres et bénéficier de la même façon du coffre-fort de clés Azure Key Vault pour stocker et protéger ses clés, Cf. section § CHIFFRER LES FORMULAIRES CLIENT DE LA BIBLIOTHEQUE SHAREPOINT ONLINE

[83] SQL SERVER CONNECTOR FOR AZURE KEY VAULT IS GENERALLY AVAILABLE:
ttps://blogs.msdn.microsoft.com/sqlsecurity/2016/06/13/sql-server-connector-for-azure-key-vault-is-generally-available/

Dans la fin du processus de traitement, une extraction journalière des commandes terminées est effectuée et génère automatiquement des formulaires Word qui sont stockés dans une bibliothèque SharePoint Online de Litware 369. Les formulaires Word contiennent des données personnelles des clients (le dossier de commande avec les caractéristiques techniques de l'installation). Il est donc important qu'elles soient protégées au niveau de la bibliothèque SharePoint Online utilisée ici.

Aucune action particulière n'est nécessaire puisque le service de cloud SharePoint Online (ou le service de stockage OneDrive Entreprise) offre par défaut **un chiffrement au repos au niveau fichier**.

> **Remarque** Chaque fichier est divisé en un ou plusieurs morceaux, selon la taille du fichier et chaque partie est chiffrée en utilisant sa propre clé unique. Les clés sont ensuite stockées chiffrées dans une base de données de contenu en ligne SharePoint avec la carte de répartition des morceaux de fichiers, informations qui seront utilisées pour reconstruire le fichier lors d'une demande d'accès.
>
> Pour plus d'informations, vous pouvez consulter le livre blanc CONTENT ENCRYPTION IN MICROSOFT OFFICE 365.

Litware 369 tire ici partie également de l'intégration récente avec Azure Key Vault.

> **Remarque** Pour plus d'informations, vous pouvez consulter le billet NEW MICROSOFT 365 FEATURES TO ACCELERATE GDPR COMPLIANCE.

Stocker et protéger les clés de chiffrement dans Azure Key Vault ci-après.

Cela consiste à mettre en œuvre la fonctionnalité BYOK (Bring Your Own Key) qui offre ainsi une sécurité supplémentaire à Litware 369. Cette fonctionnalité permet en effet de paramétrer Exchange Online pour que ce service Cloud utilise les clés d'un coffre-fort Azure Key Vault pour protéger le contenu des boites aux lettres.

> **Remarque** Pour plus d'informations, vous pouvez consulter le livre blanc CONTENT ENCRYPTION IN MICROSOFT OFFICE 365[84].

Chiffrer les formulaires Client de la bibliothèque SharePoint Online

Dans la fin du processus de traitement, une extraction journalière des commandes terminées est effectuée et génère automatiquement des formulaires Word qui sont stockés dans une bibliothèque SharePoint Online de Litware 369. Les formulaires Word contiennent des données personnelles des clients (le dossier de commande avec les caractéristiques techniques de l'installation). Il est donc important qu'elles soient protégées au niveau de la bibliothèque SharePoint Online utilisée ici.

Aucune action particulière n'est nécessaire puisque le service de cloud SharePoint Online (ou le service de stockage OneDrive Entreprise) offre par défaut **un chiffrement au repos au niveau fichier**.

> **Remarque** Chaque fichier est divisé en un ou plusieurs morceaux, selon la taille du fichier et chaque partie est chiffrée en utilisant sa propre clé unique. Les clés sont ensuite stockées chiffrées dans une base de données de contenu en ligne SharePoint avec la carte de répartition des morceaux de fichiers, informations qui seront utilisées pour reconstruire le fichier lors d'une demande d'accès.
>
> Pour plus d'informations, vous pouvez consulter le livre blanc CONTENT ENCRYPTION IN MICROSOFT OFFICE 365[85].

Litware 369 tire ici partie également de l'intégration récente avec Azure Key Vault.

[84] CONTENT ENCRYPTION IN MICROSOFT OFFICE 365 : http://aka.ms/Office365CE

[85] CONTENT ENCRYPTION IN MICROSOFT OFFICE 365: http://aka.ms/Office365CE

Remarque Pour plus d'informations, vous pouvez consulter le billet NEW MICROSOFT 365 FEATURES TO ACCELERATE GDPR COMPLIANCE[86].

Stocker et protéger les clés de chiffrement dans Azure Key Vault

Azure Key Vault[87] est un service de coffre-fort de clés et de secrets dans Azure qui permet d'assurer la sécurité des clés de chiffrement, des secrets (comme les mots de passe), et des certificats qui protègent les données.

Remarque Pour plus d'informations, vous pouvez consulter l'article QU'EST-CE QU'AZURE KEY VAULT ?[88], et visionner le webinaire INTRODUCTION TO MICROSOFT AZURE KEY VAULT[89], ainsi que la formation en ligne Microsoft Virtual Academy (MVA) AZURE KEY VAULT EN PRATIQUE[90].

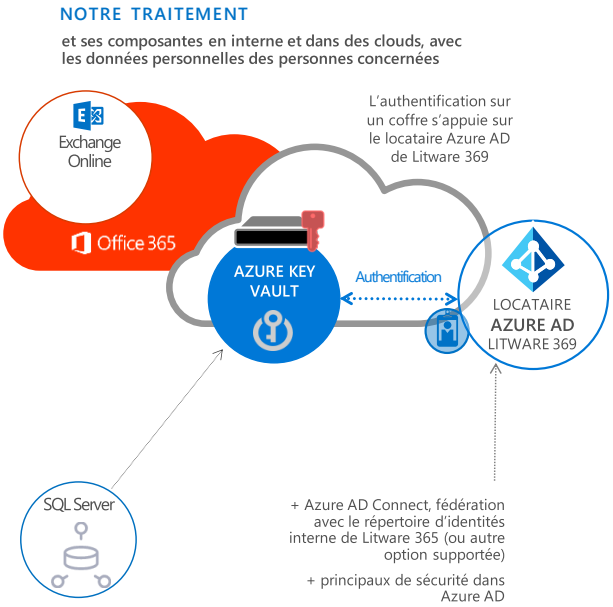

Figure 11 Gérer les clés de chiffrement avec Azure Key Vault

Avec la prise en charge d'Azure Key Vault dans un nombre sans cesse croissant de produits et de services Cloud de Microsoft à l'image ici de SQL Server, d'Exchange Online et de SharePoint Online, vous bénéficiez d'un système de gestion de clé distinct et centralisé, ainsi que de l'option d'utiliser dans le cloud des modules de sécurité matériel (Hardware Security Module en anglais ou HSM) pour votre coffre de clés.

---

[86] NEW MICROSOFT 365 FEATURES TO ACCELERATE GDPR COMPLIANCE: https://cloudblogs.microsoft.com/microsoftsecure/2017/09/25/new-microsoft-365-features-to-accelerate-gdpr-compliance/

[87] Azure Key Vault: https://azure.microsoft.com/fr-fr/services/key-vault/

[88] QU'EST-CE QU'AZURE KEY VAULT ? : https://docs.microsoft.com/fr-fr/azure/key-vault/key-vault-whatis

[89] INTRODUCTION TO MICROSOFT AZURE KEY VAULT: https://youtu.be/5p2dQdTsUvE

[90] AZURE KEY VAULT EN PRATIQUE : https://mva.microsoft.com/fr-fr/training-courses/azure-key-vault-en-pratique-fr--16572?l=svn7dFdgC_1205192797

Remarque L'utilisation des modules de sécurité matériel permet la mise en œuvre de la fonctionnalité dite de BYOK (Bring Your Own Key) qui permet d'importer depuis l'environnement interne vos propres clés dans un coffre de clés Key Vault au lieu de les générer dans celui-ci.

Pour plus d'informations, vous pouvez consulter le livre blanc BRING YOUR OWN KEY (BYOK) WITH AZURE KEY VAULT FOR OFFICE 365 AND AZURE[91].

Azure Key Vault est conçu de façon à assurer le contrôle des clés et par conséquent des données, notamment à garantir que Microsoft n'a pas accès aux clés ou ne peut pas les extraire.

Par ailleurs, Litware 369 peut surveiller et auditer l'utilisation de ses clés stockées à l'aide de la journalisation Azure, et importer les journaux dans Azure HDInsight ou son système de gestion des informations et des événements de sécurité (Security Information and Event Management en anglais ou SIEM) pour effectuer une analyse supplémentaire et détecter les menaces.

Cette approche permet à Litware 369 de garantir une séparation des rôles entre la gestion des clés et celle des données.

Par ailleurs, il suffit à Litware 369 de retirer l'usage de ses clés de chiffrement dans les politiques d'accès des coffres de clés pour que toutes les données chiffrées avec deviennent inaccessibles. Ceci revêt un intérêt particulier si Litware 369 était amené dans le futur à ne plus utiliser certains services.

Protéger les données dans les appareils mobiles et des applications mobiles

Pour cette section, le scénario de traitement des commandes, des courriels, et autres données personnelles relatives à ce dernier.

Comme décrit précédemment dans le scénario du traitement, l'enregistrement d'une commande d'alarmes connectées est réalisé par le client lui-même à partir du site web institutionnel (Cf. section § ENREGISTREMENT D'UNE COMMANDE). Une commande peut l'être également directement par un commercial de Litware 369 en démarchage chez un prospect ou lors d'un salon.

La force de vente de Litware 369, et ses commerciaux, est équipée de terminaux mobiles, pour la plus grande partie des tablettes sous Windows 10, et pour le reste, des iPads. Une application mobile a été développée pour les deux plateformes avec la technologie Xamarin qui permet aux commerciaux d'enregistrer les commandes avec une interface mobile attrayante et plus adaptée à ces terminaux avec des fonctions supplémentaires permettant par exemple de travailler hors connexion ou de suivre des dossiers clients.

Par conséquence, les appareils mobiles des commerciaux vont héberger des données personnelles des clients et, en cas de perte ou de vol, peuvent être à l'origine de fuites de données personnelles sans même que la violation de données ne soit détectée. Il est donc nécessaire de se protéger de ce risque fort en imposant certaines politiques de sécurité, comme le fait que l'appareil fasse partie de la flotte d'entreprise, que son disque soit chiffré, qu'un code PIN de 6 caractères soit obligatoire, etc.

Il convient de noter que ces critères pourront servir à imposer un accès sous condition à l'application mobile et aux services de cloud associés.

[91] BRING YOUR OWN KEY (BYOK) WITH AZURE KEY VAULT FOR OFFICE 365 AND AZURE : http://download.microsoft.com/download/F/6/3/F63C9623-053F-44DD-BFA8-C11FA9EA4B61/Bring-Your-Own-Key-with-Azure-Key-Vault-for-Office-365-and-Azure.docx

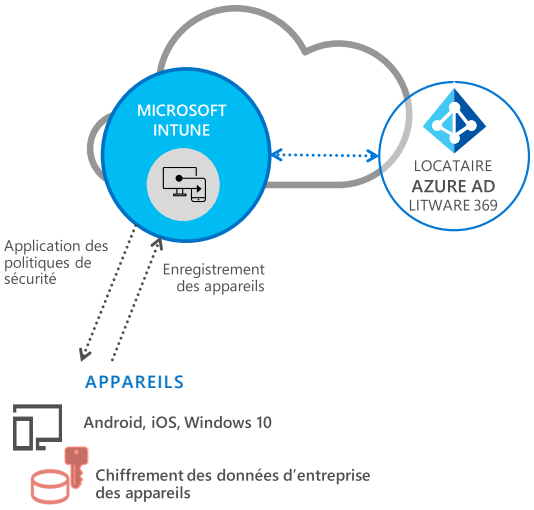

Figure 12 Sécuriser les données sur les appareils mobiles avec Microsoft Intune

Pour obtenir ce niveau de sécurité, la société Litware 369 a décidé de s'appuyer sur Microsoft Intune[92] comme outil de gestion de sa flotte de mobile.

Microsoft Intune permet de protéger les données qui peuvent être stockées sur des ordinateurs personnels et des appareils mobiles. Vous pouvez contrôler l'accès, chiffrer les périphériques, balayer des données de manière sélective et contrôler les applications qui stockent et partagent des données à caractère personnel. Microsoft Intune aide à informer les utilisateurs sur leur choix en matière de gestion en publiant une déclaration de confidentialité et des conditions d'utilisation personnalisées. Il permet également de renommer ou supprimer des périphériques.

> **Remarque** Pour plus d'informations, veuillez consulter la documentation en ligne Microsoft Intune Documentation[93], ainsi que les vidéos (courtes) Communication from the Microsoft Intune Team – Welcome to the new Intune on Azure Experience[94] et Updates to Microsoft Intune on Microsoft Azure[95].

Dans la pratique, tous les appareils mobiles des commerciaux devront être, au préalable, enregistrés dans Microsoft Intune pour être ensuite en mesure d'installer l'application mobile de gestion des commandes et des clients. L'enregistrement déclenchera l'application de politiques de sécurité qui imposeront les exigences de sécurité décrites précédemment comme le chiffrement de l'appareil et l'utilisation d'un code PIN.

---

[92] Microsoft Intune : https://www.microsoft.com/fr-fr/cloud-platform/microsoft-intune

[93] Microsoft Intune Documentation : https://docs.microsoft.com/fr-fr/intune/

[94] Communication from the Microsoft Intune Team – Welcome to the new Intune on Azure Experience: http://intunedin.net/2017/04/communication-from-the-microsoft-intune-team-welcome-to-the-new-intune-on-azure-experience/

[95] Updates to Microsoft Intune on Microsoft Azure: http://intunedin.net/2017/04/updates-to-microsoft-intune-on-microsoft-azure-new-microsoft-mechanics-video/

Remarque Microsoft Intune propose un portail d'entreprise en libre-service aux utilisateurs afin qu'ils inscrivent leurs propres périphériques et installent des applications d'entreprise via les plateformes mobiles les plus courantes. Il protège les données d'entreprise en limitant l'accès aux courriels dans Exchange Online, aux courriels Outlook et aux documents dans SharePoint Online ou OneDrive Entreprise lorsqu'un utilisateur tente d'accéder à des ressources depuis un périphérique non inscrit ou non conforme, en fonction des stratégies définies par l'administrateur.

En plus de la protection de l'appareil lui-même, en cas de perte ou de vol, le commercial pourra avertir un administrateur de Litware 369 qui pourra alors immédiatement procéder à l'effacement complet des données de l'appareil, rendant dès lors impossible toute fuite. Il convient de noter que Microsoft Intune s'appuie désormais sur Azure, est accessible depuis le portail Azure et s'intègre avec le contrôle d'accès conditionnel.

Enfin, pour les appareils Windows 10 des commerciaux qui seront enregistrés dans Microsoft Intune, en plus du chiffrement des disques avec la technologie BitLocker abordée précédemment, une protection supplémentaire est activable à travers la fonctionnalité appelée Windows Information Protection.

Windows Information Protection prend la relève là où BitLocker s'arrête. BitLocker protège l'intégralité du disque d'un appareil et Windows Information Protection et permet de bénéficier d'une séparation entre les données personnelles et les données d'entreprise en offrant un chiffrement supplémentaire au niveau fichier pour ces dernières, en plus d'un mécanisme de protection contre la fuite d'information. Les données d'entreprise ne pourront pas être copiées dans des applications qui ne sont pas considérées comme de confiance, et l'utilisateur ne pourra pas transférer les fichiers d'entreprise vers des destinations de stockage non sûres comme par exemple un partage Dropbox ou un Box personnel.

Il convient de noter à ce propos que, dans notre scénario, la copie des fichiers de commande .CSV, protégés en tant que fichiers d'entreprise **n'auraient pas pu être copiés vers des stockages externes si la fonctionnalité Windows Information Protection avait été mise en place**.

Remarque Pour plus d'informations, vous pouvez consulter l'article PROTECT YOUR ENTERPRISE DATA USING WINDOWS INFORMATION PROTECTION (WIP)[96], les billets de blog INTRODUCING WINDOWS INFORMATION PROTECTION[97], WINDOWS INFORMATION PROTECTION EXPLAINED – WINDOWS 10 CREATORS UPDATE[98] et visionner le webinaire KEEP WORK AND PERSONAL DATA SEPARATE AND SECURE USING WINDOWS INFORMATION PROTECTION IN WINDOWS APPS[99].

Faire respecter des politiques de protection des données

Cette section vise à illustrer comment fournir une protection cohérente et protéger automatiquement contre le risque de divulgation accidentelle. Dans ce contexte, le scénario de traitement concerne les composantes suivantes :

- Le serveur de fichiers Windows Server avec les fichiers CSV des commandes à traiter ;

[96] PROTECT YOUR ENTERPRISE DATA USING WINDOWS INFORMATION PROTECTION (WIP): https://docs.microsoft.com/en-us/windows/threat-protection/windows-information-protection/protect-enterprise-data-using-wip

[97] INTRODUCING WINDOWS INFORMATION PROTECTION: https://blogs.technet.microsoft.com/windowsitpro/2016/06/29/introducing-windows-information-protection/

[98] WINDOWS INFORMATION PROTECTION EXPLAINED – WINDOWS 10 CREATORS UPDATE: https://blogs.technet.microsoft.com/cbernier/2017/05/19/windows-information-protection-explained-windows-10-creators-update/

[99] KEEP WORK AND PERSONAL DATA SEPARATE AND SECURE USING WINDOWS INFORMATION PROTECTION IN WINDOWS APPS: https://www.youtube.com/watch?v=AbOgWvRxQf8

- Les courriels générés depuis le composant logiciel enfichable (add-in) Outlook, les autres courriels envoyés depuis Outlook et Exchange Online ;
- Le service de cloud SharePoint Online avec la bibliothèque de formulaires Word (dossier de commande avec les caractéristiques techniques de l'installation).

Protéger de façon permanente les fichiers contenant données personnelles avec Azure Information Protection

Au-delà de la capacité de classifier et labéliser les données (Cf. section § CLASSIFIER ET LABELISER LES DONNEES PERSONNELLES), Azure Information Protection[100] contribue à garantir que la sécurisation des données personnelles en fonction de leur type et de leur sensibilité - ce qui est une exigence clé du GDPR -, peu importe leur emplacement de stockage ou la façon dont elles sont partagées. Litware 369 peut ainsi protéger, avec le service de protection (Azure Rights Management), les données nouvelles ou existantes (c'est-à-dire les chiffrer), les partager en toute sécurité avec autrui au sein ou en dehors de l'entreprise comme avec les entreprises partenaires.

Dans la pratique, Azure Information Protection vise à fournir une plate-forme de protection des données holistique, agile, complète et flexible pour les organisations d'aujourd'hui.

> **Remarque** Pour plus d'informations, vous pouvez visionner le webinaire LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION[101].

Définir des stratégies pour empêcher que des documents sensibles (commandes) soient utilisés par des utilisateurs non autorisés

La société Litware 369 se doit de protéger les informations sensibles, en particulier les données personnelles dans le contexte de ce livre blanc, et donc notamment d'empêcher leur divulgation accidentelle.

Dans ce contexte, comme évoqué précédemment, Azure Information Protection permet de définir et d'appliquer des stratégies permettant non seulement de classifier et de labéliser des données mais également de les protéger de façon permanente où qu'elles soient et où qu'elles aillent (Cf. ci-dessus). Avec l'application de cette protection, Azure Information Protection permet d'assurer le suivi de l'utilisation des données personnelles protégées et même de révoquer l'accès à distance. Azure Information Protection inclut également des fonctionnalités enrichies de journalisation et de génération de rapports pour surveiller la distribution des données, et des options pour gérer et contrôler vos clés de chiffrement avec la prise en charge d'Azure Key Vault.

Par ailleurs, comme évoqué précédemment, la fonctionnalité de protection contre la perte de données du Centre de sécurité et conformité Office 365 permet dans le même temps d'identifier, de surveiller et de protéger automatiquement les informations sensibles dans Office 365. Cette fonctionnalité est intégrée avec Azure Information Protection et bénéficie ainsi de fait, pour la définition et la mise en œuvre des stratégies de protection des courriels et des fichiers contenant données personnelles, des mécanismes de protection d'Azure Information Protection.

---

[100] Azure Information Protection : https://www.microsoft.com/fr-fr/cloud-platform/azure-information-protection

[101] LEARN HOW CLASSIFICATION, LABELING, AND PROTECTION DELIVERS PERSISTENT DATA PROTECTION: https://youtu.be/ccBus_Yx69g

Remarque Pour plus d'informations, vous pouvez consulter l'article VUE D'ENSEMBLE DES STRATEGIES DE PROTECTION CONTRE LA PERTE DE DONNEES[102], et visionner le webinaire PROTECT YOUR SENSITIVE INFORMATION WITH OFFICE 365 DATA LOSS PREVENTION[103] ainsi que la formation en ligne Microsoft Virtual Academy (MVA) DATA LOSS PREVENTION IN OFFICE 365[104].

Les stratégies de Cloud App Security bénéficient également de la même intégration avec les mécanismes de protection d'Azure Information Protection pour protéger les fichiers contenant des données personnelles.

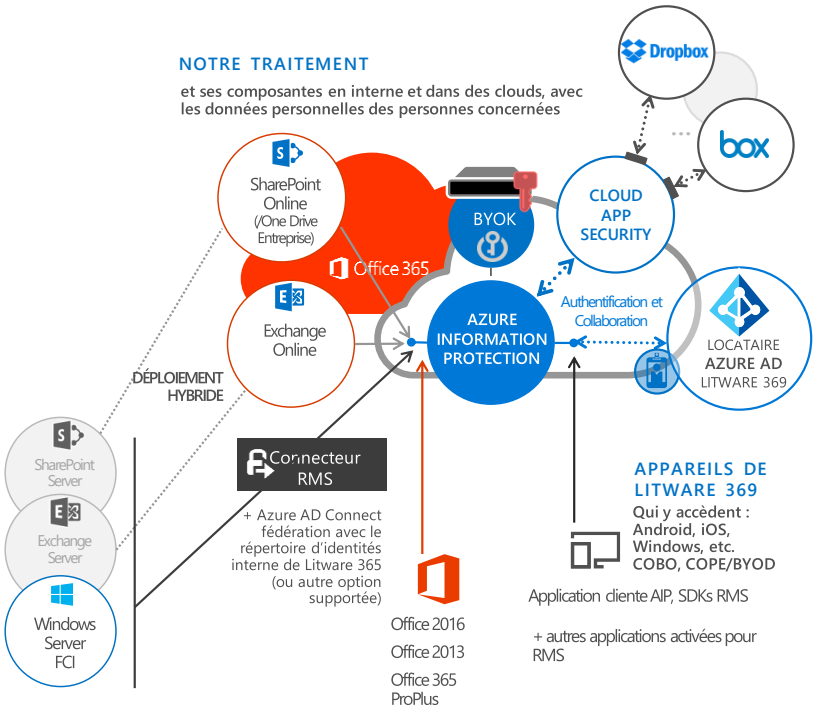

Figure 13 Protéger de façon permanente les fichiers contenant des données personnelles avec (le service de protection (Azure Rights Management) d'Azure Information Protection

Imposer un accès conditionnel aux données

En matière de cyberattaques, les attaquants visent très fréquemment, dans leurs attaques, les comptes et leurs mots de passe, comme cela a été abordé précédemment ; il s'agit de la meilleure façon de s'introduire sans être détecté(e) au sein d'un réseau d'entreprise. Ils travaillent donc pour voler ces informations d'identification.

Ainsi, le contrôle et la protection des identités doit constituer la première ligne de défense dans une approche de type « défense en profondeur ». Comme la majorité des attaques de cybersécurité remontent à des informations d'identification utilisateur perdues, faibles ou compromises, il apparait clairement qu'il est nécessaire de disposer d'un niveau de sécurité que les mots de passe ne sauraient procurer.

---

[102] VUE D'ENSEMBLE DES STRATEGIES DE PROTECTION CONTRE LA PERTE DE DONNEES : https://support.office.com/fr-fr/article/Vue-d-ensemble-des-stratégies-de-protection-contre-la-perte-de-données-1966b2a7-d1e2-4d92-ab61-42efbb137f5e

[103] PROTECT YOUR SENSITIVE INFORMATION WITH OFFICE 365 DATA LOSS PREVENTION: https://youtu.be/EFBXY-YYI9Y

[104] DATA LOSS PREVENTION IN OFFICE 365: https://mva.microsoft.com/en-us/training-courses/data-loss-prevention-in-office-365-8390?l=KgwSPyIz_2304984382

Protéger les données personnelles avec l'accès conditionnel sur la base du risque et avec une gestion des identités privilégiées

Le scénario de traitement suivant concerne pour cette section à la fois le portail Partenaires de Litware 369 et l'administration/gestion des abonnements Azure, Office 365 et Dynamics 365 et des ressources associées. Voyons comment fixer des conditions pour protéger les accès.

Mettre en place un accès conditionnel avec Azure AD

L'un des aspects essentiels d'une bonne sécurité réside dans le fait qu'elle soit presque invisible aux utilisateurs légitimes. Une friction excessive inhibe la productivité, et les utilisateurs légitimes trouveront les moyens de contourner les dispositions qui bloquent leur productivité, créant ainsi des risques (additionnels).

Bien que vous puissiez imposer pour chaque utilisateur, à chaque connexion une authentification multifacteur (MFA) – elle le sera pour les partenaires de Litware 369 -, maximiser la productivité suppose idéalement de permettre aux utilisateurs légitimes de faire leur travail avec peu d'interruptions, tout en arrêtant les personnes mal intentionnées. L'accès conditionnel dans Azure AD[105] permet de réaliser exactement cela.

Auparavant, vous auriez dû préciser : « aucun accès en dehors du réseau d'entreprise » ou « aucun accès depuis un appareil personnel » ; Aujourd'hui, la possibilité de bloquer l'accès ou de l'autoriser est offerte sous conditions. Par exemple, dans le cadre de notre illustration, une stratégie d'accès conditionnel pour l'application mobile et au « backend mobile » associé dans Azure peut reposer sur l'obligation de disposer d'un appareil enregistré pour la force de vente de Litware 369.

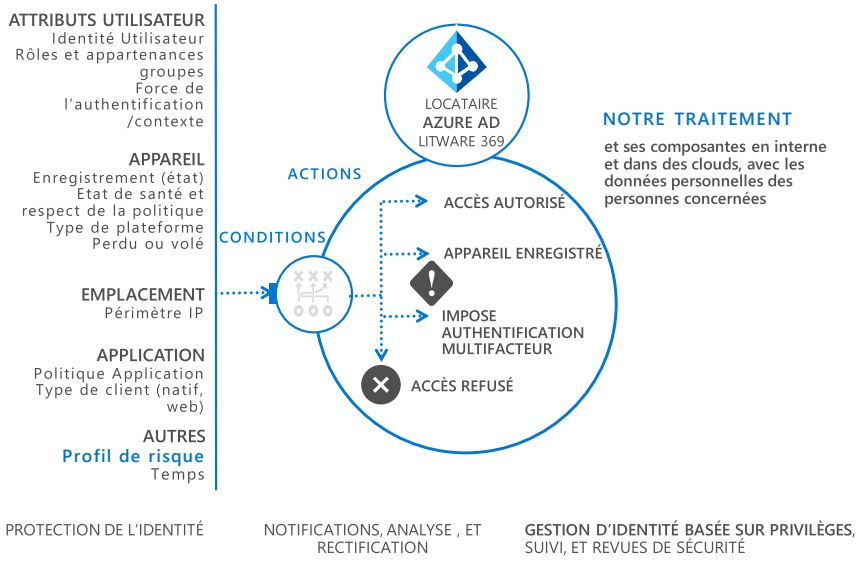

Figure 14 Contrôler les accès conditionnels avec Azure AD Premium (P1 ou P2)

[105] ACCES CONDITIONNEL DANS AZURE ACTIVE DIRECTORY : https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-conditional-access

L'accès conditionnel dans Azure AD est une fonctionnalité Azure AD Premium (P1 ou P2)[106]. Tous les utilisateurs accédant à une application ou à une ressource limitée par des stratégies d'accès conditionnel doivent disposer d'une licence Azure AD Premium.

Cet accès conditionnel se poursuit avec un session conditionnée pour SharePoint Online. De plus, la fonction proxy récemment annoncée de Cloud App Security s'intègre avec les stratégies d'accès conditionnel dans Azure AD afin de prolonger ce type de capacité à d'autres applications dans le cloud et de faire ainsi en sorte que les actions possibles au sein d'une application dépendent du contexte d'accès, une fois ce dernier accordé.

Pour autant, ces stratégies d'accès conditionnel ne se limitent pas aux seuls employés de Litware 369.

> **Remarque** Pour de plus amples informations, vous pouvez consultez l'article RAPPORT D'UTILISATION SANS LICENCE[107].

En effet, avec Azure AD B2B collaboration, Litware 369 dispose de la possibilité d'appliquer des stratégies d'authentification multifacteur[108] (MFA) pour les utilisateurs « invité » (B2B) des entreprises partenaires de Litware 369. Ces stratégies peuvent être appliquées au niveau locataire, application ou utilisateur individuel. Elles peuvent également être activées pour les employés à plein temps de Litware 369. Une telle stratégie est appliquée dans notre illustration pour le portail Partenaires.

> **Remarque importante** Les utilisateurs « invité » avec Azure AD B2B collaboration disposent d'une licence par le biais des licences Azure AD. Les fonctionnalités Azure AD payantes étendues aux utilisateurs « invité » à l'aide de la fonctionnalité de collaboration B2B, de la même façon qu'avec les stratégies d'accès conditionnel, doivent disposer d'une licence par le biais de licences Azure AD payantes. Litware 369 obtient dans la pratique 5 droits d'utilisateur « invité » avec chaque licence Azure AD payante. Autrement dit, chaque licence Azure AD payante qui fournit les droits d'utilisation des fonctionnalités payantes Azure AD à un utilisateur employé au sein de Litware 369, fournit également désormais les droits d'utilisation de ces mêmes fonctionnalités à 5 autres utilisateurs « invité » d'entreprises partenaires de Litware 369.
>
> Pour de plus amples informations, vous pouvez consultez l'article GUIDE D'ATTRIBUTION DE LICENCES POUR AZURE ACTIVE DIRECTORY B2B COLLABORATION[109].

Mettre en place un accès conditionnel sur la base du risque avec Azure AD Identity Protection

Comme l'illustre la figure précédente, il est possible d'intégrer dans les stratégies d'accès conditionnel la notion de profil de risque (accès depuis un navigateur anonymisant, depuis des endroits improbables, plusieurs tentatives d'authentification infructueuses, etc.).

Ainsi, Azure AD Identity Protection[110] permet notamment de définir des stratégies d'accès conditionnel pour atténuer les risques des connexions a priori dangereuses en bloquant les connexions ou en imposant des demandes d'authentification multifacteur. Ces stratégies sont rendues possibles par le

---

[106] Azure AD Premium (P1 ou P2) : http://www.microsoft.com/identity

[107] RAPPORT D'UTILISATION SANS LICENCE : https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-conditional-access-unlicensed-usage-report

[108] ACCES CONDITIONNEL POUR LES UTILISATEURS DE B2B COLLABORATION : https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-b2b-mfa-instructions

[109] GUIDE D'ATTRIBUTION DE LICENCES POUR AZURE ACTIVE DIRECTORY B2B COLLABORATION : https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-b2b-licensing

[110] AZURE ACTIVE DIRECTORY IDENTITY PROTECTION: https://docs.microsoft.com/fr-fr/azure/active-directory/active-directory-identityprotection

graphe de sécurité intelligent[111] (Intelligent Security Graph) de Microsoft, il s'agit de l'intelligence cumulée que nous recueillons depuis l'ensemble de nos produits, services, équipes internes mais également depuis des sources externes. En se fondant sur ces données, nous calculons le niveau de risque d'un utilisateur individuel ou celui d'une tentative de connexion. Azure AD Identity Protection notifie s'il détecte un comportement suspect, aide à l'investigation de la situation et contribue à prendre des mesures automatisées comme bloquer une tentative de connexion ou déclencher une réinitialisation du mot de passe.

D'une façon plus générale, Azure AD Identity Protection est une fonctionnalité de l'édition Azure AD Premium P2 qui permet :

- De détecter les vulnérabilités potentielles qui affectent les identités de l'organisation ;
- De configurer des réponses automatiques aux actions suspectes détectées qui sont liées aux identités de l'organisation ;
- D'examiner les incidents suspects et prendre les mesures appropriées pour les résoudre.

Remarque Pour plus d'informations, vous pouvez visionner les webinaires AZURE AD AND IDENTITY SHOW: IDENTITY PROTECTION PREVIEW[112] et RESPOND TO ADVANCED THREATS WITH AZURE ACTIVE DIRECTORY IDENTITY PROTECTION[113].

Gérer les identités privilégiées dans le Cloud avec Azure AD Privileged Identity Management (PIM)

Plus les privilèges des utilisateurs sont élevés, plus le potentiel de dommages est important si de tels comptes sont compromis. Avec la visibilité apportée sur ces identités privilégiées, Azure AD Privileged Identity Management[114] (PIM) est une fonctionnalité de l'édition Azure AD Premium P2 qui contribue à réduire le risque associé aux privilèges d'accès administrateur au moyen du contrôle, de la gestion d'accès et de la génération de rapports sur ces rôles d'administrateur critiques.

Ainsi, Azure AD Privileged Identity Management (PIM) aide à apporter une hygiène bienvenue en rendant possible une administration juste à temps (« just in time ») et administration suffisante (« just enough »). Il s'agit de donner un accès privilégié juste-à-temps temporairement ou révoquer un accès privilégié permanent de personnes deviennent le quotidien. Cette capacité est également désormais couplée avec la gestion des accès fondée sur les rôles (Role-Based Access Control en anglais ou RBAC) d'Azure pour la gestion des ressources dans Azure comme, dans le cadre de Litware369, le site web institutionnel et les portails Partenaires et Clients comme souligné précédemment.

[111] LES MILLIARDS DE POINTS DE DONNEES FONT LA DIFFERENCE : https://www.microsoft.com/fr-fr/security/intelligence

[112] AZURE AD AND IDENTITY SHOW: IDENTITY PROTECTION PREVIEW: https://channel9.msdn.com/Series/Azure-AD-Identity/Azure-AD-and-Identity-Show-Identity-Protection-Preview

[113] RESPOND TO ADVANCED THREATS WITH AZURE ACTIVE DIRECTORY IDENTITY PROTECTION: https://youtu.be/rpmjqFERIvI

[114] QU'EST-CE QU'AZURE AD PRIVILEGED IDENTITY MANAGEMENT ? : https://azure.microsoft.com/fr-fr/documentation/articles/active-directory-privileged-identity-management-configure/

Remarque Pour plus d'informations, vous pouvez visionner le webinaire INTRODUCTION A AZURE AD PRIVILEGED IDENTITY MANAGEMENT (PIM)[115].

La réduction du temps d'exposition des privilèges et l'augmentation de la visibilité de leur utilisation aident Litware 369 à poursuivre son effort dans la sécurisation de l'accès privilégié tel que développé à la section § GERER LES ROLES ET LES RESPONSABILITES.

Remarque Pour plus d'informations, vous pouvez consulter l'article SECURISATION DE L'ACCES PRIVILEGIE[116].

Gérer les identités privilégiées en interne avec notamment Privileged Access Management (PAM)

Au-delà des identités privilégiées utilisées au niveau des abonnements Azure, Office 365 et Dynamics 365, Litware 369 souhaite également octroyer des privilèges juste à temps (JIT) pour son déploiement existant d'AD. La solution Privileged Access Manager (PAM)[117] permet d'atteindre cet objectif en restreignant l'accès privilégié au sein d'un environnement AD existant.

PAM remplit deux objectifs :

1. Rétablissement du contrôle d'un environnement AD compromis en conservant un environnement bastion distinct connu pour être non affecté par des attaques malveillantes ;
2. Isolement de l'utilisation des comptes privilégiés pour réduire le risque de vol de ces informations d'identification.

PAM est une instance de PIM implémentée à l'aide de Microsoft Identity Manager (MIM).

En plus de ne plus avoir d'administrateurs permanents, Litware 369 souhaite reproduire en interne les principes d'une administration suffisante (« just enough ») comme avec PIM pour le Cloud. Pour cela, et afin de réduire le nombre de comptes avec des privilèges d'administration de domaine et le risque d'exposition associé, Litware 369 utilise la fonctionnalité JEA (« Just Enough Administration ») au sein de Windows PowerShell pour effectuer toutes les opérations de maintenance courantes sur les contrôleurs de domaine. La technologie JEA est une boîte à outils PowerShell qui définit un ensemble de commandes pour effectuer des activités privilégiées ainsi qu'un point de terminaison où les administrateurs peuvent obtenir l'autorisation pour exécuter ces commandes. La technologie JEA autorise ainsi certains utilisateurs à effectuer des tâches administratives spécifiques sur les serveurs (tels que les contrôleurs de domaine) sans leur octroyer de droits d'administrateur.

Remarque Pour plus d'informations, vous pouvez consulter l'article JUST ENOUGH ADMINISTRATION[118].

Renforcer la sécurité d'accès aux comptes des clients (personnes concernées)

Cette section étudie le scénario de traitement du portail Clients de Litware 369.

Comme abordé précédemment (Cf. section § GERER DE FAÇON SECURISEE L'ACCES B2C AUX DONNEES, APPLICATIONS ET AUTRES RESSOURCES), Azure AD B2C a permis de s'affranchir de la base de comptes dans

[115] INTRODUCTION A AZURE AD PRIVILEGED IDENTITY MANAGEMENT (PIM) : https://channel9.msdn.com/Blogs/Concretement/Episode-27-Azure-AD-PIM

[116] SECURISATION DE L'ACCES PRIVILEGIE : https://docs.microsoft.com/fr-fr/windows-server/identity/securing-privileged-access/securing-privileged-access

[117] PRIVILEGED ACCESS MANAGEMENT POUR LES SERVICES DE DOMAINE ACTIVE DIRECTORY : https://docs.microsoft.com/fr-fr/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

[118] JUST ENOUGH ADMINISTRATION: https://msdn.microsoft.com/powershell/jea/overview

SQL Server pour la gestion des accès de ses clients et de mettre en œuvre des parcours utilisateur adaptés.

Avec la définition de ces parcours Litware 369 bénéficie de la possibilité d'imposer une authentification forte pour les clients au niveau de la définition/configuration des politiques applicatives associées pour le portail Clients. Cette authentification forte repose sur l'authentification multifacteur abordé précédemment.

Celle-ci permet à Litware 369 de tirer parti de la connaissance des numéros de téléphone de ses clients, numéros de téléphone qui font partie des données personnelles collectées dans le cadre de notre scénario « représentatif » de traitement. Une mention d'information pour le traitement considéré permet d'en avertir l'utilisateur lors du recueil et de l'enregistrement de son consentement explicite.

Tout en offrant une souplesse à ses clients qui peuvent réutiliser une identité sociale comme Facebook, Google, Microsoft, Twitter, etc. à l'instar de ce qui se pratique couramment pour les sites et portails de type B2C, Litware 369 renforce dans le même temps la sécurité d'accès aux comptes de ses clients et généralise la pratique adoptée envers les employés des entreprises partenaires pour la partie B2B.

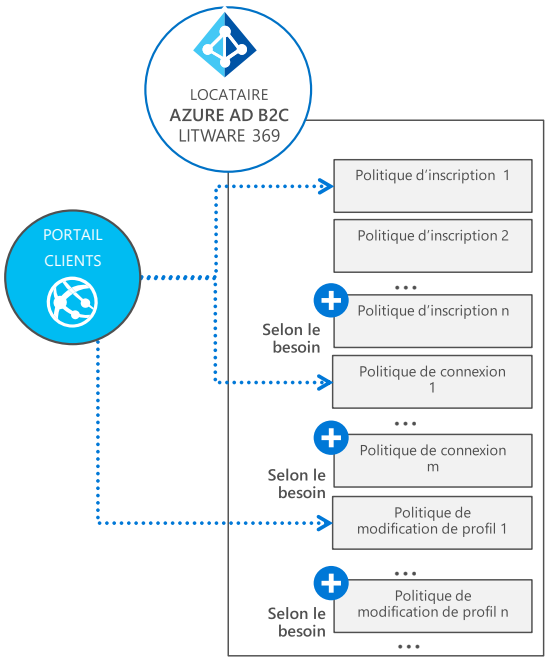

Figure 15 Mettre en œuvre des parcours utilisateur adaptés avec Azure AD B2C

Adopter une posture « Assumer des violations de données personnelles »

L'approche programmatique pour le cheminement vers la conformité avec le GDPR est pilotée par les risques et leur analyse circonstanciée permet de mettre les bonnes priorités, en particulier, comme illustré au travers de notre scénario « représentatif » de traitement de données, de préciser les mesures techniques appropriées en termes de contrôles de sécurité.

Vient ensuite la posture « **Assumer des violations de données personnelles** ». Voyons de quoi il en retourne.

Protéger l'environnement du traitement

Les exigences clé du GDPR en matière de sécurité des données personnelles s'articulent autour de 2 piliers, au-delà de l'analyse et de l'évaluation des risques :

1. Prévention et protection ;
2. Surveillance et détection.

Ces deux piliers supposent désormais d'intégrer dans les réflexions le fait troublant que des violations de données personnelles sont inévitables en dépit de toutes les dispositions prises pour atténuer les risques identifiés par l'étude préalable qui a été conduite pour ce traitement.

L'adoption d'une posture « Assumer des violations de données personnelles » permet d'intégrer ce fait. Cela représente un changement majeur qui consiste à **s'autoriser à penser que les défenses numériques soient vulnérables à un moment donné pour un traitement**.

Nous vivons dans un monde où les attaques et les vecteurs d'attaques peuvent provenir de n'importe où. L'actualité démontre malheureusement chaque jour que les attaques sont de plus en plus sophistiquées, les attaquants de plus en plus organisés, etc. C'est un monde sans périmètre, dynamique en perpétuelle évolution.

Accepter une telle posture ne veut pas dire se soumettre ; cela signifie que vous avez suivi la première étape vers l'atténuation des risques pour l'intégrité des données (personnelles) dans l'ère numérique comme en témoigne l'article ASSUMPTION OF BREACH: HOW A NEW MINDSET CAN HELP PROTECT CRITICAL DATA[119].

Quel est alors le plan B ? Quel est le plan pour détecter une intrusion ? Comment réagir face à ce type d'incident ?

Cette posture implique de passer d'un simple modèle « **Protéger et Recouvrer** » à une nouvelle stratégie et une posture plus globale comprenant aujourd'hui à minima le triptyque suivant :

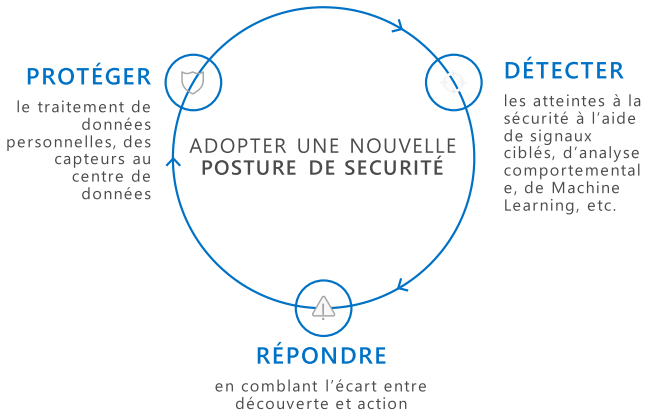

Figure 16 Adopter une nouvelle posture de sécurité

Cette stratégie de protection de l'environnement du traitement se traduit donc par la nécessité de prévenir proactivement les menaces – ce que l'on entendait jusqu'à lors par protéger -, à laquelle il est nécessaire d'ajouter celle de détecter et de répondre rapidement aux menaces. Les trois phases protéger, détecter et répondre représentent un continuum comme illustré ci-avant.

[119] ASSUMPTION OF BREACH: HOW A NEW MINDSET CAN HELP PROTECT CRITICAL DATA:
http://searchsecurity.techtarget.com/tip/Assumption-of-breach-How-a-new-mindset-can-help-protect-critical-data

Ainsi, la détection d'une attaque en cours peut éviter l'exfiltration des données personnelles et donc une violation au sens du GDPR si ces deux (nouvelles) dimensions sont correctement prises en compte.

En termes de détection, il s'agit notamment d'aller vers une approche comportementale où la détection des violations s'effectue selon le comportement (du vecteur d'attaque dans le cas d'une intrusion) en utilisant des signaux ciblés, la surveillance du comportement (« behavior analytics ») et le Machine Learning. Par exemple, la détection à temps d'une attaque en cours peut éviter l'exfiltration des données personnelles et donc une violation au sens du GDPR.

Et pour ce qui est de la réponse, c'est un domaine qui suppose l'application dynamique de contrôles de sécurité en réponse à la détection pour combler l'écart entre la découverte et l'action en réaction. Cela passe par un changement radical dans la façon de réagir.

Voyons comment ces dimensions peuvent se traduire dans notre traitement avec les produits et services de cloud que Microsoft suggère pour accompagner cette transformation en cours.

Proactivement prévenir, détecter et répondre rapidement aux menaces

Notre scénario de traitement concerne dans un premier temps le site institutionnel et les portails Partenaires et Clients de Litware 369, ainsi que les ressources Azure associées.

Aider à prévenir, détecter et répondre aux menaces qui pèsent sur les données personnelles dans Azure avec Azure Security Center

Azure Security Center[120] donne la visibilité et le contrôle sur la sécurité des ressources Azure de Litware 369. Il surveille en continu les ressources, fournit des recommandations de sécurité utiles et aide à empêcher, détecter les menaces et y répondre. Les fonctionnalités d'analyses avancées intégrées d'Azure Security Center aident à identifier les attaques qui pourraient ne pas être détectées, à en comprendre la nature profonde et à prendre les bonnes dispositions pour casser la chaîne d'attaque (« kill chain ») à temps.

> **Remarque** Pour plus d'informations, vous pouvez consulter l'article PRESENTATION DU CENTRE DE SECURITE AZURE[121] et visionner le webinaire USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS[122].

[120] Azure Security Center : https://azure.microsoft.com/fr-fr/services/security-center/

[121] PRESENTATION DU CENTRE DE SECURITE AZURE : https://docs.microsoft.com/fr-fr/azure/security-center/security-center-intro

[122] USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS: https://youtu.be/iqwaja4NCso

Remarque Pour plus d'informations sur la sécurité (dans) Azure, vous pouvez consulter la présentation des SERVICES ET TECHNOLOGIES DE SECURITE AZURE[123].

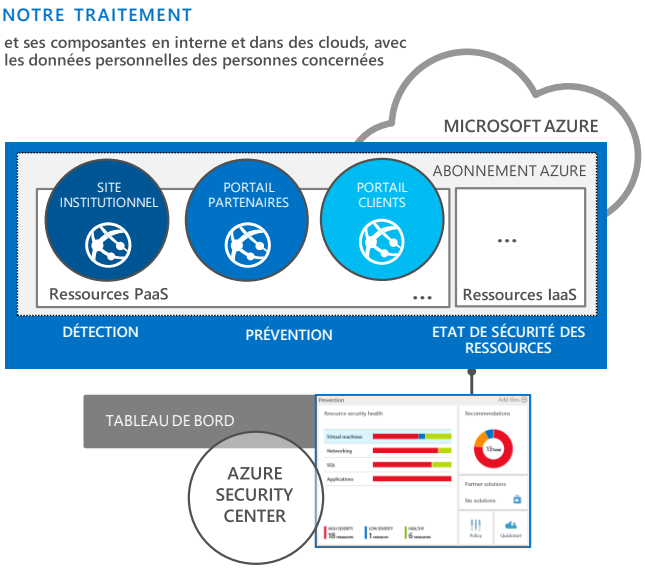

Figure 17 Aider à prévenir, détecter et répondre aux menaces avec une visibilité accrue avec Azure Security Center

Aider à prévenir, détecter et répondre aux menaces qui pèsent sur les données personnelles en interne avec Advanced Thread Analytics (ATA) ou Azure Advanced Threat Protection (ATP)

Notre scénario de traitement se concentre à présent sur l'infrastructure interne, à savoir l'annuaire Active Directory et les bases de données SQL Server. Il s'agit ici et à présent de pouvoir protéger les identités accédant aux données personnelles ou aux ressources relatives à la base de données SQL Server et générer des alertes en cas d'activité(s) suspicieuse(s).

Dans ce contexte, Advanced Thread Analytics (ATA)[124] propose une plate-forme pour l'environnement interne d'une entreprise comme Litware 369 qui aide à identifier les menaces et les attaques de sécurité avancées avant qu'elles ne causent des dommages.

Ainsi, Advanced Thread Analytics (ATA) contribue à localiser les violations et identifie les attaquants à l'aide de technologies de détection des anomalies et d'analyse des comportements innovantes. ATA est déployé à demeure et fonctionne avec le déploiement Active Directory existant de Litware 369. Il utilise le Machine Learning et l'analyse des comportements des utilisateurs ainsi que les interactions associées pour trouver des menaces avancées et persistantes et détecter des activités suspectes voire des attaques malveillantes utilisées par des cybercriminels, en identifiant les violations avant qu'elles ne portent préjudice à l'activité de Litware 369. Une analyse chronologique simple à utiliser est proposée ainsi que l'envoi d'alertes en temps quasi réel.

[123] SERVICES ET TECHNOLOGIES DE SECURITE AZURE : https://docs.microsoft.com/fr-fr/azure/security/azure-security-services-technologies

[124] Advanced Thread Analytics (ATA) : https://www.microsoft.com/fr-fr/cloud-platform/advanced-threat-analytics

Remarque Pour plus d'informations, vous pouvez consulter l'article WHAT IS ADVANCED THREAT ANALYTICS?[125] et visionner le webinaire USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS[126].

Le service Azure Advanced Threat Protection (ATP) qui vient d'être annoncé offre désormais des capacités similaires mais sous forme de service géré dans Azure.

Remarque Pour plus d'informations, vous pouvez consulter le billet INTRODUCING AZURE ADVANCED THREAT PROTECTION[127].

Analyser et attribuer avec Secure Score une évaluation (score) de la sécurité de l'abonnement Office 365

Notre scénario de traitement se focalise à présent sur les services de collaboration d'Office 365, en l'occurrence Exchange Online et SharePoint Online. Cela concerne notamment la bibliothèque de formulaires Word (dossier de commande avec les caractéristiques techniques de l'installation).

Secure Score est un outil permettant l'analyse de la sécurité des services Office 365 (Exchange Online, et SharePoint Online dans le cadre de notre traitement). Accessible à partir du site web https://securescore.office.com, cet outil affecte un score à l'environnement de Litware 369 en se basant sur les paramètres de sécurité positionnés versus l'ensemble des paramètres disponibles et applicables. Une chronologie est disponible indiquant ainsi la progression du niveau sécurité de l'environnement avec un comparatif sur la moyenne observée chez l'ensemble des autres clients Office 365.

Afin d'atténuer les risques de sécurité et d'améliorer le score, des suggestions de remédiation détaillées sont proposées.

Remarque Pour plus d'informations, vous pouvez consulter l'article INTRODUCING THE OFFICE 365 SECURE SCORE[128] et visionner le webinaire AN INTRODUCTION TO OFFICE 365 SECURE SCORE[129].

Litware 369 dispose ainsi i) de propositions adaptées de contrôles et des paramètres de sécurité afin de réduire les risques d'attaque sur les données personnelles et ii) de l'établissement d'un suivi de la progression du niveau de sécurité global.

[125] WHAT IS ADVANCED THREAT ANALYTICS?: https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata

[126] USE AZURE SECURITY CENTER TO PREVENT, DETECT, AND RESPOND TO THREATS: https://youtu.be/iqwaja4NCso

[127] INTRODUCING AZURE ADVANCED THREAT PROTECTION: https://cloudblogs.microsoft.com/enterprisemobility/2017/09/27/introducing-azure-advanced-threat-protection/

[128] INTRODUCING THE OFFICE 365 SECURE SCORE: https://support.office.com/en-US/article/Introducing-the-Office-365-Secure-Score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef?ui=en-US&rs=en-US&ad=US/

[129] AN INTRODUCTION TO OFFICE 365 SECURE SCORE: https://www.youtube.com/watch?v=h__nxWlm5Nc&feature=youtu.be

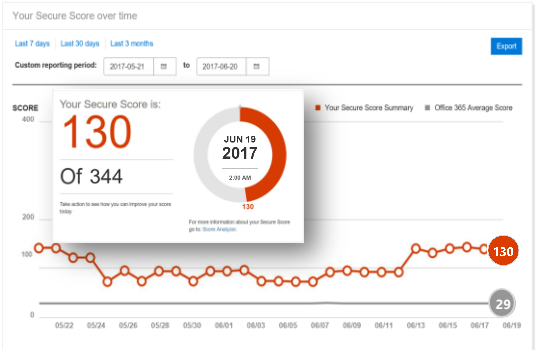

Figure 18 Analyser et attribuer avec Secure Score une évaluation (score) de la sécurité de l'abonnement Office 365

Protéger et gérer la conformité pour l'ensemble des données de Litware 369 via le Centre de sécurité et de conformité Office 365

Notre scenario de traitement reste ici le même qu'à la section précédente, c'est-à-dire avec les services de collaboration d'Office 365.

Afficher et gérer les alertes de sécurité avancée

La disponibilité de renseignements sur les menaces (Threat Intelligence) aide à découvrir de façon proactive des menaces avancées et à en protéger les ressources de Litware 369 dans Office 365. Des indications précises sur les menaces, fournies par la présence mondiale de Microsoft, le graphe de sécurité intelligent déjà abordé et des informations issues des « chasseurs de menaces cybernétiques », aident à mettre en œuvre rapidement et efficacement des alertes, des stratégies dynamiques et des solutions de sécurité.

> **Remarque** Pour plus d'informations, vous pouvez consulter le billet APPLYING INTELLIGENCE TO SECURITY AND COMPLIANCE IN OFFICE 365[130].

Auditer et suivre l'activité des utilisateurs de Litware 369 pour Office 365

La Gestion avancée de la sécurité (Advanced Security Management en anglais ou ASM) permet d'identifier un risque élevé ou une utilisation anormale, qui avertissent les administrateurs de Litware 369 de violations potentielles. En outre, il permet de définir des politiques d'activité pour suivre les actions qui présentent un risque élevé et y répondre.

[130] APPLYING INTELLIGENCE TO SECURITY AND COMPLIANCE IN OFFICE 365 : https://blogs.office.com/2016/09/26/applying-intelligence-to-security-and-compliance-in-office-365/

Remarque Pour plus d'informations, vous pouvez consulter le billet GAIN ENHANCED VISIBILITY AND CONTROL WITH OFFICE 365 ADVANCED SECURITY MANAGEMENT[131] et visionner le webinaire INTRODUCING ADVANCED SECURITY MANAGEMENT FOR OFFICE 365[132].

Aider à prévenir, détecter et répondre aux menaces qui pèsent sur les données personnelles dans Dynamics 365

Notre scénario de traitement se concentre à présent sur la conclusion de cette partie concernant le service Cloud Dynamics 365.

Comme nous avons déjà pu le développer à maintes reprises, contrôler l'accès aux données personnelles est un élément clé pour la protection et la sécurité des données.

Dynamics 365 s'appuie sur la sécurité des identités de Azure AD et permet de gérer et de contrôler l'accès aux données de plusieurs façons :

- La **sécurité basée sur les rôles** dans Dynamics 365 permet de regrouper un ensemble de privilèges qui limitent les tâches pouvant être effectuées par un utilisateur donné. Il s'agit d'une fonctionnalité cruciale, plus particulièrement lorsque les utilisateurs changent de rôles au sein d'une entreprise. Par exemple, dans le cas présent, pour des collaborateurs de Litware 369 qui rejoignent en raison d'une mobilité interne, le service Abonnements ou au contraire qui n'en ferait plus partie.
- La **sécurité basée sur les enregistrements** dans Dynamics 365 permet de limiter l'accès à des enregistrements spécifiques.
- La **sécurité au niveau des champs** dans Dynamics 365 permet de limiter l'accès à des champs spécifiques ayant un impact élevé, tels que des informations d'identification personnelle.

Dynamics 365 propose dans le même temps les capacités permettant de suivre l'activité.

Remarque Pour plus d'informations, vous pouvez consulter le blog dédié[133] et visionner le webinaire DYNAMICS 365 FOR OPERATIONS – TECH TALK: REPORTING OPTIONS[134].

Exemples de solutions

La protection des données personnelles et, une approche « Assumer les violations de données personnelles », de façon générale et non pas uniquement vis-à-vis du cadre restreint de notre illustration, peuvent tirer parti d'autres produits et solutions Cloud de Microsoft au-delà des exemples utilisés ici.

[131] GAIN ENHANCED VISIBILITY AND CONTROL WITH OFFICE 365 ADVANCED SECURITY MANAGEMENT: https://blogs.office.com/2016/06/01/gain-enhanced-visibility-and-control-with-office-365-advanced-security-management/

[132] INTRODUCING ADVANCED SECURITY MANAGEMENT FOR OFFICE 365: https://www.youtube.com/watch?v=gWTSTqNHgSg

[133] Blog Microsoft Dynamics 365: https://community.dynamics.com/b/msftdynamicsblog

[134] DYNAMICS 365 FOR OPERATIONS – TECH TALK: REPORTING OPTIONS: https://youtu.be/NzZONjKs5xA

Remarque Le livre blanc LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES[135] propose des exemples d'actions à entreprendre avec Microsoft dès aujourd'hui pour entamer votre cheminement vers la conformité avec le GDPR. Vous pouvez consulter ce livre blanc pour une illustration des mesures à prendre dans ce contexte pour la protection des données personnelles et de la façon dont les produits et services de cloud de Microsoft peuvent contribuer à la mise en œuvre (ou à la traduction effective) de celles-ci.

Rapporter - Maintenir la documentation requise, et gérer les demandes relatives aux données personnelles et les notifications de violation

Notre cheminement vers la conformité avec le GDPR nous amène logiquement à l'étape des rapports et de tout ce qui a attrait à la documentation requise.

Cette étape se traduit comme précédemment dans un ensemble d'activité(s) de la phase **VERIFIER** (du modèle PDCA) du programme GDPR suggéré par le livre blanc GDPR – S'ORGANISER ET METTRE EN PLACE LES BONS PROCESSUS POUR LA MISE EN CONFORMITE AU GDPR. Ces activités et actions associées consistent à notamment constituer et maintenir dans le temps la documentation relative à la conformité GDPR.

Voyons comment ceci peut se traduire à l'aide d'exemples de produits et de services Cloud de Microsoft.

Constituer la documentation relative à la conformité GDPR

Constituer la documentation requise pour prouver la conformité et gérer l'exercice des droits ainsi que la notification des violations couvre différents volets.

Dans le contexte qui nous intéresse et pour soutenir ces activités, il s'agit de définir l'outillage permettant de faire en sorte que tout traitement de données personnelles soit suivi et enregistré dans des documents ou journaux : que ce soit au niveau de la collecte, de l'utilisation, du transfert de données, etc.

Constituer la documentation relative aux sous-traitants

Notre scénario de traitement concerne, pour cette section, les abonnements Azure, Office 365 et Dynamics 365.

Un certain nombre de questions légitimes se posent et s'imposent avec le GDPR :

Qui a accès à vos données ? Où sont-elles ? Que fait Microsoft pour les protéger ? Comment pouvez-vous vérifier que Microsoft respecte ses engagements ?

Autant de questions qui trouvent leur réponse dans l'exploitation de la documentation complète du Centre Confiance[136] (Trust Center) de Microsoft sur la conformité, la sécurité et la protection de la vie privée. Cette documentation comprend en particulier la description des offres de services, les rapports d'audit de conformité pour les certifications obtenues mais également un corpus de documents en

[135] LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES : https://aka.ms/gdprwhitepaper

[136] Centre de confiance Microsoft : http://www.microsoft.com/fr-fr/trustcenter

termes de foires aux questions et livres blancs, de guides de conformité, d'analyses de sécurité et de tests de pénétration.

Nous sommes engagés sur la conformité avec le GDPR pour les services de cloud de Microsoft comme en témoigne la vidéo LES ENGAGEMENTS DE MICROSOFT VIS-A-VIS DU GDPR[137] de Brendon Lynch, notre responsable de la protection de la vie privée. Ceci s'inscrit dans la façon dont nous opérons nos services Cloud en mettant en œuvre des standards éthiques élevés qui fournissent la transparence sur la façon dont nous concevons nos services et protégeons les données de nos clients.

Fournir sur la base des journaux d'activité des informations non falsifiables et dignes de confiance

Au-delà de la constitution de la documentation précédente, notre scénario de traitement concerne, pour cette section, l'utilisation des ressources des abonnements Azure, Office 365 et Dynamics 365, c'est-à-dire :

- Les site web institutionnel et portails Partenaires et Clients de Litware 369 ;
- Exchange Online avec les boîtes aux lettres et courriels ;
- SharePoint Online avec la bibliothèque de formulaires Word (dossier de commande avec les caractéristiques techniques de l'installation) ;
- Dynamics 365 et les compte clients, numéros de contrats, etc.

L'objectif poursuivi consiste à aider à fournir sur la base des journaux d'activité des informations non falsifiables et dignes de confiance relatives au traitement.

Azure fournit des options configurables d'audit et de journalisation qui peuvent aider à identifier les lacunes dans les stratégies de sécurité et à y remédier en vue d'empêcher les violations.

Ainsi, par exemple, Azure Log Analytics[138] vous aide à collecter et analyser les données générées par des ressources dans votre environnement cloud ou à demeure. Il fournit des informations en temps réel à l'aide de la recherche intégrée et de tableaux de bord personnalisés pour analyser rapidement des millions d'enregistrements des charges de travail et serveurs quel que soit leur emplacement physique dans un contexte de Cloud hybride.

Remarque Pour plus d'informations, vous pouvez consulter l'article PRESENTATION DE LOG ANALYTICS[139] et visionner le webinaire COMBATING CORPORATE SECURITY THREATS: GETTING STARTED WITH LOG ANALYTICS[140].

[137] LES ENGAGEMENTS DE MICROSOFT VIS-A-VIS DU GDPR : https://aka.ms/GDPRCommitmentVideo

[138] Azure Log Analytics : https://azure.microsoft.com/fr-fr/services/log-analytics/

[139] PRESENTATION DE LOG ANALYTICS : https://docs.microsoft.com/fr-fr/azure/log-analytics/log-analytics-overview

[140] COMBATING CORPORATE SECURITY THREATS: GETTING STARTED WITH LOG ANALYTICS: https://youtu.be/1bDj0lSAvTY

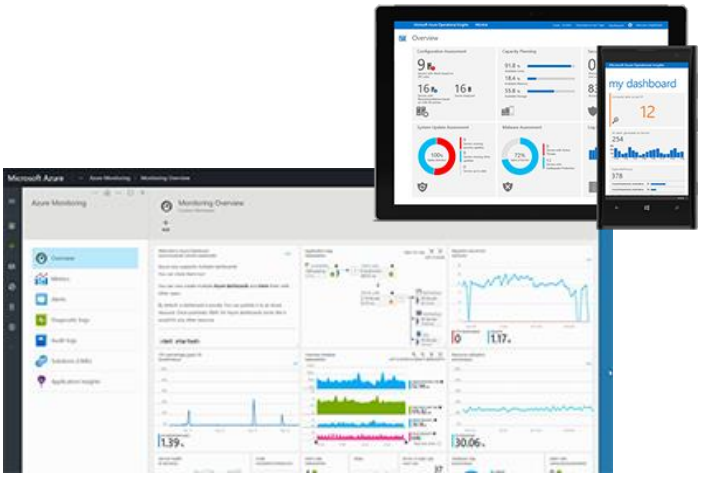

Figure 19 Disposer d'informations non falsifiables et dignes de confiance sur le traitement avec Azure Monitor/Azure Log Analytics

De même, les journaux d'audit[141] d'Office 365 permettent de surveiller et de suivre les activités des utilisateurs et administrateurs sur les charges de travail dans Office 365 de Litware 369, ce qui contribue à la détection précoce et à l'examen des problèmes liés à la sécurité et à la conformité.

Remarque Pour plus d'informations, vous pouvez visionner le webinaire OWN YOUR DATA AND SERVICE - MONITOR AND INVESTIGATE WITH OFFICE 365 AUDITING, INSIGHTS AND ALERTS[142].

Disposer d'un tableau de bord de gestion de la conformité

Au-delà des illustrations précédentes, il nous parait enfin important de souligner la prochaine disponibilité d'un gestionnaire de la conformité (Compliance Manager) destiné à vous aider à gérer votre posture de conformité depuis un seul et même emplacement pour tous les services de cloud de Microsoft.

Compliance Manager vous permettra d'effectuer une évaluation des risques en temps réel pour les services de cloud Microsoft, fournissant un score intelligent qui reflète vos performances en matière de conformité quant aux diverses exigences réglementaires de protection des données.

Vous serez également en mesure d'utiliser la gestion des contrôles intégrés et des outils de reporting afin d'améliorer et de surveiller votre posture de conformité.

[141] EFFECTUER DES RECHERCHES DANS LE JOURNAL D'AUDIT DANS LE CENTRE DE SECURITE ET CONFORMITE OFFICE 365 : https://support.office.com/fr-fr/article/Effectuer-des-recherches-dans-le-journal-d-audit-dans-le-Centre-de-s%c3%a9curit%c3%a9-et-conformit%c3%a9-Office-365-0d4d0f35-390b-4518-800e-0c7ec95e946c

[142] OWN YOUR DATA AND SERVICE - MONITOR AND INVESTIGATE WITH OFFICE 365 AUDITING, INSIGHTS AND ALERTS: https://youtu.be/CEeOCoV863U

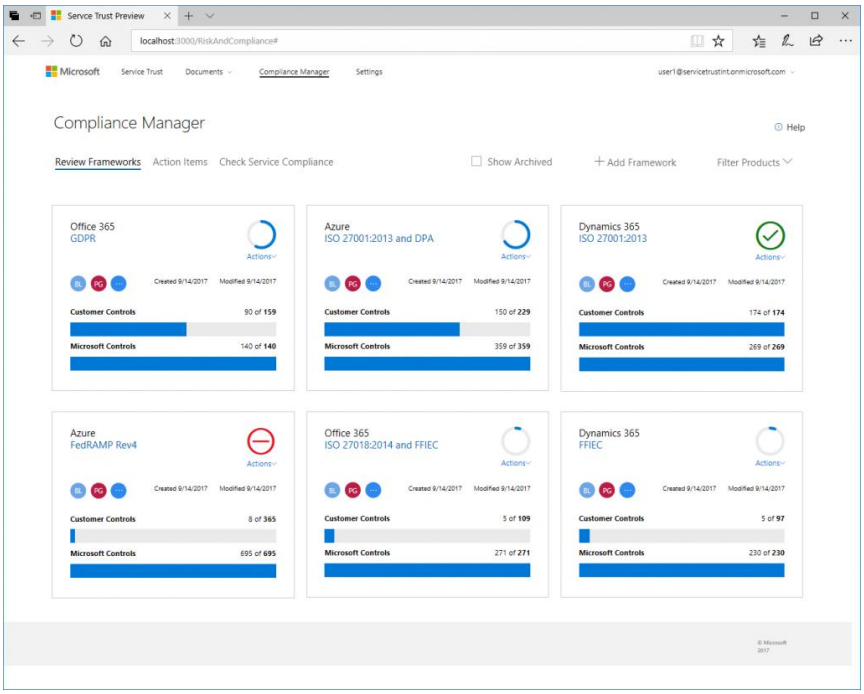

Figure 20 Exemple de tableau de bord de Compliance Manager

Remarque Pour plus d'informations, vous pouvez consulter le blog dédié[143].

Remarque importante Vous pouvez d'ores et déjà vous inscrire au programme de version préliminaire qui débutera à partir du mois de novembre 2017 : https://resources.office.com/ww-landing-compliance-manager-trial.html.

Exemples de solutions

Les journaux d'activité proposés au niveau des services de cloud de Microsoft contribuent à disposer d'informations non falsifiables et dignes de confiance relatives au traitement. Ces informations constituent l'un des pans de la documentation à produire et à maintenir, au même titre que celles relatives au sous-traitant qu'est ici Microsoft dans le cadre de l'utilisation par Litware 369 de ces services Cloud.

La production et le maintien à jour dans le temps de la documentation requise d'une façon générale, et non pas uniquement vis-à-vis du cadre restreint de notre illustration, peuvent tirer parti d'autres produits et solutions Cloud de Microsoft au-delà des exemples pris ici.

[143] MANAGE YOUR COMPLIANCE FROM ONE PLACE – ANNOUNCING COMPLIANCE MANAGER PREVIEW PROGRAM: https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Manage-Your-Compliance-from-One-Place-Announcing-Compliance/ba-p/106493

Remarque Le livre blanc LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES[144] propose des exemples d'actions à entreprendre avec Microsoft dès aujourd'hui pour entamer votre cheminement vers la conformité avec le GDPR. Vous pouvez consulter ce livre blanc pour une illustration des actions à effectuer dans ce contexte, pour la constitution et le maintien à jour dans le temps de la documentation requise sur les traitements et de la façon dont les produits et services de cloud de Microsoft peuvent contribuer à celles-ci.

[144] LE DEBUT DE VOTRE CHEMINEMENT VERS LA CONFORMITE AVEC LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES : https://aka.ms/gdprwhitepaper

En guise de conclusion

Comme indiqué en introduction de ce livre blanc, Microsoft se tient à vos côtés pour vous aider dans votre cheminement vers la conformité avec le GDPR :

- Les services Cloud de Microsoft, tels qu'Azure, Office 365 et Dynamics 365, pour ne reprendre que ceux mis en œuvre dans le cadre de notre scénario « représentatif » de traitement, vous permettent de faciliter les processus que vous devez implémenter pour assurer la conformité GDPR grâce à l'Intelligence Artificielle (IA), l'innovation et la collaboration.
- Grâce à nos solutions en local et à nos services Cloud, Microsoft vous aide à localiser et cataloguer les données personnelles de vos traitements dans vos systèmes, à construire un environnement (hybride) plus sécurisé et à simplifier la gestion et le suivi des données personnelles. Nous espérons que les illustrations données à l'aide de notre scénario « représentatif » de traitement vous permettent de mieux en appréhender les apports.
- Pour aider les organisations à répondre à leurs exigences GDPR, Microsoft investit dans des fonctionnalités et des capacités supplémentaires. Nous en avons évoqué quelques-unes dans notre progression au sein des étapes principales dans le cheminement vers la conformité avec le GDPR pour un traitement donné.
- Enfin, nous partageons les bonnes pratiques de nos propres experts sur la protection de la vie privée.

Nous espérons que ce livre blanc est l'occasion d'initier - si tel n'est pas déjà le cas - votre cheminement vers la conformité avec le GDPR. Ce règlement sera applicable à compter du 25 mai 2018.

Références

Liens utiles sur le Centre de confiance Microsoft

A propos des services et produits Microsoft sur microsoft.com/GDPR :

- Microsoft Azure,
- Microsoft Dynamics 365,
- Microsoft Enterprise Mobility + Security (EM+S),
- Microsoft Office et Office 365,
- Microsoft SQL Server et Azure SQL Database (base de données en tant que service),
- Windows 10 et Windows Server 2016.

Et pour aller plus loin, en termes d'ebooks et de livres blancs :

- An Overview of the General Data Protection Regulation[145].
- Accelerate your GDPR compliance with the Microsoft Cloud[146].
- Beginning your General Data Protection Regulation (GDPR) journey[147].
- Supporting Your EU GDPR Compliance Journey With Enterprise Mobility + Security[148].
- How Microsoft Azure Can Help Organizations Become Compliant with the GDPR[149].
- Accelerate your General Data Protection Regulation (GDPR) Compliance Journey with Microsoft 365[150].
- Guide to enhancing privacy and addressing GDPR requirements with the Microsoft SQL Platform[151].
- Accelerate GDPR with Windows 10[152].

[145] An Overview of the General Data Protection Regulation: https://aka.ms/GDPROverview

[146] Accelerate your GDPR compliance with the Microsoft Cloud: https://aka.ms/gdprebook

[147] Beginning your General Data Protection Regulation (GDPR) journey: https://aka.ms/gdprwhitepaper

[148] Supporting your EU GDPR compliance journey with Microsoft EMS: https://aka.ms/emsgdprwhitepaper

[149] How Microsoft Azure Can Help Organizations Become Compliant with the GDPR: https://aka.ms/gdpr-azure-whitepaper

[150] Accelerate your General Data Protection Regulation (GDPR) Compliance Journey with Microsoft 365: https://aka.ms/m365-gdpr-paper

[151] Guide to enhancing privacy and addressing EU GDPR requirements with the Microsoft SQL platform: http://aka.ms/gdprsqlwhitepaper

[152] Accelerate GDPR with Windows 10: https://aka.ms/WindowsGDPRwhitepaper

Ou encore de billets (sur les scénarios clé couverts par Microsoft Enterprise Mobility + Security) :

- Vue d'ensemble d'EM+S vis-à-vis du cheminement vers la conformité avec le GDPR[153].
- Azure Information Protection[154] – Comment protéger de façon persistante les données personnelles en local et dans le Cloud.
- Azure Active Directory[155] – Comment conférer un accès ou restreindre l'accès aux données personnelles.
- Cloud App Security[156] – Comment protéger les données (personnelles) dans les applications et les appareils mobiles.
- Intune[157] – Comment gagner en visibilité et contrôler les données (personnelles) dans les applications Cloud.
- Advanced Threat Analytics[158] – Comment détecter les vulnérabilités avant qu'elles ne causent des dommages

[153] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 1: https://blogs.technet.microsoft.com/enterprisemobility/2017/05/24/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance/

[154] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 2: https://blogs.technet.microsoft.com/enterprisemobility/2017/06/06/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-1/

[155] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 3: https://blogs.technet.microsoft.com/enterprisemobility/2017/06/27/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-3/

[156] How Microsoft EMS can support you in your journey to EU GDPR compliance – part 4: https://blogs.technet.microsoft.com/enterprisemobility/2017/07/07/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-4/

[157] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 5: https://blogs.technet.microsoft.com/enterprisemobility/2017/07/13/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-5/

[158] How Microsoft EMS can support you in your journey to EU GDPR compliance – Part 6: https://blogs.technet.microsoft.com/enterprisemobility/2017/08/07/how-microsoft-ems-can-support-you-in-your-journey-to-eu-gdpr-compliance-part-6/

Microsoft France
39 Quai du Président Roosevelt
92130 Issy-Les-Moulineaux