COMMENCER VOTRE CHEMINEMENT VERS LA CONFORMITÉ AVEC LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (GDPR)

Découverte

Gestion

Protection

Rapport

MICROSOFT.COM/GDPR

Microsoft

Table des matières

Clause de non-responsabilité

Ce livre blanc constitue un commentaire sur le GDPR, tel que l'interprète Microsoft, à la date de publication. Nous avons consacré énormément de temps au GDPR et nous aimerions croire que nous avons bien réfléchi à son objet et à sa signification. Toutefois, l'application du GDPR dépend largement des faits propres à chaque cas et tous les aspects et les interprétations du GDPR sont loin d'être bien établis.

Par conséquent, ce livre blanc est fourni à titre informatif seulement et ne doit en aucun cas servir de conseil légal ou déterminer comment le GDPR pourrait s'appliquer à vous et à votre organisation. Nous vous invitons à faire appel à un professionnel qualifié sur le plan juridique pour discuter du GDPR, de la manière dont il s'applique spécifiquement à votre organisation et de la meilleure façon d'assurer la conformité.

MICROSOFT N'ÉMET AUCUNE GARANTIE, EXPRESSE, IMPLICITE OU STATUTAIRE, QUANT AUX INFORMATIONS QUI FIGURENT DANS CE LIVRE BLANC. Ce livre blanc est fourni « en l'état ». Les informations et les opinions exprimées dans ce livre blanc, en ce compris les URL ainsi que d'autres références à des sites web internet, sont sujets à changement sans préavis.

Publié en mai 2017

Version 1.1

Introduction

Une nouvelle législation européenne en matière de protection de la vie privée doit entrer en vigueur le 25 mai 2018. Ce texte fixe de nouvelles exigences générales portant sur les droits, la sécurité et la conformité relatifs à la protection de la vie privée.

L'objet fondamental du Règlement général sur la protection des données (ou GDPR) réside dans la protection et la mise en œuvre des droits des personnes à la vie privée. Le GDPR définit des exigences générales strictes qui régissent la manière dont les données personnelles doivent être gérées et protégées dans le respect du choix individuel, quels que soient la destination ou le lieu d'envoi, de traitement ou de stockage des données.

Microsoft et ses clients cheminent aujourd'hui vers la réalisation des objectifs du GDPR en matière de protection de la vie privée. Chez Microsoft, nous sommes convaincus que la protection de la vie privée est un droit fondamental et nous pensons que le GDPR constitue une évolution importante dans la clarification et le respect des droits à la vie privée des personnes. Nous constatons également que le GDPR exigera de la part des entreprises dans le monde entier d'importants changements.

Nous vous accompagnerons tout au long de la transition vers le GDPR.

L'engagement de Microsoft envers le GDPR

La confiance est au cœur de notre mission qui consiste à permettre à chaque personne et à chaque organisation sur la planète de progresser. Nous adoptons une approche raisonnée dans l'établissement de la confiance, fondée sur des engagements fermes en faveur du respect de la vie privée, de la sécurité, de la conformité et de la transparence. Dans le cadre de notre préparation à l'entrée en vigueur du GDPR, nous appliquons ces principes.

Nous comprenons que la conformité avec le GDPR est une responsabilité commune. C'est pourquoi nous nous sommes engagés à atteindre la conformité de tous nos services cloud avec le GDPR au moment de son entrée en vigueur le 25 mai 2018.

Nous nous engageons également à partager notre expérience du respect de réglementations complexes afin de vous aider à tracer la voie qui permettra à votre entreprise de satisfaire aux exigences du GDPR en matière de protection de la vie privée. Grâce à l'offre la plus complète de solutions de conformité et de sécurité de tous les fournisseurs de services cloud ainsi qu'à un vaste écosystème de partenaires, nous avons tout en main pour soutenir vos initiatives actuelles et futures en matière de protection de la vie privée et de sécurité.

Dans le cadre de notre engagement à vous accompagner dans le respect du GDPR, nous avons élaboré ce livre blanc afin de vous aider à vous préparer. Ce document vous offre une vue d'ensemble du GDPR, décrit les mesures que nous prenons pour nous y préparer et propose des exemples d'actions à entreprendre avec Microsoft dès aujourd'hui pour entamer votre cheminement vers la conformité avec le GDPR.

Nous sommes impatients de vous fournir des informations supplémentaires sur la manière dont nous pouvons vous aider à vous mettre en conformité avec cet important texte de loi tout en faisant progresser les mesures de protection de la vie privée. N'hésitez pas à consulter la rubrique consacrée au GDPR dans le Microsoft Trust Center. Vous y trouverez des ressources supplémentaires et d'autres informations sur la manière dont Microsoft peut vous aider à remplir des exigences spécifiques du GDPR.

Comprendre le GDPR : remarques préliminaires

Avant de décrire spécifiquement la manière dont Microsoft peut vous aider à vous préparer au GDPR, nous souhaitons nous pencher sur certaines questions fondamentales et déterminantes relatives au règlement et à sa signification pour vous.

Qu'est-ce que le GDPR ?

Le règlement général sur la protection des données est un nouveau règlement de l'Union européenne portant sur la protection de la vie privée. Il donne aux citoyens un plus grand contrôle de leurs données personnelles, garantit la transparence de l'utilisation des données et exige des mesures de sécurité et de contrôle pour la protection des données.

Le GDPR s'applique-t-il à mon entreprise ?

Le champ d'application du GDPR est plus vaste qu'il n'y paraît de prime abord. Le règlement impose de nouvelles règles aux entreprises, agences gouvernementales, organismes à but non lucratif et autres organisations qui proposent des biens et des services aux citoyens de l'Union européenne (UE), ou qui collectent et analysent des données en lien avec des résidents de l'UE, où qu'ils se trouvent.

Contrairement aux lois sur la protection de la vie privée relevant de la compétence d'autres entités, le GDPR s'applique aux entreprises de toutes les tailles et de tous les secteurs d'activité. L'UE étant souvent perçue dans le paysage international comme un modèle exemplaire en matière de protection de la vie privée, nous nous attendons à voir d'autres régions du monde adopter les concepts du GDPR au fil du temps.

Quelle est la date d'entrée en vigueur du GDPR ?

Le GDPR entrera en vigueur le 25 mai 2018. Il remplacera l'actuelle Directive sur la protection des données personnelles (Directive 95/46/CE) qui est en vigueur depuis 1995. En réalité, le GDPR a été adopté par l'UE en avril 2016 mais il prévoit une période de transition de deux ans compte tenu des changements importants que devront mettre en œuvre certaines organisations pour s'adapter aux exigences du règlement.

Quels sont les principaux concepts du GDPR ?

Le GDPR s'articule autour de six principes :

- Exiger la transparence du traitement et de l'utilisation des données à caractère personnel.
- Limiter le traitement de données à caractère personnel à des finalités déterminées et légitimes.
- Limiter la collecte et la conservation de données à caractère personnel aux finalités prévues.
- Permettre aux personnes de corriger leurs données à caractère personnel ou d'en demander la suppression.

- Limiter la conservation de données d'identification personnelle à la durée nécessaire pour la finalité visée.
- Garantir la protection des données à caractère personnel au moyen de pratiques appropriées en matière de sécurité.

Quels sont les exemples d'exigences du GDPR associés à ces principes ?

- Au titre du GDPR, les personnes ont le droit de savoir si une organisation traite leurs données à caractère personnel et de comprendre les finalités de ce traitement. Chaque personne a le droit de faire supprimer ou corriger ses données, de demander qu'elles ne soient plus traitées, de s'opposer à la prospection et de révoquer son consentement à certaines utilisations de ses données à caractère personnel. Le droit à la portabilité des données confère aux personnes le droit de déplacer leurs données ailleurs et d'être aidées à le faire.
- Le GDPR impose aux organisations de sécuriser les données à caractère personnel conformément à leur caractère sensible. En cas de violation de données, les opérateurs de traitement des données doivent de manière générale en informer les autorités compétentes dans un délai de 72 heures. En outre, si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des individus, les organisations devront également en informer les personnes concernées dans les plus brefs délais.
- Le traitement de données à caractère personnel doit être fondé sur une base juridique. Tout consentement au traitement de données à caractère personnel doit être donné « de façon libre, spécifique, éclairée et univoque ». Le GDPR prévoit des exigences spécifiques de consentement pour la protection des enfants.
- Les organisations doivent réaliser des analyses d'impact relatives à la protection des données afin d'évaluer les risques des projets pour la protection des données et de mettre en œuvre des mesures pour les atténuer. Des registres des activités de traitement, des consentements au traitement des données et de la conformité avec le GDPR doivent être conservés.
- La conformité avec le GDPR ne constitue pas une activité ponctuelle mais bien un processus continu. Le non-respect du GDPR peut entraîner de lourdes amendes. Pour garantir le respect du GDPR, les organisations sont encouragées à adopter une culture de la protection de la vie privée afin de protéger les intérêts des personnes dans leurs données à caractère personnel.

Pour consulter une présentation plus détaillée du GDPR et mieux comprendre des termes tels que « pseudonymisation », « traitement », « responsables du traitement », « sous-traitants », « personnes concernées » et « données à caractère personnel », rendez-vous sur Microsoft.com/GDPR. Nous nous engageons à vous aider à remplir les exigences du GDPR et à protéger davantage les droits de protection de la vie privée des personnes.

Votre cheminement vers la conformité avec le GDPR en partenariat avec Microsoft

La conformité avec le GDPR constitue un défi à l'échelle de toute l'entreprise. Elle requiert du temps, des outils, des processus et des compétences et peut imposer des modifications importantes de vos pratiques de protection de la vie privée et de gestion des données. Votre transition vers la conformité avec le GDPR peut s'effectuer plus en douceur si vous utilisez un modèle de services cloud bien pensé et si vous disposez d'un programme de gouvernance efficace. Vous pouvez compter sur Microsoft et son vaste écosystème de partenaires pour vous aider à atteindre les objectifs définis par le GDPR.

Microsoft offre depuis longtemps des services cloud de confiance. Nous adoptons une approche raisonnée de la protection de la vie privée, de la sécurité, de la conformité et de la transparence, avec la ferme volonté de vous permettre d'avoir confiance en la technologie numérique sur laquelle vous comptez. En matière de conformité, notre portefeuille est le plus complet du secteur et nous avons été les premiers à adopter des normes fondamentales telles que la norme ISO/IEC 27018 relative à la protection des données personnelles dans le Cloud. Nos clients et partenaires bénéficient de l'expérience de pointe que nous avons acquise en matière de protection de la vie privée, de sécurité, de conformité et de transparence.

Dans le cadre de votre préparation à la conformité GDPR, voici ce que vous pouvez également attendre de nous :

- **Une technologie qui répond à vos besoins**. Vous pouvez tirer parti de notre vaste gamme de services cloud pour les entreprises pour remplir vos obligations dans le cadre du GDPR dans des domaines tels que la suppression, la rectification, le transfert, l'accès et l'opposition au traitement de données à caractère personnel. Vous pouvez en outre compter sur Microsoft et son vaste écosystème international de partenaires pour vous apporter une assistance spécialisée dans l'utilisation des technologies Microsoft.
- **Des engagements contractuels**. Nous vous soutenons grâce à des engagements contractuels pour nos services cloud, y compris une assistance rapide en matière de sécurité et des notifications conformes aux nouvelles exigences du GDPR. En mars 2017, les accords de licence client des services cloud Microsoft incluront des engagements de conformité avec le GDPR lors de son entrée en vigueur.
- **Le partage de notre expérience**. Nous vous parlerons de notre cheminement vers la conformité avec le GDPR afin que vous puissiez adapter les enseignements que nous en avons tirés et tracer la meilleure voie pour votre entreprise.

Premiers pas dans l'application du GDPR

Approche de plateforme du GDPR

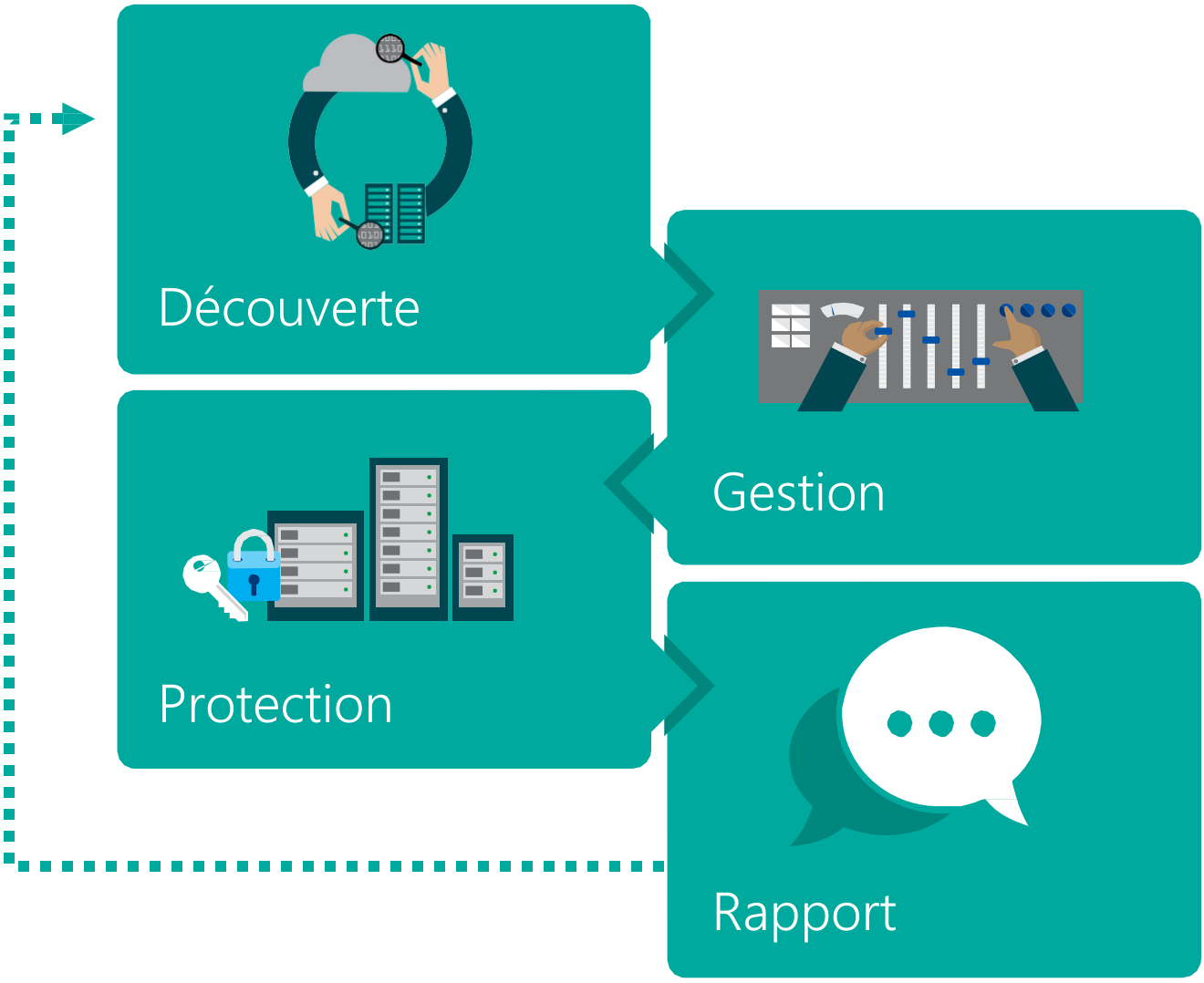
Les systèmes que vous utilisez pour créer, conserver, analyser et gérer des données peuvent s'étendre sur différents environnements informatiques tels que des appareils personnels, des serveurs sur site, des services cloud et même l'Internet des objets. Par conséquent, la majeure partie de votre paysage informatique est susceptible d'être soumise aux exigences du GDPR.

Les efforts que vous déployez pour répondre aux exigences du GDPR seront optimisés s'ils s'inscrivent dans une approche holistique des exigences et dans le contexte de toutes vos obligations réglementaires et légales en matière de protection de la vie privée. Par exemple, les mesures de sécurité visant à prévenir, détecter et combattre les vulnérabilités et les violations de données exigées par le GDPR sont similaires à celles que prévoient d'autres normes de protection des données telles que la norme ISO 27018 relative à la protection de la vie privée dans le cloud.

Au lieu de chercher à répondre individuellement aux exigences des différentes normes ou réglementations, il est préférable d'identifier un ensemble global de contrôles et de capacités en réponse à ces exigences. De même, au lieu d'évaluer des technologies et solutions individuelles par rapport à une réglementation complète telle que le GDPR, une perspective de plateforme (telle que celle qui regroupe Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure et Dynamics 365) peut offrir une vision plus nette dans la recherche de conformité avec le GDPR, mais aussi avec d'autres exigences importantes.

Nous vous conseillons de commencer votre cheminement vers la conformité avec le GDPR en ciblant quatre étapes principales :

- **Découverte**—Identifiez les données à caractère personnel dont vous disposez et leur emplacement.
- **Gestion**—Gérez l'accès aux données à caractère personnel et leur utilisation.
- **Protection**—Mettez en place des contrôles de sécurité pour la prévention, la détection et la réponse face aux vulnérabilités et aux violations de données.
- **Rapport**—Exécutez les mesures requises par les demandes de données, signalez les violations de données et conservez la documentation requise.



Nous avons sélectionné des exemples d'outils, de ressources et de fonctionnalités offerts par différentes solutions Microsoft qui peuvent être utilisés pour répondre aux exigences de chacune de ces étapes. Même si ce document ne constitue pas un guide complet, il contient certains liens vous permettant d'accéder à des informations plus détaillées. En outre, vous trouverez d'autres informations à l'adresse Microsoft.com/GDPR.

Étant donné la charge de travail impliquée, il est vivement conseillé de ne pas attendre l'entrée en vigueur du GDPR pour s'y préparer. Vous devez commencer à revoir vos pratiques en matière de gestion des données et de confidentialité dès à présent.

Les paragraphes qui suivent mettent en évidence les éléments spécifiques de chaque composante du GDPR et décrivent des méthodes d'utilisation de produits et services Microsoft disponibles actuellement pour entamer ce cheminement.

Agir aujourd'hui

Découverte : identifiez les données à caractère personnel dont vous disposez et leur emplacement

La première étape vers la conformité avec le GDPR consiste à déterminer si le règlement s'applique à votre entreprise et, le cas échéant, dans quelle mesure. Cette analyse commence par une prise en compte des données à caractère personnel dont vous disposez et de leur emplacement.

Le GDPR s'applique-t-il à mes données ?

Le GDPR réglemente la collecte, la conservation, l'utilisation et le partage de « données à caractère personnel ». Au titre du GDPR, ces données sont définies dans un sens très large comme *toutes* les données relatives à une personne physique identifiée ou identifiable.

Si votre entreprise possède des données de cette nature (dans des bases de données de clients, des formulaires de réponse complétés par des clients, des contenus d'e-mails, des photos, des enregistrements de caméras de surveillance, des registres de programmes de fidélité, des bases de données de RH ou tout autre support) ou si elle entend collecter des données de cette nature appartenant à des résidents de l'UE ou relatives à des résidents de l'UE, vous êtes tenu de respecter les exigences du GDPR. Il convient de préciser que les données à caractère personnel ne doivent pas nécessairement être conservées dans l'UE pour être soumises au GDPR. Le règlement s'applique en effet à toutes les données collectées, traitées ou conservées en dehors de l'UE si elles sont liées à des résidents de l'UE.

Dresser votre inventaire

Pour évaluer la mesure dans laquelle le GDPR *s'applique* à votre entreprise et les obligations qu'il impose le cas échéant, il est important de procéder à un inventaire des données de votre entreprise. Cette étape vous permettra de distinguer les données à caractère personnel et d'identifier les systèmes au sein desquels des données sont collectées et conservées, de déterminer les raisons pour lesquelles elles ont été collectées, la manière dont elles sont traitées et communiquées et leur délai de conservation.

Les exemples ci-dessous portent sur la manière dont nos solutions cloud et sur site peuvent spécifiquement vous aider dans le cadre de cette première étape du GDPR.

Azure

Azure étant une plateforme cloud ouverte et flexible, elle comprend un service qui permet de détecter et d'identifier facilement les sources de données. Le catalogue de données Microsoft Azure Data Catalog est un service cloud entièrement géré qui fait office de système d'enregistrement et de système de découverte des sources de données de votre entreprise. En d'autres termes, Azure Data Catalog est destiné à vous aider à découvrir, comprendre et utiliser les sources de données pour mieux exploiter vos données existantes. Une fois qu'une source de données est inscrite dans Azure Data Catalog, ses métadonnées sont indexées par le service, de sorte que vous pouvez effectuer facilement une recherche afin de découvrir les données dont vous avez besoin.

Dynamics 365

Dynamics 365 offre plusieurs fonctionnalités de visibilité et d'audit qui peuvent être utilisées grâce aux tableaux de bord Reporting et Analytics de Dynamics 365 pour identifier des données à caractère personnel :

- Dynamics 365 comprend un Assistant Rapport qui permet de créer des rapports facilement sans utiliser les requêtes XML ou SQL.
- Les tableaux de bord de Dynamics 365 offrent une vue d'ensemble des données de l'entreprise, des informations exploitables qui peuvent être consultées dans toute l'entreprise.
- Microsoft Power BI est une plateforme d'aide à la décision (BI) en libre-service qui permet de découvrir, d'analyser et de visualiser des données, ainsi que d'échanger ou de collaborer sur la base de ces informations avec des collègues.

Suite Enterprise Mobility + Security (EMS)

Enterprise Mobility + Security comprend des technologies de sécurité basées sur les identités qui vous permettent de découvrir, contrôler et protéger des données à caractère personnel détenues par votre entreprise, ainsi que de révéler de possibles angles morts et de détecter les violations de données.

Microsoft Cloud App Security est un service complet qui offre une visibilité accrue, des contrôles complets et une meilleure protection de vos données dans les applications cloud. Vous pouvez identifier les applications cloud utilisées dans votre réseau (identification de plus de 13 000 applications depuis tous les appareils) et obtenir des évaluations des risques et des analyses en continu.

Microsoft Azure Information Protection vous aide à identifier les données sensibles et à localiser leur emplacement. Vous pouvez effectuer des requêtes sur des données marquées selon leur sensibilité ou identifier de manière intelligente les données sensibles lors de la création d'un fichier ou d'un e-mail. Une fois identifiées, les données peuvent être classées et marquées automatiquement, toujours en fonction de la stratégie choisie par l'entreprise.

Office 365

Différentes solutions spécifiques d'Office 365 peuvent vous aider à identifier ou gérer l'accès aux données à caractère personnel :

- La protection contre la perte de données (DLP) d'Office et Office 365 permet d'identifier plus de 80 types courants de données sensibles, y compris des informations financières, médicales et relatives à une personne identifiable.

- La recherche de contenu dans le Centre de conformité et sécurité Office 365 permet d'effectuer des recherches dans des boîtes de messagerie électronique, des dossiers publics, des Groupes Office 365, des Microsoft Teams, des sites SharePoint Online, des emplacements One Drive Entreprise et des conversations Skype Entreprise.
- La recherche Office 365 eDiscovery peut être utilisée pour rechercher du texte et des métadonnées dans le contenu de vos ressources Office 365 (SharePoint Online, OneDrive Entreprise, Skype Entreprise Online et Exchange Online).
- Office 365 Advanced eDiscovery, qui se base sur des technologies d'apprentissage automatique, peut vous aider à identifier des documents d'intérêt pour un thème particulier (par exemple, une enquête de conformité) rapidement et plus précisément que les recherches classiques par mots-clés ou l'inspection manuelle de grandes quantités de documents. Advanced eDiscovery permet de réduire de manière significative les coûts et les efforts nécessaires pour identifier des documents et des relations entre les données en s'appuyant sur l'apprentissage automatique pour entraîner le système à explorer de manière intelligente de grands jeux de données et à identifier rapidement les éléments importants, ce qui réduit la quantité de données avant l'examen.
- Advanced Data Governance utilise des renseignements et des informations assistées par ordinateur pour vous aider à trouver les données les plus importantes pour votre entreprise, à les classer, à les soumettre à des règles et à prendre des mesures de gestion de leur cycle de vie.

SharePoint

Vous pouvez utiliser le service de recherche SharePoint et la fonctionnalité de recherche intégrée à l'application pour tracer des données à caractère personnel. Pour identifier et rechercher les contenus sensibles, SharePoint Server 2016 offre les mêmes fonctionnalités de protection contre la perte de données qu'Office 365.

SQL Server et Azure SQL Database

Le langage SQL peut être utilisé pour interroger des bases de données et pour personnaliser des outils ou des services susceptibles de contribuer à répondre à cette exigence. La recherche est entièrement prise en charge par des requêtes, même si une journalisation de traçage complet doit être effectuée au niveau de l'application. La tâche Script fournit le code pour effectuer des fonctions personnalisées, telles que des requêtes de données complexes qui ne sont pas disponibles dans les tâches et transformations intégrées fournies par les services d'intégration SQL Server. La tâche Script peut également combiner des fonctions au sein d'un même script au lieu d'utiliser plusieurs tâches et transformations. Cette suite de produits comprend également une fonctionnalité puissante d'aide à la décision qui permet à l'utilisateur final d'accéder à des informations relatives aux données.

Windows et Windows Server

Pour rechercher des données dans Windows, vous pouvez utiliser la Recherche Windows pour tracer et localiser des données à caractère personnel sur votre ordinateur local et sur tout autre appareil connecté pour lequel vous disposez des droits d'accès appropriés. Pour améliorer les capacités de localisation des données de la fonctionnalité de Recherche Windows, vous pouvez configurer les Options d'indexation dans le Panneau de configuration afin de personnaliser la Recherche Windows (par exemple en indexant le contenu des fichiers).

Gestion : gérez l'accès aux données à caractère personnel et leur utilisation

Le GDPR donne aux personnes concernées (celles que les données concernent) un plus grand contrôle de la manière dont leurs données à caractère personnel sont obtenues et utilisées. Par exemple, les personnes concernées peuvent demander que votre entreprise communique des données les concernant, les transfère à d'autres services, corrige des erreurs dans leurs données ou empêche le traitement ultérieur de certaines données dans certains cas. Dans certaines circonstances, une suite doit être donnée à ces demandes dans un délai fixe.

Gouvernance des données

Pour remplir vos obligations à l'égard des personnes concernées, vous devez comprendre les types de données à caractère personnel que votre entreprise traite, les modalités de ce traitement et ses finalités. L'inventaire des données évoqué précédemment constitue une première étape pour y parvenir. Une fois l'inventaire réalisé, il est également important d'élaborer un plan de gouvernance des données et de le mettre en œuvre. Un plan de gouvernance des données peut vous aider à définir des règles, des rôles et des responsabilités pour l'accès, la gestion et l'utilisation de données à caractère personnel. Il peut aussi contribuer à garantir la conformité de vos pratiques de gestion des données avec le GDPR. Par exemple, le plan de gouvernance des données peut donner à votre entreprise la certitude qu'elle respecte effectivement les demandes de suppression ou de transfert des données formulées par les personnes concernées.

Services cloud Microsoft

Pour appuyer votre stratégie de gouvernance des données, les services cloud de Microsoft sont élaborés selon la méthodologie Microsoft Privacy-by-Design et Privacy-by-Default. Lorsque vous confiez vos données à Azure, Office 365 ou Dynamics 365, vous en restez le seul propriétaire : vous conservez les droits, les titres et les intérêts relatifs aux données enregistrées dans les services.

Les services cloud de Microsoft mettent en place des mesures efficaces qui contribuent à protéger les données de vos clients contre un accès inapproprié ou une utilisation par des tiers non autorisés, comme le décrit le Microsoft Trust Center. Ces mesures prévoient notamment des restrictions d'accès pour le personnel et les sous-traitants de Microsoft et une définition réfléchie des conditions de réponse aux demandes de données clients émanant des autorités. Vous pouvez cependant accéder à vos données clients à tout moment et pour quelque raison que ce soit.

En outre, nous redirigeons les demandes de données émanant des autorités de manière à ce qu'elles vous soient adressées directement, sauf dans les cas où la loi l'interdit, et nous nous sommes opposés à des tentatives des autorités visant l'interdiction de la divulgation de demandes de cet ordre devant les tribunaux.

Afin de contribuer à garantir la bonne gestion des services cloud de Microsoft et de fournir des assurances à nos clients, les services cloud sont soumis au moins une fois par an à des audits sur la conformité avec plusieurs normes internationales de confidentialité des données telles que les normes HIPAA et HITECH, CSA Star Registry et plusieurs normes ISO. Ces rapports sont disponibles à l'adresse https://servicetrust.microsoft.com/Documents/ComplianceReports.

Outre ces engagements, nous vous donnons le contrôle nécessaire pour garantir les modalités de gestion des données et d'accès des utilisateurs aux différentes données au sein de votre entreprise.

Azure

Azure Active Directory est une solution de gestion des identités et des accès dans le cloud. Elle gère les identités et contrôle les accès à Azure sur site ainsi qu'à d'autres ressources, données et applications dans le cloud. La gestion des identités privilégiées d'Azure Active Directory vous permet d'attribuer des droits d'administration Just-In-Time (JIT) à titre temporaire aux utilisateurs habilités à gérer des ressources Azure.

Le contrôle d'accès basé sur un rôle d'Azure (RBAC) vous aide à gérer l'accès à vos ressources Azure. Vous pouvez ainsi accorder un accès sur la base du rôle attribué à l'utilisateur, ce qui vous permet d'octroyer uniquement les autorisations nécessaires à l'exécution des tâches des utilisateurs avec plus de facilité. Vous pouvez personnaliser le contrôle d'accès basé sur un rôle en fonction du modèle économique et de la tolérance au risque propres à votre entreprise.

Office 365

Différentes fonctionnalités des solutions Office 365 peuvent vous aider à gérer des données à caractère personnel :

- Des fonctionnalités de gouvernance des données comprises dans le Centre de conformité et sécurité dans Office 365 vous aident à archiver et protéger le contenu dans les boîtes de courrier électronique Exchange Online, les sites SharePoint Online et les emplacements One Drive Entreprise, ainsi qu'à importer des données dans votre organisation Office 365.
- La fonctionnalité de conservation d'Office 365 peut vous aider à gérer le cycle de vie des e-mails et des documents en conservant le contenu dont vous avez besoin et en supprimant le contenu lorsqu'il n'est plus nécessaire.
- Advanced Data Governance utilise des renseignements et des informations assistées par ordinateur pour vous aider à trouver les données les plus importantes pour votre entreprise, à les classer, à les soumettre à des règles et à prendre des mesures de gestion de leur cycle de vie.
- Les stratégies de gestion des informations de SharePoint Online vous permettent de contrôler la durée de conservation des contenus, d'activer des audits portant sur la manière dont les contenus sont utilisés et d'ajouter des code-barres ou des étiquettes aux documents.
- La journalisation dans Exchange Online peut vous aider à remplir les conditions de conformité légale, réglementaire et organisationnelle en enregistrant les communications par e-mail entrantes et sortantes.

Classification des données

La classification constitue un aspect important de tout plan de gouvernance des données. L'adoption d'un système de classification appliqué à l'échelle de toute l'entreprise est une mesure particulièrement utile pour répondre aux demandes des personnes concernées par les données car elle vous permet d'identifier plus rapidement les demandes relatives à des données à caractère personnel et de les traiter.

Nous proposons aujourd'hui des conseils et des outils pour vous aider à déjouer la complexité de la classification des données.

Azure

Le livre blanc Classification des données contient des conseils spécifiques de classification des données pour Azure et présente les principes qui régissent les techniques, le traitement, la terminologie et la mise en œuvre de la classification des données. La documentation contient également de nombreuses autres informations et des liens utiles.

Dynamics 365

Le Guide de planification de la sécurité et de la conformité de Microsoft Dynamics 365 (en ligne) contient des informations complètes pour comprendre les principales considérations de sécurité et de conformité associées à la planification d'un déploiement Microsoft Dynamics 365 (en ligne) dans des environnements qui peuvent inclure des services d'intégration d'annuaire d'entreprise, comme la synchronisation d'annuaire et l'authentification unique. Il comprend des informations relatives aux stratégies de protection des données et de confidentialité, à la classification des données et à l'impact.

Enterprise Mobility + Security (EMS)

Azure Information Protection peut vous aider à classifier et marquer vos données au moment de leur création ou de leur modification. La protection (chiffrement + authentification + droits d'utilisation) ou les marquages visuels peuvent ensuite être appliqués aux données sensibles. Les marquages de classification et la protection sont permanents. Ils restent sur les données de manière à ce que celles-ci restent identifiables et protégées à tout moment, quels que soient le lieu où elles sont conservées et les destinataires à qui elles sont communiquées.

Office et Office 365

- La protection contre la perte de données (DLP) d'Office et Office 365 permet d'identifier plus de 80 types courants de données sensibles, y compris des informations financières, médicales et relatives à une personne identifiable. En outre, la DLP permet aux entreprises de configurer des actions à appliquer en cas d'identification pour protéger des informations sensibles et éviter leur divulgation accidentelle.
- Advanced Data Governance utilise des renseignements et des informations assistées par ordinateur pour vous aider à trouver les données les plus importantes pour votre entreprise, à les classer, à les soumettre à des règles et à prendre des mesures de gestion de leur cycle de vie. Les données sont classées en fonction de l'analyse automatique et des recommandations stratégiques, puis des actions sont appliquées pour protéger les données existantes ou nettoyer ce qui doit l'être. Les données existantes et les sources de données tierces peuvent être assimilées dans Office 365 et classées selon le type de message. La classification par type de message permet d'effectuer des tâches de recherche, de tri et d'exportation sur les différentes sources de données, ce qui simplifie la réalisation d'examens d'e-discovery.

Windows et Windows Server

Le Microsoft Data Classification Toolkit pour Windows Server 2012 R2 fournit des exemples d'expressions de recherche et de règles que vous pouvez utiliser pour soutenir les activités de conformité menées par les professionnels de l'informatique de votre entreprise, les auditeurs, les comptables, les conseils juridiques et d'autres spécialistes de cette matière.

Protection : mettez en place des contrôles de sécurité pour la prévention, la détection et la réponse face aux vulnérabilités et aux violations de données

Les entreprises sont de plus en plus sensibles à l'importance de la sécurité des informations mais le GDPR élève cette préoccupation à un rang supérieur. Il impose aux entreprises de prendre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la perte, l'accès non autorisé ou la communication non autorisée.

Protection de vos données

La sécurité des données est un domaine complexe. Il convient d'identifier et de prendre en compte de nombreux types de risques, allant de l'intrusion physique au piratage, en passant par la malveillance d'un employé ou la perte accidentelle. L'élaboration de plans de gestion du risque et la mise en place de mesures d'atténuation du risque telles que la protection par mot de passe, les journaux d'audit et le chiffrement peuvent vous aider à garantir la conformité.

Le cloud Microsoft est conçu spécifiquement pour vous aider à comprendre les risques et à vous défendre. Il est à de nombreux égards plus sûr que les environnements informatiques sur site. Par exemple, nos centres de données sont certifiés selon des normes de sécurité reconnues internationalement, protégés par une surveillance physique 24 heures sur 24 et soumis à des contrôles d'accès stricts.

La manière dont nous sécurisons notre infrastructure de cloud n'est qu'un des aspects d'une solution de sécurité complète et chacun de nos produits, dans le cloud ou sur site, comporte des fonctionnalités de sécurité qui vous aident à sécuriser vos données.

Azure

Les services et outils d'Azure suivants peuvent vous aider à protéger des données à caractère personnel dans votre environnement de cloud :

- Le Centre de sécurité Azure vous permet de jouir de la visibilité et du contrôle nécessaires dans le cadre de la sécurité de vos ressources Azure. Il surveille vos ressources en continu et fournit des recommandations de sécurité utiles. Il vous permet de définir des stratégies pour vos abonnements Azure et vos groupes de ressources en fonction des exigences de sécurité de votre entreprise, des types d'applications que vous utilisez et du degré de sensibilité de vos données. Il utilise également des recommandations de sécurité fondées sur des stratégies afin de guider les propriétaires de services dans la mise en œuvre des contrôles requis, par exemple pour activer la protection contre les logiciels malveillants ou le chiffrement du disque pour vos ressources. Le Centre de sécurité vous aide aussi à déployer rapidement des services et dispositifs de sécurité fournis par Microsoft et des partenaires pour renforcer la protection de votre environnement de cloud.

- Le chiffrement des données dans Azure sécurise vos données au repos et en transit. Vous pouvez par exemple chiffrer automatiquement vos données à l'entrée dans le Stockage Azure à l'aide de la fonctionnalité Storage Service Encryption. Vous pouvez en outre utiliser Azure Disk Encryption pour chiffrer des systèmes d'exploitation et des disques de données utilisés par les machines virtuelles Windows et Linux. Les données sont protégées en transit entre une application et Azure, de manière à ce qu'elles gardent toujours un niveau de sécurité élevé.
- Azure Key Vault vous permet de protéger les clés de chiffrement, les certificats et les mots de passe qui contribuent à la protection de vos données. Key Vault utilise des modules de sécurité matériels (HSM) et est conçu pour vous permettre de garder le contrôle de vos clés, et par conséquent de vos données, y compris en garantissant que vos clés ne peuvent pas être visibles ni extraites par Microsoft. Vous pouvez surveiller et auditer l'utilisation de vos clés avec la journalisation Azure et importer vos journaux dans Azure HDInsight ou dans votre logiciel SIEM (Information and Event Management) pour bénéficier de capacités supplémentaires d'analyse et de détection des menaces.
- Microsoft Antimalware pour les services cloud Azure et les machines virtuelles est une fonctionnalité de protection en temps réel gratuite qui permet d'identifier et de supprimer les virus, les logiciels espions et autres logiciels malveillants destinés au vol de données, grâce à des alertes configurables qui vous avertissent lorsque des logiciels malveillants ou indésirables connus tentent de s'installer ou de s'exécuter sur vos systèmes Azure.

Dynamics 365

Vous pouvez utiliser les concepts de sécurité pour Dynamics 365 pour protéger l'intégrité et la confidentialité des données dans une organisation Dynamics 365. Vous pouvez combiner les divisions, la sécurité basée sur les rôles, la sécurité basée sur les enregistrements et la sécurité basée sur les champs pour définir l'accès global des utilisateurs aux informations dans votre organisation Dynamics 365.

- La sécurité basée sur les rôles dans Dynamics 365 vous permet de regrouper un ensemble de privilèges qui limitent les tâches pouvant être effectuées par un utilisateur. Il s'agit d'une fonctionnalité importante, en particulier lorsque les rôles des individus changent au sein de l'organisation.
- La sécurité basée les enregistrements dans Dynamics 365 vous permet de restreindre l'accès à certains enregistrements spécifiques.
- La sécurité au niveau des champs dans Dynamics 365 vous permet de restreindre l'accès à des champs spécifiques importants tels que les champs d'informations relatives à des personnes identifiables.

Enterprise Mobility + Security (EMS)

Dans la majorité des cas de violations des données, les auteurs des attaques obtiennent un accès au réseau d'une entreprise en profitant d'informations d'identification faibles, définies par défaut ou volées. Notre approche de la sécurité commence par la protection de l'identité à l'entrée, avec un accès conditionnel fondé sur les risques.

- Azure Active Directory (Azure AD) dans Enterprise Mobility + Security vous aide à protéger votre entreprise au niveau des accès en gérant et en protégeant vos identités, avec et sans privilèges. Azure AD fournit une même identité protégée pour accéder à des milliers d'applications. Azure AD Premium comprend la fonctionnalité Multi-Factor Authentication (MFA), un contrôle d'accès basé sur l'état de l'appareil, la localisation de l'utilisateur, le risque au niveau de l'identité et de la connexion, ainsi que des rapports, audits et alertes de sécurité holistiques. Azure La gestion des identités privilégiées dans AD (PIM) permet de découvrir, de restreindre et de surveiller des identités disposant de privilèges et leurs accès aux ressources par l'intermédiaire d'un assistant, d'analyses et d'alertes de sécurité. Cela permet de mettre en place des scénarios tels qu'un accès à durée limitée « just in time » et « just enough administration ».

Enterprise Mobility + Security permet de bénéficier d'une visibilité accrue de l'activité des utilisateurs, des appareils et des données sur site et dans le cloud et contribue à protéger les données grâce à des contrôles et à une mise en œuvre renforcés.

- Azure Information Protection permet de mieux contrôler vos données tout au long de leur cycle de vie, de la création à la conservation, sur site et dans les services cloud, à la réaction aux activités imprévues, en passant par le partage interne ou externe ou encore la surveillance de la distribution des fichiers.
- Cloud App Security offre une meilleure visibilité et des contrôles complets pour les applications SaaS (software as a service) et cloud utilisées par vos employés, de manière à vous permettre de connaître l'ensemble du contexte et de contrôler les données au moyen de stratégies granulaires.
- Microsoft Intune fournit des fonctionnalités de gestion des périphériques mobiles, des applications mobiles et des ordinateurs depuis le cloud. En utilisant Intune, vous pouvez donner à vos employés l'accès aux applications, données et ressources de l'entreprise depuis à peu près n'importe où et sur quasiment tous les appareils, tout en contribuant à garantir un niveau de sécurité élevé des informations de l'entreprise.

Office et Office 365

La plateforme Office 365 intègre la sécurité à tous les niveaux, du développement des applications à l'accès pour les utilisateurs, en passant par les centres de données physiques. Les applications Office 365 comprennent à la fois des fonctionnalités de sécurité intégrées qui simplifient la protection des données et la flexibilité nécessaire pour vous permettre de configurer, gérer et intégrer la sécurité de manière à répondre aux besoins spécifiques de votre entreprise. Le cadre de conformité d'Office 365 comprend plus de 1 000 contrôles qui nous permettent de garder Office 365 à la pointe des normes en constante évolution du secteur, y compris plus de 50 certifications ou attestations.

De nombreux contrôles de sécurité sont disponibles par défaut. Par exemple, SharePoint et OneDrive Entreprise utilisent le chiffrement pour les données en transit et au repos. En outre, vous pouvez configurer et déployer des certificats numériques pour camoufler des données à caractère personnel, et utiliser les contrôles d'Office Access pour accorder et restreindre les accès aux données à caractère personnel.

Office 365 comprend d'autres fonctionnalités destinées à vous aider à protéger les données et à identifier les violations :

- Secure Score vous donne des informations sur votre situation en matière de sécurité et sur les fonctionnalités disponibles pour réduire les risques tout en préservant l'équilibre entre productivité et sécurité.
- La Protection avancée contre les menaces (ATP) pour Exchange Online contribue à protéger votre messagerie électronique contre de nouvelles attaques complexes, en temps réel. Elle vous permet également de créer des stratégies pour éviter que les utilisateurs accèdent à des pièces jointes malveillantes ou à des sites Web frauduleux via un lien contenu dans un e-mail. ATP pour Exchange Online comprend une protection contre les logiciels malveillants et les virus inconnus, une protection au moment du clic contre les URL malveillantes, ainsi que des fonctionnalités complètes de signalement et de traçage des URL.
- La Gestion des droits relatifs à l'information (IRM) vous aide et aide vos utilisateurs à éviter que des informations sensibles soient imprimées, transmises, enregistrées, modifiées ou copiées par des personnes non autorisées. Avec IRM dans SharePoint Online, vous pouvez limiter les actions que les utilisateurs peuvent effectuer sur les fichiers qui ont été téléchargés à partir de listes ou de bibliothèques, telles que l'impression de copies des fichiers ou la copie de texte dans les fichiers. Avec IRM dans Exchange Online, vous pouvez contribuer à empêcher que des informations sensibles contenues dans des e-mails et des pièces jointes soient divulguées par courrier électronique, en ligne et hors ligne.

- La Gestion des appareils mobiles (MDM) pour Office 365 vous permet de définir des stratégies et des règles de sécurisation et de gestion des iPhones, iPads, appareils Android et téléphones Windows inscrits de vos utilisateurs. Par exemple, vous pouvez effacer un appareil à distance et afficher des rapports détaillés sur les appareils. Office 365 utilise aussi l'authentification multi-facteurs pour offrir une sécurité supplémentaire.

SQL Server et Azure SQL Database

SQL Server et Azure SQL Database comprennent des contrôles destinés à la gestion de l'accès aux bases de données et de l'autorisation à plusieurs niveaux :

- Le pare-feu Azure SQL Database limite l'accès aux bases de données individuelles de votre serveur Azure SQL Database en l'octroyant exclusivement aux connexions autorisées. Vous pouvez créer des règles de pare-feu au niveau du serveur et de la base de données en spécifiant les plages d'adresses IP autorisées à se connecter.
- L'authentification SQL Server vous aide à garantir que seuls les utilisateurs autorisés disposant d'informations d'identification valides peuvent accéder à votre serveur de bases de données. SQL Server prend en charge à la fois l'authentification Windows et les connexions SQL Server. L'authentification Windows offre une sécurité intégrée et est recommandée en tant qu'option la plus sûre, le processus d'authentification étant entièrement chiffré. Azure SQL Database prend en charge l'authentification Azure Active Directory qui offre une fonctionnalité d'authentification unique et est prise en charge pour les domaines gérés et intégrés.
- L'autorisation SQL Server vous permet de gérer les autorisations selon le principe des privilèges minimum. SQL Server et SQL Database utilisent la sécurité basée sur les rôles. Celle-ci prend en charge un contrôle granulaire des autorisations relatives aux données par l'intermédiaire de la gestion d'appartenances aux rôles et d'autorisations au niveau des objets.
- Le masquage dynamique des données (DDM) est une fonctionnalité intégrée qui permet de limiter l'exposition des données sensibles en les masquant aux utilisateurs ou applications sans privilège. Les champs de données désignés sont masqués directement dans les résultats de la requête alors que les données de la base de données restent inchangées. Le DDM est facile à configurer et ne nécessite aucune modification de l'application. Pour les utilisateurs d'Azure SQL Database, le masquage dynamique des données permet de découvrir automatiquement des données potentiellement sensibles et suggère l'application du masquage correspondant.

- La sécurité au niveau des lignes (RLS) est une fonctionnalité intégrée supplémentaire qui permet aux clients SQL Server et SQL Database d'appliquer des restrictions d'accès aux lignes de données. La RLS peut être utilisée pour mettre en place un accès très restreint aux lignes d'une table de base de données afin de mieux contrôler l'accès à certaines données pour les utilisateurs. Étant donné que la logique de la restriction d'accès est située dans la couche de la base de données, cette fonctionnalité simplifie considérablement la conception et la mise en œuvre de la sécurité de l'application.

SQL Server et SQL Database offrent une puissante série de fonctionnalités intégrées qui protègent les données et identifient les violations :

- Le chiffrement transparent des données protège les données au repos grâce au chiffrement de la base de données, des sauvegardes associées et des fichiers journaux au niveau du stockage physique. Le chiffrement est transparent pour l'application et repose sur l'accélération matérielle pour des performances accrues.
- Le protocole Transport Layer Security (TLS) fournit une protection des données en transit sur les connexions SQL Database.
- Always Encrypted est une fonctionnalité de pointe conçue pour protéger les données très sensibles dans les bases de données SQL Server et SQL Database. Always Encrypted permet aux clients de chiffrer des données sensibles dans des applications clientes et de ne jamais révéler les clés de chiffrement au moteur de base de données. Le mécanisme est transparent pour les applications, le chiffrement et le déchiffrement des données étant effectués de manière transparente dans un pilote client Always Encrypted.
- L'audit SQL Database et l'audit SQL Server suivent les événements de base de données et les écrivent dans un journal d'audit. L'audit vous permet de comprendre les activités de la base de données ainsi que d'analyser et d'étudier des activités de l'historique pour identifier des menaces potentielles, d'éventuelles utilisations abusives et des violations de la sécurité.
- La détection de menaces SQL Database Threat Detection permet de détecter les activités anormales de la base de données qui indiquent la présence potentielle de menaces de sécurité pour la base de données. Threat Detection utilise une série d'algorithmes complexes pour apprendre en continu et étudier le comportement des applications, et effectue un signalement immédiat en cas de détection d'une activité inhabituelle ou suspecte. Threat Detection peut vous aider à remplir l'exigence de signalement des violations de données prévue par le GDPR.

Windows et Windows Server

Windows 10 et Windows Server 2016 comportent un chiffrement de pointe, des technologies de protection contre les logiciels malveillants ainsi que des solutions d'identification et d'accès qui vous permettent de remplacer les mots de passe par des méthodes d'authentification plus sûres :

- Windows Hello constitue une alternative à l'utilisation de mots de passe pratique et adaptée aux besoins des entreprises. Windows Hello utilise une méthode naturelle (biométrique) ou familière (PIN) pour valider l'identité et offre ainsi les avantages de sécurité des cartes à puce sans exiger de périphériques supplémentaires.
- La protection antivirus Windows Defender est une puissante solution de protection contre les logiciels malveillants entièrement prête à l'emploi qui vous aide à rester protégé. Windows Defender offre une détection et une protection rapides contre les logiciels malveillants émergents et peut contribuer immédiatement à protéger vos appareils dès qu'une menace est identifiée dans n'importe quel endroit de votre environnement.
- Device Guard vous permet de verrouiller vos appareils et serveurs afin de les protéger contre des logiciels malveillants émergents et inconnus ainsi que des menaces persistantes avancées. Contrairement aux solutions basées sur la détection telles que les programmes antivirus qui doivent être mis à jour constamment pour détecter les dernières menaces, Device Guard verrouille les appareils de manière à ce qu'ils ne puissent exécuter que les applications autorisées de votre choix et offre ainsi une méthode efficace de lutte contre les logiciels malveillants.
- Credential Guard est une fonctionnalité qui isole vos informations secrètes (par exemple, des jetons d'authentification unique) de tout accès, même dans l'éventualité d'une menace portant sur tout le système d'exploitation Windows. Cette solution offre une protection essentielle contre les attaques difficiles à contrer telles que les attaques de type « pass the hash ».
- BitLocker Drive Encryption dans Windows 10 et Windows Server 2016 offre un chiffrement adapté aux entreprises qui permet de protéger vos données en cas de perte ou de vol d'un appareil. BitLocker assure un chiffrement complet du disque et des lecteurs flash pour empêcher les utilisateurs non autorisés d'accéder à vos données.
- L'intervention de la Protection des informations Windows commence là où s'achève celle de BitLocker. Tandis que BitLocker protège l'intégralité du disque d'un appareil, la Protection des informations Windows protège vos données contre les utilisateurs et applications non autorisés actifs sur un appareil. Elle vous aide également à éviter que les données passent de documents d'entreprise à des documents étrangers à l'entreprise ou à des emplacements sur le web.

- La fonctionnalité Shielded Virtual Machines vous permet d'utiliser BitLocker pour chiffrer des disques et des machines virtuelles (VM) sur Hyper-V afin d'empêcher les administrateurs piratés ou malveillants d'attaquer le contenu des VM protégées.
- Les fonctionnalités Just Enough Administration et Just in Time Administration permettent aux administrateurs d'effectuer leurs tâches et actions normales tout en vous donnant la possibilité de limiter les fonctionnalités et le temps dont ils disposent. Si la sécurité d'un identifiant doté de privilèges est compromise, cela permet de réduire les dommages potentiels dans une large mesure. Cette technique permet de ne donner aux administrateurs que le niveau d'accès nécessaire pour leur temps de travail sur le projet.

Détection des violations de données et réaction

Dans certains cas, le GDPR impose aux organisations de signaler rapidement aux organismes de régulation l'existence d'une violation des données. Dans certaines circonstances, les organisations seront également tenues d'informer les personnes concernées. Pour pouvoir remplir cette exigence, les entreprises ont tout intérêt à être en mesure de surveiller et de détecter les intrusions dans leurs systèmes.

Pour les événements qui relèvent partiellement ou entièrement de notre responsabilité de réaction, nous avons mis en place des procédures de gestion de la réponse aux incidents liés à la sécurité décrites pour Azure et Office 365.

Nous décrivons également la manière dont nous collaborons avec nos clients dans le cadre d'un Modèle de responsabilité partagée dans le livre blanc Shared Responsibilities in Cloud Computing.

En cas de détection d'une violation potentielle, nous recommandons un processus en quatre étapes que nous utilisons également dans le cadre de notre propre programme de réponse aux incidents :

- Analyse de l'impact et de la gravité de l'événement. Selon les éléments en présence, l'analyse peut donner lieu à un transfert à une équipe de réponse Cybersécurité/Protection des données.
- Réalisation d'une enquête technique ou judiciaire et identification de stratégies d'endiguement, d'atténuation et de contournement. Si l'équipe de Cybersécurité/ Protection des données estime que des données à caractère personnel peuvent avoir été exposées à une personne illégitime ou non autorisée, une procédure de signalement est entamée en parallèle conformément aux exigences du GDPR.
- Création d'un plan de récupération destiné à atténuer le problème. Les mesures d'endiguement telles que la mise en quarantaine des systèmes touchés doivent avoir lieu immédiatement et en parallèle avec le diagnostic. Des mesures d'atténuation à long terme peuvent être envisagées pour une mise en place après la disparition du risque immédiat.

- Inspection post mortem mettant en évidence les détails de l'incident, avec l'intention de réviser les stratégies, les procédures et les processus afin d'éviter que l'événement puisse se reproduire. Cette étape correspond à l'Article 31 du GDPR portant sur l'indication des faits concernant la violation, de ses effets et des mesures prises pour y remédier.

Azure

La protection des données à caractère personnel dans vos systèmes ainsi que l'établissement de rapports et d'analyses de conformité sont des éléments clés du GDPR. Les services et outils d'Azure suivants peuvent vous aider à remplir ces exigences du GDPR :

- Les services intégrés d'Azure vous permettent de comprendre plus rapidement et plus facilement le niveau global de sécurité, ainsi que de détecter les menaces et de les examiner dans votre environnement cloud. Le Centre de sécurité Azure utilise des analyses de sécurité avancées. Des innovations dans le domaine du big data et des technologies d'apprentissage automatique sont utilisées pour évaluer les événements sur l'ensemble de la trame du cloud, ce qui permet de détecter des menaces qui ne pourraient pas être identifiées au moyen d'approches manuelles et de prédire l'évolution des attaques. Ces analyses de sécurité comprennent les éléments suivants :
    - Des renseignements intégrés concernant les menaces, qui visent à identifier des comportements malveillants connus sur la base de renseignements internationaux sur les menaces de produits et services Microsoft, la Microsoft Digital Crimes Unit (DCU), le centre de réponse aux problèmes de sécurité Microsoft (MSRC) et des apports d'informations externes.
    - L'analyse comportementale qui utilise des modèles connus pour détecter les comportements malveillants.
    - La détection des anomalies, qui utilise le profilage statistique pour établir des références d'historique. Celle-ci émet des alertes en cas d'écarts par rapport aux références établies correspondant à un vecteur d'attaque potentiel.

    En outre, le Centre de sécurité fournit des alertes de sécurité prioritaires qui vous informent sur la campagne de l'attaque, y compris les événements associés et les ressources concernées.
- Azure Log Analytics offre des options configurables d'audit de sécurité et de journalisation qui peuvent contribuer à collecter et analyser des données générées par des ressources dans votre environnement cloud ou sur site. Cette solution fournit des informations en temps réel grâce à une recherche intégrée et à des tableaux de bord personnalisés pour analyser rapidement des millions de données sur l'ensemble des charges de travail et des serveurs, quel que soit leur emplacement physique. Elle permet de mettre en place une réponse rapide et un examen complet plus facilement pour tous les événements liés à la sécurité.

Dynamics 365

Nous assurons une maintenance et une mise à jour régulières de Dynamics 365 (en ligne) pour garantir la sécurité, les performances et la disponibilité, ainsi que pour proposer de nouvelles caractéristiques et fonctionnalités. Nous pouvons également être amenés à répondre à des incidents de service. L'administrateur Dynamics 365 de votre entreprise reçoit des notifications par e-mail pour chacune de ces activités. En cas d'incident de service, un représentant du service client Dynamics 365 (en ligne) peut également vous contacter par téléphone et assurer un suivi par e-mail. Vous retrouverez tous les détails relatifs aux règles et communications pour Dynamics 365 sur TechNet.

Enterprise Mobility +Security (EMS)

Nos informations complètes relatives aux menaces se fondent sur une analyse comportementale de pointe et sur des technologies de détection des anomalies afin de détecter les activités suspectes et de déceler les menaces, à la fois sur site et dans le cloud. Cette détection comprend les attaques malveillantes connues (de type « Pass the Hash » ou « Pass the Ticket » par exemple) et les failles de sécurité de votre système. Vous pouvez agir immédiatement contre les attaques détectées et bénéficier d'une récupération simplifiée grâce à une assistance efficace. Notre système de renseignements sur les menaces bénéficie des avantages du graphique de sécurité Microsoft Intelligent Security Graph, qui se fonde sur un grand nombre de jeux de données et sur l'apprentissage automatique dans le cloud :

- Microsoft Advanced Threat Analytics (ATA) est un produit sur site destiné à aider les professionnels de la sécurité informatique à protéger leur entreprise contre les attaques avancées ciblées, et ce par l'analyse, l'apprentissage et l'identification des comportements normaux et anormaux d'entités (utilisateur, périphériques et ressources). ATA identifie rapidement les menaces avancées persistantes (APT) sur site en détectant les comportements suspects d'utilisateurs et d'entités (périphériques et ressources) à l'aide de l'apprentissage automatique et des informations de systèmes Active Directory et SIEM sur site, ainsi que de journaux d'événements Windows. Il détecte également les attaques malveillantes connues (telles que « Pass the Hash »). Enfin, il fournit un historique simple des attaques comprenant des informations claires et utiles sur les attaques, de manière à vous permettre de vous concentrer rapidement sur l'essentiel.
- Cloud App Security fournit une protection contre les menaces pour vos applications cloud enrichie d'informations et de recherches étendues de Microsoft sur les menaces. Vous pouvez identifier les utilisations présentant un risque élevé et les incidents de sécurité, ainsi que détecter les comportements anormaux d'utilisateurs pour éviter les menaces. L'heuristique d'apprentissage automatique avancé de Cloud App Security s'informe sur la manière dont chaque utilisateur interagit avec chaque application SaaS et évalue le risque de chaque transaction grâce à l'analyse comportementale. Cela comprend les connexions simultanées depuis deux pays, le téléchargement soudain de téraoctets de données ou encore les échecs de connexion multiples qui pourraient cacher une attaque par force brute.

- Azure Active Directory (Azure AD) Premium offre une détection des menaces dans le cloud au niveau des identités. Azure AD surveille l'utilisation des applications et protège votre entreprise contre des menaces complexes grâce à des fonctionnalités de rapport et de surveillance de la sécurité. Des rapports d'accès et d'utilisation fournissent des informations claires sur l'intégrité et la sécurité du répertoire de votre entreprise. Azure AD fournit également une protection des identités grâce à des notifications, des analyses et des recommandations de solutions.

Office et Office 365

Office 365 comprend plusieurs fonctionnalités destinées à vous aider à identifier les violations de données et à y répondre :

- Threat Intelligence vous aide à déceler les menaces avancées dans Office 365 et à vous en protéger de manière proactive. Des renseignements approfondis (disponibles en partie grâce à la présence internationale de Microsoft, au graphique de sécurité Intelligent Security Graph et aux informations transmises par des chasseurs de cybermenaces) vous aident à activer rapidement et efficacement des alertes, des règles dynamiques et des solutions de sécurité.
- La Gestion de sécurité avancée vous permet d'identifier les utilisations à risque et anormales pour mettre en évidence des violations potentielles. En outre, elle vous permet de définir des stratégies pour les activités de manière à suivre et à combattre les actions à haut risque et les activités suspectes. Vous pouvez aussi obtenir Productivity App Discovery, qui vous permet d'utiliser les informations des fichiers journaux de votre entreprise pour comprendre l'utilisation des applications par les utilisateurs dans Office 365 et d'autres applications cloud et agir en conséquence.
- La Protection avancée contre les menaces pour Exchange Online contribue à protéger votre messagerie électronique contre de nouvelles attaques complexes, en temps réel. Elle vous permet également de créer des stratégies pour éviter que les utilisateurs accèdent à des pièces jointes malveillantes ou à des sites Web frauduleux via un lien contenu dans un e-mail.

SQL Server et Azure SQL Database

SQL Server et SQL Database offrent une puissante série de fonctionnalités intégrées qui identifient les violations de données :

- L'audit SQL Database et l'audit SQL Server suivent les événements de base de données et les écrivent dans un journal d'audit. L'audit vous permet de comprendre les activités de la base de données ainsi que d'analyser et d'étudier des activités de l'historique pour identifier des menaces potentielles, d'éventuelles utilisations abusives et des violations de la sécurité.

- La détection de menaces SQL Database Threat Detection permet de détecter les activités anormales de la base de données qui indiquent la présence potentielle de menaces de sécurité pour la base de données. Threat Detection utilise une série d'algorithmes complexes pour apprendre en continu et étudier le comportement des applications, et effectue un signalement immédiat en cas de détection d'une activité inhabituelle ou suspecte. Threat Detection peut vous aider à remplir l'exigence de signalement des violations de données prévue par le GDPR.

Windows et Windows Server

Windows Defender Advanced Threat Protection (ATP) permet à vos équipes responsables de la sécurité de détecter, d'évaluer, d'endiguer et de combattre les violations de données sur votre réseau. Windows Defender ATP vous permet de bénéficier de fonctionnalités avancées de détection, d'investigation et de réaction pour l'ensemble de vos points de terminaison, avec jusqu'à 6 mois de données d'historique, même pour les points de terminaison hors ligne, situés en dehors du domaine du réseau, reconfigurés ou supprimés. Windows Defender ATP vous aide à remplir une exigence clé du GDPR qui consiste à disposer de procédures claires pour la détection, les enquêtes et le signalement des violations de données.

Rapport : exécutez les mesures requises par les demandes de données, signalez les violations de données et conservez la documentation requise

Le GDPR établit de nouvelles normes en matière de transparence, de responsabilité et de tenue de registres. Vous devrez faire preuve d'une transparence accrue, non seulement dans la manière dont vous gérez les données à caractère personnel, mais également dans la manière dont vous tenez activement à jour la documentation décrivant vos processus et l'utilisation des données à caractères personnel.

Conservation des documents

Les entreprises qui traitent des données à caractère personnel devront tenir des registres relatifs aux finalités du traitement, aux catégories de données à caractère personnel traitées, à l'identité des tiers auxquels les données sont transmises, à la réception ou non de données à caractère personnel par des pays tiers (ceux-ci devant être désignés également) et au fondement légal de ces transferts, aux mesures de sécurité organisationnelles et techniques et aux délais de conservation des données applicables à différents jeux de données. L'une des solutions pour y parvenir consiste à utiliser des outils d'audit. Ceux-ci peuvent vous aider à garantir que tout traitement de données (qu'il s'agisse de la collecte, de l'utilisation, de la communication ou d'une autre forme de traitement) fait l'objet d'un suivi et d'un enregistrement appropriés.

Les services cloud de Microsoft proposent des services d'audit intégrés qui peuvent vous aider à remplir cette exigence.

Azure, Office 365 et Dynamics 365

Vous trouverez dans le Portail d'approbation des services des informations complètes sur les différentes ressources de conformité, de sécurité, de confidentialité et d'approbation d'Azure, Office 365 et Dynamics 365, y compris des rapports et des attestations. Des rapports d'audits indépendants de tiers et des rapports d'évaluation GRC (gouvernance, gestion des risques et conformité) vous aident à rester informé de la manière dont les services cloud de Microsoft répondent aux normes internationales qui concernent votre entreprise. Les documents relatifs à l'approbation vous permettent de comprendre la manière dont les services cloud de Microsoft protègent vos données et dont vous pouvez gérer la sécurité des données et la conformité pour vos services cloud.

Azure

L'audit et la journalisation des événements liés à la sécurité ainsi que des alertes associées forment des éléments importants d'une stratégie efficace de protection des données.

Les fonctionnalités de journalisation et d'audit d'Azure vous permettent de :

- Créer une piste d'audit pour des applications déployées dans Azure et des machines virtuelles créées depuis Azure Virtual Machines Gallery.

- Réaliser une analyse centralisée d'importants jeux de données en collectant des événements de sécurité depuis Azure Infrastructure as a service (IaaS) et Platform as a service (PaaS). Vous pouvez utiliser Azure HDInsight pour ajouter et analyser ces événements et les exporter vers des systèmes SIEM sur site pour une surveillance continue.
- Surveiller les rapports d'accès et d'utilisation en tirant parti de la journalisation Azure des opérations administratives, dont l'accès au système, pour créer une piste d'audit en cas de modifications involontaires ou non autorisées. Vous pouvez récupérer des journaux d'audit pour votre espace locataire Azure Active Directory et consulter les rapports d'accès et d'utilisation.
- Exporter des alertes de sécurité vers des systèmes SIEM sur site en utilisant Azure Diagnostics, qui peut être configuré pour collecter des journaux d'événements de sécurité Windows et d'autres journaux spécifiques à la sécurité.
- Obtenir des outils de surveillance, de rapports et d'alertes de sécurité depuis Azure Marketplace.

Microsoft Azure Monitor permet aux entreprises de consulter et de gérer facilement l'ensemble de leurs tâches de surveillance des données à partir d'un tableau de bord central. Vous obtenez des données de performances et d'utilisation détaillées et actualisées, un accès au journal d'activités qui consigne chaque appel d'API et des journaux de diagnostic qui vous aident à tracer les problèmes dans vos ressources Azure. En outre, vous pouvez configurer des alertes et des actions automatiques. Azure Monitor s'intègre dans vos outils existants, de sorte que vous bénéficiez de fonctionnalités de surveillance et d'analyse de bout en bout en combinant Azure Monitor et les outils d'analyse dont vous disposez déjà.

Office et Office 365

- La Certification du service dans le Centre de sécurité et conformité Office 365 fournit des informations approfondies pour la réalisation d'analyses de risque, ainsi que des détails relatifs aux rapports de conformité Microsoft et un statut transparent des contrôles audités, notamment :
    - Les pratiques mises en place par Microsoft en matière de sécurité des données client stockées dans Office 365.
    - Des rapports d'audit tiers indépendants sur Office 365.
    - Des détails sur les tests et les implémentations des contrôles en matière de sécurité, de confidentialité et de conformité qui permettent aux clients de respecter les normes, lois et réglementations dans les différents secteurs, telles que les normes ISO 27001 et ISO 27018, ainsi que la loi américaine HIPAA (Health Insurance Portability and Accountability Act).

- Les journaux d'audit Office 365 vous permettent de surveiller et de suivre les activités des utilisateurs et des administrateurs pour toutes les charges de travail dans Office 365, ce qui participe à une détection et une investigation précoces des problèmes de sécurité et de conformité. Vous pouvez utiliser la page de recherche des journaux d'audit d'Office 365 pour commencer à consigner les activités des utilisateurs et des administrateurs dans votre entreprise. Une fois le journal d'audit préparé par Office 365, vous pouvez effectuer une recherche dans le journal pour trouver des activités très variées, notamment les téléchargements vers OneDrive ou SharePoint Online, ou encore les réinitialisations de mots de passes d'utilisateurs. Exchange Online peut être configuré de manière à suivre les modifications effectuées par des administrateurs et à suivre tout accès à une boîte de messagerie d'une personne autre que le propriétaire de la boîte de messagerie.
- Le Customer Lockbox vous permet de contrôler la manière dont un ingénieur du support technique de Microsoft peut accéder à vos données dans le cadre d'une intervention d'assistance. Si l'ingénieur doit avoir accès à vos données pour résoudre un problème, le Customer Lockbox vous permet d'accepter ou de refuser la demande d'accès. Si vous l'acceptez, l'ingénieur peut accéder aux données. Chaque demande est assortie d'un délai d'expiration. En outre, une fois le problème résolu, la demande est clôturée et l'accès est annulé.

Enterprise Mobility + Security (EMS)

Azure Information Protection fournit d'importantes fonctionnalités de journalisation et de rapports permettant d'analyser la distribution des données sensibles. Le suivi des documents permet aux utilisateurs et aux administrateurs de surveiller les activités portant sur des données partagées et d'annuler les accès en cas d'événement imprévu. Azure Information Protection offre également des fonctionnalités d'analyse des données non structurées situées dans des partages de fichiers, sur des sites SharePoint et dans des bibliothèques, des répertoires en ligne ou encore des disques d'ordinateurs de bureau ou d'ordinateurs portables. Avec un accès aux fichiers, vous pouvez analyser le contenu de chaque fichier et déterminer s'il contient certaines catégories de données à caractère personnel. Vous pouvez ensuite classer et marquer chaque fichier en fonction du type de données qu'il contient. En outre, vous pouvez générer des rapports concernant cette procédure, avec des informations relatives aux fichiers analysés, aux règles de classification correspondantes et au marquage apposé.

Windows et Windows Server

Le journal des événements Windows offre des fonctionnalités de journalisation étendues qui permettent aux administrateurs d'afficher des informations enregistrées au sujet du système d'exploitation, de l'application et des activités des utilisateurs. Ce système de journalisation peut être configuré de manière à effectuer un audit d'actions détaillées des utilisateurs et des applications, y compris l'accès aux fichiers, l'utilisation de l'application et les modifications de règles, notamment. Le journal des événements Windows permet également aux administrateurs de transférer des événements de clients et de serveurs vers un emplacement centralisé à des fins de signalement et d'audit.

Outils et documentation de signalement des services cloud

Comme toute autre base de données ou tout autre système traitant des données à caractère personnel, votre utilisation des services cloud doit faire l'objet d'un enregistrement et d'une compréhension appropriés pour votre entreprise. Par exemple, votre entreprise devra comprendre les données à caractère personnel détenues par les fournisseurs de services au nom de votre entreprise, la relation contractuelle qui régit ces fournisseurs de services et la destination des données à la fin de la relation de service.

Nous vous aidons à gérer ces informations en proposant des outils de rapport simples et clairs concernant votre compte dans le cloud Microsoft, ainsi qu'une documentation complète concernant nos services cloud, leur mode de fonctionnement et notre relation contractuelle avec vous.

Information des personnes concernées

Le GDPR modifiera les exigences en matière de protection des données et définira de plus strictes obligations pour les opérateurs de traitement de données et les contrôleurs de données en ce qui concerne le signalement de piratages de données à caractère personnel qui entraînent un risque pour les droits et libertés des individus. En vertu de ce nouveau règlement, comme le prévoient les Articles 17, 31 et 32, l'opérateur de traitement de données doit informer sans délai le contrôleur de données de tout piratage de données à caractère personnel ayant été porté à sa connaissance.

Une fois informé de ce piratage, le contrôleur de données doit le signaler à l'autorité compétente en matière de protection des données dans un délai de 72 heures. Si le piratage présente un risque élevé pour les droits et libertés des individus, les contrôleurs doivent également en informer les personnes concernées dans les plus brefs délais. Cela signifie que si vous faites appel à un opérateur de traitement des données dans votre rôle de contrôleur des données, vous devez veiller à ce que vos contrats intègrent un ensemble clair d'attentes au sujet des notifications de violations potentielles.

Pour les événements qui relèvent partiellement ou entièrement de la responsabilité de réaction de Microsoft, nous avons mis en place des procédures de gestion de la réponse aux incidents liés à la sécurité décrites pour Azure, Office 365 et Dynamics 365. Nous rappelons également nos engagements en faveur du GDPR dans la formulation de nos contrats.

Les produits et services Microsoft, comme Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 et Windows 10, offrent des solutions capables de vous aider dès aujourd'hui à détecter et à évaluer les menaces liées à la sécurité et les violations de données, tout en respectant les obligations de signalement prévues par le GDPR.

Gestion des demandes des personnes concernées

Parmi les éléments les plus importants du GDPR figurent les droits des « personnes concernées » énoncés dans les articles de la Section 2 (Information et accès aux données), de la Section 3 (Rectification et effacement) et de la Section 4 (Droit d'opposition et prise de décision individuelle automatisée).

Ces obligations peuvent avoir des répercussions sur votre environnement informatique et sur vos activités en qualité de responsable du traitement, ainsi que dans l'environnement et les activités de tous vos sous-traitants agissant en qualité d'opérateurs de traitement de données.

La bonne gouvernance des données est un élément clé de la législation sur la protection de la vie privée et elle est mise en évidence dans la plupart des lois et des réglementations portant sur la protection des données et le respect de la vie privée. L'un des principaux éléments de la gouvernance au titre du GDPR est la désignation d'un délégué à la protection des données dans certaines circonstances définies dans les Articles 35, 36 et 37. Le délégué à la protection des données doit être associé à toutes les questions relatives à la protection des données à caractère personnel.

Un deuxième élément important de la gouvernance au titre du GDPR est la réalisation de l'examen de conformité de la protection des données qui donne lieu à une analyse d'impact relative à la protection des données sous la direction du délégué à la protection des données. L'Article 33a décrit spécifiquement les obligations en indiquant que dans les deux ans suivant une analyse d'impact relative à la protection des données, le contrôleur des données doit effectuer un examen de la conformité afin de démontrer que le traitement des données à caractère personnel est conforme à l'analyse d'impact relative à la protection des données à caractère personnel.

Le Microsoft Trust Center fournit des informations sur les manières dont nous pouvons accompagner votre cheminement, y compris une rubrique spéciale consacrée aux Positions et engagements de Microsoft envers le GDPR.